Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Πρωτόκολλα Ασφαλών Υπολογισμών Πολλών Συμμετεχόντων

Κωνσταντίνος Μίχος

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Πρωτόκολλα Ασφαλών Υπολογισμών Πολλών Συμμετεχόντων

Κωνσταντίνος Μίχος

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2021

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η συνεχόμενη και ραγδαία ανάπτυξη τις τεχνολογίας, έχει οδηγήσει σε παροχή διευκολύνσεων στην καθημερινότητα των ανθρώπων. Ταυτόχρονα όμως, η εξέλιξη αυτή καθιστά ολοένα και πιο επιτακτική την ανάγκη για ασφαλή επικοινωνία και ανταλλαγή πληροφοριών, λόγω της αξίας αυτών και της ύπαρξης αντιπάλων που επιθυμούν να τις αποκτήσουν στην κατοχή τους. Σε αυτό το πλαίσιο, είναι πολύ σημαντική η ύπαρξη και η συνεισφορά των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων (SMC), που έρχονται για να δώσουν λύση σε ζητήματα που αφορούν την ασφαλή ανταλλαγή δεδομένων και εκτέλεση υπολογισμών μεταξύ πολλών οντοτήτων.

Η παρούσα μεταπτυχιακή διατριβή, εστιάζει στην μελέτη των συγκεκριμένων πρωτοκόλλων. Πιο συγκεκριμένα, μελετάται αναλυτικά η έννοια των SMC πρωτοκόλλων, με παρουσίαση των σημαντικότερων τεχνικών και των εφαρμογών που αυτές τυγχάνουν, καθώς και των επιπέδων ασφαλείας που επιτυγχάνουν, σύμφωνα πάντα με τον Γενικό Κανονισμό της Προστασίας των Προσωπικών Δεδομένων της Ευρωπαϊκής Ένωσης. Επιπρόσθετα, σκοπός της παρούσης διατριβής είναι η μελέτη των χαρακτηριστικών και της απόδοσης της τεχνικής Shamir Secret Sharing και η σύγκριση δύο διαφορετικών φόρμουλων παρεμβολής που μπορεί να χρησιμοποιηθούν σε αυτή. Ακόμη, σκοπός αποτελεί η εξέταση του κατά πόσο μπορεί να χρησιμοποιηθεί η τεχνική του Shamir για την επίτευξη καλής ψευδωνυμοποίησης, καθώς και η εξέταση του ερευνητικού ερωτήματος για το αν μπορεί να αξιοποιηθεί η συγκεκριμένη διαδικασία, με σκοπό να προασπιστεί η ιδιωτικότητα, σε περιπτώσεις όπου υπάρχει η ανάγκη να αποθηκεύονται δεδομένα και ενέργειες χρηστών, σε περιβάλλοντα όπως αυτό μίας αλυσίδας Blockchain. Για την επίτευξη των παραπάνω στόχων χρησιμοποιήθηκαν εικονικά περιβάλλοντα, στα οποία έλαβαν χώρα τα πειράματα και έγιναν οι μετρήσεις.

Από τα αποτελέσματα της μεταπτυχιακής διατριβής, προκύπτει ότι σημαντική επιρροή στο χρόνο εκτέλεσης της τεχνικής, ασκεί το μέγεθος του μηνύματος και ο αριθμός των shares που δημιουργούνται. Την ίδια στιγμή, από τη σύγκριση των δύο φόρμουλων παρεμβολής, προέκυψε ότι η φόρμουλα του Newton είναι πιο αποτελεσματική, ακόμα και σε περίπτωση εισαγωγής νέων σημείων. Τέλος, αναπτύχθηκε στην πράξη περίπτωση εφαρμογής της τεχνικής του Shamir για καλή ψευδωνυμοποίηση και παρουσιάστηκε μία νέα ιδέα για μελλοντική αξιοποίησή της στην αλυσίδα Blockchain.

Summary

The continuous and rapid development of technology, has led to the provision of facilities in the daily lives of people. At the same time, however, this development makes the need for secure communication and exchange of information increasingly imperative, due to the value they may have and the existence of rivals who wish to acquire this information. In this context, the existence and contribution of secure multiparty computation protocols (SMC), which come to face issues related to the secure exchange of data and execution of computations between multiple entities, is very important.

This master dissertation focuses on the study of those protocols. Specifically, the concept of SMC protocols is studied in detail, with a presentation of the most important techniques and applications that they can be applied, as well as the security levels they achieve, always in accordance with the General Data Protection Regulation of EU. Additionally, the purpose of this dissertation is to study the properties and the efficiency of the Shamir Secret Sharing technique and to compare two different interpolation formulas that can be used in it. The purpose is to examine whether the Shamir technique can be used to achieve good pseudonymization, as well as to examine the research question of whether this process can be used to protect privacy, in cases where exists the need to store data and actions in environments where there may occur security issues, like the Blockchain. To achieve the above objectives, virtual environments were used, in which the experiments took place and the measurements were made.

From the results of the dissertation, it appears that the execution time of the technique highly depends on the size of the message and the number of shares that are created. At the same time, comparing the two interpolation formulas, it was concluded that Newton's formula is more effective, even if new points are introduced. Finally, the application of Shamir's technique for good pseudonymization was developed in practice, whereas a novel idea for a future use in the Blockchain was presented.

Ευχαριστίες

Πρώτα από όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου στην παρούσα μεταπτυχιακή διατριβή και καθηγητή μου στη θεματική ενότητα της Κρυπτογραφίας, κ. Κωνσταντίνο Λιμνιώτη, για την ανάθεση σε εμένα του συγκεκριμένου θέματος, για την πολύτιμη βοήθεια και τις συμβουλές που μου παρείχε, σε όλα τα στάδια υλοποίησης της μεταπτυχιακής μου διατριβής, καθώς και την άμεση ανταπόκριση του σε οποιαδήποτε δυσκολία ή ερώτηση μπορεί εγώ να έθετα. Η διάθεση και ο χαρακτήρας του, σε συνδυασμό με όλα τα παραπάνω, αποτέλεσαν τον κινητήριο μοχλό και ένα σπουδαίο στήριγμα προκειμένου να επιτευχθούν οι στόχοι που είχαν τεθεί και να ολοκληρωθεί η παρούσα μεταπτυχιακή διατριβή.

Ακολούθως, θα ήθελα να ευχαριστήσω όλους τους καθηγητές μου στις θεματικές ενότητες του προγράμματος σπουδών Ασφάλεια Υπολογιστών και Δικτύων, και πιο συγκεκριμένα τους κ. Σιαηλή, κ. Λογοθέτη, κ. Μαυρίδη και κα. Περατικού, για όλες τις γνώσεις που μου μετέδωσαν, οι οποίες αποτέλεσαν σημαντικό εργαλείο που εφαρμόστηκε στην παρούσα διατριβή και επρόκειτο να με συντροφεύουν στο υπόλοιπο της καριέρας μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου, για την ψυχολογική υποστήριξη που μου παρείχαν και την αγάπη που μου έδειξαν, σε όλες τις στιγμές, εύκολες και δύσκολες, από την αρχή των σπουδών μου μέχρι και την ολοκλήρωση της μεταπτυχιακής μου διατριβής.

Σας ευχαριστώ όλους πάρα πολύ από τα βάθη της καρδιάς μου!

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Ευρετήριο Ακρωνυμίων

SMC	Secure Multiparty Computations
GDPR	General Data Protection Regulation
PSI	Private Set Intersection
OT	Oblivious Transfer
OT_1^2	1-Out-Of-2 Oblivious Transfer
DNA	Deoxyribonucleic acid
SSS	Shamir Secret Sharing
GT	Greater Than Problem
RSA	Rivest – Shamir - Adleman
COVID-19	Coronavirus Disease of 2019
SSL	Secure Sockets Layer
TLS	Transport Layer Security
IoT	Internet Of Things

H/Y	Ηλεκτρονικός Υπολογιστής
CPU	Central Processing Unit
GHz	Gigahertz
Mhz	Megahertz
GB	GigaByte
IDS	Intrusion Detection System
IP	Internet Protocol

Κεφάλαιο 1

Εισαγωγή

Τα τελευταία χρόνια, η ανάπτυξη της τεχνολογίας και του διαδικτύου, έχει οδηγήσει στην όλο και πιο ευρεία χρήση τους. Στόχος τόσο της δημιουργίας τους, όσο και του συνδυασμού τους, ήταν και εξακολουθεί να είναι να παρέχουν, με το πέρασμα των χρόνων, όλο και περισσότερες διευκολύνσεις στην καθημερινότητα των ανθρώπων. Μία από αυτές, που εξακολουθεί να παίζει σημαντικό ρόλο, είναι η ευκολία που παρέχουν σχετικά με την αποθήκευση και την ανταλλαγή πληροφοριών και δεδομένων μεταξύ διαφορετικών ατόμων ή συστημάτων. Παρέχεται δηλαδή η δυνατότητα για εξ' αποστάσεως επικοινωνία. Ταυτόχρονα όμως, λόγω της μεγάλης αξίας που μπορεί να έχουν οι πληροφορίες, έκαναν την εμφάνιση τους και απειλές που συνδέονται με την εκμετάλλευση των ευπαθειών των συστημάτων. Αντίπαλοι πραγματοποιούν επιθέσεις με σκοπό την εισβολή στα συστήματα ή στα δίκτυα έτσι ώστε να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες. Αυτό είχε ως αποτέλεσμα να υπάρξει ανάπτυξη του κυβερνοεγκλήματος.

Την ίδια στιγμή έκανε την εμφάνισή της και η χρήση των παράλληλων - κατανεμημένων συστημάτων (distributed computing). Τα συστήματα αυτά αποτελούνται από δύο ή και περισσότερες ανεξάρτητες - αυτόνομες οντότητες, οι οποίες βρίσκονται μακριά η μία από την άλλη, αλλά είναι συνδεδεμένες με τέτοιο τρόπο ώστε να μπορέσουν να εκτελέσουν έναν κοινό υπολογισμό. Το σημαντικότερο πλεονέκτημα των κατανεμημένων συστημάτων αποτελεί τόσο το γεγονός της από κοινού συνεργασίας, όσο και ότι αυτό επιτυγχάνεται μέσω μιας μεθόδου συμφέρουσας, από άποψη κόστους (Kshemkalyani & Singhal, 2008). Χαρακτηριστικό παράδειγμα ενός κατανεμημένου συστήματος αποτελεί ένα σύστημα cloud, που χρησιμοποιείται για τη δημιουργία αντιγράφων ασφαλείας αρχείων και το οποίο αποτελείται από πολλούς servers και συστήματα, που συνεργάζονται για να πετύχουν αυτόν τον στόχο. Πάντα όμως υπάρχει το πρόβλημα της

ασφαλούς επικοινωνίας ανάμεσα στις οντότητες, υπό την έννοια ότι δεν θα έπρεπε η μία οντότητα να αποκαλύψει στην άλλη περισσότερες πληροφορίες από ο,τι πρέπει αλλά και να μπορέσει μια ξένη - μη εξουσιοδοτημένη οντότητα κατευθυνόμενη από κάποιον αντίπαλο. Σε θεωρητικό επίπεδο, το πρόβλημα αυτό θα μπορούσε να λυθεί με την ύπαρξη μιας έμπιστης τρίτης πλευράς, μιας επιπρόσθετης έμπιστης οντότητας, στην οποία θα μπορούσε να ανατεθεί η ευθύνη για την ασφαλή εκτέλεση του υπολογισμού, με την συνεργασία των υπόλοιπων οντοτήτων, εγχείρημα που είναι επικίνδυνο, λόγω των διάφορων κινδύνων που επικρατούν καθώς και του ανταγωνισμού.

Στο πλαίσιο αυτό, εμφανίστηκε η ιδέα των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων (Secure Multi–Party Computations – SMC), με σκοπό να επιλύσουν το πρόβλημα της ασφαλούς επικοινωνίας μεταξύ πολλών μερών, κατά τρόπο ώστε να μη μαθαίνει κανείς περισσότερη πληροφορία από ό,τι πρέπει. Πρόκειται για συναρτήσεις υπολογισμού που χρησιμοποιούνται με σκοπό την επεξεργασία εισόδων που στέλνονται από διαφορετικές οντότητες και την παραγωγή εξόδων που αποστέλλονται πίσω σε αυτές. Τα πρωτόκολλα Secure Multi-Party Computation, θα πρέπει να ικανοποιούν τις ιδιότητες που έχουν να κάνουν με το ότι οι εκάστοτε οντότητες θα μαθαίνουν μόνο τις απολύτως απαραίτητες πληροφορίες καθώς και ότι θα λαμβάνουν τα σωστά αποτελέσματα μετά την εκτέλεση των υπολογισμών (Lindell, 2020), χωρίς την ανάγκη ύπαρξης μίας έμπιστης τρίτης οντότητας. Με τα πρωτόκολλα αυτά, μπορούν να αντιμετωπιστούν πλήθος προβλημάτων που υπάρχουν, ικανοποιώντας ταυτόχρονα και τις δύο αυτές σημαντικές ιδιότητες (Du & Atallah, 2002). Υπάρχουν πλήθος διαφορετικών τεχνικών που μπορούν να εφαρμοστούν. Μια από τις σημαντικότερες τεχνικές που χρησιμοποιούν τα πρωτόκολλα αυτά, είναι αυτή που παρουσίασε ο Shamir αναφορικά με το διαμοιρασμό μυστικού, τη λεγόμενη πλέον Shamir Secret Sharing τεχνική (Bayatbabolghani & Blanton, 2018; Evans et al., 2018), η οποία μπορεί να θεωρηθεί ως μία περίπτωση της λεγόμενης κρυπτογραφίας κατωφλίου (threshold cryptography). Ταυτόχρονα, τεχνικές ασφαλών υπολογισμών βρίσκουν εφαρμογή σε προβλήματα που έγκεινται στον ασφαλή υπολογισμό εύρεσης κοινών στοιχείων δύο συνόλων (Private Set Intersection - PSI), όπου υπάρχουν διάφορα πρωτόκολλα που το επιτυγχάνουν – μία πρόσφατη δε τεχνική μπορεί να εφαρμοστεί με τέτοιο τρόπο ώστε να παρέχεται μέσω του πρωτοκόλλου αυτού πολύ καλή ισορροπία ανάμεσα στο κόστος επικοινωνίας (πλήθος μηνυμάτων που πρέπει να ανταλλαγούν μέσω δικτύου) και στο

κόστος υπολογισμών (Chase & Miao, 2020). Ταυτόχρονα υπάρχει ένα γνωστό πρωτόκολλο που υλοποιεί τη λειτουργία PSI και το οποίο βελτιώνει ως προς την απόδοση άλλα γνωστά συναφή πρωτόκολλα. (Pinkas et al., 2015). Πολλά από τα πρωτόκολλα ασφαλών υπολογισμών βασίζονται σε μία επιμέρους λειτουργία γνωστή με το όνομα Oblivious Transfer (Evans et al., 2018; Lindell, 2020). Όλες οι παραπάνω διαφορετικές περιπτώσεις πρωτοκόλλων, μπορούν να βρουν πλήθος εφαρμογών σε διάφορους τομείς. Τα SMC πρωτόκολλα μπορούν να έχουν εφαρμογή σε ηλεκτρονικές εκλογές, σε ηλεκτρονική ανταλλαγή συμβολαίων, σε ηλεκτρονικές δημοπρασίες καθώς και σε διάφορες κρυπτογραφικές δραστηριότητες (Evans et al., 2018; Goldwasser, 1997). Επιπλέον, μπορούν να χρησιμοποιηθούν για την προστασία κρυπτογραφικών κλειδιών αλλά και σε προσπάθειες οργανισμών να ελέγξουν για κοινά στοιχεία, όπως λίστες πελατών, χωρίς να αποκαλύψουν στοιχεία η μία στην άλλη, για παράδειγμα χρησιμοποιώντας της διαφημίσεις (Lindell, 2020). Τέλος τα πρωτόκολλα SMC μπορούν να χρησιμοποιηθούν σε συστήματα μηχανικής μάθησης (machine learning) (Evans et al., 2018; Lindell, 2020).

1.1 Σκοπός της Έρευνας

Αντικείμενο της διατριβής αποτελεί η μελέτη, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, των πρωτόκολλων ασφαλών υπολογισμών πολλών συμμετεχόντων (Secure Multi-Party Computations), σε σχέση με τους σκοπούς για τους οποίους μπορούν να χρησιμοποιηθούν και να εξυπηρετήσουν. Ειδικότερα, θα μελετηθούν οι σημαντικότερες τεχνικές SMC και πρωτόκολλα που υπάρχουν, σε μία ολιστική προσέγγιση, προκειμένου να διαφανούν τα διαφορετικά είδη πρωτοκόλλων που εμπίπτουν σε αυτήν την μεγάλη κατηγορία. Επιπλέον θα εξεταστούν οι εφαρμογές που μπορεί να έχουν τα πρωτόκολλα αυτά καθώς και στα επίπεδα ασφαλείας που αυτά επιτυγχάνουν. Στο πλαίσιο αυτό θα εξεταστούν τα πρωτόκολλα αυτά και σε ποιο βαθμό ικανοποιούν νομικές απαιτήσεις ιδιωτικότητας που υπάρχουν, σε σχέση πάντοτε και με την νομοθεσία που υπάρχει σχετικά με την προστασία των προσωπικών δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR). Η σύνδεση αυτή είναι ιδιαίτερα σημαντική δεδομένου ότι πολλά από αυτά τα πρωτόκολλα φαίνεται να αντιμετωπίζουν αποδοτικά απαιτήσεις της νομοθεσίας που άπτονται της αρχής της ελαχιστοποίησης των δεδομένων (η οποία

αποτελεί μία βασική προϋπόθεση νόμιμης επεξεργασίας προσωπικών δεδομένων) και, ταυτόχρονα, δεν φαίνεται να έχει αξιοποιηθεί επαρκώς στην πράξη.

Περαιτέρω, στο πλαίσιο της διατριβής θα επιχειρηθεί μια περαιτέρω ανάλυση του πρωτοκόλλου διαμοιρασμού μυστικού του Shamir, ως προς τις εξής πτυχές: α) θα μελετηθεί η δυνατότητα χρήσης του πρωτοκόλλου αυτού για την δημιουργία κατάλληλων ψευδωνύμων σε αρχεία καταγραφής (log files) ενός συστήματος (Biskup & Flegel, 2000), έτσι ώστε να μην αποκαλύπτονται περισσότερα δεδομένα για τους χρήστες από ό,τι πρέπει (όπως η αναγνώριση όλων των κινήσεων κάθε χρήστη με δυνατότητα ταυτοποίησης), παρά μόνο αν κάποιες κινήσεις χρήζουν περαιτέρω διερεύνησης – όπως π.χ. εάν είναι "ύποπτες" για πραγματοποίηση επίθεσης, β) θα επιχειρηθούν πρακτικές δοκιμές του πρωτοκόλλου, προκειμένου να εξεταστεί, και να αξιολογηθεί αντιστοίχως, ως προς το χρόνο εκτέλεσής του σε συμβατικούς υπολογιστές,γ) στο ως άνω πλαίσιο θα διερευνηθεί περαιτέρω μία πολύ πρόσφατη παραλλαγή του πρωτοκόλλου που βασίζεται στην παρεμβολή Newton και όχι στη Lagrange, προκειμένου να εξεταστεί εάν η παραλλαγή αυτή προσφέρει πλεονεκτήματα στο εν λόγω σενάριο εφαρμογής (Bezzateev et al., 2020), δ) θα διερευνηθεί η δυνατότητα ενσωμάτωσης της ως άνω τεχνικής σε περιπτώσεις χρήσης τεχνολογιών blockchain ως υποστηρικτικό μέσον για την ασφάλεια πληροφοριών (Brotsis et al., 2019; Kolokotronis et al., 2019; Minoli & Occhiogrosso, 2018; Reyna et al., 2018), προκειμένου να αμβλυνθούν τα ζητήματα ιδιωτικότητας και προστασίας προσωπικών δεδομένων που εγείρονται σε αυτές τις περιπτώσεις.

1.2 Βασικά Ερευνητικά Ερωτήματα

Προκειμένου να μπορέσει όχι μόνο να πραγματοποιηθεί η παρούσα έρευνα, αλλά και να εξυπηρετηθεί ο σκοπός της που αναφέρθηκε προηγουμένως, θα πρέπει να τεθούν και να απαντηθούν τα ακόλουθα βασικά ερευνητικά ερωτήματα :

- Κατηγοριοποίηση πρωτοκόλλων ασφαλών υπολογισμών, με κριτήριο τις εφαρμογές στις οποίες μπορούν να τύχουν εφαρμογής.

- Αποτίμηση των ως άνω πρωτοκόλλων, σε σχέση με τις απαιτήσεις προστασίας προσωπικών δεδομένων που επιτάσσει η νομοθεσία και για τις οποίες μπορούν τα πρωτόκολλα αυτά να αποτελούν λύση.

- Διερεύνηση τρόπου υλοποίησης μίας παραλλαγής του πρωτοκόλλου διαμοιρασμού μυστικού του Shamir, προκειμένου να παρέχει λύσεις ψευδωνυμοποίησης σε προκλήσεις ως προς την ιδιωτικότητα που εγείρονται σε συγκεκριμένες εφαρμογές χρήσης τεχνολογίας blockchain ως υποστηρικής τεχνολογίας για την επίτευξη ασφάλειας συστημάτων.

1.3 Αναγκαιότητα και Σπουδαιότητα της Έρευνας

Τα πρωτόκολλα υπολογισμών πολλών συμμετεχόντων παρέχουν τη δυνατότητα να γίνονται κατανεμημένοι υπολογισμοί από διαφορετικές οντότητες, με ασφαλή τρόπο. Η χρησιμοποίησή τους μπορεί ουσιαστικά να οδηγήσει στην αξιοποίηση και την περαιτέρω επεξεργασία προσωπικών δεδομένων, χωρίς να τίθενται σε κίνδυνο η ασφάλεια τους. Λόγω της τεχνολογικής εξέλιξης, τα πρωτόκολλα αυτά, παρ' όλο που στην αρχή είχαν μόνο θεωρητικό υπόβαθρο, εντούτοις με το πέρασμα των χρόνων άρχισαν να έχουν πάρα πολλές εφαρμογές στη καθημερινότητα, όπως για παράδειγμα σε ηλεκτρονικές ψηφοφορίες, σε δημοπρασίες, στην ψηφιακή υπογραφή συμβολαίων, σε τεχνολογίες blockchain ακόμα και σε προσπάθειες εταιρειών να ελέγξουν για κοινά στοιχεία, όπως λίστες πελατών, χωρίς να αποκαλύψουν στοιχεία η μία στην άλλη. Για το λόγο αυτό είναι να αναγκαίο να παρουσιαστούν τα σημαντικότερα πρωτόκολλα υπολογισμών πολλών συμμετεχόντων, προκειμένου να κατανοηθούν τα προβλήματα που επιλύουν κυρίως ως προς την ασφάλεια των προσωπικών δεδομένων, οι τεχνικές που χρησιμοποιούνται καθώς και να παρουσιαστούν εκτενέστερα οι εφαρμογές που έχουν. Έτσι, θα μπορέσει να ενισχυθεί το θετικό κλίμα για την όλο και περισσότερη και πιο έντονη χρησιμοποίηση τους με το πέρασμα του χρόνου και να καλυφθούν κενά που υπάρχουν σχετικά με αυτά. Επιπλέον, θα μπορέσει να ενισχυθεί και η υπάρχουσα βιβλιογραφία σχετικά με τα

πρωτόκολλα υπολογισμών πολλών συμμετεχόντων και να υπάρχουν σημαντικές πληροφορίες για αυτά συγκεντρωμένες.

Ταυτόχρονα, η παρούσα διατριβή επιχειρεί να συγκεράσει πρόσφατες εξελίξεις στο χώρο προκειμένου να προτείνει μία νέα λύση που να αντιμετωπίζει ζητήματα ιδιωτικότητας που εγείρονται κατά τη χρήση τεχνολογιών blockchain για υποστήριξη υπηρεσιών ασφάλειας. Η χρήση blockchain φαίνεται να αποτελεί μία πολύ σημαντική λύση για την καταγραφή "συμβάντων" σε ένα σύστημα, τα οποία να μην τυγχάνουν αμφισβήτησης ως προς την εγκυρότητά τους και τη χρονική τους ακολουθία, έτσι ώστε να μπορούν να αξιολογηθούν, σε συγκεκριμένα περιβάλλοντα, για την ανίχνευση ή/και αποτροπή επιθέσεων ασφαλείας. Προς αυτήν την κατεύθυνση, διερευνάται η χρήση του πρωτοκόλλου διαμοιρασμού μυστικού του Shamir για την παραγωγή κατάλληλων ψευδωνύμων που να επιτρέπουν την επίτευξη του ως άνω στόχου, χωρίς όμως να αποκαλύπτονται πληροφορίες ταυτοποιημένων χρηστών που μπορούν να οδηγήσουν σε παρακολούθησή τους (π.χ. για δημιουργία προφίλ χρηστών ερήμην τους).

1.4 Μεθοδολογία

Η έρευνα που απαιτείται να γίνει για την υποστήριξη της παρούσας διατριβής, θα περιλαμβάνει στο πρώτο τμήμα της τη μελέτη της αρθρογραφίας και της βιβλιογραφίας, με σκοπό τη συγκέντρωση των πρωτοκόλλων SMC, την κατηγοριοποίηση τους και την παρουσίαση τους με βάση το είδος τους. Στη συνέχεια θα γίνει η παρουσίαση των δημοφιλέστερων SMC τεχνικών, καθώς και των εφαρμογών τους, πραγματοποιώντας παράλληλα και έναν έλεγχο του τρόπου αποτίμησης των επιπέδων ασφαλείας που αυτά επιτυγχάνουν, σύμφωνα πάντα με το Γενικό Κανονισμό της Ευρωπαϊκής Ένωσης, για την προστασία των προσωπικών δεδομένων. Στο δεύτερο τμήμα της η έρευνα θα περιλαμβάνει την ανάπτυξη πειραματικού περιβάλλοντος, με σκοπό την περαιτέρω εμβάθυνση στην τεχνική Διαμοιρασμού Μυστικού του Shamir, στο οποίο θα πραγματοποιηθούν μετρήσεις των χρόνων για την υλοποίηση των ενεργειών που περιλαμβάνει η συγκεκριμένη τεχνική. Επιπλέον, θα γίνει μία προσπάθεια για ανάδειξη της φόρμουλας παρεμβολής του Newton, ως μία περίπτωση που μπορεί να εφαρμοστεί

στη συγκεκριμένη τεχνική, αντί για την αντίστοιχη του Lagrange, πραγματοποιώντας και μια σύγκριση μεταξύ τους. Τέλος, το δεύτερο αυτό τμήμα της διατριβής θα περιλαμβάνει και έρευνα για την πιθανότητα εφαρμογής της τεχνικής του Shamir με σκοπό την επίτευξη καλής ψευδωνυμοποίησης, καθώς πρόταση για μελλοντική αξιοποίηση αυτής σε συνδυασμό με τη φόρμουλα παρεμβολής του Newton, με σκοπό την ψευδωνυμοποίηση προσωπικών δεδομένων τα οποία αποθηκεύονται σε δομές blockchain.

1.5 Δομή της Μεταπτυχιακής Διατριβής

Η παρούσα διατριβή θα έχει την ακόλουθη δομή :

- Το Κεφάλαιο 2 θα περιλαμβάνει μια αναφορά σε σενάρια και εφαρμογές οι οποίες δεν μπορούν να λειτουργήσουν, ικανοποιώντας της απαιτήσεις του Γενικού Κανονισμού για την Προστασία των Δεδομένων – GDPR, με σκοπό να φανεί η αναγκαιότητα για τη χρησιμοποίηση των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων.

- Το Κεφάλαιο 3 θα αναφέρεται στον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων – GDPR, με αναφορά στους σημαντικότερους ορισμούς και νομικές βάσεις που σχετίζονται με την παρούσα διατριβή.

- Το Κεφάλαιο 4 θα περιλαμβάνει μια παρουσίαση της έννοιας των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων. Στη συνέχεια, θα γίνει προσπάθεια να παρουσιαστούν οι δύο σημαντικότεροι τρόποι ορισμού της ασφάλειας των πρωτοκόλλων αυτών, καθώς και ορισμένα ζητήματα που προκύπτουν. Επιπλέον, θα γίνει αναφορά και στην εφαρμοσιμότητά τους.

- Το Κεφάλαιο 5 θα περιλαμβάνει μια παρουσίαση των σημαντικότερων τεχνικών που υπάρχουν. Θα γίνει προσπάθεια να εξεταστούν τα πρωτόκολλα SMC και ως προς τις νομικές απαιτήσεις που ανακύπτουν από τη νομοθεσία σχετικά με τη προστασία των προσωπικών δεδομένων.

- Το Κεφάλαιο 6 θα περιλαμβάνει μια παρουσίαση των σημαντικότερων εφαρμογών των πρωτοκόλλων SMC καθώς και των τεχνικών που αναφέρθηκαν στο Κεφάλαιο 5 και μπορούν να χρησιμοποιηθούν για την υλοποίηση τους.

- Το Κεφάλαιο 7 θα περιλαμβάνει παρουσίαση των αποτελεσμάτων από πειράματα που εκτελέστηκαν στο πλαίσιο της διατριβής, καθώς και συναφείς παρατηρήσεις που έγιναν σχετικά με τους χρόνους εκτέλεσης της τεχνικής του Shamir, προκειμένου να αποτυπωθεί η αποτελεσματικότητά της, για διάφορες παραμέτρους, ακόμα και σε συμβατικό υπολογιστή. Περαιτέρω, θα διερευνηθεί και θα παρουσιαστεί μία διαφοροποίηση της τεχνικής η οποία βασίζεται στη χρήση παρεμβολής Newton αντί για Langrange, καθώς και των σημαντικότερων πλεονεκτημάτων που μπορεί να προσφέρει.

- Το Κεφάλαιο 8 θα περιλαμβάνει την παρουσίαση μίας περίπτωσης ψευδωνυμοποίησης, η οποία θα βασίζεται στην τεχνική διαμοιρασμού μυστικού του Shamir, καθώς και την τεκμηρίωση μίας πρότασης για μελλοντική αξιοποίηση αυτής σε συνδυασμό με τη φόρμουλα παρεμβολής του Newton, με σκοπό την ψευδωνυμοποίηση προσωπικών δεδομένων τα οποία αποθηκεύονται σε δομές blockchain.

- Το Κεφάλαιο 9 θα περιλαμβάνει τον Επίλογο της παρούσης μεταπτυχιακής διατριβής.

Κεφάλαιο 2

Η χρησιμότητα των SMC πρωτοκόλλων

Ένα από τα σημαντικότερα ζητήματα που έχει κάνει την εμφάνισή του, είναι το γεγονός της διασφάλισης της εμπιστευτικότητας της επικοινωνίας μεταξύ των ανθρώπων. Το πρόβλημα αυτό γίνεται όλο και πιο έντονο, όταν αυξάνεται ο αριθμός των συμμετεχόντων στην επικοινωνία. Είναι πολλές οι περιπτώσεις στις οποίες είναι δύσκολο να υπάρξει επικοινωνία μεταξύ πλευρών, που να περιλαμβάνει ανταλλαγή δεδομένων-πληροφοριών, χωρίς να υπάρξει διαρροή ή αποκάλυψη, εκούσια ή ακούσια, προσωπικών ευαίσθητων πληροφοριών, κατά τη διάρκεια ή μετά την εκτέλεση του υπολογισμού-διαδικασίας. Ουσιαστικά αυτό συμβαίνει σε περιπτώσεις που πρέπει να γίνουν υπολογισμοί ανάμεσα σε πολλές οντότητες. Χαρακτηριστικές περιπτώσεις ύπαρξης του συγκεκριμένου προβλήματος είναι οι εξής (Du & Atallah, 2002; Goldwasser, 1997; Lindell, 2020):

- Ας γίνει η υπόθεση ότι κάποιος άνθρωπος Α, θέλει να κάνει εξετάσεις, για να διαπιστώσει αν πάσχει από κάποια συγκεκριμένη ασθένεια. Ταυτόχρονα γνωρίζει ότι υπάρχει μια εταιρεία Ε που διενεργεί τέτοιου είδους εξετάσεις, παίρνοντας το DNA του υποψήφιου ασθενή και συγκρίνοντας το με μία βάση δεδομένων που περιέχει δείγματα DNA με χαρακτηριστικά που παραπέμπουν σε ορισμένες ασθένειες. Έτσι λοιπόν ο Α μπορεί να στείλει δείγμα από το DNA του, και να λάβει το αποτέλεσμα από την εταιρεία για την ασθένεια από την οποία πάσχει. Ο ασθενής όμως μπορεί να έχει αμφιβολίες για τον βαθμό στον οποίο η συγκεκριμένη διαδικασία διασφαλίζει την ιδιωτικότητά του. Επομένως, η παραπάνω διαδικασία, εφόσον υπάρχει αυτή η αμφιβολία, γίνεται αντιληπτό ότι δεν μπορεί από μόνη της να γίνει αποδεκτή, καθώς δεν μπορεί να διασφαλίσει ότι η εταιρεία δεν θα μάθει καμία ιδιωτική – ευαίσθητη πληροφορία του ασθενή, όπως το DNA του ή το αποτέλεσμα της διαδικασίας.

- Έστω ότι υπάρχει μια εταιρεία Α, η οποία μετά από από μια αρκετά δαπανηρή έρευνα αγοράς, αποφάσισε ότι το θα ήταν αρκετά ευεργετικό για την ίδια το να επεκτείνει το μερίδιο αγοράς της μέχρι ένα συγκεκριμένο σημείο-περιοχή. Ταυτόχρονα, η εταιρεία Α αντιλαμβάνεται και φοβάται την ύπαρξη μιας ακόμα ανταγωνιστικής εταιρείας Β, η οποία σκοπεύει και εκείνη να επεκτείνει το μερίδιο αγοράς της μέχρι μια συγκεκριμένη περιοχή. Οι δύο εταιρείες δεν επιθυμούν να φτάσουν στην ίδια περιοχή τα μερίδια αγοράς τους. Θέλουν να γνωρίζουν λοιπόν σε ποιο σημείο καλύπτει η μία την άλλη, χωρίς όμως να ανταλλάξουν σημαντικές ιδιωτικές τους πληροφορίες, όπως για παράδειγμα την γεωγραφική τους τοποθεσία. Το κόστος του να συμβεί κάτι τέτοιο είναι μεγάλο, γιατί εκτός από το οικονομικό σκέλος, μια τέτοια αποκάλυψη μπορεί να δώσει την ευκαιρία ακόμα και σε κάποιες τρίτες εταιρείες, να ανεβάσουν την προσφορά τους για να αποκτήσουν πλεονέκτημα. Η επίλυση λοιπόν της συγκεκριμένης επικοινωνίας φαίνεται δύσκολη.

- Έστω ότι υπάρχουν δύο οργανισμοί, οι οποίοι επιθυμούν να συνεργαστούν για κοινό τους όφελος, θέλοντας ταυτόχρονα να ικανοποιήσουν και ορισμένες δικές τους ανάγκες. Οι συγκεκριμένες όμως απαιτήσεις συνδέονται με προσωπικά τους στοιχεία, που μπορεί να έχουν σχέση ακόμα και με την οικονομική τος κατάσταση, τις προτιμήσεις των πελατών ή τους ρυθμούς των πωλήσεων. Έτσι λοιπόν κανένας από τους δύο οργανισμούς δεν θέλει να κάνει γνωστό στον άλλο οργανισμό κάποια από αυτά τα στοιχεία. Υπάρχει επομένως το πρόβλημα για το πως μπορεί να γίνει η συνεργασία αυτή, χωρίς να υπάρξει κοινοποίηση των ιδιωτικών τους στοιχείων.

- Η ηλεκτρονική ψηφοφορία. Πρόκειται για τη διαδικασία κατά την οποία πρέπει να διασφαλιστεί ότι η καταμέτρηση των ψήφων θα γίνει χωρίς να αποκαλυφθεί η επιλογή του κάθε ψηφοφόρου, καθώς είναι αναφαίρετο δικαίωμα του ψηφοφόρου να διατηρεί την ανωνυμία της ψήφου του, κατά τη εκλογική διαδικασία. Ταυτόχρονα, θα πρέπει η επιλογή της ψήφου να γίνεται από το κάθε ψηφοφόρο ανεξάρτητα, χωρίς να επηρεάζονται δηλαδή από τις επιλογές των ψηφοφόρων. Επιπλέον, οι αρχές θα πρέπει να ελέγχουν ότι οι ψήφοι προέρχονται από νόμιμους

ψηφοφόρους, από άτομα δηλαδή που έχουν το δικαίωμα να συμμετέχουν στη διαδικασία της ψηφοφορίας.

- Η περίπτωση της ηλεκτρονικής προσφοράς για την υπογραφή συμβολαίων. Σύμφωνα με αυτή, διαφορετικά άτομα κάνουν προσφορές, και το άτομο με την οικονομικότερη προσφορά θα επιλεγεί. Η διαδικασία αυτή όμως είναι δύσκολο να λάβει χώρα, δεδομένου ότι πρέπει ο κάθε υποψήφιος να γνωρίζει τη δική του προσφορά και καμία άλλη πληροφορία για τις υπόλοιπες.

- Έστω ότι μία ομάδα ατόμων μπορεί να αποκρυπτογραφήσει ένα αρχείο-μήνυμα μόνο στην περίπτωση που συμμετέχουν όλοι, ή ένας συγκεκριμένος αριθμός από αυτούς. Το πρόβλημα όμως βρίσκεται στο κατά πόσο αυτό μπορεί να υλοποιηθεί, χωρίς να γίνει γνωστό ποιο κομμάτι του κλειδιού αποκρυπτογράφησης κατέχει ο καθένας.

Όλα τα παραπάνω είναι μερικά παραδείγματα από εφαρμογές στις οποίες υπάρχουν προβλήματα υλοποίησης της επικοινωνίας και της εκτέλεσης υπολογισμών μεταξύ διαφορετικών οντοτήτων, λόγω του γεγονότος ότι καταπατείται το δικαίωμα της ιδιωτικότητας, αφού είναι υπαρκτός ο κίνδυνος της αποκάλυψης περισσότερων πληροφοριών από ότι απαιτείται και είναι νόμιμο (βλ. Κεφάλαιο 3). Αξίζει να αναφερθεί ότι αυτό συμβαίνει λόγω της ύπαρξης ενός θεσμικού πλαισίου για την ύπαρξη των προσωπικών δεδομένων, σύμφωνα με το οποίο καθορίζονται ορισμένες προϋποθέσεις νομιμότητας για την προστασία των προσωπικών δεδομένων. Σύμφωνα με την νομοθεσία του Ευρωπαϊκού Κοινοβουλίου σε θέματα προστασίας των ατόμων για την προστασία των προσωπικών δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR), υπάρχουν ορισμένες παράμετροι, τις οποίες οι παραπάνω εφαρμογές δεν θεωρείται ότι καλύπτουν (Δρ. Κωνσταντίνος Λιμνιώτης & Ιωάννης Μαυρίδης, 2019; Ευρωπαϊκό Κοινοβούλιο, 2016). Πιο συγκεκριμένα:

- Στο παράδειγμα με τις εξετάσεις μέσω του γενετικού υλικού DNA, εάν η εταιρεία μάθει σε ποιον ανήκει το υλικό και εξάγει συμπεράσματα επί ταυτοποιημένου, για την ίδια, προσώπου, χωρίς ο ασθενής να το γνωρίζει και χωρίς να συναινεί (ο οποίος θεωρεί ότι θα τηρηθεί η ανωνυμία του), τότε έχουμε ουσιαστικά

παράβαση της νομοθεσίας του GDPR. Μάλιστα, πρέπει να επισημανθεό ότι τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου, ανήκουν στην κατηγορία των ευαίσθητων προσωπικών δεδομένων .

- Στην περίπτωση με τις εταιρείες που συνεργάζονται, οποιαδήποτε διαρροή πληροφοριών, όπως τα οικονομικά ή άλλα στοιχεία τους (τραπεζικά, φορολογικά, στοιχεία υγείας, τραπεζικές κινήσεις, στοιχεία λογαριασμών) αποτελεί παράβαση του κανονισμού GDPR. Αυτό ισχύει καθώς όλα τα παραπάνω στοιχεία αποτελούν προσωπικά δεδομένα των πελατών της εταιρείας, και οποιαδήποτε κοινοποίηση στοιχείων σε τρίτους για τους σκοπούς που περιγράφησαν παραπάνω δεν έχουν νομική βάση στον GDPR (βλ. Επόμενο Κεφάλαιο).

- Στην περίπτωση με την ηλεκτρονική ψηφοφορία, δεδομένου ότι η ψήφος θεωρείται προσωπικό δεδομένο που πρέπει να διατηρεί τη μυστικότητά του, οποιαδήποτε ενέργεια που δεν συμβαδίζει με αυτό, καταπατάει – πέραν άλλων νομοθεσιών αναφορικά με τη μυστικότητα της ψήφου και την ελεύθερη επιλογή ψήφου του κάθε ψηφοφόρου - και την νομοθεσία του GDPR.

Ένας βασικός τρόπος για να λυθούν τα παραπάνω προβλήματα, και να μπορέσουν να λειτουργήσουν αποτελεσματικά οι παραπάνω υπολογισμοί, είναι με την εφαρμογή κάποιας κατάλληλης προηγμένης μεθόδου που εμπίπτει στην κατηγορία των των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων.

Κεφάλαιο 3

Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR)

Στο παρών κεφάλαιο της μεταπτυχιακής διατριβής, θα γίνει μία αναφορά σε ορισμένες βασικές έννοιες, προϋποθέσεις νομιμότητας και γενικά στοιχείων και περιπτώσεων που περιλαμβάνονται στο κείμενο και αναφέρονται τόσο σε προηγούμενα κεφάλαια όσο και στα επόμενα, όπως αυτά ορίζονται στον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation – GDPR) (Ευρωπαϊκό Κοινοβούλιο, 2016). Θα παρουσιαστούν δηλαδή όλες οι προϋποθέσεις και οι περιπτώσεις, σύμφωνα τις οποίες θα μπορεί να χαρακτηριστεί ως νόμιμη ή ως παράνομη η επεξεργασία των προσωπικών δεδομένων, ενέργεια που επιτελούν τα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων.

3.1 Βασικοί ορισμοί

Στην ενότητα 3.1, θα παρουσιαστούν ορισμένοι βασικοί ορισμοί, σχετικά με έννοιες που χρησιμοποιούνται, προκειμένου να αποφευχθεί οποιαδήποτε λανθασμένη παρανόηση τους, όπως αυτοί αναφέρονται στο άρθρο 4 του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων. Οι συγκεκριμένοι ορισμοί, αναφέρονται σε έννοιες που σχετίζονται άμεσα με τα προσωπικά δεδομένα και την διαδικασία επεξεργασίας τους, γεγονός που συνδέεται άμεσα με τη φύση και τις λειτουργίες που εκτελούν τα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων. Πιο συγκεκριμένα (Ευρωπαϊκό Κοινοβούλιο, 2016):

- Για τον όρο των "*Δεδομένων προσωπικού χαρακτήρα" (*ή προσωπικά δεδομένα όπως είθισται να αποκαλούνται), ο Κανονισμός τα αναφέρει ως "κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου." Στην ουσία, ή έννοια των προσωπικών δεδομένων είναι ευρεία αφού οποιαδήποτε πληροφορία δύναται έστω και υπό προϋποθέσεις να αντιστοιχηθεί σε συγκεκριμένο φυσικό πρόσωπο, τότε αποτελεί προσωπικό του δεδομένο. Κατ' αυτήν την έννοια, ακόμα και αναγνωριστικά συσκευών του χρήστη αποτελούν προσωπικά του δεδομένα.

- Για τον όρο της *επεξεργασίας*, ο Κανονισμός την αναφέρει ως "κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή."

- Για τον όρο της *ψευδωνυμοποίησης,* ο Κανονισμός την αναφέρει ως την "επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο."

- Για τον όρο του *υπευθύνου της επεξεργασίας,* ο Κανονισμός τον αναφέρει ως *"*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνος ή από κοινού με άλλα πρόσωπα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους."

- Για τον όρο του *εκτελούντος της επεξεργασίας,* ο Κανονισμός τον αναφέρει ως *"*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας."

- Για τον όρο του *αποδέκτη,* ο Κανονισμός τον αναφέρει ως *"*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν (4.5.2016 L 119/33 Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης EL) δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας."

- Για τον όρο του *τρίτου,* ο Κανονισμός τον αναφέρει ως το *"*οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή

του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα."

- Για τον όρο της *συγκατάθεσης του υποκειμένου των δεδομένων,* ο Κανονισμός τον αναφέρει ως την "κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν."

- Για τον όρο της *παραβίασης των δεδομένων προσωπικού χαρακτήρα,* ο Κανονισμός την αναφέρει ως την "παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία."

3.2 Προϋποθέσεις νομιμότητας της προστασίας προσωπικών δεδομένων

Στην παρούσα ενότητα, θα γίνει παρουσίαση των βασικών αρχών που πρέπει να διέπουν την επεξεργασία των προσωπικών δεδομένων, όπως αυτές αναφέρονται στο άρθρο 5 του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (Ευρωπαϊκό Κοινοβούλιο, 2016). Οι βασικές αυτές αρχές αναφέρονται στις προϋποθέσεις που πρέπει να ισχύουν και τα χαρακτηριστικά που πρέπει να διαθέτει η επεξεργασία των προσωπικών δεδομένων, προκειμένου να θεωρηθεί ότι λειτουργεί με νόμιμο τρόπο.

Πιο συγκεκριμένα, σχετικά με τα δεδομένα προσωπικού χαρακτήρα, αναφέρεται ότι αυτά θα πρέπει (Ευρωπαϊκό Κοινοβούλιο, 2016):

- Να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»).

- Να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς (σύμφωνα με το άρθρο 89 παράγραφος 1 του GDPR) («περιορισμός του σκοπού»).

- Να είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»).

- Να είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»).

- Να διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»).

- ❿ Να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

Σχετικά με τον υπεύθυνο της επεξεργασίας, αναφέρεται ότι φέρει την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»), δηλαδή με όλα όσα αναφέρθηκαν προηγουμένως.

Στο σημείο αυτό σκόπιμο είναι να δοθεί ιδιαίτερη έμφαση στην αρχή της ελαχιστοποίησης των δεδομένων: σύμφωνα με αυτή, κανείς δεν θα πρέπει να μαθαίνει περισσότερη πληροφορία (δεδομένα προσωπικού χαρακτήρα) από ό,τι απαιτείται για την επίτευξη των (νόμιμων και διαφανών) σκοπών του. Τα πρωτόκολλα SMC τα οποία αποτελούν το αντικείμενο της παρούσας διατριβής συνεισφέρουν σημαντικά σε αυτήν την κατεύθυνση, διότι ο σκοπός τους είναι ακριβώς η πραγματοποίηση κάποιου υπολογισμού χωρίς να αποκαλυφθεί τίποτα περισσότερο από το αποτέλεσμα του υπολογισμού σε άλλους: αν λοιπόν οι υπολογισμοί αυτοί έχουν να κάνουν με προσωπικά δεδομένα, η συνάφεια των πρωτοκόλλων SMC με την αρχή της ελαχιστοποίησης των δεδομένων καθίσταται φανερή.

3.3 Νομικές βάσεις για την επεξεργασία προσωπικών δεδομένων

Στη παρούσα ενότητα, θα γίνει μία αναφορά στις νομικές βάσεις για την προστασία των προσωπικών δεδομένων, όπως αυτές αναφέρονται στο άρθρο 6 του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (Ευρωπαϊκό Κοινοβούλιο, 2016). Ουσιαστικά, γίνεται αναφορά στις προϋποθέσεις που πρέπει να ισχύουν, ώστε να μπορεί να χαρακτηριστεί ως νόμιμος ως σκοπός για τον οποίο πραγματοποιείται η επεξεργασία των προσωπικών αυτών δεδομένων.

Πιο συγκεκριμένα, η διαδικασία της επεξεργασίας των προσωπικών δεδομένων, θεωρείται ότι λειτουργεί σύμφωνα με την νομοθεσία, όταν ικανοποιεί τουλάχιστον μία από τις ακόλουθες περιπτώσεις (Ευρωπαϊκό Κοινοβούλιο, 2016) :

- Όταν το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.

- Όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.

- Όταν η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.

- Όταν η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

- Όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

- Όταν η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

Ακόμα, αναφέρεται ότι τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν πιο ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού όσον αφορά την επεξεργασία για τη συμμόρφωση με την παράγραφο 1 στοιχεία γ) και ε), καθορίζοντας ακριβέστερα ειδικές απαιτήσεις για την επεξεργασία και άλλα μέτρα προς εξασφάλιση σύννομης και θεμιτής επεξεργασίας, μεταξύ άλλων για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX.

Στο ίδιο μήκος κύματος, αναφέρεται στον Κανονισμό ότι η βάση για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχεία γ) και ε) ορίζεται σύμφωνα με:

α) το δίκαιο της Ένωσης, ή β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας. Με απλά λόγια, για να είναι νομική βάση της επεξεργασίας μία εκ των στοιχ. γ) και ε), θα πρέπει να υπάρχει νόμος που να επιβάλλει την επεξεργασία.

Τέλος, όταν η επεξεργασία για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών που αναφέρονται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων:

- Τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας.

- Το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας.

- Τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε

επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10.

- Τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων.

- Την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

Ως προς το τελευταίο σκέλος, θα πρέπει να επισημανθεί ότι κατάλληλες εγγυήσεις ενδεχομένως να προκύπτουν και από τη χρήση πρωτοκόλλων SMC (δεν το αναφέρει ρητά ο Κανονισμός μεν, αλλά οι ιδιότητες των πρωτοκόλλων SMC μπορεί να είναι αντίστοιχες με ιδιότητες μίας καλής ψευδωνυμοποίησης, όπως θα δούμε στο υπόλοιπο μέρος της παρούσας διατριβής).

3.4 Νομικές βάσεις για την επεξεργασία ευαίσθητων προσωπικών δεδομένων

Στην παρούσα τελευταία ενότητα του κεφαλαίου 3, θα γίνει μια παρουσίαση των περιπτώσεων όπου είναι κατ' εξαίρεση επιτρεπτή η επεξεργασία των ευαίσθητων προσωπικών δεδομένων, όπως αυτή αναφέρεται στο άρθρο 9 του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (Ευρωπαϊκό Κοινοβούλιο, 2016).

Πιο συγκεκριμένα αναφέρεται ότι (Ευρωπαϊκό Κοινοβούλιο, 2016):

- Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή

δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό. Τα ανωτέρω αποτελούν δεδομένα ειδικών κατηγοριών ή ευαίσθητα δεδομένα.

- Η παράγραφος 1 δεν εφαρμόζεται στις ακόλουθες περιπτώσεις (εξαιρέσεις που επιτρέπουν την επεξεργασία) :

- Όταν το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων.

- Όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων.

- Όταν η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί.

- Όταν η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων.

- Όταν η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

- Όταν η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα.

- Όταν η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

- Όταν η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3.

- Όταν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου.

- Όταν η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

- Τα δεδομένα προσωπικού χαρακτήρα που αναφέρονται στην παράγραφο 1 μπορεί να τύχουν επεξεργασίας για τους σκοπούς που προβλέπονται στην παράγραφο 2 στοιχείο η), όταν τα δεδομένα αυτά υποβάλλονται σε επεξεργασία από ή υπό την ευθύνη επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς ή από άλλο πρόσωπο το οποίο υπέχει επίσης υποχρέωση τήρησης του απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς.

- Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία.

Τέλος, θα πρέπει να γίνει αναφορά και σε δύο σημαντικές έννοιες που αναφέρονται στο άρθρο 25 του Κανονισμού σχετικά με την προστασία των δεδομένων, ήδη από το σχεδιασμό και εξ' ορισμού. Πιο συγκεκριμένα αναφέρεται ότι (Δρ. Κωνσταντίνος Λιμνιώτης & Ιωάννης Μαυρίδης, 2019; Ευρωπαϊκό Κοινοβούλιο, 2016):

- Ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων (όπως η ελαχιστοποίηση των δεδομένων) και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι

απαιτήσεις του GDPR και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων (Άρθρο 25, παρ. 1).

Με άλλα λόγια, ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει ότι για την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί εφαρμόζει μέτρα, π.χ. προσαρμοσμένα στην αρχή της αναλογικότητας (ώστε η επεξεργασία να είναι η ελάχιστη δυνατή), τα οποία μέτρα έχουν καθοριστεί ήδη κατά το σχεδιασμό της επεξεργασίας (*Προστασία των δεδομένων ήδη από το σχεδιασμό - data protection by design*)

⑩ Ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας (…) Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα σε τρίτους χωρίς την παρέμβαση του υποκειμένου των δεδομένων (Άρθρο 25, παρ. 1).

Με άλλα λόγια, ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει ότι για την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί η προκαθορισμένη ρύθμιση είναι η πιο φιλική προς την ιδιωτικότητα (*Προστασία των δεδομένων εξορισμού - data protection by default*)

Κεφάλαιο 4

Πρωτόκολλα Ασφαλών Υπολογισμών πολλών Συμμετεχόντων

Στο κεφάλαιο αυτό θα γίνει μια παρουσίαση της έννοιας των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων, καθώς επίσης και των ορισμών που υπάρχουν για την ασφάλεια των πρωτοκόλλων αυτών. Επιπλέον, θα γίνει αναφορά, τόσο στην εφαρμοσιμότητάς τους, όσο και στις διάφορες τεχνικές που υπάρχουν, καθώς και στις εφαρμογές που μπορεί να έχουν τα πρωτόκολλα αυτά.

4.1 Βασικές Έννοιες

Στο σημείο αυτό και πριν την είσοδο στο κυρίως τμήμα του 4ου κεφαλαίου, που αναφέρεται στα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων, σκόπιμο είναι να παρουσιαστούν ορισμένοι βασικοί ορισμοί που θα χρησιμοποιηθούν.

- Πρωτόκολλα SMC (Secure Multi-Party Computations): Πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων.

- Οντότητες (Parties): Οι διάφοροι συμμετέχοντες στους υπολογισμούς.

- Αντίπαλοι (Adversaries): Οντότητες που προσπαθούν να προκαλέσουν προβλήματα στη λειτουργία των SMC πρωτοκόλλων. Συνήθως είναι κακόβουλοι και προσπαθούν να εκμεταλλευτούν και να διαφθείρουν οντότητες που συμμετέχουν στον υπολογισμό, προκειμένου να τις θέσουν υπό τον έλεγχο τους.

- Είσοδοι (Inputs): Οι πληροφορίες-δεδομένα που παρέχουν οι οντότητες και που θα χρησιμοποιηθούν από την συνάρτηση για την εκτέλεση του υπολογισμού.

- Συνάρτηση (Function): Η διαδικασία επεξεργασίας των εισόδων.

- Έξοδοι (Outputs): Τα αποτελέσματα που προκύπτουν από την επεξεργασία των εισόδων.

- Κατευθυνόμενες οντότητες (Corrupted Parties): Οντότητες που έχουν τεθεί υπό τον έλεγχο αντιπάλων.

- Μη-κατευθυνόμενες οντότητες (Honest Parties): Οντότητες που λειτουργούν φυσιολογικά, δίχως να ελέγχονται από κανέναν.

4.2 Η 'Εννοια του SMC

Τα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων αποτέλεσαν μια ιδέα η οποία αναπτύχθηκε αρχικά σε θεωρητικό επίπεδο. Ο Yao ήταν ο πρώτος που ανέπτυξε την ιδέα των ασφαλών υπολογισμών, παρουσιάζοντας αρχικά το πρόβλημα των εκατομμυριούχων (Evans et al., 2018; Yao, 1982). Σύμφωνα με το πρόβλημα αυτό, δύο εκατομμυριούχοι θέλουν να ανακαλύψουν ποιος από τους δύο είναι πλουσιότερος, χωρίς όμως να μάθουν τίποτα ο ένας για την περιουσία του άλλου.

Με το πέρασμα των χρόνων, άρχισε να γίνεται πιο επιτακτική η ανάγκη για να υπάρχουν υπολογισμοί ανάμεσα σε περισσότερες από δύο οντότητες, οι οποίες όμως πρέπει να παρουσιάζουν κάποια ικανοποιητικά επίπεδα ασφάλειας. Η ιδέα για γενίκευση σε n οντότητες αναπτύχθηκε σε μεγάλο βαθμό στη συνέχεια, μέσω μια προσπάθειας που πραγματοποιήθηκε για την επίτευξη υπολογισμών ανάμεσα σε πολλές πλευρές, ικανοποιώντας παράλληλα ορισμένες βασικές προδιαγραφές ασφαλείας (Goldreich et al., 1987). Σε αυτό το σημείο εμφανίζονται τα πρωτόκολλα SMC. Τα πρωτόκολλα SMC έρχονται να λύσουν το πρόβλημα της ασφαλούς επικοινωνίας (πραγματοποίηση υπολογισμών με ασφάλεια/μυστικότητα) πολλών συμμετεχόντων. Γενικότερα, σαν SMC

θα μπορούσε να θεωρηθεί ένας υπολογισμός ανάμεσα σε δύο ή και περισσότερες οντότητες, οι οποίες δίνουν στη συνάρτηση υπολογισμού κάποια ιδιωτική είσοδο, και λαμβάνουν σαν αποτέλεσμα μία έξοδο, δεδομένου ότι ο υπολογισμός γίνεται με ασφαλή τρόπο. Με έναν πιο μαθηματικό συλλογισμό, οι υπολογισμοί πολλών συμμετεχόντων μπορούν να οριστούν σαν την περίπτωση στην οποία υπάρχουν 1, 2, ……. , n διαφορετικές οντότητες, οι οποίες παρέχουν η κάθε μία x_1, x_2 , ……. , x_n εισόδους στην συνάρτηση-διαδικασία υπολογισμού, και πρέπει να υπολογίσουν μέσω μιας συνάρτησης f και των εισόδων αυτών τις αντίστοιχες εξόδους f (x_1, x_2 , ……. , x_n) = (y_1, y_2, …. , y_n) , με ασφαλή όμως τρόπο (Bogetoft et al., 2009). Ο ασφαλής αυτός τρόπος αναφέρεται στο γεγονός ότι οι οντότητες θα πρέπει να μάθουν μόνο όποια πληροφορία προέρχεται από τις εξόδους που προορίζονται για την κάθε μία από αυτές, και τίποτα άλλο. Αξίζει να αναφερθεί ένα χαρακτηριστικό παράδειγμα SMC όπου τρεις διαφορετικές οντότητες, στη συγκεκριμένη περίπτωση άνθρωποι, δίνουν σε μια συνάρτηση F από μία τιμή, τις x, y, z , και αυτή η συνάρτηση υπολογίζει την μεγαλύτερη από αυτές τις τιμές, δηλαδή F (x, y, z) = max (x, y, z) (Archer et al., 2018). Η ιδιότητα της ασφάλειας έγκειται στο γεγονός ότι η κάθε οντότητα θα λάβει σαν πληροφορίες εξόδου μόνο την πληροφορία για το ποια είναι η μεγαλύτερη τιμή, και συνεπώς αν αυτή συμπίπτει με την δική τους είσοδο. Γενικότερα, πρέπει να αναφερθεί ότι τα πρωτόκολλα αυτά μπορούν να συμβάλλουν σημαντικά στην επίλυση οποιουδήποτε κρυπτογραφικού προβλήματος με ασφάλεια, στην ιδανική όμως περίπτωση όπου δεν υπάρχουν αντίπαλοι που προσπαθούν να προκαλέσουν προβλήματα στην ομαλή λειτουργία τους, δηλαδή όταν το πρόβλημα λαμβάνει χώρα σε έναν ιδανικό-φανταστικό κόσμο.

4.3 Η Ασφάλεια των SMC

Στη συγκεκριμένη ενότητα, θα γίνει μια προσπάθεια να παρουσιαστεί η ασφάλεια των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων, μέσα από την παρουσίαση κάποιων ορισμών της. Πιο συγκεκριμένα θα παρουσιαστεί ο ορισμός της ασφάλειας, στηριζόμενη είτε σε έναν συγκεκριμένο αριθμό από ιδιότητες που πρέπει να ισχύουν, είτε στηριζόμενη στη φυσιολογική αναμενόμενη λειτουργία που πρέπει ένα πρωτόκολλο να έχει στον ιδεατό και στον πραγματικό κόσμο. Τέλος, θα γίνει αναφορά και σε ορισμένες βασικές παραμέτρους που προκύπτουν από τον ορισμό της ασφάλειας.

4.3.1 Η Ασφάλεια Βασισμένη σε Ιδιότητες

Το πρόβλημα στους υπολογισμούς πολλών συμμετεχόντων βρίσκεται στο γεγονός ότι μπορεί να δημιουργηθεί κίνδυνος από οντότητες, συνήθως κατευθυνόμενες από αντιπάλους, που επιθυμούν είτε να προκαλέσουν κάποιο πρόβλημα στον υπολογισμό, είτε να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες (Lindell, 2020). Αν γινόταν μία προσπάθεια να υπάρξει ορισμός της ασφάλειας των SMC πρωτοκόλλων, τότε, προκειμένου να χαρακτηριστεί ένας υπολογισμός ως ασφαλής, θα πρέπει να ικανοποιεί τις εξής δύο βασικές ιδιότητες, αυτές της *ιδιωτικότητας* (privacy) και της *ορθότητας* (correctness) (Archer et al., 2018; Lindell, 2020). Η ιδιότητα της *ιδιωτικότητας* έχει να κάνει με το γεγονός ότι κάθε οντότητα που συμμετέχει στον υπολογισμό, θα πρέπει να μαθαίνει μόνο ό,τι είναι απολύτως απαραίτητο και αναφέρεται σε αυτές. Πιο συγκεκριμένα, θα πρέπει κάθε οντότητα να μπορεί να μαθαίνει μόνο ό,τι προκύπτει από την έξοδο, από την οποία θα μπορεί να προκύπτουν οι όποιες πληροφορίες και για τις υπόλοιπες οντότητες. Όσον αφορά τη δεύτερη ιδιότητα, αυτή της *ορθότητας*, εκείνη αναφέρεται στο γεγονός ότι κάθε οντότητα θα πρέπει να λαμβάνει και να μαθαίνει την σωστή έξοδο (output), χωρίς αυτή να έχει τροποποιηθεί-αλλοιωθεί από κάποιον αντίπαλο.

Παράλληλα όμως με τις δύο αυτές ιδιότητες, υπάρχουν και άλλες απαιτήσεις που πρέπει να ικανοποιούνται. Υπάρχουν επομένως οι εξής ακόμα τρεις ιδιότητες (Lindell, 2020) :

- *Η ανεξαρτησία των εισόδων (Independence of Inputs)*. Σύμφωνα με την ιδιότητα αυτή οι κατευθυνόμενες οντότητες θα πρέπει να επιλέγουν τις εισόδους τους ανεξάρτητα από αυτές των μη-κατευθυνόμενων οντοτήτων (δηλαδή οι συμμετέχοντες δεν πρέπει να είναι σε θέση να επιλέγουν συγκεκριμένες εισόδους με βάση τις εισόδους των άλλων συμμετεχόντων). Αυτό μπορεί να συμβάλλει στο ότι οι είσοδοι που θα θέτει κάποιος χρήστης δεν θα επηρεάζονται από πληροφορίες που μπορεί να γίνουν γνωστές για τις εισόδους άλλων οντοτήτων. Αξίζει να σημειωθεί ότι η συγκεκριμένη ιδιότητα, δεν αποτελεί κομμάτι της *ιδιωτικότητας*. Η *ανεξαρτησία των εισόδων* αναφέρεται στο αν μπορεί να επηρεαστεί η επιλογή των εισόδων, ενώ από την άλλη μεριά η *ιδιωτικότητα* αναφέρεται στο είδος των πληροφοριών που γίνονται γνωστές από τις εξόδους.

- *Η εγγυημένη παράδοση των εξόδων (Guaranteed Output Delivery).* Η συγκεκριμένη ιδιότητα αναφέρεται στο γεγονός ότι δεν θα πρέπει οποιοσδήποτε αντίπαλος να μπορεί, μέσω άλλων κατευθυνόμενων οντοτήτων, να παρέμβει και να διακόψει τον υπολογισμό, έτσι ώστε οι μη-κατευθυνόμενες οντότητες να μην λάβουν την έξοδο που θα έπρεπε να λάβουν. Ουσιαστικά δηλαδή δεν θα πρέπει να μπορεί κάποιος αντίπαλος να πραγματοποιήσει διακοπή των υπηρεσιών που προσφέρει η συνάρτηση-υπολογισμός και που έχουν να κάνουν με τις εξόδους τους.

- *Δικαιοσύνη – Αμεροληψία (Fairness).* Πρόκειται για μια ιδιότητα, η οποία έχει να κάνει με το γεγονός ότι θα πρέπει να υπάρχει ισότητα στο θέμα των οντοτήτων που λαμβάνουν τις εξόδους τους. Πιο συγκεκριμένα, οι κατευθυνόμενες οντότητες θα πρέπει να μπορούν να λαμβάνουν τις εξόδους τους μόνο εφ' όσον αυτό μπορούν να το κάνουν και οι μη-κατευθυνόμενες οντότητες. Οτιδήποτε δεν συμβαδίζει με την ιδιότητα αυτή, δεν θεωρείται ότι καλύπτει ως προς την ασφάλεια τον υπολογισμό και επομένως δεν θα πρέπει να συμβαίνει. Αξίζει να σημειωθεί ότι *η εγγυημένη παράδοση των εξόδων* συνεπάγεται και *δικαιοσύνη*, αλλά δεν ισχύει το αντίστροφο. Εφόσον όλες οι οντότητες πρέπει να λάβουν την έξοδο, τότε είναι απίθανο να λάβουν έξοδο οι κατευθυνόμενες οντότητες, ενώ οι μη-κατευθυνόμενες όχι (Cohen & Lindell, 2016). Η αντίστροφη κατεύθυνση όμως δεν είναι τόσο ξεκάθαρη. Σε περίπτωση που υπάρχει πρωτόκολλο με δύο οντότητες, οι μη-κατευθυνόμενες οντότητες μπορούν, αν δεν λάβουν έξοδο, να την υπολογίσουν χρησιμοποιώντας τη δική τους είσοδο και μια προεπιλεγμένη είσοδο για την άλλη οντότητα. Σε πρωτόκολλο όμως πολλών συμμετεχόντων, αυτό δεν είναι εύκολο, καθώς οι μη-κατευθυνόμενες οντότητες δεν γνωρίζουν ποιες είναι οι κατευθυνόμενες, και επομένως δεν μπορούν να προχωρήσουν σε μια παρόμοια ενέργεια.
Σε όλες τις παραπάνω ιδιότητες, θα μπορούσε να προστεθεί και αυτή της *ανθεκτικότητας (robustness)*, σύμφωνα με την οποία κανένα υποσύνολο των κατευθυνόμενων από αντιπάλους οντοτήτων, που επιθυμούν είτε να διαρρεύσουν πληροφορίες, είτε πιο γενικά να αποκλίνουν από τις οδηγίες που υπάρχουν κατά την εκτέλεση ενός πρωτοκόλλου, να μην μπορεί να αναγκάσει τις μη-κατευθυνόμενες οντότητες να εξάγουν κάποιο λανθασμένο αποτέλεσμα (Archer et al., 2018).

Εφόσον οι παραπάνω ιδιότητες ικανοποιούνται σε κάποιο SMC πρωτόκολλο, τότε θα μπορούσε να ειπωθεί ότι το πρωτόκολλο αυτό θεωρείται ασφαλές. Παρόλα αυτά, παρά

το γεγονός ότι οι ιδιότητες αυτές είναι πολύ σημαντικές, εντούτοις δεν μπορούν να αποτελέσουν από μόνες τους έναν ολοκληρωμένο ορισμό για την ασφάλεια των SMC πρωτοκόλλων (Lindell, 2020; Zhao et al., 2018). Αυτό οφείλεται στο γεγονός ότι μπορεί να υπάρξουν ιδιότητες που να μην ικανοποιούνται σε κάποιο πρωτόκολλο, λόγω της φύσης του. Αντίθετα υποστηρίζεται ότι για να θεωρηθεί ένα πρωτόκολλο SMC ασφαλές, θα πρέπει εκτός από τις παραπάνω ιδιότητες, να είναι ανθεκτικό και ως προς οποιαδήποτε τύπου επίθεση μπορεί να γίνει εναντίον του. Για το λόγο αυτό, θεωρούν ότι ένας σαφής, με στέρεες βάσεις ορισμός, θα πρέπει να περιλαμβάνει τις έννοιες του πραγματικού και του ιδεατού κόσμου.

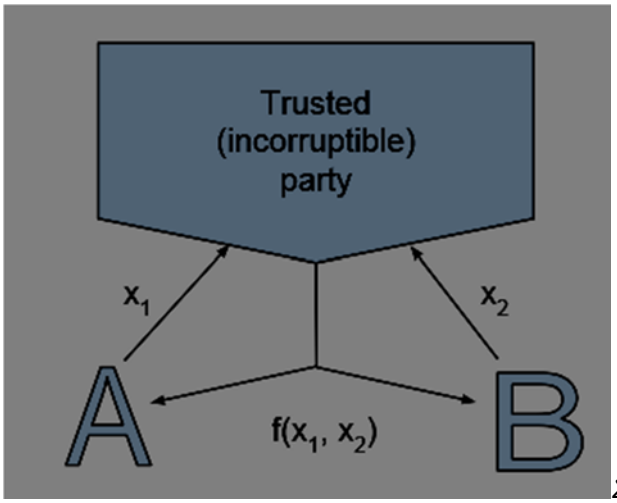
4.3.2 Η Ασφάλεια Βασισμένη στην Ύπαρξη Πραγματικού και Ιδεατού κόσμου

Προκειμένου να υπάρξει μια πιο ικανοποιητική προσέγγιση, που θα μπορούσε να οδηγήσει σε έναν πιο ολοκληρωμένο ορισμό της ασφάλειας των SMC πρωτοκόλλων, υπάρχει η άποψη ότι αυτή πρέπει να περιλαμβάνει τις έννοιες του πραγματικού και του ιδεατού κόσμου (Ishai et al., 2006; Lindell, 2020). Σύμφωνα με την άποψη αυτή, ο ιδεατός κόσμος αποτελεί μια περίπτωση στην οποία υπάρχει μία τρίτη έμπιστη αρχή, στην οποία οι υπόλοιπες οντότητες στέλνουν τις εισόδους τους. Ουσιαστικά, η αρχή αυτή ασχολείται με την εκτέλεση του υπολογισμού, χρησιμοποιώντας τις εισόδους που λαμβάνει, και στη συνέχεια με την παράδοση των εξόδων που προκύπτουν στις οντότητες που αυτές αντιστοιχούν. Παράλληλα, η μόνη ενέργεια που έχουν να κάνουν οι οντότητες είναι να στείλουν τις εισόδους τους στην έμπιστη αρχή, γεγονός που οδηγεί στο συμπέρασμα ότι ο μόνος τρόπος με τον οποίο μπορεί να παρέμβει ένας αντίπαλος, είναι να προσπαθήσει να επηρεάσει τις εισόδους που στέλνουν οι κατευθυνόμενες από εκείνον οντότητες. Ο ιδεατός κόσμος είναι ένα ιδανικό μοντέλο, το οποίο μπορεί να παρέχει το υψηλότερο επίπεδο ασφάλειας που μπορεί να προσφέρει ένα υπολογισμός πολλών συμμετεχόντων (Ran Canetti et al., 2001). Παρά το γεγονός ότι ο ιδεατός κόσμος αποτελεί μια ιδανική από άποψη ασφάλειας περίπτωση, αξίζει να αναφερθεί ότι εξακολουθούν να έχουν ισχύ όλες οι ιδιότητες της ασφάλειας που αναφέρθηκαν προηγουμένως.

Με έναν πιο μαθηματικό συλλογισμό, ο ιδεατός κόσμος μπορεί να παρουσιαστεί σαν την περίπτωση όπου n οντότητες με εισόδους $x_1, x_2, \ldots\ldots, x_n$ επιθυμούν να υπολογίσουν την

έξοδο y=f(x_1, x_2 , ……. , x_n) (Covington & Golbek, 2015). Την διαδικασία αυτή αναλαμβάνει μια έμπιστη αρχή, η οποία είναι μη-κατευθυνόμενη, και η οποία υπολογίζει την έξοδο y και στη συνέχεια την ανακοινώνει σε όλες τις οντότητες.

Παρακάτω φαίνεται από το σχήμα μία απλή περίπτωση όπου υπάρχουν δύο οντότητες και η έμπιστη αρχή. Οι δύο οντότητες στέλνουν τις εισόδους στην έμπιστη αρχή, αυτή εκτελεί τον υπολογισμό και στις συνέχεια επιστρέφει στις οντότητες την αντίστοιχη έξοδο.

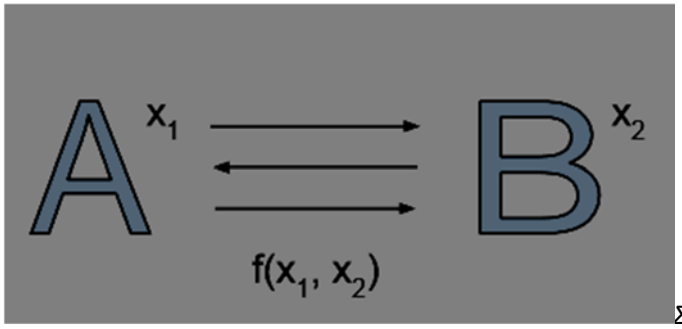


Σχήμα 1: Υπολογισμός ανάμεσα σε δύο οντότητες Α και Β και μία έμπιστη αρχή

Πηγή: " Secure Multiparty Computation ", (Covington & Golbek, 2015)

Από την άλλη μεριά, ο πραγματικός κόσμος δεν περιλαμβάνει πάντα κάποια έμπιστη τρίτη αρχή. Αυτό οφείλεται στο γεγονός ότι δεν μπορεί πάντοτε να υπάρχει απόλυτη εμπιστοσύνη, καθώς πάντα υπάρχει η περίπτωση η οντότητα αυτή να είναι κατευθυνόμενη, λόγω των διάφορων κινδύνων που επικρατούν καθώς και του ανταγωνισμού και των εγκλημάτων του κυβερνοχώρου. Για το λόγο αυτό, οι οντότητες είναι αναγκασμένες από μόνες τους να πραγματοποιήσουν τον υπολογισμό, αλληλεπιδρώντας μεταξύ τους, και αφού γίνει αυτό, όλες οι οντότητες θα πρέπει να πληροφορηθούν το αποτέλεσμα της εξόδου.

Παρακάτω φαίνεται από το σχήμα μία απλή περίπτωση όπου υπάρχουν δύο οντότητες, που εκτελούν μόνες τους τον υπολογισμό, χρησιμοποιώντας τη συνάρτηση f και τις εισόδους τους, και στη συνέχεια λαμβάνουν και οι δύο την έξοδο.



Σχήμα 2: Υπολογισμός ανάμεσα σε δύο οντότητες Α και Β χωρίς έμπιστη αρχή.

Πηγή: "Secure Multiparty Computation ", (Covington & Golbek, 2015)

Συνδυάζοντας λοιπόν τόσο τον ιδεατό, όσο και τον πραγματικό κόσμο, μπορεί να διατυπωθεί η έννοια της ασφάλειας, μέσω του ορισμού που αναφέρει ότι για να θεωρηθεί ένα πρωτόκολλο SMC ασφαλές, θα πρέπει να ισχύει ότι κανένας αντίπαλος δεν μπορεί να προκαλέσει στον πραγματικό κόσμο περισσότερο κακό από ότι είναι δυνατό να προκληθεί στον ιδεατό κόσμο (Ishai et al., 2006; Lindell, 2020). Αυτό με άλλα λόγια σημαίνει ότι για κάθε αντίπαλο που πραγματοποιεί μια επιτυχημένη επίθεση στον πραγματικό κόσμο, υπάρχει και ένας αντίπαλος που θα πραγματοποιήσει μία επίθεση στον ιδεατό κόσμο, η οποία θα έχει την ίδια επίδραση και τα ίδια αποτελέσματα. Ουσιαστικά ο ιδεατός κόσμος χρησιμοποιείται για εξακρίβωση ότι πρόκειται για ένα

ασφαλές πρωτόκολλο. Γίνεται σαφές ότι στον ιδεατό κόσμο δεν μπορούν να πραγματοποιηθούν με επιτυχία επιθέσεις. Επομένως για να υπάρξει ο ισχυρισμός ότι ένα πρωτόκολλο είναι ασφαλές, θα πρέπει να αποτύχουν όλου του είδους οι επιθέσεις που μπορούν να γίνουν στον πραγματικό κόσμο καθώς επίσης και να υπάρχει ταύτιση των αποτελεσμάτων που προκύπτουν από την εκτέλεση του πρωτοκόλλου και στους δύο κόσμους.

Χρησιμοποιώντας τις δύο προηγούμενες περιπτώσεις, είναι σε μεγάλο βαθμό εφικτό να προκύψει ένας πιο ευκολονόητος ορισμός της ασφάλειας ενός πρωτοκόλλου (Ishai et al., 2006; Lindell, 2020). Στη συγκεκριμένη περίπτωση, η ασφάλεια βασίζεται στη σύγκριση που μπορεί να γίνει ανάμεσα στην έξοδο που προκύπτει από την εκτέλεση του πρωτοκόλλου στον πραγματικό και στον ιδεατό κόσμο. Πιο συγκεκριμένα, πρόκειται για την περίπτωση όπου γίνεται σύγκριση της εξόδου που προκύπτει από τον αντίπαλο και τις μη-κατευθυνόμενες οντότητες στον πραγματικό κόσμο και από την έξοδο που προκύπτει από την εκτέλεση στον ιδεατό κόσμο. Έτσι λοιπόν, για κάθε αντίπαλο που υπάρχει και εκτελεί μία επίθεση στον πραγματικό κόσμο, θα πρέπει να υπάρχει και ένας αντίστοιχος αντίπαλος που να εκτελεί μια επίθεση στον ιδεατό κόσμο. Μάλιστα, για να ικανοποιείται η ιδιότητα της ασφάλειας, θα πρέπει οι διανομές των αντιπάλων και των συμμετεχουσών οντοτήτων στις εισόδους και τις εξόδους , τόσο στον πραγματικό, όσο και στον ιδεατό κόσμο να είναι ακριβώς ίδιες, κατά τέτοιο τρόπο ώστε η εκτέλεση του πρωτοκόλλου στον πραγματικό κόσμο να προσομοιώνει τον ιδεατό κόσμο. Επομένως προκύπτει ο ορισμός της ασφάλειας έχοντας την εξής ονομασία : το παράδειγμα της προσομοίωσης του πραγματικού και του ιδεατού κόσμου (the ideal/real simulation paradigm).

Από τα παραπάνω, γίνεται λοιπόν σαφές ότι μέσω του ορισμού αυτού ικανοποιούνται όλες οι ιδιότητες της ασφάλειας που αναφέρθηκαν προηγουμένως (Lindell, 2020). Ποιο συγκεκριμένα, από τον ανωτέρω ορισμό προκύπτει πως η ιδιωτικότητα ικανοποιείται από το γεγονός ότι η έξοδος που λαμβάνει ο αντίπαλος είναι η ίδια, τόσο στον πραγματικό, όσο και στον ιδεατό κόσμο. Η ορθότητα ικανοποιείται από το γεγονός ότι οι μη-κατευθυνόμενες οντότητες λαμβάνουν την ίδια έξοδο τόσο στον πραγματικό, όσο και στον ιδεατό κόσμο, καθώς και από το ότι στον ιδεατό κόσμο όλες οι μη-κατευθυνόμενες οντότητες λαμβάνουν τις σωστές εξόδους, όπως αυτές έχουν υπολογιστεί και τους έχουν

σταλθεί από την τρίτη έμπιστη οντότητα. Σχετικά με την ανεξαρτησία των εισόδων, στον ιδεατό κόσμο, οι κατευθυνόμενες οντότητες δεν γνωρίζουν τίποτα για τις εισόδους των μη-κατευθυνόμενων οντοτήτων, τη χρονική στιγμή που αποφασίζουν και στέλνουν τις δικές τους εισόδους, και επομένως επιλέγουν ανεξάρτητα από τις εισόδους των μη-κατευθυνόμενων οντοτήτων τι θα στείλουν. Τέλος, αξίζει να τονιστεί ότι οι ιδιότητες της εγγυημένης παράδοσης των εξόδων και της δικαιοσύνης ικανοποιούνται στον πραγματικό κόσμο, καθώς πάντα η έμπιστη τρίτη οντότητα επιστρέφει σωστά όλες τις εξόδους (Lindell, 2020). Βέβαια, αξίζει να αναφερθεί ότι μπορεί ο ορισμός να "χαλαρώσει" κάποιες φορές και να μην ισχύουν οι ιδιότητες της δικαιοσύνης και της εγγυημένης παράδοσης των εξόδων. Στην συγκεκριμένη περίπτωση το επίπεδο ασφαλείας που επιτυγχάνεται ονομάζεται ασφάλεια με διακοπή (security with abort), κατά την οποία ο αντίπαλος μπορεί εφόσον το επιθυμεί να ματαιώσει τον υπολογισμό μόλις παραλάβει τις εξόδους του (Ishai et al., 2011). Επομένως μπορεί να έχει σαν αποτέλεσμα να λαμβάνουν τις εξόδους οι κατευθυνόμενες οντότητες, ενώ οι μη-κατευθυνόμενες όχι.

4.4 Επιπρόσθετες Παράμετροι του Ορισμού

Μέχρι στιγμής έγινε αναφορά στο γεγονός ότι ένας αντίπαλος μπορεί να έχει θέσει υπό τον έλεγχό του έναν αριθμό από οντότητες και να τις κατευθύνει, προκειμένου πραγματοποιήσει μία επίθεση και να προκαλέσει προβλήματα στην ασφαλή εκτέλεση του υπολογισμού ενός πρωτοκόλλου. Θα πρέπει να γίνει όμως και αναφορά σε ένα ακόμα χαρακτηριστικό που μπορεί να έχει ένας αντίπαλος, και πιο συγκεκριμένα στη δύναμή του. Η δύναμη του αντιπάλου ουσιαστικά διαμορφώνεται από δύο βασικές παραμέτρους, την επιτρεπόμενη συμπεριφορά του αντιπάλου και την στρατηγική απόκτησης του ελέγχου των οντοτήτων.

4.4.1 Επιτρεπόμενη Συμπεριφορά του Αντιπάλου

Στόχος ενός πρωτοκόλλου ασφαλών υπολογισμών πολλών συμμετεχόντων, είναι να προστατέψει τις μη-κατευθυνόμενες οντότητες από οποιαδήποτε επιθετική συμπεριφορά ενός αντιπάλου. Εφόσον κάποιος αντίπαλος αποφασίσει να πραγματοποιήσει κάποια επίθεση, τότε μπορεί είτε να προχωρήσει σε μια απλή συγκέντρωση πληροφοριών, είτε να προσπαθήσει να χρησιμοποιήσει και να οδηγήσει τις

κατευθυνόμενες από αυτόν οντότητες στο να συμπεριφερθούν κακόβουλα, με σκοπό να εξυπηρετήσουν δικούς του σκοπούς. Επομένως, η επιτρεπόμενη συμπεριφορά του αντιπάλου έχει άμεση σχέση με την συμπεριφορά και τις ενέργειες που επιτρέπονται στις κατευθυνόμενες από εκείνον οντότητες. Σύμφωνα με τη βιβλιογραφία (Cohen & Lindell, 2016; Lindell, 2020; Ευστάθιος Ζάχος et al., 2015), ανάλογα με τις συμπεριφορά τους, οι αντίπαλοι μπορούν να ταξινομηθούν σε τρεις κατηγορίες :

- *Παθητικός αντίπαλος* (Semi-honest ή Passive ή Honest-but-curious adversary). Σύμφωνα με τη συγκεκριμένη κατηγορία αντιπάλων, ένας παθητικός αντίπαλος ακολουθεί σε γενικές γραμμές τους περισσότερους κανόνες του πρωτοκόλλου, πράγμα το οποίο συμβαίνει και με τις κατευθυνόμενες από εκείνον οντότητες. Παρ' όλα αυτά έχει τη δυνατότητα να πραγματοποιήσει και δικές του ενέργειες. Αυτό σημαίνει ότι έχει τη δυνατότητα να αποκτήσει πρόσβαση εκτός από τις εξόδους, και στην εσωτερική κατάσταση και σε εσωτερικές πληροφορίες των οντοτήτων που ελέγχει, και πιο συγκεκριμένα σε πληροφορίες που μπορεί να περιλαμβάνουν ακόμα και τα μηνύματα και τις συνομιλίες των οντοτήτων αυτών. Ο σημαντικότερος λόγος που το κάνει αυτό είναι για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε σημαντικές ιδιωτικές-ευαίσθητες πληροφορίες, καταπατώντας έτσι την εμπιστευτικότητά τους και γενικότερα την ιδιωτικότητα. Σε γενικές γραμμές πρόκειται για ένα αδύναμο μοντέλο αντιπάλου, αλλά εφόσον η ασφάλεια του πρωτοκόλλου καλύπτει αυτό την κατηγορία αντιπάλων, αυτό αυτόματα συνεπάγεται ότι δεν θα υπάρξει καμία διαρροή δεδομένων και πληροφοριών. Από την άλλη όμως μεριά, μπορεί να έχει πολλές εφαρμογές, όπως για παράδειγμα στην περίπτωση συνεργασίας πολλών επιχειρήσεων για κάποιο έργο που έχουν να αναλάβει να πραγματοποιήσουν από κοινού, όπου δεν θα ήθελαν να συμπεριφερθούν ανέντιμα σκεπτόμενοι τις συνέπειες, αλλά από την άλλη θα ήθελαν να αποκτήσουν πρόσβαση σε ιδιωτικές πληροφορίες των υπολοίπων, για να κερδίσουν έδαφος και να βρίσκονται ένα βήμα πιο μπροστά από εκείνους (Zhao et al., 2018).
- *Κακόβουλος-Ενεργός αντίπαλος* (Active ή malicious adversary). Σύμφωνα με τη συγκεκριμένη κατηγορία αντιπάλων, οι οντότητες οι οποίες βρίσκονται υπό τον έλεγχό τους, έχουν τη δυνατότητα να αποκλίνουν αυθαίρετα από τους κανόνες του πρωτοκόλλου, σύμφωνα πάντα με τις οδηγίες του αντιπάλου που τις ελέγχει.

Εφόσον ένα πρωτόκολλο είναι ασφαλές απέναντι σε ενεργούς αντιπάλους, τότε αυτό σημαίνει ότι μπορεί να εγγυηθεί την ασφάλεια απέναντι σε οποιαδήποτε είδους επίθεση αντιπάλου. Παρ' όλα αυτά, προκειμένου να επιτευχθεί ένα τέτοιο επίπεδο ασφάλειας, θα πρέπει να μπορεί να γίνει αποδεκτό ένα μεγάλο σε βάρος τίμημα, έτσι ώστε να είναι αποτελεσματικό το πρωτόκολλο. Αυτό σημαίνει ότι πρόκειται για ένα μοντέλο που μπορεί να εφαρμοστεί ανάμεσα σε ανταγωνιστές, με σκοπό να επηρεάσουν το αποτέλεσμα ενός υπολογισμού, έτσι ώστε να αυξήσουν το δικό τους κέρδος, χωρίς να ενδιαφέρονται για τυχόν συνέπειες, με σημαντικότερη το γεγονός ότι μπορεί να γίνουν αντιληπτοί να λειτουργούν κακόβουλα και αυτό να τους επιφέρει συνέπειες οικονομικές, συνέπειες στη φήμη τους ή ακόμα και να οδηγηθούν σε δικαστικές διαμάχες (Zhao et al., 2018).

- *Μυστικός αντίπαλος* (covert adverasry). Σύμφωνα με τη συγκεκριμένη κατηγορία αντιπάλων, ο αντίπαλος μπορεί να συμπεριφερθεί κακόβουλα, με σκοπό να καταφέρει να "σπάει" το πρωτόκολλο. Σε περίπτωση όμως που προσπαθήσει κάτι τέτοιο, είναι σχεδόν βέβαιο ότι θα γίνει αντιληπτός από τις μη-κατευθυνόμενες οντότητες. Ουσιαστικά πρόκειται για μια περίπτωση όπου θα πρέπει να ζυγίσει τα δεδομένα ο αντίπαλος και να αποφασίσει, αν αξίζει να πάρει το ρίσκο, υπολογίζοντας τόσο τα κέρδη όσο και τις συνέπειες του να γίνει αντιληπτός (Zhao et al., 2018). Όπως χαρακτηριστικά θεωρείται, πρόκειται για ένα μοντέλο που μπορεί να εφαρμοστεί εύκολα σε πολιτικές καταστάσεις, όχι όμως σε επιχειρήσεις.

Αξίζει να αναφερθεί η άποψη που υποστηρίζει ότι μπορεί να υπάρξει άλλη μία κατηγορία αντιπάλων, αυτή των fail -stop αντιπάλων, οι οποίοι μπορεί να δώσουν εντολή στις κατευθυνόμενες οντότητες να λειτουργήσουν σαν αυτοί να ήταν παθητικοί αντίπαλοι, αλλά μπορεί και να τις διατάξουν να σταματήσουν την επίθεση νωρίτερα (Cohen & Lindell, 2016).

Έχοντας αναφέρει τα παραπάνω είδη αντιπάλων, είναι συνετό να αναφερθεί και η άποψη ότι μπορούν να οριστούν ακόμα δύο είδη αντιπάλων, ανάλογα με τις δυνατότητες που μπορεί εκείνοι να έχουν (Ran Canetti, 2000; Ευστάθιος Ζάχος et al., 2015). Πιο συγκεκριμένα, οι δύο κατηγορίες είναι οι εξής :

- Ο αντίπαλος που έχει απεριόριστη ισχύ, γεγονός που σημαίνει ότι έχει τη δυνατότητα να αντιμετωπίσει οποιαδήποτε κατάσταση του εμφανιστεί και να παραβιάσει οποιοδήποτε επίπεδο ασφαλείας υπάρχει στο πρωτόκολλο SMC. Μάλιστα στη συγκεκριμένη περίπτωση τα κανάλια επικοινωνίας είναι απόλυτα ασφαλή αλλά ο αντίπαλος έχει απεριόριστη υπολογιστική ισχύ (Ran Canetti, 2000). Στην συγκεκριμένη επομένως περίπτωση, ως στόχο ασφάλειας αναφερόμαστε στην πληροφοριοθεωρητική ασφάλεια (information-theoretic security).

- Ο αντίπαλος έχει περιορισμένη ισχύ, γεγονός που σημαίνει ότι δεν έχει τη δυνατότητα να αντιμετωπίσει οποιοδήποτε πρόβλημα του εμφανιστεί, δηλαδή να αντιμετωπίσει οποιαδήποτε κατάσταση και να παραβιάσει οποιοδήποτε επίπεδο ασφαλείας υπάρχει στο πρωτόκολλο SMC. Αυτό ουσιαστικά σημαίνει ότι ο αντίπαλος έχει απεριόριστο πιθανοτικό χρόνο και μπορεί να μάθει οποιαδήποτε πληροφορία σχετικά με την επικοινωνία ανάμεσα στις οντότητες, ακόμα και ολόκληρο το περιεχόμενο της (Ran Canetti, 2000). Στη συγκεκριμένη περίπτωση, ως στόχο ασφάλειας αναφερόμαστε στην υπολογιστική ασφάλεια (computational security).

4.4.2 Στρατηγική Απόκτησης Ελέγχου των Οντοτήτων

Η συγκεκριμένη στρατηγική έχει να κάνει ουσιαστικά με το πότε και το πως ένας αντίπαλος θέτει υπό τον έλεγχο του ορισμένες οντότητες. Υπάρχουν λοιπόν τρία βασικά μοντέλα (Cohen & Lindell, 2016; Lindell, 2020; Ευστάθιος Ζάχος et al., 2015), στα οποία αξίζει να δοθεί μεγαλύτερη έμφαση, και πρόκειται για τα εξής :

- Το *στατικό μοντέλο* (static corruption model). Σύμφωνα με το μοντέλο αυτό το σύνολο των οντοτήτων το οποίο θα ελέγχεται από τον αντίπαλο διαμορφώνεται πριν από την έναρξη του πρωτοκόλλου. Η επίθεση δηλαδή του αντιπάλου με σκοπό την απόκτηση ελέγχου των οντοτήτων γίνεται πριν να ξεκινήσει το πρωτόκολλο. Χαρακτηριστικό του συγκεκριμένου μοντέλου είναι ότι κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου, οι οντότητες δεν αλλάζουν κατάσταση,

δηλαδή οι μη-κατευθυνόμενες παραμένουν μη-κατευθυνόμενες και ομοίως οι κατευθυνόμενες παραμένουν κατευθυνόμενες.

- Το ευπροσάρμοστο μοντέλο (adaptive corruption model). Σύμφωνα με το συγκεκριμένο μοντέλο, ο αντίπαλος, αντί να διαμορφώσει από πριν τις κατευθυνόμενες οντότητες, προχωράει στην απόκτηση ελέγχου οντοτήτων κατά τη διάρκεια εκτέλεσης του υπολογισμού. Έχει τη δυνατότητα ο αντίπαλος να προχωρήσει σε μια τέτοια ενέργεια οποιαδήποτε στιγμή το επιθυμεί, ανάλογα με την δική του οπτική. Ουσιαστικά θα μπορούσε να ειπωθεί ότι το μοντέλο αυτό προσομοιάζει την περίπτωση ενός χάκερ που επιτίθεται σε ένα σύστημα κατά τη διάρκεια της λειτουργίας του (Lindell, 2020). Χαρακτηριστικό αυτού του πρωτοκόλλου είναι ότι μια οντότητα που είναι μη-κατευθυνόμενη μπορεί στη συνέχεια να αλλάξει, αλλά εφόσον γίνει κατευθυνόμενη θα παραμείνει σε αυτή την κατάσταση από εκείνο το σημείο και μετά.

- Το προληπτικό-κινητό μοντέλο (proactive ή mobile corruption model). Σύμφωνα με το μοντέλο αυτό, οι οντότητες μπορούν να παραμένουν κατευθυνόμενες για ένα συγκεκριμένο χρονικό διάστημα. Μάλιστα, οι μη-κατευθυνόμενες οντότητες μπορούν να γίνουν κατευθυνόμενες κατά τη διάρκεια του υπολογισμού και το αντίθετο. Ένα τέτοιο μοντέλο μπορεί να ειπωθεί ότι μπορεί για παράδειγμα να εφαρμοστεί στην περίπτωση που ένας χάκερ αποκτήσει πρόσβαση σε ένα σύστημα ή ένα δίκτυο, ξεκινήσει την επίθεση του και μετά από ένα χρονικό διάστημα τον ανακαλύψουν και χάσει τον έλεγχο των οντοτήτων και κατ' επέκταση του συστήματος (Lindell, 2020). Ένα επιπλέον χαρακτηριστικό αυτού του μοντέλου είναι ότι μπορεί ο αντίπαλος να αντλεί πληροφορίες μόνο από το κομμάτι του συστήματος που έχει θέσει υπό τον έλεγχο του.

4.4.3 Η Σύνθεση ενός Πρωτοκόλλου SMC

Αποτελεί πραγματικότητα το γεγονός ότι ένα πρωτόκολλο ασφαλών υπολογισμών πολλών συμμετεχόντων, όταν βρίσκεται στην φάση του σχεδιασμού του, θα πρέπει να μπορεί να χωριστεί σε πολλά μικρά επιμέρους τμήματα (Ran Canetti, 2000). Μάλιστα ο Canetti παρουσιάζει τρία συγκεκριμένα βήματα για να πραγματοποιηθεί η παραπάνω

σκέψη και ταυτόχρονα να παρέχεται ασφάλεια στην εκτέλεση των υπολογισμών του πρωτοκόλλου. Πιο συγκεκριμένα, πρόκειται για τα εξής τρία βήματα :

- Να πραγματοποιηθεί σχεδιασμός ενός υψηλού επιπέδου πρωτοκόλλου, το οποίο θα μπορεί σε γενικές γραμμές να καλύψει την ασφάλεια τόσο ολόκληρου του υπολογισμού, όσο και των επιμέρους τμημάτων-εργασιών του.

- Να σχεδιαστούν πρωτόκολλα, τα οποία θα μπορέσουν να διασφαλίσουν την ασφαλή εκτέλεση των επιμέρους εργασιών.

- Να κατασκευαστεί ένα πλήρως ανεπτυγμένο και πετυχημένο πρωτόκολλο, το οποίο ουσιαστικά θα συνδυάζει όλα τα επιμέρους πρωτόκολλα, τα οποία θα αποτελούν κομμάτια του πρωτοκόλλου υψηλού επιπέδου που θα αφορά ολόκληρη την εργασία που πρόκειται να γίνει.

Ολόκληρη η παραπάνω διαδικασία ονομάζεται αρθρωτή σύνθεση του πρωτοκόλλου (modular composition). Στο ίδιο μήκος κύματος, υποστηρίζεται η άποψη ότι ένα πρωτόκολλο ασφαλών υπολογισμών πολλών συμμετεχόντων δεν αποτελεί μια αυτόνομη εργασία που λειτουργεί από μόνο του, αλλά αντίθετα αποτελεί κομμάτι ενός συστήματος (Lindell, 2020). Μάλιστα, θεωρεί ότι το πρωτόκολλο το οποίο αποτελεί κομμάτι ενός μεγαλύτερου συστήματος, λειτουργεί ακριβώς με τον ίδιο τρόπο που θα λειτουργούσε εάν μία τρίτη έμπιστη αρχή αναλάμβανε την εκτέλεση του υπολογισμού αντί για τις οντότητες. Με αυτό τον τρόπο ορίζει ο Lindell την σύνθεση των πρωτοκόλλων, υποστηρίζοντας την άποψη του Canetti για την ύπαρξη υπο-πρωτοκόλλων.

Στο πλαίσιο της ύπαρξης ταυτόχρονης εκτέλεσης πολλών πρωτοκόλλων, τίθεται το ερώτημα του κατά πόσο θα πρέπει το SMC πρωτόκολλο να εκτελείται ταυτόχρονα με άλλα πρωτόκολλα και διαδικασίες (Lindell, 2020). Στο άρθρο αυτό υποστηρίζεται η άποψη ότι ακόμα και στην περίπτωση που το πρωτόκολλο αποτελεί υπο-πρωτόκολλο ενός άλλου πρωτοκόλλου, θα πρέπει να εκτελείται αυτόνομα και οποιεσδήποτε εργασίες και μηνύματα να στέλνονται και να εκτελούνται πριν ή μετά την εκτέλεση του. Στην περίπτωση που ένα πρωτόκολλο θεωρηθεί ασφαλές, τότε δεν σημαίνει ότι θα διατηρήσει

αυτή την κατάσταση στην περίπτωση της ταυτόχρονης εκτέλεσης του με άλλα πρωτόκολλα. Για το λόγο αυτό, θα πρέπει το πρωτόκολλο να λειτουργεί σύμφωνα με τον ορισμό του “universal composability” (R. Canetti, 2001) για να θεωρηθεί ασφαλές, δεδομένου ότι αυτός ο ορισμός εφόσον ικανοποιείται, ουσιαστικά παρέχει την εγγύηση ότι το πρωτόκολλο θα λειτουργεί σαν να βρίσκεται στον ιδεατό κόσμο, έχοντας καλύψει τα θέματα ασφαλείας, χωρίς να επηρεάζεται από την ταυτόχρονη λειτουργία άλλων πρωτοκόλλων.

4.5 Ζητήματα που Προκύπτουν από τον Ορισμό

Έχοντας προχωρήσει στην παραπάνω ανάλυση των στοιχείων που έχουν να κάνουν με τον ορισμό της ασφάλειας ενός SMC πρωτοκόλλου, θα πρέπει να γίνει μια αναφορά σε ορισμένα θέματα που προκύπτουν, με σκοπό αυτά να ξεκαθαριστούν.

4.5.1 Το Ιδεατό Μοντέλο και η Χρήση των SMC Πρωτοκόλλων στην Πράξη

Στην υποενότητα 4.3.2 έγινε αναφορά στην ασφάλεια των SMC πρωτοκόλλων βασισμένη στις έννοιες του ιδεατού και του φανταστικού κόσμου. Πρέπει όμως να αναφερθούν και μερικές σημαντικές πτυχές αυτού του παραδείγματος. Πιο συγκεκριμένα, προτού ληφθεί η απόφαση για τη χρήση ενός πρωτοκόλλου κάτω από αυτές τις συνθήκες, θα πρέπει αυτός που σχεδιάζει την ασφάλεια του πρωτοκόλλου να σκεφτεί τον τρόπο με το οποίο η ασφάλεια του συστήματος θα παραμένει στα υψηλότερα επίπεδα, όπως στην περίπτωση που μια τρίτη, έμπιστη και ανεξάρτητη αρχή αναλαμβάνει την εκτέλεση των υπολογισμών (Lindell, 2020). Αυτό σημαίνει ότι δεν απαιτείται να γίνει ενδελεχής κατανόηση του τρόπου με τον οποίο λειτουργεί το πρωτόκολλο αυτό ή γενικά τα πρωτόκολλα, ή ακόμα και να υπάρξει εξειδίκευση πάνω σε θέματα που έχουν να κάνουν με το πως ορίζεται η ασφάλεια. Εφ’όσον το σύστημα παραμένει ασφαλές στην συγκεκριμένη περίπτωση, θα μπορεί να είναι ασφαλές και στον πραγματικό κόσμο καθώς επίσης και στις περισσότερες περιπτώσεις χρησιμοποίησης του SMC πρωτοκόλλου. Η κατανόηση λοιπόν αυτής της περίπτωσης παρέχει τη δυνατότητα για κατανόηση όλως των υπόλοιπων τμημάτων του συστήματος, του πρωτοκόλλου και της ασφάλειας που αυτό παρέχει.

4.5.2 Επιτρεπόμενοι Είσοδοι

Όπως αναφέρθηκε και στην προηγούμενη ενότητα, το ιδεατό μοντέλο μπορεί να παρέχει αρκετά υψηλά επίπεδα ασφάλειας. Ένα SMC πρωτόκολλο παρέχει τη δυνατότητα για μια εκτέλεση του ιδεατού κόσμου στην πράξη. Παρ' όλα αυτά, πρέπει να γίνει μια αναφορά στο γεγονός ότι οι αντίπαλοι μπορούν να δώσουν στη συνάρτηση υπολογισμού οποιαδήποτε είσοδο επιθυμούν, χωρίς να υπάρχει κάποιος ιδιαίτερος τρόπος να περιοριστεί αυτό. Χαρακτηριστικό είναι το παράδειγμα σύμφωνα με το οποίο, δύο οντότητες προσπαθούν να μάθουν ποια από τις δύο λαμβάνει το μεγαλύτερο μισθό (Lindell, 2020). Στο συγκεκριμένο παράδειγμα, δεν μπορεί κανείς να αποκλείσει το γεγονός να δώσει κάποιος από τους δύο την μεγαλύτερη δυνατή τιμή σαν τον μισθό του, και στη συνέχεια να πάρει σαν έξοδο ότι παίρνει τον μεγαλύτερο μισθό. Για το λόγο αυτό, υποστηρίζεται η άποψη πως αν η ασφάλεια της εφαρμογής εξαρτάται από την παροχή σωστών εισόδων από τις οντότητες, τότε μπορούν να χρησιμοποιηθούν μηχανισμοί, όπως για παράδειγμα να απαιτείται η χρησιμοποίηση υπογεγραμμένων εισόδων, που η πιστοποίηση της γνησιότητάς τους θα αποτελεί κομμάτι του υπολογισμού SMC (Lindell, 2020). Αξίζει να αναφερθεί ότι δεν πρόκειται όμως για κάτι εύκολα υλοποιήσιμο, καθώς το κόστος για την δημιουργία τέτοιου είδους μηχανισμών, για την ένταξη τους ως κομμάτι του υπολογισμού και για την εφαρμογή τους είναι αρκετά μεγάλο και πολύ δύσκολο να γίνει ανεκτό.

4.5.3 Ασφάλεια της Διαδικασίας και των Εξόδων

Μία ακόμα περίπτωση πάνω στην οποία υπάρχουν πολλές παρεξηγήσεις που πρέπει να λυθούν, είναι το γεγονός ότι τα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων μπορούν να παρέχουν ασφάλεια στη διαδικασία υπολογισμού, γεγονός που σημαίνει ότι δεν θα γίνει γνωστό οποιοδήποτε στοιχείο – πληροφορία από τον υπολογισμό αυτόν καθ' αυτόν (Lindell, 2020). Από την άλλη μεριά όμως, δεν μπορεί κανείς να ισχυριστεί με μεγάλη σιγουριά ότι οι έξοδοι που θα προκύψουν από τη συνάρτηση υπολογισμού δεν θα αποκαλύψουν κάποια ευαίσθητη πληροφορία. Χαρακτηριστικό είναι το παράδειγμα που μπορεί να εξηγήσει τον παραπάνω ισχυρισμό, το οποίο έχει να κάνει με δύο οντότητες που επιθυμούν να υπολογίσουν τον μέσο όρο των μισθών τους (Lindell, 2020). Η έξοδος του υπολογισμού αυτού θα είναι ο μέσος όρος.

Μία οντότητα όμως μπορεί να χρησιμοποιήσει τον μέσο όρο και τον δικό της μισθό για να ανακαλύψει τον μισθό της άλλης οντότητας, χρησιμοποιώντας απλούς μαθηματικούς υπολογισμούς. Από το παράδειγμα αυτό προκύπτει το συμπέρασμα ότι το γεγονός της χρησιμοποίησης SMC πρωτοκόλλων δεν συνεπάγεται απαραίτητα την επίλυση όλων των θεμάτων προστασίας δεδομένων και των πιθανών κενών που μπορεί να υπάρχουν. Αντίθετα, τα SMC πρωτόκολλα μπορούν να ασφαλίσουν μόνο την διαδικασία του υπολογισμού με απόλυτη σιγουριά. Επομένως, προκύπτει το ερώτημα ποιες είναι οι συναρτήσεις που μπορούν να επιλύσουν τέτοιου είδους ζητήματα που μπορεί να προκύψουν, η απάντηση του οποίου δεν είναι ξεκάθαρη, καθώς εξαρτάται και από τις τεχνικές που χρησιμοποιούνται (Lindell, 2020).

4.6 Εφαρμοσιμότητα των SMC Πρωτοκόλλων

Στην προηγούμενη ενότητα, όπου παρουσιάστηκε ο ορισμός της ασφάλειας των SMC πρωτοκόλλων, αναφέρθηκε το γεγονός ότι ένα πρωτόκολλο μπορεί να θεωρηθεί ότι είναι ασφαλές, θα πρέπει να παρουσιάζει στον πραγματικό κόσμο, τα ίδια επίπεδα ασφαλείας με τον ιδεατό κόσμο. Αυτό ουσιαστικά σημαίνει ότι δεν θα πρέπει στον πραγματικό κόσμο να έχει τη δυνατότητα ο αντίπαλος να πραγματοποιήσει επιτυχημένη επίθεση. Θα πρέπει δηλαδή να μπορεί το πρωτόκολλο να παρέχει επίπεδα ασφαλείας, ανάλογα με αυτά του ιδεατού κόσμου, και να μπορεί να λειτουργεί με τον ίδιο τρόπο όπως στον ιδεατό κόσμο, σαν να υπάρχει δηλαδή μία τρίτη έμπιστη οντότητα η οποία εκτελεί τον υπολογισμό. Πάνω σε αυτό, έχει διατυπωθεί το ερώτημα του κατά πόσο είναι εφικτό να υπάρξουν πρωτόκολλα που να ικανοποιούν τη παραπάνω θέση ως προς την ασφάλεια τους (Lindell, 2020). Υποστηρίζει ότι μπορεί να υπάρξει πρακτική εφαρμογή της ιδέας αυτής σε οποιοδήποτε κατανεμημένο σύστημα, με σκοπό να ασφαλιστεί σε μεγάλο βαθμό η διαδικασία υπολογισμού που χρησιμοποιούν. Όπως αναφέρεται χαρακτηριστικά στη βιβλιογραφία, μπορούν να υπάρξουν τρεις περιπτώσεις σύμφωνα με τις οποίες μπορεί να επιτευχθεί ένα ασφαλές πρωτόκολλο (Lindell, 2020; Ευστάθιος Ζάχος et al., 2015). Για χάρη ευκολίας θα χρησιμοποιηθούν οι εξής συμβολισμοί, όπου με n συμβολίζεται ο αριθμός όλων των οντοτήτων και t ο αριθμός των οντοτήτων που μπορεί να μετατραπούν σε κατευθυνόμενες. Οι τρεις λοιπόν περιπτώσεις είναι οι εξής :

- Στην περίπτωση που t< n/3, δηλαδή όταν ο αριθμός των οντοτήτων που μπορούν να τεθούν υπό τον έλεγχο ενός αντιπάλου είναι μικρότερος από το ένα τρίτο του συνολικού αριθμού των οντοτήτων, μπορούν να δημιουργηθούν και να εφαρμοστούν πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων, τα οποία θα ικανοποιούν τόσο την ιδιότητα της δικαιοσύνης, όσο και αυτή της εγγυημένης παράδοσης των εξόδων. Μάλιστα, θα μπορεί με αυτό τον τρόπο να επιτευχθεί ο ισχυρότερος τύπος ασφάλειας ενός πρωτοκόλλου που μπορεί να πετύχει κάποιος (Ishai et al., 2006). Εάν ισχύει η συγκεκριμένη περίπτωση,τότε θα μπορέσει αυτή να επιτευχθεί με τη χρησιμοποίηση είτε ενός ασύγχρονου από σημείο σε σημείο δικτύου με κανάλια που χρησιμοποιούν αυθεντικοποίηση, είτε με ιδιωτικά κανάλια που παρέχουν πληροφοριοθεωρητική ασφάλεια (Cohen & Lindell, 2016; Lindell, 2020).

- Στην περίπτωση που t< n/2, δηλαδή όταν ο αριθμός των οντοτήτων που μπορούν να τεθούν υπό τον έλεγχο ενός αντιπάλου είναι μικρότερος από το μισό του συνολικού αριθμού των οντοτήτων και έχουμε δηλαδή πλειοψηφία μη-κατευθυνόμενων οντοτήτων, μπορούν να δημιουργηθούν και να εφαρμοστούν πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων, τα οποία θα ικανοποιούν τις ιδιότητες της δικαιοσύνης και της εγγυημένης παράδοσης των εξόδων, και θα έχουν ισχύ για οποιαδήποτε συνάρτηση μπορεί να παρέχει πληροφοριοθεωρητική ασφάλεια, χρησιμοποιώντας ακόμα και κανάλια μετάδοσης.

- Στην περίπτωση που t≥ n/2, δηλαδή όταν ο αριθμός των οντοτήτων που μπορούν να τεθούν υπό τον έλεγχο ενός αντιπάλου είναι μεγαλύτερος ή ίσος από το μισό του συνολικού αριθμού των οντοτήτων, και άρα όχι περιορισμένος, μπορούν και πάλι να επιτευχθούν πρωτόκολλα SMC, τα οποία όμως δεν θα ικανοποιούν τις ιδιότητες της δικαιοσύνης και της εγγυημένης παράδοσης των εξόδων.

- Στην περίπτωση που t< n, για οποιαδήποτε τιμή του t, στη βιβλιογραφία αναφέρεται ότι μπορεί να επιτευχθεί υπολογιστική ασφάλεια, σύμφωνα με την οποία μπορεί να υπάρχει ανιχνεύσιμη μετάδοση, όπου είτε όλες οι οντότητες ματαιώνουν τη διαδικασία και δεν λαμβάνουν καθόλου εξόδους, είτε όλες

λαμβάνουν και αποδέχονται την τιμή της μετάδοσης (Cohen & Lindell, 2016; Lindell, 2020; Ευστάθιος Ζάχος et al., 2015). Πρόκειται λοιπόν για μια περίπτωση που ικανοποιεί την ιδιότητα της δικαιοσύνης, όχι όμως της εγγυημένης παράδοσης των εξόδων.

Κεφάλαιο 5

Τεχνικές SMC

Στο συγκεκριμένο κεφάλαιο θα γίνει μία προσπάθεια να παρουσιαστούν οι σημαντικότερες τεχνικές που χρησιμοποιούν τα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων. Ασφαλώς δεν θα μπορέσουν να παρουσιαστούν όλες οι τεχνικές, καθώς υπάρχει μία ευρεία συλλογή από αυτές, ανάλογα με τις απαιτήσεις που

υπάρχουν και με τις εφαρμογές στις οποίες θα εφαρμοστούν. Το γεγονός αυτό καθιστά αδύνατη την εξ' ολοκλήρου παρουσίασή τους. Παρ' όλα αυτά, δεδομένου ότι πρόκειται για βασικό τμήμα της παρούσας διατριβής, θα επιχειρηθεί μια προσπάθεια να παρουσιαστούν οι βασικότερες και δημοφιλέστερες από αυτές, προκειμένου να δημιουργηθεί μία σαφή εικόνα για τον τρόπο με τον οποίο λειτουργούν. Ταυτόχρονα θα επιχειρηθεί μία αποτίμηση αυτών των πρωτοκόλλων, σε σχέση με τις λύσεις που μπορούν να παρέχουν, σε θέματα σχετικά με τις απαιτήσεις της νομοθεσίας και τα προβλήματα που υπάρχουν σχετικά με την προστασία των προσωπικών δεδομένων. Τέλος, θα γίνει και μια κατηγοριοποίηση των επιμέρους κατηγοριών που προκύπτουν σε κάθε περίπτωση τεχνικής.

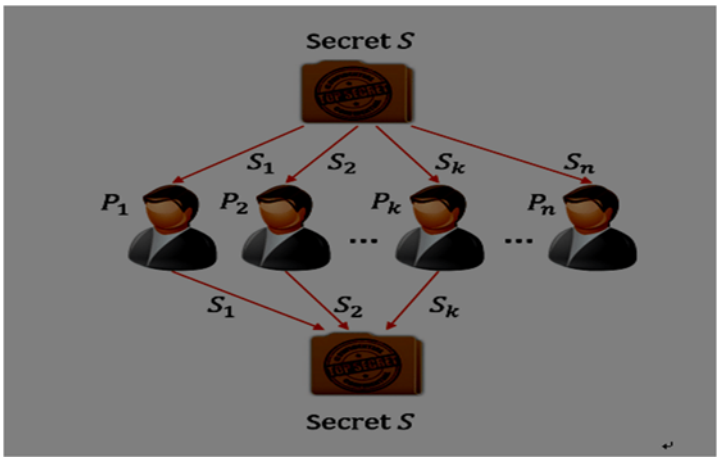
5.1 Η Τεχνική Διαμοιρασμού Μυστικού του Shamir (Shamir Secret Sharing)

Πρόκειται για μία από τις πρώτες τεχνικές που αναπτύχθηκαν, η οποία εντάσσεται στην κατηγορία των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων. Τα πρωτόκολλα SMC τα οποία εφαρμόζονται σε περιβάλλον, στο οποίο η πλειοψηφία των οντοτήτων είναι μη-κατευθυνόμενες, χρησιμοποιούν σαν βασικό τους εργαλείο την συγκεκριμένη τεχνική.

Η παρούσα τεχνική έρχεται να λύσει το πρόβλημα, σύμφωνα με το οποίο ένα μυστικό πρέπει να μοιραστεί ανάμεσα σε πολλές πλευρές. Πιο συγκεκριμένα, έστω ότι υπάρχουν τα δεδομένα D, τα οποία είναι κάποια ευαίσθητα δεδομένα ή πληροφορίες. Ο σκοπός της χρήσης της συγκεκριμένης τεχνικής είναι να χωριστούν τα δεδομένα D σε n τμήματα, D_1, D_2, …. , D_n , κατά τέτοιο τρόπο ώστε να ικανοποιούνται οι εξής δύο ιδιότητες :

- Σε περίπτωση που οι οντότητες γνωρίζουν k ή περισσότερα κομμάτια D_i από τα δεδομένα, να μπορούν να υπολογίσουν εύκολα τα δεδομένα D. Με άλλα λόγια, σε περίπτωση που θέλουν οι k ή περισσότερες οντότητες, έχουν τη δυνατότητα να ανακατασκευάσουν τα αρχικά δεδομένα, δεδομένου ότι η κάθε οντότητα γνωρίζει ένα τμήμα D_i από αυτά.

- Σε περίπτωση που οι οντότητες γνωρίζουν λιγότερα από k κομμάτια D_i από τα δεδομένα, τότε δεν θα μπορούν να υπολογίσουν τα αρχικά δεδομένα D. Δηλαδή, σε περίπτωση που θέλουν λιγότερες από k οντότητες, δεν θα έχουν τη δυνατότητα να ανακατασκευάσουν τα αρχικά δεδομένα. Επομένως δεν θα μπορούν να μάθουν καμία πληροφορία σχετικά με το μυστικό που είναι τα δεδομένα D.



Σε περίπτωση που ισχύουν οι δύο παραπάνω ιδιότητες, τότε σχηματίζεται το (k,n)-σχήμα-κατωφλίου ((k,n)-threshold-sheme ή αλλιώς το (k+1)-από n-threshold secret-sharing scheme). (Lindell, 2020; Shamir, 1979)

Η συγκεκριμένη τεχνική λειτουργεί με τον εξής τρόπο. Δεδομένης της υπόθεσης ότι υπάρχουν k σημεία στον δισδιάστατο χώρο, τα (x_1,y_1), (x_2,y_2),…. , (x_k,y_k) , υπάρχει ένα και μόνο ένα πολυώνυμο q(x), το οποίο έχει βαθμό k-1, τέτοιο ώστε να ισχύει ότι $q(x_i)=y_i$ για οποιοδήποτε i.

Εάν γίνει η υπόθεση ότι τα δεδομένα που θέλουμε να προστατεύσουμε είναι κάποιος αριθμός, και χρειάζεται να χωριστεί σε D_i τμήματα, τότε θα πρέπει να επιλεχθεί ένα τυχαίο πολυώνυμο $q(x)=a_0 + a_1x +\ldots\ldots + a_{k-1}x^{k-1}$,βαθμού k-1, τέτοιο ώστε να ισχύει ότι $a_0=D$, και να μπορούν επομένως να υπολογιστούν τα $D_1=q(1)$,….. , $D_n=q(n)$. Προκειμένου να πραγματοποιηθεί η ανακατασκευή του πολυωνύμου, μπορούν να χρησιμοποιηθούν

τα πολυώνυμα Lagrange $l_1(x)$, $l_2(x)$, … , $l_k(x)$, τα οποία θα χρησιμοποιηθούν για την ανακατασκευή, μέσω του υπολογισμού του $q(x)=\Sigma_{i=1}^{t+1} l_i(x) * y_i$. Εάν γίνουν γνωστά ένα υποσύνολο k των D_i, τότε μπορούν να βρεθούν οι συντελεστές του πολυωνύμου, με τη χρήση της διαδικασίας που ονομάζεται παρεμβολή (interpolation) και στη συνέχεια να υπολογιστεί το D, για το οποίο θα ισχύει ότι $D=q(0)$. Εάν είναι γνωστά έστω και k-1 από αυτά, τότε δεν θα μπορεί να προχωρήσει ο υπολογισμός του D.

Για να γίνει πιο κατανοητή αλλά και πιο εύκολη η προηγούμενη διαδικασία, χρησιμοποιείται η modulo αριθμητική, δηλαδή όλοι οι υπολογισμοί γίνονται στο σύνολο Z_P . Αν γίνει η υπόθεση ότι το D είναι ένας ακέραιος αριθμός, τότε θα πρέπει να επιλεχθεί ένας πρώτος αριθμός p, ο οποίος να είναι μεγαλύτερος τόσο από το D, όσο και από το n. Στη συνέχεια, οι συντελεστές του πολυωνύμου q(x), θα υπολογιστούν με μία απλή τυχαία κατανομή των ακεραίων στο σύνολο [0,p). Επομένως οι τιμές D_1, D_2, …. , D_n , θα υπολογιστούν με τη χρήση της πράξης modulo p. Έτσι θα κατασκευαστεί το πολυώνυμο q(x). Τότε για κάθε i =1,2,…., n , θα μπορεί να υπολογιστεί το $y_i=q(i)$.

Αν από την άλλη μεριά γίνει η υπόθεση ότι ο αντίπαλος μπορεί να γνωρίζει τα k-1 ή λιγότερα από τα τμήματα των αρχικών δεδομένων D, δεν θα μπορέσει να ανακτήσει ολόκληρα τα δεδομένα. Πιο συγκεκριμένα, για κάθε υποψήφια τιμή D’ που θα θεωρεί ότι είναι ίση με τα δεδομένα D, θα μπορεί να κατασκευάσει ένα και μόνο πολυώνυμο q’(x), βαθμού k-1, για το οποίο να ισχύει ότι $q(0)=D'$, και $q(i)=D_i$, για κ-1 περιπτώσεις. Με αυτό τον τρόπο, θα προκύπτουν πολλά πιθανά πολυώνυμα, χωρίς όμως να μπορεί να καταλήξει στο σωστό, γεγονός που καθιστά αδύνατη την εύρεση των δεδομένων D.

Μια σημαντική προϋπόθεση για να μπορεί να εφαρμοστεί η τεχνική του Shamir είναι ότι θα πρέπει όλες οι οντότητες να είναι τίμιες, γεγονός που δεν ισχύει πάντοτε (Ευστάθιος Ζάχος et al., 2015). Για παράδειγμα :

- Ο διανομέας μπορεί να προχωρήσει σε λανθασμένη διανομή των κομματιών D_i στις οντότητες, δηλαδή σε παράδοση λάθος τμημάτων, εκούσια ή ακούσια, γεγονός που μπορεί να προκαλέσει προβλήματα στην μετέπειτα εφαρμογή της τεχνικής και τελικά στην ανακατασκευή των συνολικών δεδομένων D. Για το λόγο

αυτό θα πρέπει να μπορούν οι οντότητες-παραλήπτες να επαληθεύουν με κάποιο τρόπο ότι έχουν λάβει τα σωστά τμήματα D_i .

- Κατά τη διάρκεια της ανακατασκευής, μπορεί να υπάρξουν οντότητες που να μην παρέχουν τα σωστά κομμάτια D_i που έλαβαν από τον διανομέα, είτε λόγω λάθους απροσεξίας είτε γιατί μπορεί να λειτουργούν απρόσεκτα. Για το λόγο αυτό θα πρέπει να υπάρχει ένας μηχανισμός ελέγχου της αυθεντικότητας των κομματιών D_i που στέλνουν οι οντότητες, ο οποίος να εφαρμόζεται πριν την έναρξη της διαδικασίας ανακατασκευής.

Μερικές σημαντικές ιδιότητες της συγκεκριμένης τεχνικής είναι οι εξής (Shamir, 1979):

- Το μέγεθος του κάθε τμήματος D_i δεν μπορεί να υπερβαίνει το μέγεθος των δεδομένων D.

- Όταν το k παραμείνει σταθερό, τότε μπορούν να προστεθούν ή να αφαιρεθούν κομμάτια D_i , χωρίς να επηρεάζονται τα υπόλοιπα.

- Υπάρχει η δυνατότητα αλλαγής των τμημάτων, χωρίς να αλλαχθούν τα δεδομένα D. Αυτό μπορεί να επιτευχθεί με τη χρήση ενός διαφορετικού πολυωνύμου q(x), γεγονός όμως που θα προκαλέσει προβλήματα στην ασφάλεια.

- Μπορεί να χρησιμοποιηθούν πλειάδες (tuples) τιμών του πολυωνύμου του D_i ,με αποτέλεσμα η τεχνική να χρησιμοποιηθεί με τέτοιο τρόπο ώστε ο αριθμός των κομματιών D_i που απαιτείται για να ανακαλυφθεί το D, να καθορίζεται από τη σημαντικότητα τους.

Ανάλογα με τη σχέση που υπάρχει ανάμεσα στα n και k, μπορεί να υπάρξουν δύο διαφορετικές κατηγορίες της τεχνικής secret sharing, η μία που περιλαμβάνει οντότητες στην πλειοψηφία τους κατευθυνόμενες και άλλη το αντίθετο (Bayatbabolghani & Blanton, 2018). Ανάλογα με την κατηγορία, θα προκύψουν και διαφορετικές περιπτώσεις threshold scheme. Για παράδειγμα, στην περίπτωση που η πλειοψηφία των οντοτήτων

είναι κατευθυνόμενες, είναι συνηθισμένο να ισχύει k< n/3 για το μοντέλο με παθητικούς αντιπάλους και k< n/2 για το μοντέλο με τους κακόβουλους αντιπάλους.

5.2 Η τεχνική της Μη-Συνειδητής Μεταφοράς (Oblivious Transfer)

Η κατηγορία πρωτοκόλλων Oblivious Transfer (OT), αναφέρεται στην περίπτωση όπου ένας αποστολέας S, θέλει να στείλει το μήνυμα του M σε έναν αποδέκτη R, χωρίς να γνωρίζει αν και κατά πόσο θα το παραλάβει ο αποστολέας. Η χρησιμοποίηση του πρωτοκόλλου αυτού, συνεπάγεται και την απαίτηση για ικανοποίηση των εξής τριών ιδιοτήτων – αξιωμάτων (Even et al., 1982) :

- Στην περίπτωση που ο αποστολέας εκτελέσει σωστά το πρωτόκολλο αυτό, τότε ο αποδέκτης θα παραλάβει και θα διαβάσει το μήνυμα με πιθανότητα ½. Σε περίπτωση που ο αποδέκτης δεν διαβάσει το μήνυμα, τότε από την εκτέλεση του πρωτοκόλλου δεν θα λάβει καμία επιπλέον πληροφορία.

- Η πιθανότητα a-posteriori, δηλαδή η εκ των υστέρων πιθανότητα να διαβάσει ο αποδέκτης το μήνυμα μετά την εκτέλεση του πρωτοκόλλου παραμένει ½, δεδομένου πάντα ότι ο αποστολέας εκτέλεσε σωστά το πρωτόκολλο.

- Σε περίπτωση που ο αποστολέας προσπαθήσει να παρακάμψει το πρωτόκολλο, προκειμένου να ελαχιστοποιήσει την πιθανότητα ο αποδέκτης να παραλάβει το μήνυμα, τότε η προσπάθεια μπορεί πολύ εύκολα να ανιχνευτεί.

Προκειμένου να γίνει πιο κατανοητή η λειτουργία του πρωτοκόλλου αυτού, θα γίνει μια παρουσίαση του τρόπου με τον οποίο λειτουργεί, όπως την εισήγαγε ο Rabin, μέχρι να γενικευτεί στη συνέχεια και στις υπόλοιπες υπο-περιπτώσεις (Bhushan Sonawane; Rabin, 1981):

- Ο αποστολέας επιλέγει δύο μεγάλους πρώτους αριθμούς p και q, τέτοιους ώστε να ισχύει ότι N=p*q. Επιπλέον, επιλέγει έναν αριθμό e, τέτοιον ώστε να είναι πρώτος με το γινόμενο (p-1)*(q-1).

- Ο αποστολέας στέλνει στον παραλήπτη τους αριθμούς N, e, καθώς και το M^emodN, όπου M είναι το μήνυμα. Πρέπει να σημειωθεί ότι, για να μπορέσει στο σημείο αυτό ο παραλήπτης να ανακαλύψει το M, πρέπει να γνωρίζει τους πρώτους παράγοντες p και q του N – κάτι που δεν είναι εφικτό όταν το N είναι της τάξης των 2048 ψηφίων (σε αυτήν την ιδιότητα στηρίζει την ασφάλειά του ο γνωστός κρυπτογραφικός αλγόριθμος RSA).

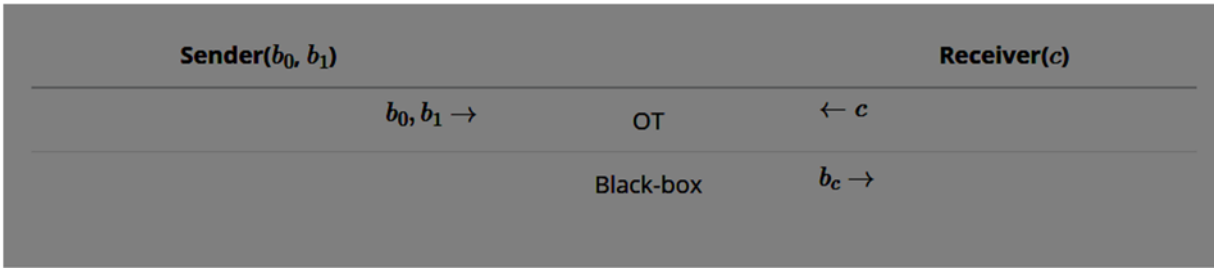
- Ο παραλήπτης επιλέγει έναν τυχαίο αριθμό x στο σύνολο [1, N-1] και στέλνει πίσω στον αποστολέα το x^2modN.

- Ο αποστολέας υπολογίζει τις τετραγωνικές ρίζες του x^2modN, επιλέγει μία από αυτές τυχαία, την y, και στην στέλνει στον παραλήπτη.

- Εφόσον ο παραλήπτης λάβει το y και αυτό είναι ίσο με x ή το -x modulo N, τότε μπορεί να παραγοντοποιήσει το N (μέσω μίας γνωστής μαθηματικής διαδικασίας που ονομάζεται Chinese Remainder Theorem η οποία όμως δεν θα μας απασχολήσει εδώ) και άρα να αποκρυπτογραφήσει το M^e και να παραλάβει το μήνυμα M. Άλλη παρόμοια διαδικασία είναι ο παραλήπτης, εφόσον λάβει το y, να υπολογίσει τον gcd(x+y,N) και να πάρει το p. Αν πάλι λάβει το N-y, μπορεί να υπολογίσει το q. Σε περίπτωση που δεν παραλάβει κάτι από αυτά, τότε ο παραλήπτης δεν μπορεί να λάβει το μήνυμα του αποστολέα.

Έχοντας σαν βάση το πρωτόκολλο Oblivious Transfer, προέκυψε μία υπο-περίπτωση του πρωτοκόλλου αυτού, γνωστό και ως 1-out-of-2-Oblivious Transfer (OT_1^2) (Even et al., 1982; Ευστάθιος Ζάχος et al., 2015). Σύμφωνα με αυτή, ο αποστολέας μεταφέρει, έχοντας πλήρη άγνοια, ένα μήνυμα, το οποίο μήνυμα ο παραλήπτης το επιλέγει ανάμεσα σε δύο μυστικά μηνύματα, με πιθανότητα ½. Πιο συγκεκριμένα, αν θεωρηθεί ότι το πρωτόκολλο OT είναι ένα black box, τότε από το παρακάτω σχήμα μπορεί να γίνει πιο εύκολα

αντιληπτό πως παράγονται οι είσοδοι και οι έξοδοι, στην πιο απλή περίπτωση χρήσης του πρωτοκόλλου OT:



Σχήμα 4: Λειτουργία πρωτοκόλλου OT_1^2

Πηγή: " https://www.esat.kuleuven.be/cosic/blog/co6gc-introduction-to-oblivious-transfer/ ", (Kelong Cong, 2020b)

Από το παραπάνω σχήμα, προκύπτει ότι στην περίπτωση που ο αποστολέας δώσει σαν είσοδο δύο bit, b_0 και b_1, και ο αποδέκτης ένα bit, το c, τότε ο αποδέκτης θα πάρει σαν έξοδο το b_c. Αυτό σημαίνει ότι αν το c=0, θα λάβει το b_0, ενώ αν το c=1 θα λάβει το b_1 (Kelong Cong, 2020b). Ο αποστολέας δεν γνωρίζει ποιο από τα δύο bits τελικά έλαβε ο παραλήπτης.

Αξίζει να τονιστεί το γεγονός ότι η συγκεκριμένη τεχνική μπορεί να είναι ασφαλής, μόνο στην περίπτωση που ισχύει η προϋπόθεση ότι ο αποστολέας δεν θα μάθει ποτέ το bit c του αποδέκτη, καθώς και ότι ο αποδέκτης δεν θα μάθει ποτέ το bit b_{1-c} που δεν επέλεξε.

Το πρωτόκολλο OT ικανοποιεί τα τρία ανάλογα αξιώματα με αυτά αναφέρθηκαν προηγουμένως (Even et al., 1982):

- Στην περίπτωση που ο αποστολέας εκτελέσει σωστά το πρωτόκολλο αυτό, τότε ο αποδέκτης θα παραλάβει και θα διαβάσει ένα ακριβώς μήνυμα από τα δύο με πιθανότητα ½ για το κάθε ένα. Σε περίπτωση που ο αποδέκτης δεν διαβάσει κανένα από τα δύο μηνύματα, τότε από την εκτέλεση του πρωτοκόλλου δεν θα λάβει καμία επιπλέον πληροφορία.

- Η πιθανότητα a-posteriori, δηλαδή η εκ των υστέρων πιθανότητα να διαβάσει ο αποδέκτης το ένα από τα δύο μηνύματα μετά την εκτέλεση του πρωτοκόλλου

παραμένει ½, δεδομένου πάντα ότι ο αποστολέας εκτέλεσε σωστά το πρωτόκολλο.

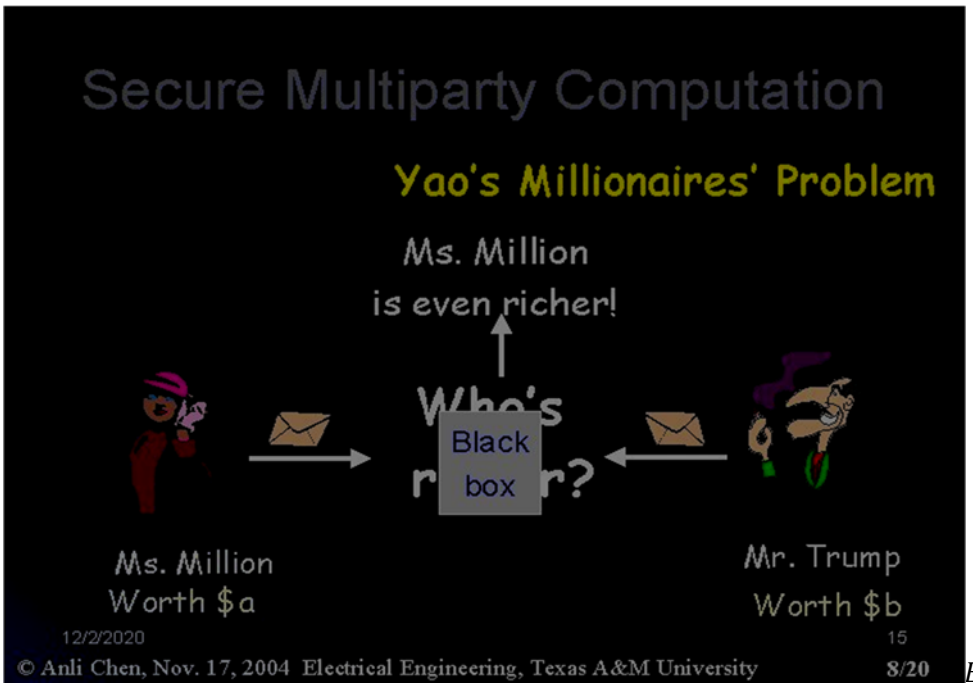
- Σε περίπτωση που ο αποστολέας προσπαθήσει να παρακάμψει το πρωτόκολλο, προκειμένου να μεγιστοποιήσει την πιθανότητα ο αποδέκτης να προβλέψει ποιο από τα δύο μηνύματα θα επιλέξει να διαβάσει ο αποδέκτης, τότε η προσπάθεια μπορεί πολύ εύκολα να ανιχνευτεί.

Λαμβάνοντας υπόψη τα δύο αυτά πρωτόκολλα, το OT και το OT_1^2, αποδείχθηκε ότι εφόσον μπορεί το ένα πρωτόκολλο να ισχύει, τότε θα μπορεί να ισχύει και το άλλο. (Crépeau, 1995; Even et al., 1982) Μάλιστα, μπορεί να προκύψει και η γενική περίπτωση 1-out-of-n Oblivious Transfer, όπου ο παραλήπτης επιλέγει να μάθει το i-οστό από τα n μηνύματα, καθώς και η ακόμα πιο γενική περίπτωση k-out-of-n-Oblivious Transfer. (Even et al., 1982; Guo et al., 2013; Ευστάθιος Ζάχος et al., 2015)

Η τεχνική Oblivious Transfer μπορεί να χρησιμοποιηθεί σαν διεργασία και σε άλλα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση του πρωτοκόλλου Garbed Circuits, όπου εκεί η τεχνική OT μπορεί να χρησιμοποιηθεί για την αποστολή της εισόδου από την πρώτη οντότητα που ανακατεύει τον κύκλο υπολογισμών στην δεύτερη συμμετέχουσα οντότητα. (Kelong Cong, 2020b)

5.3 Το Πρωτόκολλο των Εκατομμυριούχων

Πρόκειται για μια ειδική περίπτωση τεχνικής, που διαφορετικά είναι γνωστή και ως το πρωτόκολλο της μυστικής σύγκρισης. Είναι ένα πρωτόκολλο, που όπως αναφέρθηκε και προηγουμένως, εισήχθηκε σαν ιδέα από τον Yao (Yao, 1982). Ο βασικός στόχος χρήσης του, όπως είναι εύκολα κατανοητό, είναι για να γίνει σύγκριση ανάμεσα σε δύο διαφορετικά μεγέθη. Χαρακτηριστικό είναι το παράδειγμα που αναφέρθηκε προηγουμένως, όπου δύο εκατομμυριούχοι επιθυμούν να ανακαλύψουν ποιος από τους δύο είναι πλουσιότερος, χωρίς να θέλει όμως ο ένας να μάθει άλλος περισσότερες λεπτομέρειες για την περιουσία του.



Εικόνα 1: Yao's Millionaires Problem,

Πηγή " https://slidetodoc.com/a-secure-multiparty-computation-scheme-for-privacypreserving-association/" ,(Anli Chen, 2004)

Το συγκεκριμένο πρωτόκολλο θα μπορούσε να λειτουργήσει και με τον εξής τρόπο (Guo et al., 2013). Έστω ότι υπάρχουν οι συμμετέχοντες Α και Β, οι οποίοι δίνουν σαν είσοδο τους μυστικούς αριθμούς i και j. Τότε οι δύο χρήστες χρησιμοποιούν ξεχωριστά ο καθένας, την συνάρτηση GT=(i , j)=[i>j], όπου η GT ονομάζεται έτσι από το “Greater Than problem”. Η συγκεκριμένη συνάρτηση, αποτελεί αποτέλεσμα χρήσης τεχνικών όπως η Μη-Συνειδητή Μεταφορά (OT) ή η ομομορφική κρυπτογράφηση. Αν GT=(i , j)=1, τότε i>j, ενώ αν GT=(i , j)=0, τότε i≤j.

Το πρωτόκολλο των εκατομμυριούχων μπορεί να γενικευτεί και σε περιπτώσεις όπου υπάρχουν m συμμετέχοντες, όπως στην περίπτωση που πρέπει να γίνει μια μυστική ψηφοφορία ή μία μυστική διαπραγμάτευση για κάποια πώληση-αγορά (Yao, 1982). Παρά το γεγονός ότι η ύπαρξη πολλών συμμετεχόντων μπορεί να σημαίνει την ύπαρξη πολλών οντοτήτων που μπορούν να διαφθαρούν, εντούτοις το πρωτόκολλο αυτό δίνει τη δυνατότητα στις μη-κατευθυνόμενες οντότητες να μπορούν να ανιχνεύσουν οποιαδήποτε κακόβουλη ενέργεια.

5.4 Η Τεχνική Garbled Circuit Evaluation

Η συγκεκριμένη τεχνική εισήχθηκε αρχικά από τον Yao. Σύμφωνα με αυτή, δύο οντότητες P_1 και P_2, επιθυμούν να υπολογίσουν μία συνάρτηση f με ασφαλή τρόπο, έτσι ώστε οι είσοδοι που θα δώσουν σε αυτή να παραμένουν ιδιωτικοί, δηλαδή να μην γίνονται γνωστοί σε κανέναν. Το πρωτόκολλο του Yao "αλλοιώνει" κατάλληλα ένα λογικό (Boolean) κύκλωμα, έτσι ώστε να γίνονται οι υπολογισμοί χωρίς να ανακαλύπτονται πληροφορίες περί των εισόδων του. Περιλαμβάνει τα εξής βήματα (Kelong Cong, 2020a; Konstantinos Gkikas, 2014; Yakoubov, 2017):

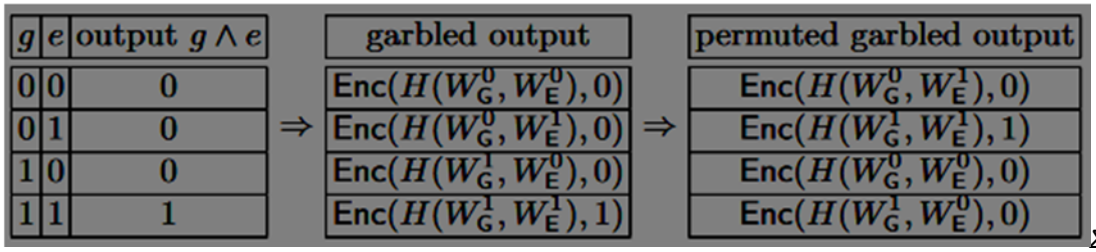
- Έστω ότι υπάρχουν οι οντότητες G και E, στις οποίες αντιστοιχούν τα bit g και e και θέλουν να υπολογίσουν το αποτέλεσμα της πύλης AND ($g \wedge e$), χωρίς να αποκαλύψουν η μία στην άλλη καμία πληροφορία για τα bits τους.

g	e	output $g \wedge e$
0	0	0
0	1	0
1	0	0
1	1	1

- Η οντότητα G αναλαμβάνει να ανακατέψει τον παραπάνω πίνακα αληθείας. Αυτό το πραγματοποιεί, παράγοντας τις τέσσερις τυχαίες συμβολοσειρές W_G^0 , W_G^1, W_E^0 και W_E^1.

- Στη συνέχεια, η οντότητα G χρησιμοποιεί όλα τα πιθανά σενάρια τιμών που μπορεί να πάρουν τα bit g και e (δηλαδή τα ζεύγη (g= 0,e= 0),(g= 0,e= 1),(g= 1,e= 0) και

(g= 1,e= 1). Χρησιμοποιεί αυτά τα ζευγάρια των συμβολοσειρών που προκύπτουν από τα παραπάνω σενάρια, τα οποία βάζει σε μία συνάρτηση παραγωγής συμμετρικών κλειδιών κρυπτογράφησης H, και αυτό το κλειδί το χρησιμοποιεί για την κρυπτογράφηση της εξόδου g ∧ e. Θα προκύψει λοιπόν ένας πίνακας, του οποίο πριν στείλει στην οντότητα E, ανακατεύει τη σειρά. Τα βήματα αυτά μαζί με το τελικό αποτέλεσμα φαίνονται στο ακόλουθο σχήμα :



Σχήμα 5: Βήματα δημιουργίας "Ανακατεμένου πίνακα" και τελικός πίνακας,

Πηγή : "A gentle introduction to Yao's Garbled Circuits", (Yakoubov, 2017)

- Μόλις η οντότητα G δημιουργήσει τον τελευταίο πίνακα, τον στέλνει στην οντότητα E.

- Μόλις η οντότητα E παραλάβει τον παραπάνω “ανακατεμένο” πίνακα, χρειάζεται να αποκρυπτογραφήσει τα bit g και e που κρυπτογραφήθηκαν με το $H(W_G^g, W_E^e)$. Για να προχωρήσει όμως στην αποκρυπτογράφηση, χρειάζεται αντίστοιχα τα W_G^g και W_E^e από την οντότητα G.

- Για την οντότητα G, είναι σχετικά εύκολο να στείλει το W_G^g, καθώς γνωρίζει το g. Δεδομένου ότι όλες οι τιμές είναι τυχαίες και ανεξάρτητες, μπορεί να το στείλει

χωρίς να μάθει η οντότητα Ε καμία πληροφορία για το g. Σχετικά όμως με το W_E^e, δεν μπορεί η οντότητα G να στείλει και τα δυο (W_E^0 και W_E^1), καθώς αυτό θα δώσει τη δυνατότητα στην οντότητα Ε να προχωρήσει σε δύο αποκρυπτογραφήσεις. Επιπλέον, η οντότητα Ε, δεν μπορεί απλά να ζητήσει από την οντότητα G τη συμβολοσειρά από τις δύο που επιθυμεί, καθώς με αυτό τον τρόπο, θα δώσει στην οντότητα G τη δυνατότητα να μάθει το e. Για το λόγο αυτό, θα χρησιμοποιήσουν την τεχνική της Μη-Συνειδητής Μεταφοράς (Oblivious Transfer) , προκειμένου να μάθει η οντότητα Ε τη συμβολοσειρά W_E^e, χωρίς να αποκαλύψει το bit e.

Μέσω της συγκεκριμένης τεχνικής μπορεί να διασφαλιστεί ότι καμία από τις δύο οντότητες δεν θα μάθει κάποια επιπλέον πληροφορία της άλλης οντότητας. Βέβαια, το συγκεκριμένο πρωτόκολλο έχει σχεδιαστεί για να παρέχει ασφάλεια απέναντι σε παθητικούς αντιπάλους (semi-honest adversaries), όχι όμως απέναντι σε κακόβουλους αντιπάλους (malicious adversaries). Για να καλυφθεί και αυτή η συγκεκριμένη περίπτωση ασφαλείας, θα πρέπει να γίνουν τα εξής τρία βήματα (Snyder, 2014) :

- Θα πρέπει να δημιουργηθούν 1-out-of-2-Oblivious Transfer (OT_1^2) πρωτόκολλα τα οποία είναι ασφαλή απέναντι σε κακόβουλους αντιπάλους.

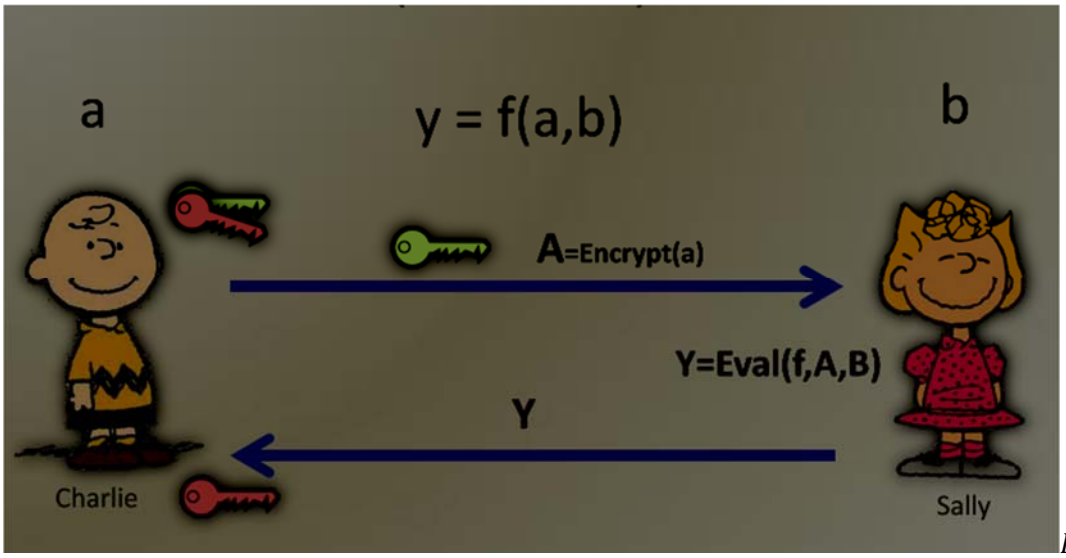
- Θα πρέπει να διασφαλιστεί ότι η οντότητα που κατασκευάζει το κύκλωμα θα πρέπει να κατασκευάσει σωστά το "ανακατωμένο"κύκλωμα.

- Θα πρέπει να αποτραπεί η οντότητα G από το να αποκτήσει οποιοδήποτε πλεονέκτημα από τη διαδικασία αποστολής στην οντότητα Ε διεφθαρμένων τιμών για τις εισόδους της.

Τέλος, για να καλυφθεί στην περίπτωση κακόβουλων αντιπάλων ότι θα υπάρχει δικαιοσύνη, αυτό μπορεί να επιτευχθεί με το να διασφαλιστεί ότι η οντότητα Ε θα επιστρέψει την έξοδο στην οντότητα G στο τέλος του πρωτοκόλλου (Snyder, 2014).

5.5 Η Τεχνική της Ομομορφικής Κρυπτογράφησης

Η ομομορφική κρυπτογράφηση είναι μια τεχνική η οποία μπορεί να εφαρμοστεί σε πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων. Πρόκειται για μια διαδικασία, η οποία επιτρέπει τους υπολογισμούς πάνω σε κρυπτοκείμενα, δηλαδή κρυπτογραφημένα δεδομένα, τα οποία μπορούν να συνδυαστούν με τέτοιο τρόπο, ώστε το κρυπτοκείμενο που προκύπτει, αν αποκρυπτογραφηθεί, να ταιριάζει επακριβώς με το αρχικό κείμενο, αν οι υπολογισμοί είχαν γίνει σε εκείνο (Zhao et al., 2018). Ουσιαστικά θα πρέπει το κρυπτοκείμενο που προκύπτει, να αντιστοιχεί στον υπολογισμό μιας άλλης συνάρτησης στα μηνύματα και το αποτέλεσμα να μπορεί να ανακτηθεί, με τη χρήση απλής αποκρυπτογράφησης (Ευστάθιος Ζάχος et al., 2015). Με την ομομορφική κρυπτογράφηση λοιπόν, μπορούν να γίνουν υπολογισμοί πάνω σε κρυπτοκείμενα, και να προκύψουν σωστά αποτελέσματα. Μάλιστα τα δεδομένα δεν θα χρειαστεί να αποκρυπτογραφηθούν καθώς υπόκεινται σε επεξεργασία σε μορφή κρυπτοκειμένων, ιδιότητα που παίζει σημαντικό ρόλο για την δημιουργία ασφαλών πρωτοκόλλων (Zhao et al., 2018). Η συγκεκριμένη τεχνική λοιπόν, μπορεί να προσφέρει σημαντικές λύσεις στην προστασία των προσωπικών δεδομένων, ικανοποιώντας την νομοθεσία που υπάρχει σχετικά με την προστασία των προσωπικών δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR) (Arampatzis, 2020).



Εικόνα 2: Ομομορφική κρυπτογράφηση ,

Πηγή : " Homomorphic Encryption for Secure Multi-Party Computation " (Weerasooriya W.A.A.C.P., 2014)

Απαραίτητη προϋπόθεση είναι να χρησιμοποιηθεί το ίδιο δημόσιο κλειδί σε όλα τα κρυπτοκείμενα (Ευστάθιος Ζάχος et al., 2015). Ουσιαστικά, η ομομορφική κρυπτογράφηση παρουσιάζει ομοιότητες με άλλες μορφές κρυπτογράφησης, αφού εκτός από το δημόσιο κλειδί, χρησιμοποιεί και το ιδιωτικό κλειδί, το οποίο πρέπει να έχει στην διάθεση του όποιος θέλει να αποκτήσει πρόσβαση στα κρυπτογραφημένα δεδομένα (Arampatzis, 2020).

Υπάρχουν δύο είδη ομομορφικής κρυπτογράφησης (Arampatzis, 2020; Zhao et al., 2018):

- Η πλήρως ομομορφική κρυπτογράφηση (Fully Homomorphic Encryption). Πρόκειται για μέθοδο που μπορεί να χρησιμοποιηθεί στα πρωτόκολλα SMC, καθώς επιτρέπει την εκτέλεση υπολογισμών στα κρυπτογραφημένα δεδομένα. Το σύστημα βοηθάει στην εκτέλεση των υπολογισμών, χωρίς όμως να γνωρίζει καμία πληροφορία για τα δεδομένα. Μόλις ολοκληρωθούν οι υπολογισμοί, τα δεδομένα επιστρέφονται στο ιδιοκτήτη τους, ο οποίος τα αποκρυπτογραφεί για να λάβει το αποτέλεσμα των υπολογισμών. Εκτός από προστασία των δεδομένων, σημαντική εφαρμογή που μπορεί να έχει η συγκεκριμένη κατηγορία είναι και στην εκτέλεση διαδικτυακών εκλογών με ασφάλεια. Γενικότερα έχει μεγάλες υπολογιστικές δυνατότητες, οι οποίες ακόμα δεν έχουν αξιοποιηθεί. Ένας σημαντικός περιορισμός της συγκεκριμένης περίπτωσης είναι το γεγονός ότι σε περίπτωση που χρησιμοποιηθεί μεγάλη βάση δεδομένων, στην οποία εμπλέκονται πολλοί χρήστες, και πρέπει να προστατευθούν τα δεδομένα κατά τη διάρκεια εκτέλεσης υπολογισμών, μπορεί η χρησιμοποίηση της θα είναι πολύπλοκη και δύσκολη, εάν αποφασιστεί να χρησιμοποιηθούν διαφορετικές βάσεις δεδομένων και κλειδιά κρυπτογράφησης για κάθε χρήστη. Επιπλέον, ένα ακόμα αρνητικό χαρακτηριστικό αυτής είναι το γεγονός ότι απαιτείται πολύς χρόνος για την εκτέλεση των υπολογισμών (Arampatzis, 2020).

- Η μερικώς ομομορφική κρυπτογράφηση (Somewhat Homomorphic Encryption). Η συγκεκριμένη μέθοδος μπορεί να χρησιμοποιηθεί κάτω υπό συγκεκριμένες περιπτώσεις, με συγκεκριμένες συναρτήσεις που χρησιμοποιούν περιορισμένες πράξεις. Οι αλγόριθμοι της κατηγορίας αυτής είναι εύκολο να εφαρμοστούν, γι'

αυτό και ήδη χρησιμοποιείται, αλλά η υπολογιστική εφαρμοσιμότητά τους είναι μικρή.

5.6 Η Κρυπτογράφηση Κατωφλίου (Threshold Cryptography)

Η συγκεκριμένη τεχνική χρησιμοποιείται με σκοπό την εκτέλεση υπολογισμών ανάμεσα σε πολλές οντότητες. Η διαφορά της με άλλες κρυπτογραφικές τεχνικές, είναι το γεγονός ότι καμία από τις οντότητες δεν έχει στην κατοχή της το μυστικό-ιδιωτικό κλειδί (Lindell, 2020). Σε αντίθεση με άλλες τεχνικές, δεν υπάρχει μόνο μία οντότητα που να έχει την δυνατότητα να αποκρυπτογραφήσει το μήνυμα, αλλά αντίθετα το μυστικό κλειδί διαμοιράζεται σε πολλές οντότητες, με απαραίτητη προϋπόθεση την συμμετοχή ενός υποσυνόλου αυτών για να πραγματοποιηθεί η αποκρυπτογράφηση (Ευστάθιος Ζάχος et al., 2015). Αυτό συμβαίνει κυρίως για να αποτραπούν προσπάθειες κλοπής του, αφού ένας αντίπαλος θα πρέπει να πραγματοποιήσει με επιτυχία επιθέσεις σε πολλές οντότητες, για να καταφέρει να το αποκτήσει (Lindell, 2020).

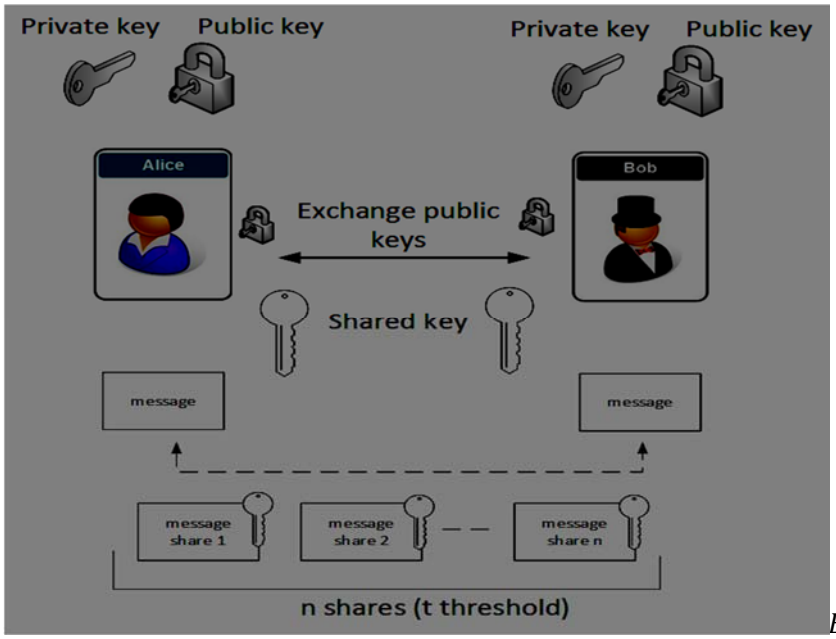
Η τεχνική Threshold Cryptography ακολουθεί τα εξής τέσσερα βήματα (Ευστάθιος Ζάχος et al., 2015):

- Τη δημιουργία των κλειδιών, μέσω ενός έμπιστου διανομέα, με τη χρήση άλλων τεχνικών όπως η τεχνική Shamir Secret Sharing και τη διανομή του στις οντότητες.

- Την κρυπτογράφηση του μηνύματος.

- Την αποκρυπτογράφηση από τις διάφορες οντότητες, των τμημάτων του μηνύματος.

- Τον συνδυασμό των τμημάτων για την ανάκτηση του αρχικού μηνύματος.



Εικόνα 3: Κρυπτογράφηση Κατωφλίου

Πηγή : "https://asecuritysite.com/encryption/ecc_thres" (William J Buchanan, n.d.)

Ένα χαρακτηριστικό παράδειγμα του συγκεκριμένου πρωτοκόλλου, είναι αυτό που χρησιμοποιεί τον αλγόριθμο RSA για δύο οντότητες. Αρχικά πρέπει να αναφερθεί ο τρόπος λειτουργίας του αλγορίθμου RSA. Ο συγκεκριμένος αλγόριθμος χρησιμοποιεί το

δημόσιο κλειδί (N,e) και το ιδιωτικό κλειδί d τα οποία προκύπτουν με τον εξής τρόπο (Δρ. Κωνσταντίνος Λιμνιώτης, 2019) :

- Το $N=p*q$, όπου p και q είναι δύο τυχαίοι μεγάλοι πρώτοι αριθμοί.
- Το $\varphi(N)=(p-1)*(q-1)$
- Επιλέγεται τυχαίος αριθμός e, τέτοιος ώστε $gcd(e, \varphi(N))=1$
- Υπολογίζεται το $d=e^{-1}(\text{mod } \varphi(N))$

Για την κρυπτογράφηση λοιπόν ενός μηνύματος m γίνεται ο υπολογισμός $c=m^e(\text{mod}N)$ και για την αποκρυπτογράφηση γίνεται ο υπολογισμός $m=c^d(\text{mod}N)$.

Ο αλγόριθμος RSA χρησιμοποιείται για περιπτώσεις κρυπτογράφησης και ψηφιακής υπογραφής, αλλά στη συγκεκριμένη περίπτωση θα χρησιμοποιηθεί η αντίστροφη διαδικασία, για να αποδειχθεί κατά πόσο είναι ασφαλές να γίνει η επικοινωνία ανάμεσα σε δύο οντότητες, χωρίς να γνωρίζει και να μπορεί καμία από τις δύο να υπολογίσει την συνάρτηση. Θα ακολουθηθούν λοιπόν τα εξής βήματα (Lindell, 2020):

- Έστω δύο τυχαίοι αριθμοί d_1 και d_2 , για τους οποίους ισχύει ότι $d_1 + d_2 = d(\text{mod}\varphi(N))$.
- Η πρώτη οντότητα υπολογίζει το $m_1=c^{d1}\text{mod}N$ και η δεύτερη το $m_2=c^{d2}\text{mod}N$.
- Οι δύο οντότητες ανταλλάσουν μεταξύ τους τους δύο προηγούμενους υπολογισμούς.
- Η κάθε οντότητα υπολογίζει το $m= m_1 * m_2$. Στη συνέχεια επιβεβαιώνουν ότι κατέληξαν στην σωστή έξοδο, χρησιμοποιώντας τη σχέση $m^e=c\text{mod}N$, η οποία εφόσον ισχύει, δίνει σαν έξοδο το m. Ο συγκεκριμένος υπολογισμός επαληθεύεται ως εξής :

$m = c^{d1} * c^{d2}\text{ mod}N = c^{d1 + d2 \text{ mod } \varphi(N)}\text{mod}N = c^d\text{ mod}N.$

Όσον αφορά την ασφάλεια της συγκεκριμένης τεχνικής, αυτή φαίνεται από το γεγονός ότι δεδομένης της εισόδου m και του d_1 που λαμβάνει από την δεύτερη οντότητα, μπορεί να υπολογίσει το $m_2 = c^{d2} \text{mod} N = c^{d2-d1+d1} \text{mod} N = c/c^{d1} \text{mod} N$. Αυτό σημαίνει ότι η πρώτη οντότητα δεν μαθαίνει τίποτα περισσότερο από την έξοδο του πρωτοκόλλου, αφού μπορεί να δημιουργήσει τα μηνύματα που λαμβάνει στο πρωτόκολλο από μόνη της από την δική του είσοδο και την έξοδο του. (Lindell, 2020)

Κεφάλαιο 6

Εφαρμογές των πρωτοκόλλων SMC

Στο παρόν κεφάλαιο θα γίνει αναφορά σε διάφορες εφαρμογές στις οποίες μπορεί να χρησιμοποιηθούν και να εφαρμοστούν τα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων. Είναι προφανές ότι υπάρχουν πάρα πολλές εφαρμογές, αλλά στο παρών κεφάλαιο θα γίνει μια αναφορά στις σημαντικότερες και ίσως πιο γνωστές από αυτές. Ταυτόχρονα, σε κάθε μία εφαρμογή, θα γίνει αναφορά και στις τεχνικές που μπορούν να χρησιμοποιηθούν σε κάθε περίπτωση εφαρμογής.

6.1 Η Ηλεκτρονική Ψηφοφορία

Η ηλεκτρονική ψηφοφορία αποτελεί ένα από τα πιο σημαντικά και ταυτόχρονα γνωστά παραδείγματα εφαρμογής των πρωτοκόλλων SMC. Για να θεωρηθεί ένα πρωτόκολλο SMC ότι μπορεί να χρησιμοποιηθεί στη συγκεκριμένη περίπτωση, θα πρέπει όπως αναφέρθηκε και στο κεφάλαιο 2, να διασφαλιστεί ότι η καταμέτρηση των ψήφων θα γίνει χωρίς να αποκαλυφθεί η επιλογή του κάθε ψηφοφόρου, ότι η επιλογή των ψήφων γίνεται από το κάθε ψηφοφόρο ανεξάρτητα, χωρίς να επηρεάζονται δηλαδή από τις επιλογές των ψηφοφόρων καθώς και ότι οι ψήφοι προέρχονται από νόμιμους ψηφοφόρους. Είναι απαραίτητο δηλαδή να υπάρχει διαφάνεια στην εκλογική διαδικασία (Guo et al., 2013). Επιπλέον, θα πρέπει οποιαδήποτε στιγμή το σύστημα να είναι διαθέσιμο και η καταμέτρηση των ψήφων να μπορεί να γίνει σε ένα σχετικά σύντομο χρονικό διάστημα (Ευστάθιος Ζάχος et al., 2015).

Έχουν προταθεί διάφορα πρωτόκολλα SMC για την ασφαλή εκτέλεση ηλεκτρονικών ψηφοφοριών. Χαρακτηριστική είναι η περίπτωση, σύμφωνα με την οποία μπορούν τα αποτελέσματα της ψηφοφορίας να κρυπτογραφηθούν τοπικά και ανέβουν στο blockchain (Yang et al., 2020). Στη συνέχεια, το τελικό αποτέλεσμα ψηφοφορίας αποκαλύπτεται στο δίκτυο blockchain μετά την εκτέλεση της στατιστικής διαδικασίας από τον αθροιστή και τον διακομιστή των υπολογιστών.

Μία δεύτερη περίπτωση είναι εκείνη στην οποία μπορούν να χρησιμοποιηθούν τα ομομορφικά συστήματα (Ευστάθιος Ζάχος et al., 2015), σύμφωνα με τα οποία οι ψήφοι κρυπτογραφούνται, με τη χρησιμοποίηση ενός δημοσίου κλειδιού μιας εκλογικής αρχής και τοποθετούνται σε έναν αυθεντικοποιημένο πίνακα ανακοινώσεων. Στη συνέχεια οι ψήφοι συνδυάζονται, η εκλογική αρχή λαμβάνει το κρυπτογραφημένο άθροισμα των ψήφων, το αποκρυπτογραφεί με το ιδιωτικό της κλειδί και το ανακοινώνει.

Μία τρίτη περίπτωση, είναι αυτή στην οποία μπορούν να χρησιμοποιηθούν τα δίκτυα μίξης (mixing networks) (Ευστάθιος Ζάχος et al., 2015). Σύμφωνα με αυτό το πρωτόκολλο, χρησιμοποιούνται οι μίκτες, οι οποίοι λαμβάνουν τις κρυπτογραφημένες ψήφους και αφαιρούν τη συσχέτιση ανάμεσα στην ψήφο και τον ψηφοφόρο. Μετά από αυτό το βήμα, οι ψήφοι μπορούν να αποκρυπτογραφηθούν και να καταμετρηθούν.

Μια τέταρτη περίπτωση, μπορεί να προκύψει με τη χρησιμοποίηση των τυφλών υπογραφών (blind signatures) (Ευστάθιος Ζάχος et al., 2015). Σύμφωνα με το συγκεκριμένο πρωτόκολλο, ο ψηφοφόρος υποβάλλει μια έκδοση της ψήφου του υπογεγραμμένης με τυφλή υπογραφή με πληροφορίες για την ταυτοποίηση του. Η εκλογική αρχή επαληθεύει ότι έχει δικαίωμα ψήφου και του το επιστρέφει υπογεγραμμένο. Ο ψηφοφόρος αφού το παραλάβει υπογεγραμμένο, το παραθέτει στον αυθεντικοποιημένο πίνακα ανακοινώσεων, με ανωνυμία. Στη συνέχεια, η εκλογική αρχή λαμβάνει τα υπογεγραμμένα ψηφοδέλτια και επαληθεύει την υπογραφή τους, με σκοπό να τα καταμετρήσει. Ταυτόχρονα, για να μην υπάρξει οποιαδήποτε διαρροή πληροφοριών, από την συμμετοχή της εκλογικής αρχής, μπορούν να χρησιμοποιηθούν η εκλογική αρχή η οποία θα γνωρίζει την ταυτότητα των ψηφοφόρων, αλλά όχι το περιεχόμενο της ψήφου και η αρχή καταμέτρησης, που θα γνωρίζει την ψήφο αλλά όχι την ταυτότητα των ψηφοφόρων.

Τέλος, αξίζει να αναφερθεί η περίπτωση, σύμφωνα με την οποία μπορεί να χρησιμοποιηθεί στην ηλεκτρονική ψηφοφορία ένας συνδυασμός οπτικής κρυπτογραφίας (Visual Cryptography) και μηχανισμών SMC (Naidu et al., 2016). Η οπτική κρυπτογραφία χρησιμοποιείται για την κρυπτογράφηση των οπτικών δεδομένων που θα χρησιμοποιηθούν για την αυθεντικοποίηση του ψηφοφόρου. Το σύστημα αυτό χρησιμοποιείται για την αποτροπή ψηφοφορίας ατόμων με ψευδή στοιχεία και λειτουργεί με την καταγραφή του αποτυπώματος του ψηφοφόρου. Αυτό συγκρίνεται με μία βάση δεδομένων για να διασταυρωθεί ότι όντως έχει ο υποψήφιος ψηφοφόρος την ταυτότητα που υποστηρίζει και επομένως δικαίωμα ψήφου. Στη συνέχεια μπορεί να ολοκληρωθεί η διαδικασία ψηφοφορίας και της καταγραφής των ψήφων, με τη χρήση άλλων μεθόδων SMC που αναφέρθηκαν προηγουμένως.

6.2 Οι Ηλεκτρονικές Δημοπρασίες

Οι ηλεκτρονικές δημοπρασίες αποτελούν μία ακόμα περίπτωση στην οποία μπορούν να εφαρμοστούν τεχνικές SMC. Αποτελεί βασική προτεραιότητα για αυτές να διασφαλίζεται η ιδιωτικότητα. Πιο συγκεκριμένα, θα πρέπει να μπορεί να διασφαλιστεί ότι κανένας συμμετέχων στην δημοπρασία δεν θα μαθαίνει οποιαδήποτε πληροφορία για τις προσφορές των υπόλοιπων συμμετεχόντων (Evans et al., 2018). Το μόνο που θα πρέπει να γίνει γνωστό είναι η νικητήρια προσφορά, με την προϋπόθεση ότι θα γνωστοποιηθεί στο τέλος της διαδικασίας. Έτσι λοιπόν, δεν θα πρέπει να χρησιμοποιηθεί από κάποιον η προσφορά ενός συμμετέχοντος για να κατασκευαστεί μια άλλη προσφορά μεγαλύτερη. Γενικότερα θα πρέπει ακόμα και η πρώτη προσφορά που θα καταθέσει κάποιος να μείνει κρυφή, με σκοπό να μην αποκτήσουν άλλοι συμμετέχοντες πλεονέκτημα. Η μόνη περίπτωση στην οποία θα αποκαλυφθούν πληροφορίες, είναι εκείνη στην οποία όλοι οι συμμετέχοντες θα αποκαλύψουν τις γνώσεις τους, γεγονός που θα αποκαλύπτει όλες τις προσφορές σε όλου του είδους τις δημοπρασίες. Υπάρχουν πολλά πρωτόκολλα που μπορούν να λύσουν όποια προβλήματα υπάρχουν σε μια ηλεκτρονική δημοπρασία. Χαρακτηριστικό παράδειγμα αποτελεί το πρωτόκολλο που βασίζεται στην δημοπρασία του Vickrey, κατά την οποία αυτός που κάνει την υψηλότερη προσφορά κερδίζει, αλλά αντί να πληρώσει την αξία της δικής του προσφοράς, πληρώνει την αξία της δεύτερης υψηλότερης προσφοράς (Evans et al., 2018). Ένα δεύτερο παράδειγμα δημοπρασίας στο οποίο εφαρμόστηκαν SMC τεχνικές, αποτελεί αυτό που εφαρμόστηκε στην Δανία, με

σκοπό τη δημιουργία πλατφόρμας για τις δημοπρασίες σχετικά με τα ζαχαρότευτλα (Bogetoft et al., 2009; Evans et al., 2018). Στη συγκεκριμένη περίπτωση αναφέρεται ότι οι υπολογισμοί πραγματοποιήθηκαν ανάμεσα σε τρεις πλευρές, την εταιρεία Danisco, την ένωση των αγροτών και την κυβέρνηση. Ο λόγος που χρησιμοποιήθηκαν ήταν το γεγονός ότι οι αγρότες δεν ήθελαν να γίνουν γνωστά στοιχεία στις άλλες δύο πλευρές, όπως οι δυνατότητες τους και τα κόστη. Αξίζει να αναφερθεί ότι χρησιμοποιήθηκαν διάφορες τεχνικές SMC ως εργαλεία, με κυριότερη και πιο γνωστή την τεχνική Secret Sharing, η οποία προτιμήθηκε από άλλες πιο κοστοβόρες μεθόδους, όπως η ομομορφική κρυπτογράφηση. (Bogetoft et al., 2009; Evans et al., 2018)

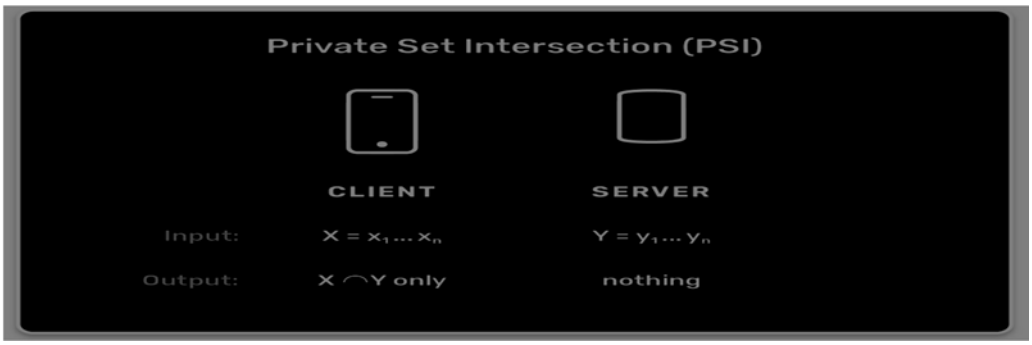
6.3 Η Χρήση Μηχανισμών SMC από τις Κυβερνήσεις

Αποτελεί πραγματικότητα το γεγονός ότι οι κυβερνήσεις των διαφόρων χωρών κατέχουν πληροφορίες οι οποίες αναφέρονται στους πολίτες. Πολλές φορές, οι πληροφορίες αυτές έχουν να κάνουν με ευαίσθητα δεδομένα της προσωπικής τους ζωής. Η ορθή χρήση και επεξεργασία αυτών των δεδομένων, μπορεί να αποτελέσει ένα ισχυρό και αποτελεσματικό εργαλείο για τις κυβερνήσεις, προκειμένου να αντιμετωπίσουν διάφορα προβλήματα που υπάρχουν (π.χ. για τη διαφύλαξη της δημόσιας υγείας) και να βελτιώσουν την ποιότητα ζωής των πολιτών. Ταυτόχρονα όμως υπάρχει ο κίνδυνος της παραβίασης της ιδιωτικής ζωής των πολιτών, καθώς εύκολα μπορούν να παραβιαστούν τα δικαιώματα των πολιτών σχετικά με τα ευαίσθητα προσωπικά τους δεδομένα και να κατηγορηθούν ότι προσπαθούν να δημιουργήσουν μία καινούρια πραγματικότητα συνεχούς ελέγχου της καθημερινότητας και της προσωπικής τους ζωής. Αυτός είναι και ένας βασικός λόγος που αποτρέπει τις διάφορες κυβερνήσεις στο να προχωρήσουν στην εκμετάλλευση αυτών των πληροφοριών. Σε αυτό το σημείο όμως, θα μπορούσαν να χρησιμοποιηθούν διάφοροι μηχανισμοί και τεχνικές SMC (Evans et al., 2018; Lindell, 2020). Χαρακτηριστικό είναι το παράδειγμα της κυβέρνησης στην Εσθονία, η οποία χρησιμοποίησε μηχανισμούς και τεχνικές SMC, θέλοντας να επεξεργαστεί κρυπτογραφημένα δεδομένα που προέρχονταν από τις καταγραφές του φόρου εισοδήματος και τις καταγραφές από την ανώτερη εκπαίδευση, με σκοπό να προχωρήσουν σε μια ανάλυση για το αν οι μαθητές που εργάζονται κατά τη διάρκεια των σπουδών τους αποτυγχάνουν σε μεγαλύτερα ποσοστά από αυτούς που αφοσιώνονται στις σπουδές τους και μόνο. Ουσιαστικά πραγματοποιήθηκε υπολογισμός ανάμεσα σε

τρεις πλευρές, την Εσθονική Αρχή Πληροφοριακών Συστημάτων, το Υπουργείο Οικονομικών και την εταιρεία Cybernetica που παρείχε το πρωτόκολλο Sharemind. Με την χρήση λοιπόν του μηχανισμού SMC, κατάφεραν να εγγυηθούν ότι τα προσωπικά δεδομένα και το φορολογικό απόρρητο δεν θα καταπατηθούν, αλλά ταυτόχρονα θα μπορέσουν να εκμεταλλευτούν τα δεδομένα αυτά στο έπακρον (Evans et al., 2018; Lindell, 2020).

6.4 Η Χρήση Μηχανισμών SMC για Διασταύρωση Στοιχείων - Private Set Intersection

Πρόκειται για μία εφαρμογή μηχανισμών SMC, η οποία μπορεί να χρησιμοποιηθεί από δύο διαφορετικές οντότητες, οι οποίες κατέχουν δύο ιδιωτικά σύνολα τιμών, δηλαδή κάποιες ιδιωτικές πληροφορίες, και επιθυμούν να τις διασταυρώσουν, προκειμένου να ανακαλύψουν ποιες από αυτές είναι κοινές, χωρίς όμως να αποκαλύψουν η μία στην άλλη καμία πληροφορία παρά μόνο τα στοιχεία-τιμές που θα διασταυρωθούν (Lindell, 2020). Τα πρωτόκολλα που χρησιμοποιούνται στην συγκεκριμένη περίπτωση, επιτρέπουν στις οντότητες να μαθαίνουν μόνο περιορισμένες λειτουργίες της διασταύρωσης, όπως για παράδειγμα τον αριθμό των στοιχείων που διασταυρώνονται ή αν το μέγεθος της διασταύρωσης υπερβαίνει κάποιο όριο (Ion et al., 2017).



6.4.1 Κατηγοριοποίηση Πρωτοκόλλων για Χρήση στην Εφαρμογή Private Set Intersection

Υπάρχουν πολλοί τρόποι με τους οποίους μπορεί να γίνει μια κατηγοριοποίηση των πρωτοκόλλων που χρησιμοποιούνται για την εφαρμογή της περίπτωσης Private Set Intersection. Τα πρωτόκολλα αυτά θα μπορούσαν να χωριστούν στις εξής κατηγορίες (Kolesnikov et al., 2016; Lindell, 2020; Pinkas et al., 2015, 2018):

- Η εφαρμογή Private Set Intersection με τη χρήση της τεχνικής oblivious pseudorandom function evaluation. Στη συνέχεια θα γίνει μια παρουσίαση της εφαρμογής Private Set Intersection με τη χρήση ενός συγκεκριμένου πρωτοκόλλου. Αρχικά πρέπει να αναφερθεί ότι μία ψευδοτυχαία συνάρτηση F, είναι μία συνάρτηση, που λειτουργεί χρησιμοποιώντας μία κωδικοποίηση (Kolesnikov et al., 2016; Lindell, 2020)τέτοια ώστε οι έξοδοι που παράγει η συνάρτηση αυτή, για δοθέντες γνωστές εισόδους, να έχουν την ιδιότητα να φαίνονται ότι είναι τελείως τυχαίες. Από μια πιο μαθηματική οπτική λοιπόν, δοθείσας μιας λίστας που αποτελείται από τα στοιχεία $x_1, x_2, \ldots, x_n$, μπορούν να υπολογιστούν οι τιμές $F_k(x_1), F_k(x_2), \ldots, F_k(x_n)$ και μάλιστα να φαίνονται ότι είναι τυχαίες. Μάλιστα, δοθέντων των $F_k(x_i)$, είναι ανέφικτο να υπολογιστούν οι τιμές των x_i.

Στη συνέχεια, προκειμένου να λειτουργήσει η εφαρμογή αυτή σωστά, θα χρησιμοποιηθεί ένα εργαλείο, το οποίο ονομάζεται oblivious pseudorandom function evaluation (Kolesnikov et al., 2016; Lindell, 2020). Σύμφωνα με αυτό, η πρώτη οντότητα δίνει σαν είσοδο το k, η δεύτερη το x, και η δεύτερη οντότητα λαμβάνει το $F_k(x)$. Ενώ συμβαίνει αυτό, η πρώτη οντότητα δεν μαθαίνει τίποτα για το x, και αντίστοιχα η δεύτερη οντότητα μαθαίνει μόνο $F_k(x)$, αλλά τίποτα περισσότερο από αυτό, διατηρώντας ουσιαστικά μυστικό το k.

Στο επόμενο βήμα της συγκεκριμένης εφαρμογής Private Set Intersection, ας γίνει η υπόθεση ότι οι δύο οντότητες που αναφέρθηκαν προηγουμένως έχουν τις λίστες με τα στοιχεία $x_1, x_2, \ldots, x_n$ η πρώτη, και $y_1, y_2, \ldots, y_n$ η δεύτερη. Ιδανικά, αποτελεί κομμάτι της συγκεκριμένης υπόθεσης το γεγονός ότι οι δύο λίστες έχουν ακριβώς τον ίδιο αριθμό στοιχείων n. Η εφαρμογή περιλαμβάνει στη συνέχεια τα ακόλουθα βήματα (Lindell, 2020) :

Η μία οντότητα επιλέγει έναν αριθμό k, που θα χρησιμοποιηθεί στην ψευδοτυχαία συνάρτηση.

Οι δύο οντότητες χρησιμοποιούν το εργαλείο oblivious pseudorandom function evaluation που αναφέρθηκε προηγουμένως. Κατά την i-οστή εκτέλεση, η μία οντότητα δίνει σαν είσοδο τον αριθμό k και η δεύτερη οντότητα την τιμή y_i. Σαν αποτέλεσμα, η δεύτερη οντότητα μαθαίνει τις τιμές $F_k(y_1)$, $F_k(y_2)$,….., $F_k(y_n)$, ενώ παράλληλα η πρώτη οντότητα δεν μαθαίνει απολύτως τίποτα για τις τιμές y_1, y_2 , ……. , y_n.

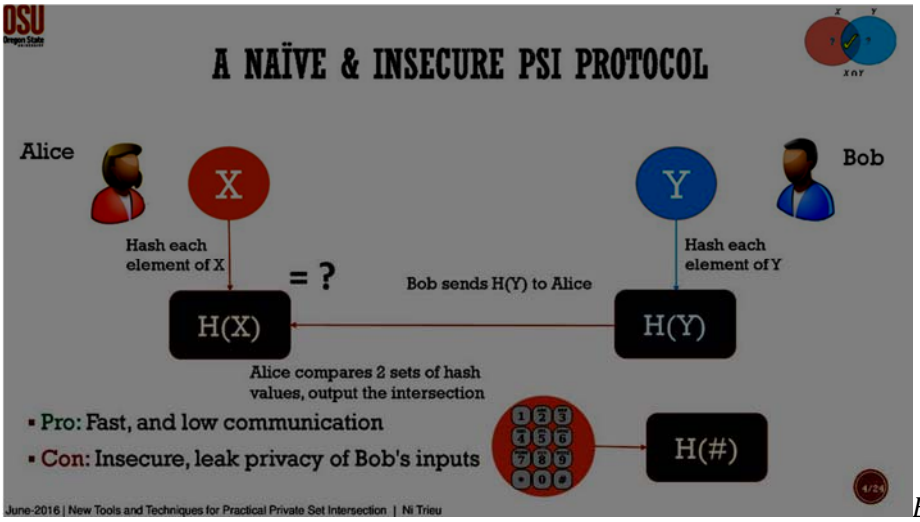
Η πρώτη οντότητα, γνωρίζοντας το k, υπολογίζει τις τιμές $F_k(x_1)$, $F_k(x_2)$,….., $F_k(x_n)$και στέλνει τη λίστα στη δεύτερη οντότητα.

Η δεύτερη οντότητα διασταυρώνει τις λίστες $F_k(x_1)$, $F_k(x_2)$,….., $F_k(x_n)$ και $F_k(y_1)$, $F_k(y_2)$,….., $F_k(y_n)$ και βρίσκει τις τιμές y_i για τις οποίες οι τιμές $F_k(y_j)$, ενέργεια που μπορεί να εκτελέσει καθώς γνωρίζει την σχέση που υπάρχει ανάμεσα στις τιμές y_i και $F_k(y_j)$.

Με αυτό τον τρόπο ολοκληρώνεται η χρησιμοποίηση της εφαρμογής για τη Private Set Intersection για τη διασταύρωση στοιχείων με τη χρήση του συγκεκριμένου OPF εργαλείου, ικανοποιώντας το γεγονός ότι η πρώτη οντότητα δεν μαθαίνει τίποτα για τις τιμές y_i . Η δεύτερη οντότητα αντίστοιχα δεν μαθαίνει καμία πληροφορία για τις τιμές x_j οι οποίες δεν αποτελούν κομμάτι της διασταύρωσης. Αξίζει να αναφερθεί το γεγονός ότι η συγκεκριμένη εφαρμογή παρέχει ασφάλεια στη περίπτωση των παθητικών αντιπάλων, κάτι που μπορεί να έχει μεγαλύτερα επίπεδα δυσκολίας στην περίπτωση των κακόβουλων αντιπάλων, δεδομένης της πιθανής επιλογής τους να χρησιμοποιήσουν διαφορετικό κλειδί k για κάθε στοιχείο (Lindell, 2020). Στη συγκεκριμένη περίπτωση θα έχει τη δυνατότητα να παρατηρήσει ότι η τιμή y_1 αποτελεί στοιχείο της εισόδου αν και μόνο αν ήταν το πρώτο στοιχείο στη λίστα της δεύτερης οντότητας.

⑩ Τα πρωτόκολλα Naive Hashing. Τα συγκεκριμένα πρωτόκολλα χρησιμοποιούνται στην περίπτωση που υπάρχουν δύο οντότητες και θέλουν να συγκρίνουν στοιχεία τους με την βοήθεια των hashes. Πιο συγκεκριμένα, η πρώτη οντότητα υπολογίζει τα hashes των στοιχείων της, τα στέλνει στη δεύτερη οντότητα, και εκείνη

πραγματοποιεί τη σύγκριση, χρησιμοποιώντας τα hashes των δικών της στοιχείων. Αξίζει βέβαια να αναφερθεί, ότι η συγκεκριμένη περίπτωση δεν παρέχει ιδιαίτερα υψηλά επίπεδα ασφάλειας, καθώς η δεύτερη οντότητα μπορεί να πραγματοποιήσει επίθεση brute force για να ανακαλύψει τα στοιχεία της πρώτης.



Εικόνα 5: Naive Hashing Private Set Intersection

Πηγή : " Privacy Preserving analytics Private Set Intersection (PSI)" (Ni Trieu, n.d.)

- Τα πρωτόκολλα Server-Aided PSI. Τα συγκεκριμένα πρωτόκολλα έχουν μεγάλες ομοιότητες με την κατηγορία των Naive Hashing, με τη διαφορά ότι εδώ χρησιμοποιείται μια τρίτη, όχι όμως απόλυτα εμπιστεύσιμη οντότητα. Τα πρωτόκολλα αυτά λειτουργούν με ασφάλεια, με μόνη περίπτωση να υπάρξει κίνδυνος εφόσον κάποια από τις εμπλεκόμενες οντότητες συνωμοτήσει με την τρίτη οντότητα.

- Τα Public key cryptography based PSI πρωτόκολλα. Πρόκειται για μια κατηγορία πρωτοκόλλων PSI, που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού, όπως είναι ο αλγόριθμος Diffie-Hellmann, το πρωτόκολλο του Freedman, τον αλγόριθμο RSA και την ομομορφική κρυπτογράφηση.

- Τα OT based PSI πρωτόκολλα. Η κατηγορία αυτή των πρωτοκόλλων χρησιμοποιεί τα Bloom φίλτρα και τις OT επεκτάσεις. Τα βήματα που ακολουθεί είναι η κρυπτογράφηση των στοιχείων, η αντιστοίχιση τους σε bins, και στη συνέχεια η χρησιμοποίηση του πρωτοκόλλου OT για την παραγωγή τυχαίων masks για τα στοιχεία, κατά τέτοιο τρόπο ώστε η διασταύρωση των masks να αντιστοιχεί στην διασταύρωση των αρχικών στοιχείων εισόδου.

- Τα Circuit based PSI πρωτόκολλα. Τα πρωτόκολλα αυτά χρησιμοποιούν αριθμητικούς ή Boolen circuits, εφαρμόζοντας ουσιαστικά τα Garbled Circuits που είχε εισάγει σαν ιδέα ο Yao.

6.4.2 Η Χρήση της Εφαρμογής Private Set Intersection για Διάγνωση και Ιχνηλάτηση Ασθενειών

Όπως αναφέρθηκε και στο δεύτερο κεφάλαιο, το γενετικό υλικό ενός ανθρώπου, μπορεί να χρησιμοποιηθεί για να διαγνωστεί εάν ο συγκεκριμένος άνθρωπος πάσχει από κάποια ασθένεια, αν έχει προδιάθεση να εμφανίσει κάποια ασθένεια, ποια φαρμακευτική αγωγή θα ήταν κατάλληλη για την περίπτωση του. Παράλληλα όμως, για να υπάρχει απόλυτη νομιμότητα, θα πρέπει το γενετικό υλικό να χρησιμοποιηθεί με κατάλληλο τρόπο, έτσι ώστε να μην παραβιάζεται η ιδιωτικότητα του συγκεκριμένου ανθρώπου (Lindell, 2020). Για παράδειγμα, θα μπορούσε να δώσει ο υποψήφιος ασθενής το γενετικό του υλικό σε κάποια εταιρεία ή νοσοκομείο, για να το συγκρίνει με μία βάση δεδομένων που περιέχει δείγματα γενετικού υλικού με χαρακτηριστικά που παραπέμπουν σε ορισμένες ασθένειες. Παρόλα αυτά, θα πρέπει να διασφαλιστεί ότι η συγκεκριμένη διαδικασία θα πραγματοποιηθεί, χωρίς να μάθει ούτε η εταιρεία ούτε κανένας άλλος πληροφορίες όπως το γενετικό υλικό, ή με ποια ασθένεια ταιριάζει αυτό. Πολλές τεχνικές έχουν προταθεί, αλλά καμία από αυτές δεν κατάφερε να πετύχει. Σε αυτό το σημείο εμφανίζονται οι τεχνικές SMC, που μπορούν να χρησιμοποιηθούν με μεγάλη αποτελεσματικότητα. Μάλιστα μπορεί να χρησιμοποιηθεί μια μεγάλη ποικιλία από αυτές, με βάση την εφαρμογή Private Set Intersection, όπως η ομομορφική κρυπτογράφηση και η τεχνική των Garbled Circuits (Dugan & Zou, 2016). Πιο συγκεκριμένα, η εφαρμογή Private Set Intersection μπορεί να χρησιμοποιηθεί για τη σύγκριση των γενετικών υλικών που αναφέρθηκε στο προηγούμενο παράδειγμα, και τη διασταύρωση τους, χωρίς καμία

διαρροή και παραβίαση της ιδιωτικότητας. Η ομομορφική κρυπτογράφηση μπορεί να χρησιμοποιηθεί με σκοπό την κρυπτογράφηση του γενετικού υλικού και την ανταλλαγή του ανάμεσα στις δύο πλευρές. Τέλος, η τεχνική των Garbled Circuits μπορεί να χρησιμοποιηθεί για τεστ πατρότητας ή για την εύρεση της καταγωγής, με τη χρησιμοποίηση γενετικού υλικού και το "ανακάτωμα" και τη χρησιμοποίηση των εισόδων ,που θα δοθούν από τις δύο πλευρές (εργαστήριο, εξεταζόμενος), σε μια κοινή συνάρτηση για την εύρεση του επιθυμητού αποτελέσματος με ασφάλεια.

Αξίζει να αναφερθεί η δυνατότητα που υπάρχει, να χρησιμοποιηθούν τα πρωτόκολλα που συνδέονται με την εφαρμογή Private Set Intersection για την αντιμετώπιση της πανδημίας του ιού COVID-19 με τη χρήση μιας απλής εφαρμογής στο κινητό τηλέφωνο (Robin Roehm et al., 2020). Πιο συγκεκριμένα, κάθε χρήστης της συγκεκριμένης εφαρμογής, ο οποίος έχει διαγνωστεί θετικός στον ιό από κάποιο νοσοκομείο, θα μπορεί να ανεβάζει το στοιχείο αυτό σε έναν server που θα συνδέεται με την εφαρμογή. Στη συνέχεια, οποιοσδήποτε χρήστης της συγκεκριμένης εφαρμογής, μπορεί να συνδεθεί στον server, και να μάθει διαπιστώσει εάν έχει πρόσφατα έρθει σε επαφή με κάποιο άτομο θετικό στον συγκεκριμένο ιό. Η εφαρμογή PSI είναι αυτό που μπορεί να δώσει λύση στο πρόβλημα της διασταύρωσης των στοιχείων ενός χρήστη με αυτά του server, χωρίς να υπάρξει γνωστοποίηση των λοιπών στοιχείων τα οποία δεν είναι κοινά και στα δύο σύνολα.

6.4.3 Η Εφαρμογή Private Set Intersection για την Εύρεση Σχέσης Διαφημίσεων-Πωλήσεων

Ένα δεύτερο είδος εφαρμογών στο οποίο μπορούν να εφαρμοστούν τα SMC πρωτόκολλα είναι για την καταγραφή της σχέσης που υπάρχει ανάμεσα στις διαφημίσεις και τις πωλήσεις. Η συγκεκριμένη εφαρμογή απαιτεί τη σύγκριση ανάμεσα σε δύο λίστες ατόμων (Ion et al., 2017; Lindell, 2020). Πρόκειται για τη λίστα με τα άτομα στα οποία έγινε η προώθηση και η προβολή των διαφημίσεων και τη λίστα με τα άτομα τα οποία

αγόρασαν τα συγκεκριμένα προϊόντα. Σε περίπτωση που δεν έχει γίνει η αγορά με τη χρήση του διαδικτύου, τότε θα πρέπει να γίνει σύγκριση ανάμεσα στις αντίστοιχες λίστες ατόμων. Το πρόβλημα στη συγκεκριμένη εφαρμογή είναι το γεγονός ότι πρέπει η διασταύρωση να πραγματοποιηθεί, χωρίς να αποκαλυφθεί καμία άλλη πληροφορία εκτός από το μέγεθος της διασταύρωσης. Για το λόγο αυτό μπορεί να χρησιμοποιηθεί η εφαρμογή Private Set Intersection με τη χρήση της τεχνικής της ομομορφικής κρυπτογράφησης. Έτσι λοιπόν μπορούν να βρεθούν όχι μόνο τα κοινά άτομα στις λίστες, αλλά και πόσα χρήματα ξόδεψαν συνολικά αυτά τα άτομα που προχώρησαν στις αγορές αφού είδαν τις διαφημίσεις (Ion et al., 2017). Αξίζει να αναφερθεί το γεγονός ότι το συγκεκριμένο πρωτόκολλο έχει ήδη χρησιμοποιηθεί για αυτό τον σκοπό από πολλές εταιρείες, ανάμεσα τους και η Google.

Μία χαρακτηριστική περίπτωση, που μπορεί να χρησιμοποιηθεί η εφαρμογή Private Set Intersection, και έχει να κάνει με διαφημίσεις, είναι αυτή στην περίπτωση του Facebook σχετικά με την διαδικασία του προσαρμοσμένου κοινού (custom audience) που εφαρμόζει (Facebook Security, 2013; Πληροφορίες για την κωδικοποίηση στοιχείων πελατών με hash, n.d.). Πιο συγκεκριμένα, ένας πιθανός διαφημιστής, ακολουθεί την εξής διαδικασία :

- Ανεβάζει στον browser του μία λίστα με τις διευθύνσεις e-mail ή τα τηλέφωνα των ατόμων στα οποία θέλουν να στείλουν διαφημίσεις.

- Ο browser δημιουργεί τα hashes όλων αυτών των στοιχείων, τοπικά στον υπολογιστή.

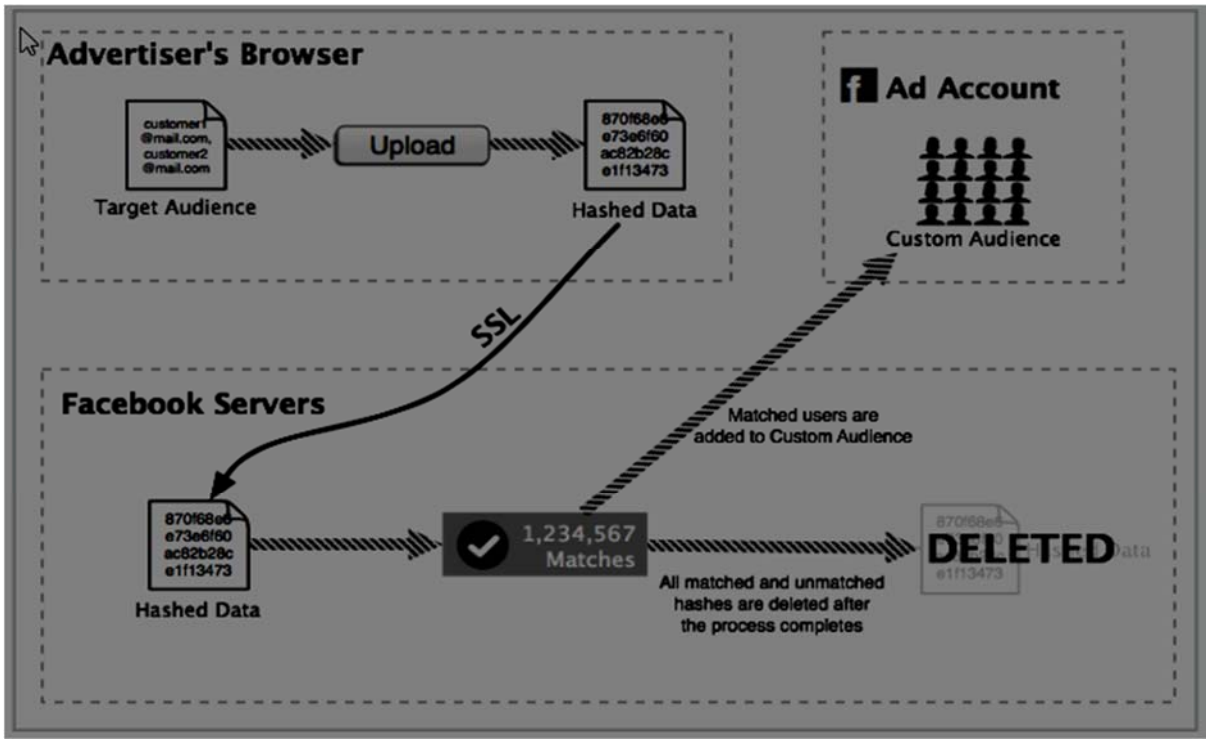
- Στη συνέχεια συνδέεται μέσω SSL με τους αντίστοιχους λογαριασμούς των χρηστών στο Facebook, προχωράει στην αυθεντικοποίηση και στη συνέχεια παρέχει τη λίστα των hashes στην εφαρμογή που προωθεί τις διαφημίσεις.

Από την άλλη μεριά, το Facebook προχωράει στην εξής διαδικασία :

- Έχει αρχικά προϋπολογίσει τα hashes για κάθε χρήστη και προχωράει στη σύγκριση της λίστας αυτών των hashes με τη λίστα που έχει λάβει από τους διαφημιστές.

- Για τα hashes τα οποία ταιριάζουν, οι αντίστοιχοι χρήστες του Facebook χαρακτηρίζονται ως προσαρμοσμένο κοινό (custom audience), στους οποίους στέλνονται τελικά οι διαφημίσεις.

Η παραπάνω διαδικασία φαίνεται συνοπτικά και στο ακόλουθο σχήμα :



Σχήμα 6: Διαδικασία δημιουργίας προσαρμοσμένου κοινού (Custom Audience) ,

Πηγή : " Custom Audiences: Data Security Overview", (Facebook Security, 2013)

Για λόγους ιδιωτικότητας, το Facebook αναφέρει ότι μετά το πέρας αυτής της διαδικασίας, όλα τα hashes διαγράφονται και η μόνη πληροφορία που μπορεί να δουν οι διαφημιστές είναι ο αριθμός των χρηστών που έχουν αντιστοιχηθεί. Παρόλα αυτά εγείρονται αμφιβολίες σχετικά με το κατά πόσο μπορεί να είναι ασφαλής η παραπάνω διαδικασία, χωρίς να διαρρεύσουν τα προσωπικά στοιχεία των χρηστών – έρευνες έχουν καταδείξει ότι γνωρίζοντας το ψηφιακό αποτύπωμα μίας ηλεκτρονικής διεύθυνσης,

υπάρχει σοβαρή πιθανότητα να μπορεί κανείς να βρει την ηλεκτρονική διεύθυνση αυτή (Demir et al., 2018) . Σε αυτό το σημείο έρχεται λοιπόν η εφαρμογή Private Set Intersection. Δεδομένου ότι το Facebook δεν χρησιμοποιεί την βέλτιστη από άποψη ιδιωτικότητας υλοποίηση που μπορεί να εφαρμοστεί, μπορεί να χρησιμοποιήσει το Private Set Intersection, με σκοπό να προχωρήσει στην ασφαλή διασταύρωση των κοινών στοιχείων που υπάρχουν ανάμεσα στις δύο λίστες, των διαφημιστών και του Facebook, χωρίς να υπάρξει κάποια απρόοπτη διαρροή πληροφοριών από καμία πλευρά. Εδώ πρόκειται για μία χαρακτηριστική ρεαλιστική περίπτωση όπου φαίνεται ότι δεν υπάρχει συμμόρφωση με την αρχή της προστασίας δεδομένων από το σχεδιασμό (data protection by design), με αποτέλεσμα να καταστρατηγείται και η αρχή της ελαχιστοποίησης των δεδομένων.

6.5 Η Χρήση των Τεχνικών SMC στο Διαδίκτυο των Πραγμάτων

Αποτελεί πραγματικότητα το γεγονός ότι τα τελευταία χρόνια, τα έξυπνα περιβάλλοντα, τα οποία περιλαμβάνουν διάφορες συσκευές και αισθητήρες, έχουν εισέλθει στην καθημερινή ζωή των ανθρώπων. Όλα αυτά έξυπνα περιβάλλοντα, τα οποία αποτελούν σημαντικό κομμάτι του Διαδικτύου των Πραγμάτων (IoT), λειτουργούν συλλέγοντας πληροφορίες (von Maltitz & Carle, 2018). Αυτές μπορεί να είναι πληροφορίες, αποτελούν δεδομένα τα οποία στέλνονται για επεξεργασία. Προκύπτουν όμως διάφορα ζητήματα, τα οποία έχουν να κάνουν με την ιδιωτικότητα και την προστασία αυτών των προσωπικών δεδομένων. Για παράδειγμα, τα δεδομένα αφού συλλεχθούν από τους αισθητήρες, και πριν να προωθηθούν στις διάφορες υπηρεσίες σχετικά με την κατανάλωση των δεδομένων, πρέπει να αποθηκευτούν και να αναλυθούν από μία τρίτη πλευρά. Στη φάση αυτή λοιπόν υπάρχει ο κίνδυνος να χαθούν, να προωθηθούν σε λάθος προορισμό, να γίνουν στόχος επίθεσης ή να χρησιμοποιηθούν για αμφίβολους σκοπούς. Για το λόγο αυτό, και για την αποφυγή χρησιμοποίησης μιας τρίτης οντότητας και για να προστατευτούν τα δεδομένα, μπορούν να χρησιμοποιηθούν μηχανισμοί και τεχνικές SMC. Η τρίτη οντότητα μπορεί να αντικατασταθεί από μία πύλη, η οποία δεν έρχεται σε επαφή με τα δεδομένα, δηλαδή δεν αποκτά πρόσβαση σε αυτά (von Maltitz & Carle, 2018). Αυτό που κάνει είναι να διαχειρίζεται την ροή των δεδομένων με σκοπό να

εκτελεστούν οι υπολογισμοί SMC. Ταυτόχρονα είναι υπεύθυνη και για τον χειρισμό των συνεδριών των SMC υπολογισμών, αφού προσδιορίζει όλες τις διαστάσεις της συνεδρίας, και τις προωθεί στον μηχανισμό. Προωθεί δηλαδή την ταυτότητα και τα σημεία σύνδεσης των συνεργατών, τα δεδομένα που θα επεξεργαστούν καθώς και το πρωτόκολλο που θα χρησιμοποιηθεί. Στη συνέχεια διαχειρίζεται τον ίδιο τον υπολογισμό. Σε περίπτωση που ο υπολογισμός είναι επιτυχημένος, λαμβάνει το αποτέλεσμα και τα προωθεί, ενώ σε αντίθετη περίπτωση προσπαθεί να ανακτήσει και να επανεκκινήσει την συνεδρία που απέτυχε. Με την χρήση λοιπόν τον μηχανισμών SMC, μπορεί με μεγαλύτερη ασφάλεια να γίνει επεξεργασία δεδομένων που προέρχονται από έξυπνα περιβάλλοντα.

Αν και στο (von Maltitz & Carle, 2018) δεν περιγράφεται συγκεκριμένη περίπτωση εφαρμογής SMC πρωτοκόλλων σε IoT εφαρμογές, καθίσταται εν τούτοις σαφές ότι τα περιθώρια είναι πολλά. Σε αυτήν την κατεύθυνση εξάλλου κινείται και η νέα πρόταση που παρουσιάζει η παρούσα διατριβή στο Κεφάλαιο 8 στη συνέχεια.

6.6 Η Προστασία των Κρυπτογραφικών Κλειδιών

Μία πολύ σημαντική εφαρμογή των SMC αποτελεί η δυνατότητα που παρέχουν για προστασία των κλειδιών που χρησιμοποιούνται στην κρυπτογράφηση. Χαρακτηριστικό παράδειγμα αποτελεί η τεχνική Threshold Cryptography, η οποία μπορεί να χρησιμοποιηθεί σε διάφορες περιπτώσεις κρυπτογραφικών υπολογισμών, όπως η αποκρυπτογράφηση και η υπογραφή, χωρίς το ιδιωτικό κλειδί να βρίσκεται σε ένα μόνο μέρος (Lindell, 2020). Η τεχνική αυτή χρησιμοποιείται σε μεγάλο ποσοστό από πολλές εταιρείες, οι οποίες προτιμούν τη χρήση αυτής, παρά τη χρήση άλλου είδους εξοπλισμών. Όπως αναφέρθηκε και στην ενότητα 5.6, σε αντίθεση με περιπτώσεις άλλων τεχνικών, στη συγκεκριμένη δεν υπάρχει μόνο μία οντότητα που να έχει την δυνατότητα να αποκρυπτογραφήσει το μήνυμα, αλλά αντίθετα το ιδιωτικό κλειδί διαμοιράζεται σε πολλές οντότητες, με απαραίτητη προϋπόθεση την συμμετοχή ενός υποσυνόλου αυτών για να πραγματοποιηθεί η αποκρυπτογράφηση (Ευστάθιος Ζάχος et al., 2015). Πιο συγκεκριμένα, η κάθε εταιρεία χρησιμοποιεί τον μηχανισμό SMC, για να παράγει κλειδιά και να εκτελέσει τους υπολογισμούς, χωρίς το κλειδί να αποθηκεύεται σε ένα συγκεκριμένο μέρος, όπου μπορεί να υπάρχει ο κίνδυνος να κλαπεί. Έτσι, εφαρμόζοντας

τον διαμερισμό του κλειδιού σε πολλά μέρη, αυτόματα καθίσταται εξαιρετικά δυσχερής η κλοπή όλων αυτών (Lindell, 2020).

Μία δεύτερη περίπτωση χρήσης της συγκεκριμένης τεχνικής είναι για την προστασία των κλειδιών που χρησιμοποιούνται για τις υπογραφές για την προστασία των κρυπτονομισμάτων και άλλων παρόμοιων τεχνολογιών (Lindell, 2020). Αυτό επιτυγχάνεται με το διαμερισμό των κλειδιών ανάμεσα σε πελάτες και παραγωγούς, καθιστώντας πιο ασφαλή τις ηλεκτρονικές συναλλαγές, ενισχυμένες με αυστηρές πολιτικές, προκειμένου να επιτραπεί μία τέτοιου είδους συναλλαγή.

Χαρακτηριστικό είναι το παράδειγμα της εταιρείας Dyadic, που χρησιμοποιεί τη συγκεκριμένη τεχνική, μοιράζοντας το μυστικό κλειδί σε πολλές πλευρές, γεγονός που καθιστά δύσκολο το έργο οποιουδήποτε επιτιθέμενου (Peeter Laud & Liina Kamm, 2015). Επομένως όλες οι λειτουργίες οι οποίες μπορεί να απαιτούν αυτό το κλειδί, όπως για παράδειγμα η υπογραφή ή η δημιουργία σύνδεσης SSL / TLS ή άλλου τύπου κρυπτογράφησης, μπορούν να πραγματοποιηθούν με τη χρήση των μηχανισμών SMC για το διαμερισμό του κλειδιού. Αξίζει να αναφερθεί ότι το σύστημα αυτό μπορεί να χρησιμοποιηθεί για τον έλεγχο της ορθότητας του κωδικού πρόσβασης κατά τη σύνδεση, έτσι ώστε η ίδια η βάση δεδομένων χρήστη-κωδικού πρόσβασης να είναι κοινόχρηστη.

6.7 Οι Τεχνικές SMC στο Bitcoin

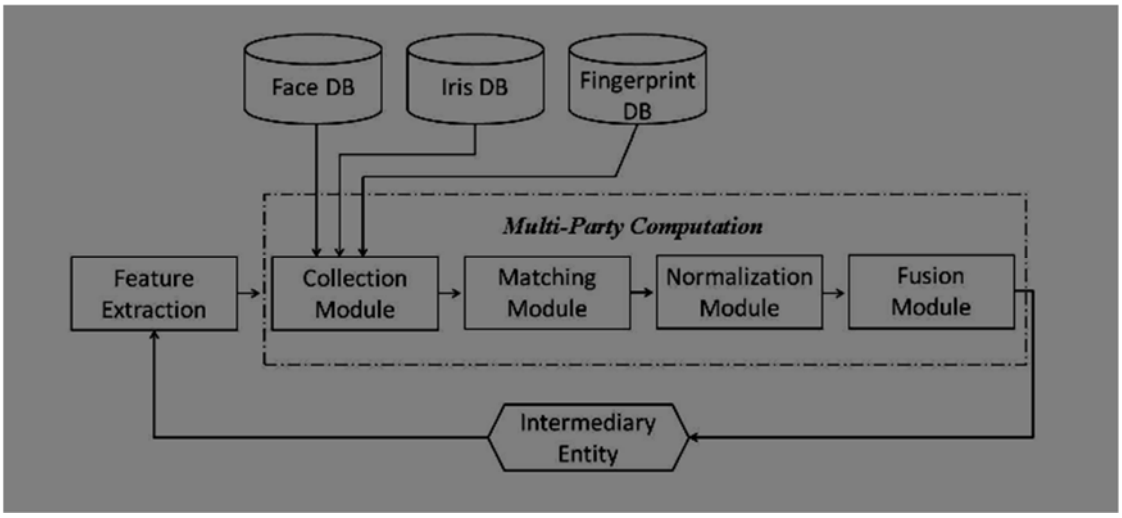
Οι τεχνικές SMC μπορούν να εφαρμοστούν στην περίπτωση που χρειάζεται να πουληθούν μυστικές πληροφορίες σχετικά με το Bitcoin (Andrychowicz et al., 2014). Έστω ότι υπάρχουν για παράδειγμα δύο άτομα, η Alice και ο Bob, οι οποίοι γνωρίζουν ότι το σετ X περιέχει κάποιες πολύτιμες πληροφορίες, όπως για παράδειγμα δεδομένα τα οποία είναι υπογεγραμμένα με τη χρήση ενός μυστικού κλειδιού από μια δημόσια αρχή. Έστω ότι η Alice γνωρίζει ένα υποσύνολο A του X και ο Bob ένα υποσύνολο B του X. Ο στόχος και των δύο είναι να πουλήσουν ο ένας στον άλλο τα στοιχεία που περιέχονται

στην ένωση A U B, κατά τέτοιο τρόπο ώστε ο κάθε ένας να πληρώσει μόνο για τα στοιχεία που περιέχονται στην ένωση, αλλά δεν ανήκουν στο σύνολο που γνωρίζουν. Με μια πιο μαθηματική ματιά, η Alice θα πρέπει να πληρώσει στον Bob το |B\A| - |A\B| σε Bitcoin. Σε περίπτωση που η τιμή αυτή είναι αρνητική, τότε θα πρέπει ο Bob να πληρώσει τη συγκεκριμένη αρνητική τιμή. Η συγκεκριμένη περίπτωση όμως έχει το πρόβλημα ότι σε περίπτωση που η Alice φανερώσει στον Bob ένα στοιχείο του συνόλου A, τότε αυτός μπορεί να ισχυριστεί ότι το γνωρίζει. Για το λόγο αυτό μπορούν να χρησιμοποιηθούν μηχανισμοί SMC, όπως το πρωτόκολλο που έχει προταθεί, σύμφωνα με το οποίο μπορεί να επιτευχθεί η ακριβής μεταφορά των ποσών των Bitcoin, και μάλιστα αυτό να συμβαίνει αν και μόνο αν και οι δύο πλευρές μαθαίνουν την αληθινή έξοδο του υπολογισμού (Andrychowicz et al., 2014).

6.8 Η Χρήση Τεχνικών SMC στην Αυθεντικοποίηση Μέσω Βιομετρικών Χαρακτηριστικών

Οι μέθοδοι αυθεντικοποίησης με τη χρήση βιομετρικών χαρακτηριστικών, όπως για παράδειγμα με την αναγνώριση προσώπου, θεωρούνται ότι είναι από τις πιο έγκυρες μεθόδους. Παρ' όλα αυτά, υπάρχει κάποιες ανησυχίες σχετικά με το κατά πόσο καταπατείται η ιδιωτικότητα σε αυτή την περίπτωση. Πιο συγκεκριμένα, ας υποθέσουμε ότι χρειάζεται να γίνει αυθεντικοποίηση ενός ατόμου. Στη περίπτωση αυτή, το άτομο αυτό κατέχει ένα βιομετρικό χαρακτηριστικό, το οποίο θα πρέπει να ταυτοποιηθεί και να ταιριάξει με το αντίστοιχο βιομετρικό χαρακτηριστικό που υπάρχει σε μια βάση δεδομένων, που κατέχει τα βιομετρικά χαρακτηριστικά αυτών που επιτρέπεται να αποκτήσουν πρόσβαση. Στον πραγματικό κόσμο, μια τέτοια περίπτωση αυθεντικοποίησης, θα μπορούσε να χρησιμοποιείται για την αυθεντικοποίση των ατόμων που έχουν δικαίωμα πρόσβασης σε απόρρητα δεδομένα μιας εταιρείας. Όμως δεδομένου ότι τα δεδομένα βιομετρικού χαρακτήρα αποτελούν ευαίσθητα δεδομένα σύμφωνα με τον GDPR, απαιτούνται ακόμα μεγαλύτερες δικλείδες ασφαλείας για τη νόμιμη χρήση τους και την ασφάλειά τους. Επομένως προκύπτει το συμπέρασμα ότι η διαδικασία αυτή, θα πρέπει να μπορεί να επιτευχθεί, χωρίς να αποκαλυφθούν ούτε τα βιομετρικά χαρακτηριστικά του ατόμου, ούτε όμως και η διαδικασία αυθεντικοποίησης. Για το λόγο αυτό, έχει προταθεί η χρησιμοποίηση τεχνικών SMC, με σκοπό να

επιτευχθούν υψηλά επίπεδα ασφάλειας, μέσω της κρυπτογράφησης και της διανομής τόσο των δεδομένων όσο και των κλειδιών, ή με τη χρήση μεθόδων για διασταύρωση στοιχείων μιας λίστας με άλλα στοιχεία. Χαρακτηριστικά, μπορούν να χρησιμοποιηθούν οι τεχνικές Oblivious Transfer, Garbled Circuits, Private Set Intersection, καθώς και η Ομομορφική Κρυπτογράφηση. (Bringer et al., 2013)



Σχήμα 7: Πρωτόκολλα Ασφαλών Υπολογισμών Πολλών Συμμετεχόντων για βιομετρική αυθεντικοποίηση,

Πηγή : "Privacy-Preserving Multibiometric Authenticationin Cloud with Untrusted Database Providers", (Christina-Angeliki Toli, et al., n.d.)

Κεφάλαιο 7

Τεχνική διαμοιρασμού μυστικού του Shamir: Περαιτέρω ανάλυση

Στο συγκεκριμένο κεφάλαιο δίνεται ιδιαίτερη έμφαση στην τεχνική διαμοιρασμού μυστικού του Shamir (Shamir Secret Sharing (SSS)). Πιο συγκεκριμένα, αρχικά θα παρουσιαστούν αποτελέσματα πειραμάτων που εκτελέστηκαν στο πλαίσιο της διατριβής, καθώς και συναφείς παρατηρήσεις που έγιναν σχετικά με τους χρόνους εκτέλεσης της συγκεκριμένης τεχνικής, προκειμένου να αποτυπωθεί η αποτελεσματικότητά της, για διάφορες παραμέτρους, ακόμα και σε συμβατικό υπολογιστή. Περαιτέρω, με εφαλτήριο μία πολύ πρόσφατη έρευνα (Bezzateev et al., 2020), θα διερευνηθεί και θα παρουσιαστεί μία διαφοροποίηση της τεχνικής η οποία βασίζεται στη χρήση παρεμβολής Newton αντί για Langrange. Η εν λόγω διαφοροποίηση μπορεί να επιφέρει σημαντικά πλεονεκτήματα σε ορισμένες περιπτώσεις, όπως θα αναλυθεί και στο επόμενο κεφάλαιο.

7.1 Πειραματικό Περιβάλλον Αποτίμησης Απόδοσης της Τεχνικής SSS

Στο παρόν κεφάλαιο της διατριβής, επιχειρήθηκε μία εκτίμηση των χρόνων εκτέλεσης της τεχνικής του Shamir. Ως υλοποίηση της τεχνικής, χρησιμοποιήθηκε μία έκδοση ενός εργαλείου, η οποία αποτελείται από command line εντολές.
Ο όρος “shares” που χρησιμοποιείται, αναφέρεται στον αριθμό των τμημάτων του μηνύματος που δημιουργούνται με τη χρήση της τεχνικής και το “threshold” (τιμή κατωφλίου”) στον αριθμό αυτών που, αν συνδυαστούν, μπορούν να οδηγήσουν στην επανάκτηση του αρχικού μηνύματος.

Όπως διαπιστώθηκε, ο αριθμός των thresholds που ορίστηκε για να χρησιμοποιηθεί αργότερα στην ανακατασκευή του αρχικού μηνύματος, δεν επηρεάζει ουσιαστικά τον χρόνο εκτέλεσης της εντολής για τη δημιουργία των shares. Παρ’ όλα αυτά, πραγματοποιήθηκε μία καταγραφή ενδεικτικών τιμών shares, προκειμένου να γίνει φανερή οποιαδήποτε διαφορά.

Απαραίτητη (και προφανής) προϋπόθεση που πρέπει να ισχύει είναι ο αριθμός των threshold να είναι μικρότερος ή ίσος του αριθμού των shares.

Το κατά πόσο θα είναι μεγαλύτερος ο συνολικός αριθμός των shares σε σχέση με αυτά που θα χρησιμοποιηθούν για την ανακατασκευή του μηνύματος δεν επηρεάζει ουσιαστικά τον χρόνο ανακατασκευής. Για τον λόγο αυτό στην ανακατασκευή ορίστηκαν να χρησιμοποιηθούν όλα ή τα περισσότερα shares για την ανακατασκευή.

Το ανώτατο επιτρεπόμενο όριο δημιουργίας shares που επιτρέπει το συγκεκριμένο εργαλείο είναι 255 στον αριθμό.

Το μέγεθος των shares που δημιουργείται εξαρτάται από το μέγεθος του αρχικού μηνύματος, όχι όμως από τον αριθμό των shares που επιλέχθηκαν να δημιουργηθούν. Όσα shares και να επιλεχθούν να δημιουργηθούν, θα έχουν μεταξύ τους το ίδιο μέγεθος.

Η τελευταία command line εντολή παίρνει τα x (που ορίστηκαν) πρώτα shares για την ανακατασκευή.

Χρησιμοποιείται, για την μέτρηση του χρόνου, πριν από την εκτέλεση κάθε εντολής η λέξη **time**. Ο συγκεκριμένος χρόνος, που μετρήθηκε με αυτή την εντολή, αναφέρεται στη χρονική διάρκεια από την επιλογή του “enter” για να τρέξει η συγκεκριμένη εντολή, μέχρι η συγκεκριμένη εντολή να ολοκληρωθεί. Οι χρόνοι που καταγράφηκαν αναφέρονται σε μεγέθη μικρότερα του 1 sec. Ο συγκεκριμένος χρόνος μπορεί να επηρεαστεί από διάφορους παράγοντες, όπως το αν υπάρχουν και άλλα παράθυρα, ή διεργασίες που εκτελούνται στο background. Επιπλέον οι διαφορές που καταγράφονται, αναφέρονται σε επίπεδα εκατοστών και χιλιοστών του δευτερολέπτου. Για το λόγο αυτό παρατηρήθηκε ότι οι εκτελέσεις ίδιας εντολής έδιναν κάθε φορά διαφορετικά

αποτελέσματα. Σε γενικές γραμμές οι αποκλίσεις που υπάρχουν στις διάφορες περιπτώσεις μηνυμάτων, shares και shares που συνδυάζονται, είναι πάρα πολύ μικρές. Αν γινόταν προσπάθεια για καταγραφή των χρόνων ως προς τα δέκατα ή τα εκατοστά των δευτερολέπτων μόνο, οι διαφορές θα ήταν μικρές και δε θα μπορούσαν να είναι εμφανής. Για το λόγο αυτό σε κάθε μήνυμα και σε κάθε περίπτωση shares και threshold, πραγματοποιήθηκε καταγραφή τριών χρόνων που προκύπτουν από τρεις απανωτές εκτελέσεις της ίδιας εντολής, διατηρώντας ουσιαστικά την ίδια κατάσταση ως προς τις διεργασίες που πραγματοποιούνται.

Αξίζει να τονιστεί ότι ο δημιουργός του εργαλείου αναφέρει στην περίπτωση των command line εντολών, ότι πρέπει να οριστούν τα k πρώτα shares για να ανακατασκευαστεί το αρχικό μήνυμα. Παρ' όλα αυτά, επιχειρήθηκε να αλλάξει η σειρά των shares στο αρχείο shares.txt , χωρίς να προκύψει κάποιο διαφορετικό αποτέλεσμα.

Η όλη διαδικασία πραγματοποιήθηκε με τη χρήση ηλεκτρονικού υπολογιστή, και πιο συγκεκριμένα με τη χρήση εικονικού περιβάλλοντος. Τα χαρακτηριστικά φαίνονται στον παρακάτω πίνακα

Μοντέλο Η/Υ : Dell Inspiron 5570
Επεξεργαστής Η/Υ : Intel® Core(TM) i7 – 7500U CPU @ 2.70 GHz , 2904Mhz
Λειτουργικό Σύστημα : Microsoft Windows 10 Home
Χωρητικότητα : 224 GB

Πίνακας 2: Χαρακτηριστικά Η/Υ

Λειτουργικό Σύστημα Εικονικού μηχανήματος : Ubuntu 20.10 (63-bit)
Βασική Μνήμη : 4500 MB

Επεξεργαστές : 2
Κάρτα δικτύου 1 : Intel PRO/1000 MT Desktop (Γεφυρωμένη κάρτα, Intel® Dual Band Wireless -AC 3165

Πίνακας 3: Χαρακτηριστικά εικονικού μηχανήματος Ubuntu

7.1.1 Εκτίμηση Χρόνων για τη Δημιουργία των Shares

Στη συνέχεια, θα γίνει παρουσίαση των χρόνων που υπολογίστηκαν, για τη δημιουργία των shares, για τέσσερα διαφορετικά μεγέθη μηνυμάτων. Αξίζει να τονιστεί ότι ο όρος threshold αναφέρεται στον αριθμό των shares που ορίστηκαν στην αρχή ότι θα χρησιμοποιηθούν αργότερα για την ανακατασκευή του μηνύματος.

Για τον υπολογισμό των χρόνων με τη χρήση των command line εντολών, χρησιμοποιήθηκε η εντολή **time echo "arxiko mhnuma" | secret-share-split -n arithmosshares -t arithmosthreshold >shares.txt**

Μήνυμα : Hello!

Μέγεθος μηνύματος : 6 bytes

Ανώτατο όριο shares : 255

Threshold																			
	2			8			30			100			150			255			
Sha-res	Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			
2	0.003	0.003	0.003																
3	0.003	0.003	0.004																
4	0.003	0.004	0.003																

5	0.003	0.003	0.003															
8	0.003	0.003	0.003															
10	0.003	0.003	0.004	0.003	0.003	0.004												
15	0.003	0.003	0.004	0.003	0.003	0.003												
20	0.003	0.003	0.003	0.004	0.003	0.003												
30	0.004	0.003	0.003	0.003	0.003	0.004	0.004	0.003	0.004									
50	0.003	0.004	0.004	0.004	0.004	0.004	0.004	0.004	0.004									
75	0.004	0.004	0.004	0.005	0.003	0.004	0.003	0.005	0.004									
100	0.004	0.004	0.005	0.004	0.005	0.004	0.004	0.005	0.005	0.005	0.006	0.005						
150	0.004	0.005	0.005	0.004	0.005	0.006	0.006	0.005	0.005	0.006	0.007	0.007	0.007	0.008	0.007			
200	0.005	0.006	0.006	0.006	0.006	0.005	0.007	0.006	0.006	0.007	0.007	0.008	0.008	0.008	0.008			
255	0.007	0.007	0.006	0.005	0.006	0.007	0.006	0.007	0.007	0.009	0.008	0.008	0.008	0.010	0.010	0.011	0.012	0.012

Πίνακας 4: Εκτίμηση χρόνων για τη δημιουργία shares, για μήνυμα μεγέθους 6 bytes, με τη χρήση των Command Line εντολών.

Μήνυμα : My name is Konstantinos Michos

Μέγεθος μηνύματος : 30 bytes

Ανώτατο όριο shares : 255

	Threshold																	
	2			8			30			100			150			255		
Sha-res	Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)		
2	0.005	0.003	0.003															
3	0.003	0.003	0.003															

4	0.003	0.003	0.005															
5	0.011	0.004	0.003															
8	0.003	0.003	0.003	0.004	0.004	0.003												
10	0.003	0.003	0.003	0.004	0.003	0.003												
15	0.004	0.003	0.003	0.004	0.003	0.003												
20	0.003	0.004	0.003	0.003	0.004	0.004												
30	0.004	0.004	0.003	0.003	0.004	0.004	0.004	0.003	0.004									
50	0.004	0.005	0.004	0.005	0.004	0.004	0.004	0.004	0.004									
75	0.005	0.004	0.004	0.005	0.003	0.003	0.005	0.004	0.005									
100	0.005	0.005	0.005	0.004	0.004	0.005	0.004	0.005	0.005	0.006	0.006	0.006						
150	0.006	0.006	0.006	0.006	0.006	0.006	0.007	0.006	0.007	0.006	0.008	0.008	0.006	0.007	0.008			
200	0.006	0.005	0.006	0.007	0.007	0.007	0.007	0.007	0.007	0.008	0.008	0.008	0.009	0.010	0.009			
255	0.009	0.008	0.008	0.008	0.010	0.008	0.008	0.008	0.008	0.010	0.010	0.009	0.010	0.010	0.009	0.013	0.013	0.013

Πίνακας 5: Εκτίμηση χρόνων για τη δημιουργία shares,για μήνυμα μεγέθους 30 bytes, με τη χρήση των Command Line εντολών.

Μήνυμα : My name is Konstantinos Michos and this is my dissertation for my master in Cybersecurity

Μέγεθος μηνύματος : 89 bytes

Ανώτατο όριο shares : 255

	Threshold																	
	2			8			30			100			150			255		
Sha-res	Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)		
2	0.004	0.003	0.003															

3	0.004	0.003	0.003															
4	0.004	0.004	0.004															
5	0.004	0.003	0.003															
8	0.004	0.003	0.003	0.003	0.004	0.004												
10	0.003	0.003	0.003	0.003	0.003	0.003												
15	0.003	0.004	0.003	0.004	0.004	0.004												
20	0.005	0.004	0.003	0.004	0.004	0.004												
30	0.005	0.006	0.004	0.004	0.004	0.003	0.004	0.004	0.004									
50	0.005	0.005	0.005	0.004	0.005	0.005	0.005	0.004	0.005									
75	0.005	0.005	0.005	0.005	0.005	0.005	0.005	0.005	0.005									
100	0.006	0.006	0.006	0.006	0.005	0.006	0.005	0.006	0.006	0.006	0.007	0.007						
150	0.007	0.007	0.007	0.008	0.006	0.008	0.006	0.008	0.008	0.010	0.009	0.008	0.009	0.010	0.009			
200	0.009	0.008	0.008	0.009	0.009	0008	0.012	0.013	0.009	0.010	0.011	0.009	0.011	0.011	0.011			
255	0.011	0.009	0.010	0.010	0.013	0.011	0.011	0.011	0.012	0.012	0.013	0.012	0.011	0.013	0.013	0.015	0.018	0.022

Πίνακας 6: Εκτίμηση χρόνων για τη δημιουργία shares, για μήνυμα μεγέθους 89 bytes, με τη χρήση των Command Line εντολών.

Μήνυμα : My name is Konstantinos Michos and this is my dissertation for my master in Cybersecurity The theme is secure multiparty computations protocols and techniques that can be used for the safe execution of computations between two or more parties in order to ensure that they should learn only their output and nothing more such as information about the other parties and their inputs

Μέγεθος μηνύματος : 380 bytes

Ανώτατο όριο shares : 255

Threshold

	2			8			30			100			150			255		
Sha-res	Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)		
2	0.003	0.003	0.003															
3	0.004	0.004	0.003															
4	0.004	0.003	0.003															
5	0.004	0.004	0.004															
8	0.003	0.004	0.004	0.004	0.004	0.004												
10	0.004	0.003	0.004	0.003	0.003	0.005												
15	0.004	0.004	0.004	0.005	0.005	0.005												
20	0.004	0.005	0.005	0.004	0.005	0.004												
30	0.005	0.005	0.005	0.006	0.006	0.005	0.006	0.004	0.005									
50	0.007	0.007	0.008	0.006	0.007	0.007	0.007	0.006	0.008									
75	0.009	0.009	0.009	0.010	0.009	0.008	0.009	0.007	0.009									
100	0.011	0.010	0.011	0.010	0.010	0.010	0.011	0.011	0.011	0.011	0.011	0.010						
150	0.015	0.014	0.014	0.012	0.015	0.015	0.017	0.014	0.016	0.014	0.016	0.016	0.013	0.016	0.016			
200	0.017	0.019	0.015	0.017	0.016	0.018	0.018	0.017	0.017	0.019	0.018	0.020	0.020	0.019	0.020			
255	0.021	0.021	0.020	0.026	0.022	0.021	0.020	0.019	0.021	0.022	0.021	0.024	0.024	0.022	0.021	0.028	0.022	0.024

Πίνακας 7: Εκτίμηση χρόνων για τη δημιουργία shares, για μήνυμα μεγέθους 380 bytes, με τη χρήση των Command Line εντολών.

Το συμπέρασμα που προκύπτει από παρατήρηση των παραπάνω πινάκων, είναι ότι υπάρχει μία αύξηση στον χρόνο που χρειάζεται το σύστημα για να εκτελέσει τη συγκεκριμένη εντολή, όσο αυξάνεται τόσο ο αριθμός των shares που επιθυμούμε να δημιουργηθούν. Επιπλέον, σε αύξηση στον χρόνο εκτέλεσης οδηγεί ο αριθμός των thresholds που ορίζονται, δηλαδή του αριθμού των shares που θα χρειαστούν για την ανακατασκευή του μηνύματος. Τέλος, μετά την εξέταση και την εφαρμογή της εντολής σε 4 μηνύματα διαφορετικού μεγέθους, προέκυψε η παρατήρηση ότι σημαντική επιρροή στον χρόνο εκτέλεσης ασκεί το μέγεθος του αρχικού μηνύματος που θα επιλεγεί.

7.1.2 Εκτίμηση Χρόνων για την Ανακατασκευή του Αρχικού Μηνύματος

Στη συνέχεια, υλοποιήθηκε μία προσπάθεια για εκτίμηση του χρόνου για την ανακατασκευή του αρχικού μηνύματος με την χρήση των command line εντολών. Αυτό πραγματοποιήθηκε με τον συνδυασμό ενός υποσυνόλου (shares combined - SCM) όλων των shares (total shares created - TSCR) που προέκυψαν από την εκτέλεση της πρώτης εντολής. Η διαδικασία επαναλήφθηκε και πάλι για τέσσερα διαφορετικά μηνύματα διαφορετικών μεγεθών, προκειμένου να προκύψουν τα απαραίτητα συμπεράσματα.

Για τον υπολογισμό των χρόνων με τη χρήση των command line εντολών, χρησιμοποιήθηκε η εντολή **time head -n arithmosthreshold shares.txt | secret-share-combine.**

Μήνυμα : Hello! **Μέγεθος μηνύματος :** 6 bytes **Ανώτατο όριο shares :** 255						
Shares Combined						
	2	8	30	100	150	255
TSCR	Time (sec.)	Time (sec.)	Time (sec.)	Time (sec.)	Time (sec.)	Time (sec.)

2	0.016	0.003	0.002															
3	0.002	0.003	0.002															
4	0.002	0.002	0.002															
5	0.003	0.002	0.002															
8	0.003	0.003	0.002	0.002	0.003	0.003												
10	0.003	0.003	0.003	0.003	0.003	0.003												
15	0.003	0.003	0.003	0.003	0.003	0.003												
20	0.003	0.002	0.002	0.004	0.004	0.002												
30	0.002	0.003	0.002	0.003	0.003	0.002	0.003	0.003	0.003									
50	0.003	0.002	0.003	0.003	0.003	0.003	0.003	0.003	0.003									
75	0.003	0.003	0.002	0.004	0.002	0.003	0.003	0.003	0.003									
100	0.002	0.003	0.002	0.003	0.003	0.002	0.003	0.003	0.003	0.004	0.004	0.003						
150	0.003	0.003	0.002	0.003	0.002	0.003	0.003	0.003	0.004	0.004	0.004	0.003	0.005	0.005	0.005			
200	0.002	0.002	0.003	0.002	0.003	0.002	0.003	0.002	0.003	0.003	0.004	0.004	0.005	0.006	0.005			
255	0.003	0.002	0.003	0.003	0.003	0.002	0.003	0.003	0.002	0.004	0.004	0.003	0.004	0.004	0.005	0.024	0.008	0.008

Πίνακας 8: Εκτίμηση χρόνων για την ανακατασκευή του αρχικού μηνύματος μεγέθους 6 bytes, με τη χρήση των Command Line εντολών.

Μήνυμα : My name is Konstantinos Michos

Μέγεθος μηνύματος : 30 bytes

Ανώτατο όριο shares : 255

	Shares Combined					
	2	8	30	100	150	255
TSCR	Time (sec.)	Time (sec.)	Time (sec.)	Time (sec.)	Time (sec.)	Time (sec.)

2	0.003	0.003	0.003															
3	0.004	0.003	0.003															
4	0.003	0.003	0.002															
5	0.003	0.002	0.003															
8	0.002	0.003	0.002	0.002	0.002	0.003												
10	0.003	0.003	0.003	0.003	0.003	0.003												
15	0.003	0.003	0.003	0.003	0.003	0.003												
20	0.003	0.003	0.002	0.003	0.003	0.003												
30	0.003	0.003	0.002	0.003	0.003	0.003	0.003	0.003	0.003									
50	0.002	0.002	0.002	0.003	0.003	0.003	0.003	0.003	0.003									
75	0.003	0.003	0.002	0.003	0.003	0.002	0.003	0.003	0.003									
100	0.003	0.002	0.002	0.003	0.003	0.003	0.003	0.004	0.003	0.004	0.004	0.004						
150	0.003	0.002	0.003	0.003	0.002	0.003	0.003	0.003	0.003	0.004	0.004	0.004	0.005	0.004	0.005			
200	0.003	0.003	0.002	0.003	0.003	0.003	0.003	0.003	0.003	0.004	0.004	0.004	0.005	0.004	0.005			
255	0.003	0.003	0.003	0.003	0.003	0.003	0.017	0.002	0.003	0.004	0.003	0.004	0.005	0.006	0.006	0.009	0.008	0.009

Πίνακας 9: Εκτίμηση χρόνων για την ανακατασκευή του αρχικού μηνύματος μεγέθους 30 bytes, με τη χρήση των Command Line εντολών.

Μήνυμα : My name is Konstantinos Michos and this is my dissertation for my master in Cybersecurity

Μέγεθος μηνύματος : 89 bytes

Ανώτατο όριο shares : 255

Shares Combined

	2			8			30			100			150			255		
TSCR	Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)		
2	0.003	0.003	0.003															
3	0.003	0.003	0.003															
4	0.003	0.003	0.003															
5	0.003	0.003	0.002															
8	0.003	0.003	0.003	0.003	0.003	0.003												
10	0.003	0.002	0.003	0.003	0.003	0.002												
15	0.003	0.002	0.002	0.003	0.002	0.002												
20	0.002	0.003	0.003	0.003	0.002	0.003												
30	0.003	0.003	0.003	0.003	0.003	0.002	0.003	0.003	0.003									
50	0.003	0.003	0.003	0.003	0.003	0.002	0.003	0.003	0.003									
75	0.004	0.003	0.003	0.003	0.003	0.002	0.003	0.003	0.003									
100	0.002	0.002	0.002	0.003	0.003	0.002	0.003	0.003	0.003	0.004	0.004	0.004						
150	0.003	0.003	0.002	0.003	0.002	0.002	0.003	0.005	0.002	0.004	0.004	0.004	0.006	0.006	0.004			
200	0.003	0.003	0.002	0.003	0.003	0.002	0.003	0.003	0.003	0.004	0.004	0.004	0.007	0.005	0.006			
255	0.003	0.002	0.002	0.003	0.003	0.003	0.003	0.003	0.003	0.007	0.004	0.004	0.004	0.005	0.005	0.009	0.007	0.009

Πίνακας 10: Εκτίμηση χρόνων για την ανακατασκευή του αρχικού μηνύματος μεγέθους 89 bytes, με τη χρήση των Command Line εντολών.

Μήνυμα : My name is Konstantinos Michos and this is my dissertation for my master in Cybersecurity The theme is secure multiparty computations protocols and techniques that can be used for the safe execution of computations between two or more parties in order to ensure that they should learn only their output and nothing more such as information about the other parties and their inputs

Μέγεθος μηνύματος : 380 bytes

Ανώτατο όριο shares : 255

Shares Combined																		
	2			8			30			100			150			255		
TSCR	Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)			Time (sec.)		
2	0.003	0.003	0.003															
3	0.003	0.003	0.003															
4	0.002	0.003	0.002															
5	0.003	0.003	0.003															
8	0.002	0.003	0.002	0.002	0.003	0.003												
10	0.003	0.003	0.002	0.003	0.002	0.003												
15	0.003	0.003	0.003	0.003	0.003	0.003												
20	0.004	0.003	0.003	0.003	0.003	0.003												
30	0.003	0.003	0.003	0.003	0.003	0.003	0.004	0.003	0.003									
50	0.002	0.003	0.003	0.003	0.003	0.003	0.004	0.003	0.003									
75	0.003	0.003	0.003	0.003	0.003	0.003	0.008	0.003	0.003									
100	0.003	0.003	0.003	0.003	0.003	0.003	0.004	0.004	0.004	0.006	0.005	0.005						
150	0.003	0.003	0.003	0.003	0.003	0.003	0.003	0.003	0.003	0.005	0.006	0.007	0.012	0.007	0.007			
200	0.003	0.003	0.003	0.003	0.003	0.003	0.004	0.003	0.003	0.006	0.005	0.005	0.008	0.007	0.008			
255	0.003	0.003	0.003	0.003	0.003	0.003	0.004	0.003	0.005	0.004	0.005	0.005	0.007	0.009	0.005	0.013	0.012	0.012

Πίνακας 11: Εκτίμηση χρόνων για την ανακατασκευή του αρχικού μηνύματος μεγέθους 380 bytes, με τη χρήση των Command Line εντολών.

Παρατηρώντας τα αποτελέσματα που προέκυψαν από τους παραπάνω πίνακες, προκύπτει το συμπέρασμα ότι η αύξηση στον αριθμό του συνολικού αριθμού των shares

που δημιουργήθηκαν με την προηγούμενη εντολή, δεν επηρεάζει σημαντικά τον χρόνο για την επανάκτηση του αρχικού μηνύματος. Αντίθετα, αυτό που διαδραματίζει σημαντικό ρόλο και έχει επιρροή στον χρόνο εκτέλεσης είναι ο αριθμός των shares που συνδυάζονται για να επανακτηθεί το μήνυμα. Τέλος, το μέγεθος του μηνύματος παίζει μικρό ρόλο, κυρίως όταν δημιουργούνται ή συνδυάζονται μεγάλος αριθμός από shares. Σε γενικές γραμμές κινούνται δηλαδή στους ίδιους χρόνους, με μικρές διαφορές στην περίπτωση που τα shares που παρήχθησαν στο σύνολο τους ήταν 255 και αυτά που συνδυάστηκαν πάλι 255.

7.2 Τεχνική SSS με Παρεμβολή Newton – Σύγκριση με την Παρεμβολή Langrange

Όπως αναφέρθηκε και στο κεφάλαιο 5, η τεχνική Shamir Secret Sharing μπορεί να χρησιμοποιηθεί για τη διάσπαση ενός μυστικού-μηνύματος σε πολλά μέρη και το μοίρασμα των κομματιών αυτών στις διάφορες εμπλεκόμενες πλευρές. Σύμφωνα με την τεχνική αυτή, μπορεί να οριστεί ένας συγκεκριμένος αριθμός από αυτά τα μέρη, η γνώση των οποίων ή περισσότερων από αυτών μπορεί να οδηγήσει στην ανακατασκευή του αρχικού μηνύματος. Στο κομμάτι της ανακατασκευής του μηνύματος, ακολουθείται η διαδικασία της παρεμβολής (interpolation). Το πολυώνυμο που έχει προταθεί και χρησιμοποιείται στην διαδικασία της παρεμβολής, στην τεχνική του Shamir είναι αυτό του Lagrange. Παρ' όλα αυτά έχουν υπάρξει και προτάσεις για χρησιμοποίηση διαφορετικών πολυωνύμων, όπως για παράδειγμα η φόρμουλα παρεμβολής που βασίζεται στο πολυώνυμο του Newton

7.2.1 Παρουσίαση των Δύο Φόρμουλων Παρεμβολής, Lagrange και Newton

Στη συνέχεια θα πραγματοποιηθεί παρουσίαση, τόσο της παραδοσιακής φόρμουλας παρεμβολής που χρησιμοποιείται πιο συχνά και είναι πιο ευρέως γνωστή, δηλαδή αυτής που βασίζεται στο πολυώνυμο του Lagrange, καθώς επίσης και μιας ακόμα ενδιαφέρουσας περίπτωσης που έχει προταθεί, αυτής δηλαδή που βασίζεται στο πολυώνυμο του Newton (Bezzateev et al., 2020).

7.2.1.1 Η Φόρμουλα Παρεμβολής του Lagrange

Η συγκεκριμένη φόρμουλα παρεμβολής του Lagrange, συνήθως αποτελεί αντικείμενο αναφοράς σαν ένα πολυώνυμο. Πιο συγκεκριμένα, όπως αναφέρθηκε και νωρίτερα, ας γίνει η υπόθεση ότι υπάρχουν n+1 ζευγάρια αριθμών (x_0 , y_0) , (x_1 , y_1) , (x_2, y_2) ,...., (x_n, y_n). Για τα ζευγάρια αυτά ισχύει ότι οι τιμές των x_i και y_i που αποτελούν ένα ζευγάρι είναι διαφορετικές μεταξύ τους, δηλαδή ότι $x_i \neq x_j$, για όλες τις τιμές $i \neq j$. Τότε υπάρχει ένα και μόνο ένα πολυώνυμο L(x) βαθμού n, για το οποίο ισχύει ότι : $L(x_j) = y_j$ για όλες τις τιμές του j=0,1,…,n , τέτοιες ώστε :

L(x) =  , όπου $l_i (x)$ =  είναι πολυώνυμα για τα οποία ισχύουν οι εξής ιδιότητες :

1) deg $l_i(x) = n$

2) $l_i (x) = 1$

3) $l_i (x) = 0$ αν ισχύει ότι $j \neq i$.

7.2.1.2 Η Φόρμουλα Παρεμβολής του Newton

Προκειμένου να παρουσιαστεί η φόρμουλα παρεμβολής του Newton, ας γίνει η υπόθεση ότι υπάρχουν n+1 ζευγάρια αριθμών (x_0 , y_0) , (x_1 , y_1) , (x_2, y_2) ,...., (x_j , yj), …, (x_n, y_n). Από αυτά τα ζευγάρια αριθμών, οι τιμές που παίρνουν τα x_j , για j = 0, 1, … , n, ονομάζονται σημεία παρεμβολής. Επιπλέον, οι τιμές που παίρνουν τα y_j, για j = 0, 1, … , n, ονομάζονται τιμές παρεμβολής. Επομένως, δοθείσης της συνάρτησης παρεμβολής f, οι τιμές παρεμβολής καθορίζονται από τη σχέση $y_j = f (x_j)$, για οποιαδήποτε τιμή j=0,….,n. Με αυτό τον τρόπο μπορεί να ορισθεί το βασικό κομμάτι-πολυώνυμο του πολυωνύμου του Newton ως εξής :

$n_i(x)$ =  , όπου i = 1, ….., n και $n_0(x) = 1$.

Χρησιμοποιώντας το παραπάνω πολυώνυμο, μπορεί να ορισθεί το πολυώνυμο του Newton ως εξής :

$P_n(x)$ =  $= K_0 + K_1 (x-x_0) + K_2 (x-x_0)(x-x_1) + ... + K_n (x-x_0)(x-x_1) .... (x-x_{n-1})$,

για το οποίο ισχύει ότι $P_n(x_j) = f(x_j)$, για οποιαδήποτε τιμή j=0,….,n.

Αξίζει σε αυτό το σημείο να αναφερθεί ότι ο γενικός τύπος για τον υπολογισμό των K_i είναι ο εξής :

K_i =  , όπου το $f[x_1, ... , x_i]$ είναι διαιρεμένη διαφορά n-οστής τάξης.

Για παράδειγμα το K_1 θα υπολογίζονταν ως εξής :

K_1 =  , όπου το $f[x_0, x_1]$ είναι διαιρεμένη διαφορά 1ης τάξης.

7.2.2 Η Χρήση των Δύο Φορμουλών Παρεμβολής, Lagrange και Newton, στην Τεχνική Shamir Secret Sharing

Όπως αναφέρθηκε και στο κεφάλαιο 5, και πιο συγκεκριμένα στην ενότητα 5.1, η τεχνική Shamir Secret Sharing χρησιμοποιείται για το μοίρασμα ενός μυστικού μηνύματος-πληροφορίας D, σε n κομμάτια που θα παραλάβουν οι n συμμετέχουσες οντότητες, κατά τέτοιο τρόπο ώστε για η ανακατασκευή του μηνύματος να μπορεί να πραγματοποιηθεί μόνο αν k ή περισσότερα τμήματα είναι γνωστά. Δεδομένης της χρήσης ενός πρώτου αριθμού p > D για την κατασκευή του πολυωνύμου Lagrange και για την δημιουργία των

κομματιών D_1, D_2, … , D_n , κατασκευάζεται το πολυώνυμο $L(x)=a_0 + a_1x +\ldots\ldots + a_nx^n$, βαθμού n , για το οποίο ισχύει ότι $a_0 = D$ και οι υπόλοιποι συντελεστές $a_1,\ldots, a_{n-1}$ επιλέγονται τυχαία. Επομένως τα μυστικά κομμάτια υπολογίζονται χρησιμοποιώντας τις σχέσεις $D_1=L(1)$, $D_2 =L(2),\ldots,D_n=L(n)$.

Στη συνέχεια, και μετά την παρουσίαση των γενικών εννοιών και τύπων των δύο φόρμουλων, θα γίνει αναφορά για το πως μπορούνε αυτές να χρησιμοποιηθούν στην τεχνική Shamir Secret Sharing, στο κομμάτι της διαδικασίας που έχει να κάνει με την ανακατασκευή του αρχικού μηνύματος. (Bezzateev et al., 2020)

7.2.2.1 Ανακατασκευή του Αρχικού Μηνύματος με τη Χρήση της Φόρμουλας Παρεμβολής Lagrange

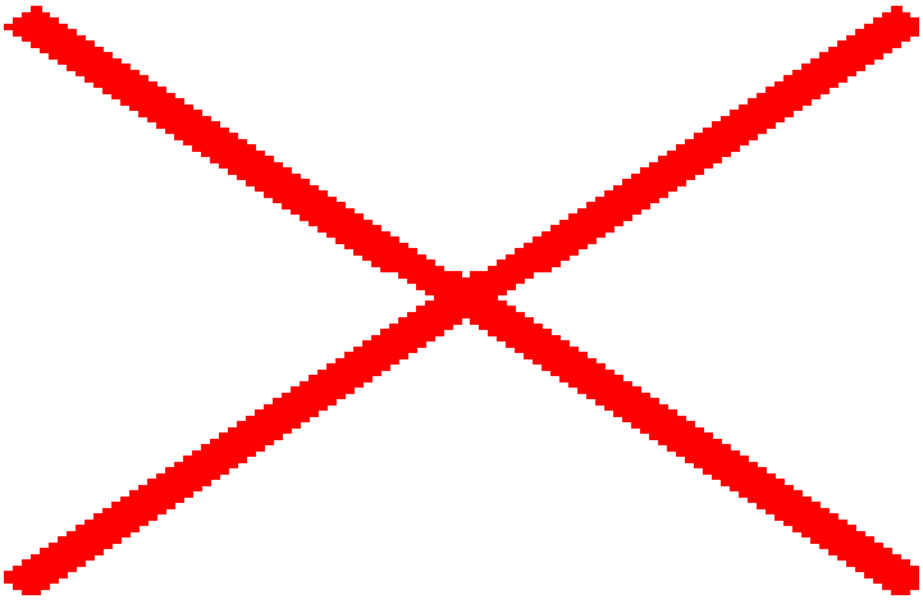
Η πιο συνηθισμένη μέθοδος που είχε προταθεί από τον Shamir και χρησιμοποιείται για την ανακατασκευή του αρχικού μηνύματος, είναι η φόρμουλα παρεμβολής του Lagrange. Για την ανακατασκευή του μηνύματος θα χρησιμοποιηθούν τα ζευγάρια αριθμών (x_0, y_0) , (x_1, y_1) , (x_2, y_2) ,…., (x_n, y_n), τα οποία αποτελούν ουσιαστικά αποτελούν τα μυστικά, αφού $D_i=(x_i, y_i= L(x_i))$. Οι σχέσεις που θα χρησιμοποιηθούν για την ανακατασκευή του αρχικού μηνύματος D μετασχηματίζονται ως εξής :

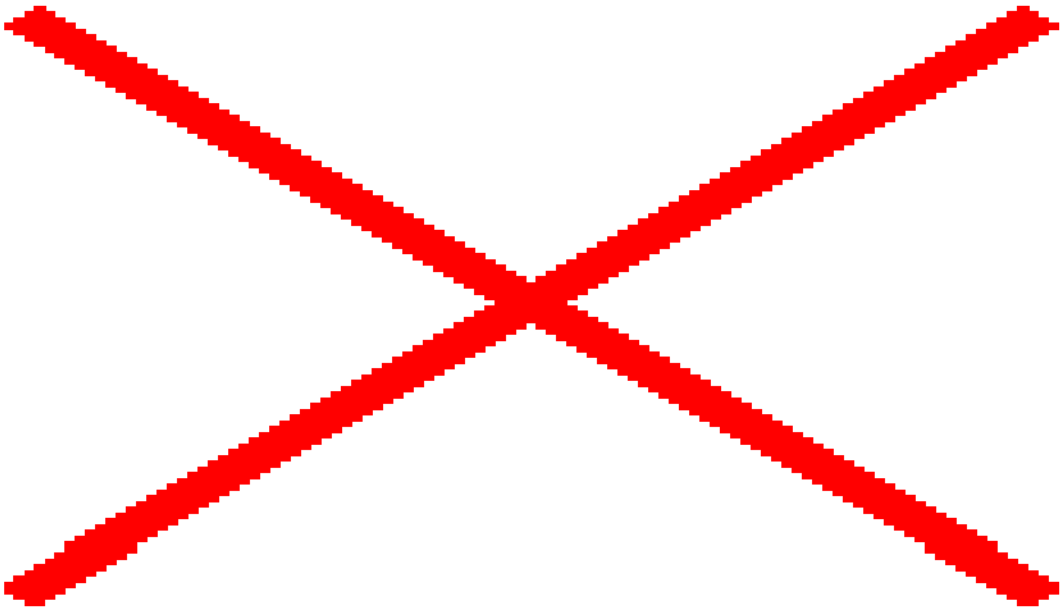
για την οποία σχέση ισχύει ότι 

Με αυτό τον τρόπο, καταλήγει κανείς στο πολυώνυμο $L(x)=a_0 + a_1x +\ldots\ldots + a_nx^n$ και μπορεί εύκολα να αντιληφθεί ότι η τιμή του πολυωνύμου που δεν συνοδεύεται από κάποια δύναμη του x, αποτελεί ουσιαστικά το αρχικό μυστικό D.

Για παράδειγμα (Crypto Wiki, n.d.) έστω ότι το αρχικό μυστικό μήνυμα είναι το D=1234, η συνάρτηση $f(x)= 1234 + 166x + 94x^2$ και έχουν παραχθεί τα σημεία $D_1=(1, 1494)$, $D_2=(2, 1942)$, $D_3=(3, 2578)$, $D_4=(4, 3402)$, $D_5=(5, 4414)$, $D_6=(6, 5614)$, από τα οποία έχει ορισθεί ότι απαιτούνται το λιγότερο 3 για να πραγματοποιηθεί η ανακατασκευή του D. Έστω ότι θα χρησιμοποιηθούν τα σημεία $(x_0, y_0)=(2, 1942)$, $(x_1, y_1)=(4, 3402)$ και $(x_2, y_2)=(5, 4414)$.

Προκειμένου να υπολογισθεί το αρχικό πολυώνυμο χρησιμοποιείται ο τύπος :





Έτσι λοιπόν προέκυψε το αρχικό πολυώνυμο Lagrange, από το οποίο προκύπτει σωστά ότι το αρχικό μήνυμα είναι το D=1234.

7.2.2.2 Ανακατασκευή του Αρχικού Μηνύματος με τη Χρήση της Φόρμουλας Παρεμβολής Newton

Όπως αναφέρθηκε και νωρίτερα, το πολυώνυμο Newton, αποτελεί μια εναλλακτική πρόταση για την ανακατασκευή του αρχικού μηνύματος στην τεχνική του Shamir. Ο τύπος, με βάση τον οποίο μπορεί να υπολογιστεί το πολυώνυμο αυτό βαθμού n, είναι ο εξής :

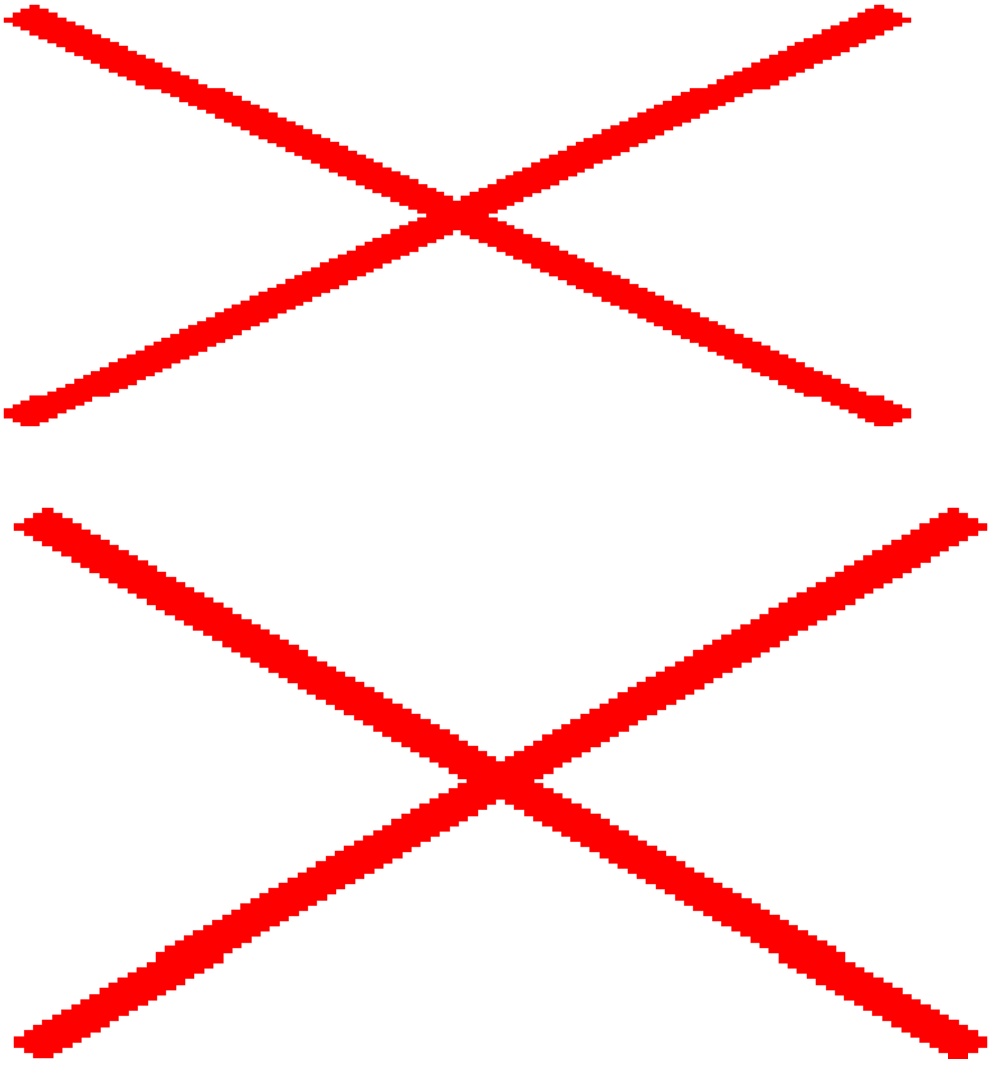
$P_n(x) =$  $= K_0 + K_1 (x-x_0) + K_2 (x-x_0)(x-x_1) + ... + K_n (x-x_0)(x-x_1) .... (x-x_{n-1}) =$

$=$ 

Για παράδειγμα, έστω ότι συνεχίζεται να χρησιμοποιείται το αρχικό μήνυμα που αναφέρθηκε και στην περίπτωση του πολυωνύμου Lagrange, το D=1234, και η

συνάρτηση $f(x)= 1234 + 166x + 94x^2$ και έχουν παραχθεί τα σημεία $D_1=(1, 1494)$, $D_2=(2, 1942)$, $D_3=(3, 2578)$, $D_4=(4, 3402)$, $D_5=(5, 4414)$, $D_6=(6, 5614)$, από τα οποία έχει ορισθεί ότι απαιτούνται το λιγότερο 3 για να πραγματοποιηθεί η ανακατασκευή του D. Έστω ότι θα χρησιμοποιηθούν και πάλι τα σημεία $(x_0, y_0)=(2, 1942)$, $(x_1, y_1)=(4, 3402)$ και $(x_2, y_2)=(5, 4414)$.

Δεδομένου ότι τρία σημεία μπορούν να οδηγήσουν στην ανακατασκευή του αρχικού μηνύματος, θα πρέπει να υπολογιστεί το $P_2(x)$. Επομένως προκύπτει ότι :



Έτσι λοιπόν προέκυψε το αρχικό πολυώνυμο Newton, από το οποίο προκύπτει σωστά ότι το αρχικό μήνυμα είναι το D=1234.

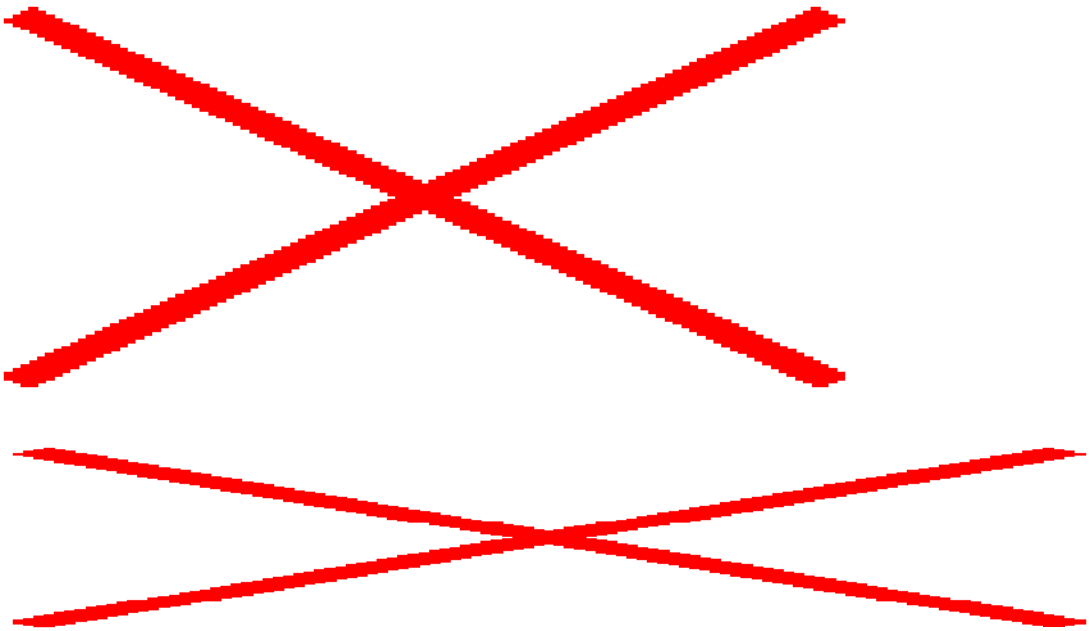
7.2.3 Σύγκριση των Δύο Φορμουλών Παρεμβολής – Πλεονεκτήματα και Μειονεκτήματα

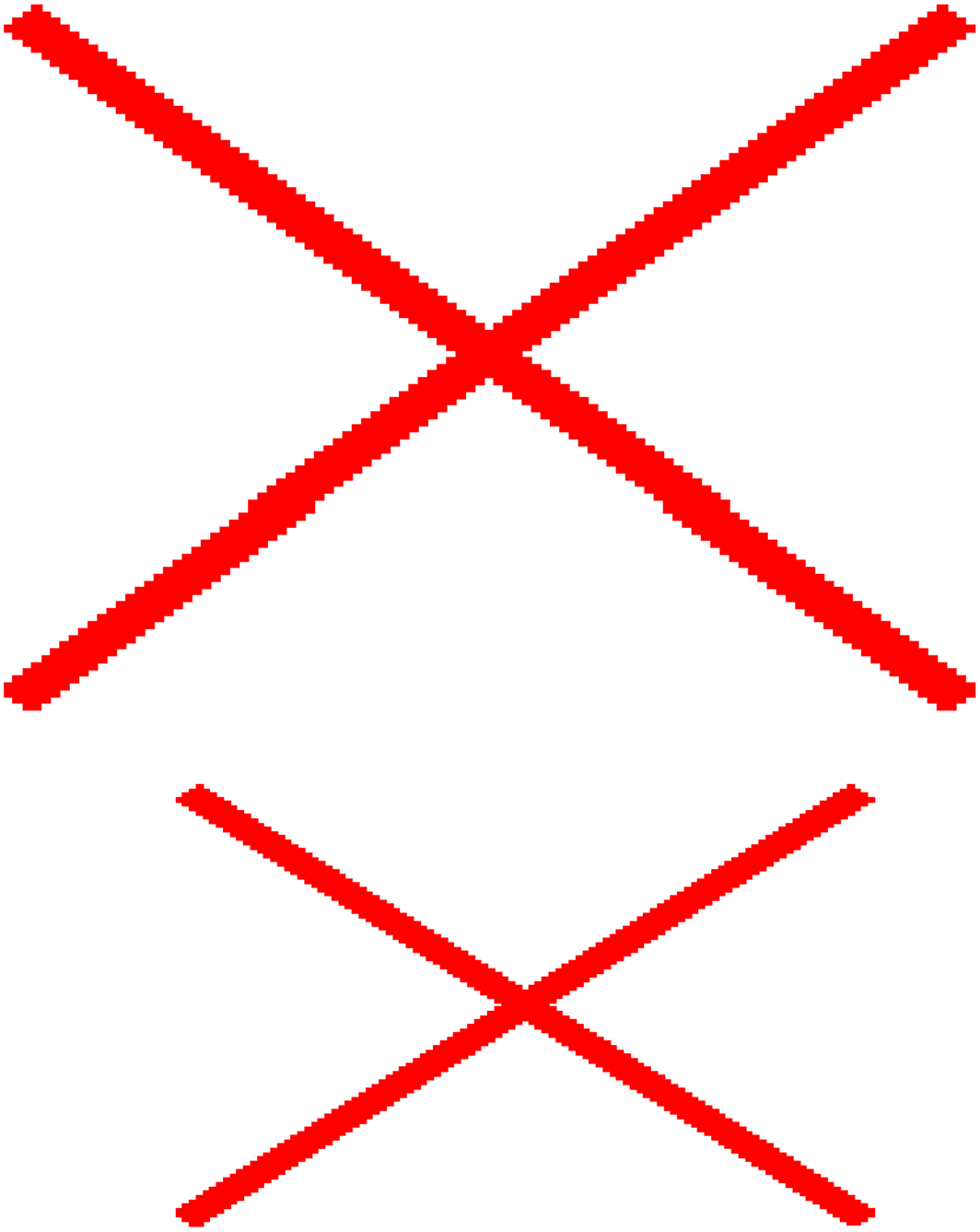
Στη συνέχεια, θα επιχειρηθεί να γίνει μία σύγκριση των δύο φόρμουλων παρεμβολής Lagrange και Newton, παρουσιάζοντας τα πλεονεκτήματα και τα μειονεκτήματα τη κάθε μίας, όπως αυτά προκύπτουν μετά από την προσθήκη ενός νέου σημείου για τον υπολογισμό του πολυωνύμου και του αρχικού μηνύματος (Bezzateev et al., 2020).

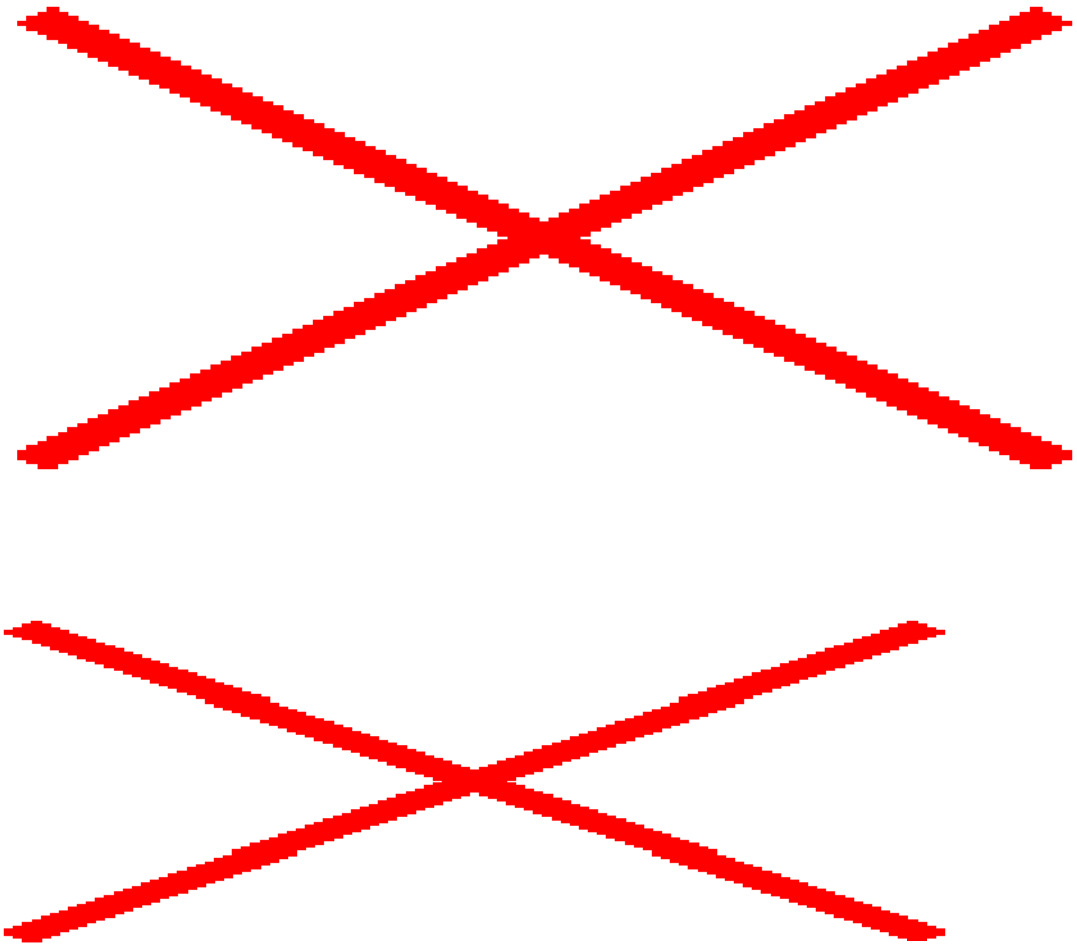
7.2.3.1 Πρόσθεση Ενός Νέου Σημείου Προερχόμενου από το Πολυώνυμο

Συνεχίζοντας το παράδειγμα με το μυστικό D=(1234), ας γίνει η υπόθεση ότι θα χρησιμοποιηθεί ακόμα ένα σημείο για την επανάκτηση του αρχικού μηνύματος, σημείο που ανήκει στο πολυώνυμο. Θα χρησιμοποιηθούν δηλαδή τα σημεία $(x_0, y_0)=(2, 1942)$, $(x_1, y_1)=(4, 3402)$, $(x_2, y_2)=(5, 4414)$ και το $(x_3, y_3) = (6, 5614)$.

Προκειμένου να γίνει αυτό με την μέθοδο Lagrange, θα πρέπει να γίνουν οι εξής πράξεις :





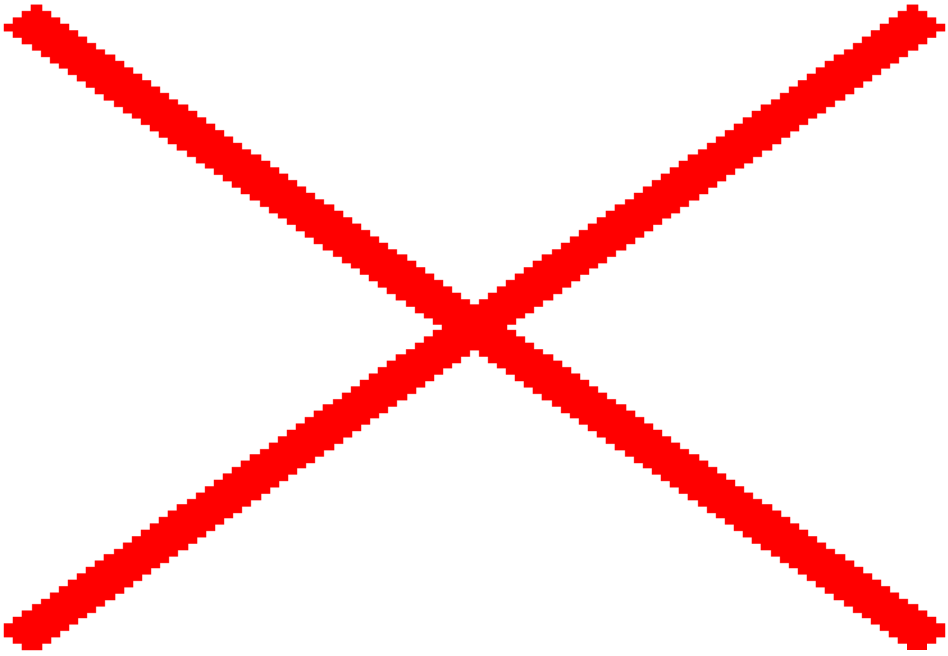


Έτσι λοιπόν προέκυψε το αρχικό πολυώνυμο Lagrange, από το οποίο προκύπτει σωστά ότι το αρχικό μήνυμα είναι το D=1234.

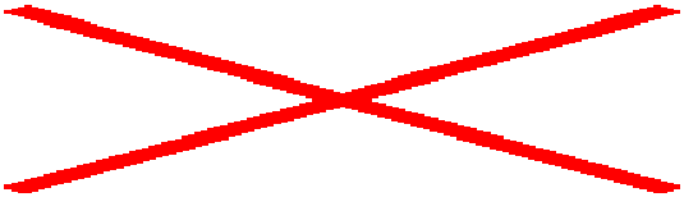
Στη συνέχεια θα γίνει προσπάθεια να επαναληφθεί η διαδικασία ανακατασκευής του αρχικού μηνύματος, με τη χρήση της φόρμουλας παρεμβολής του Newton και με το δεδομένο ότι θα προστεθεί και πάλι ένα επιπλέον γνωστό σημείο, προερχόμενο από το πολυώνυμο.

Έστω ότι χρησιμοποιείται το αρχικό μήνυμα που αναφέρθηκε και στην περίπτωση του πολυωνύμου Lagrange, το D=1234, με τη συνάρτηση $f(x)= 1234 + 166x + 94x^2$ και έστω ότι θα χρησιμοποιηθούν και πάλι τα σημεία $(x_0, y_0)=(2, 1942)$, $(x_1, y_1)=(4, 3402)$ και $(x_2, y_2)=(5, 4414)$ και το $(x_3, y_3) = (6, 5614)$.

Προκειμένου να πραγματοποιηθεί αυτό με την μέθοδο Newton, αρκεί όπως φαίνεται και από τον τύπο, να υπολογισθεί το κομμάτι  και να προστεθεί στους προηγούμενους υπολογισμούς. Έτσι λοιπόν, θα πρέπει να γίνουν οι εξής πράξεις :



και



Επομένως προκύπτει ότι :

Άρα χρησιμοποιώντας και τους προηγούμενους υπολογισμούς, η σχέση μετασχηματίζεται ως εξής :

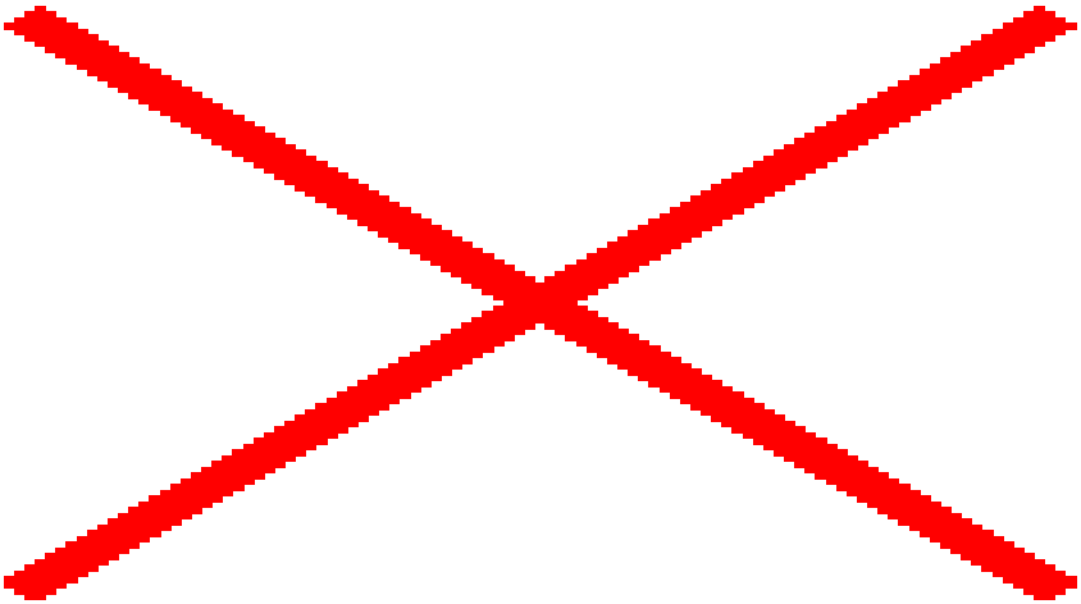
Ουσιαστικά λοιπόν, το αποτέλεσμα παραμένει ως έχει και προκύπτει σωστά ότι το αρχικό μήνυμα είναι το D=(1234).

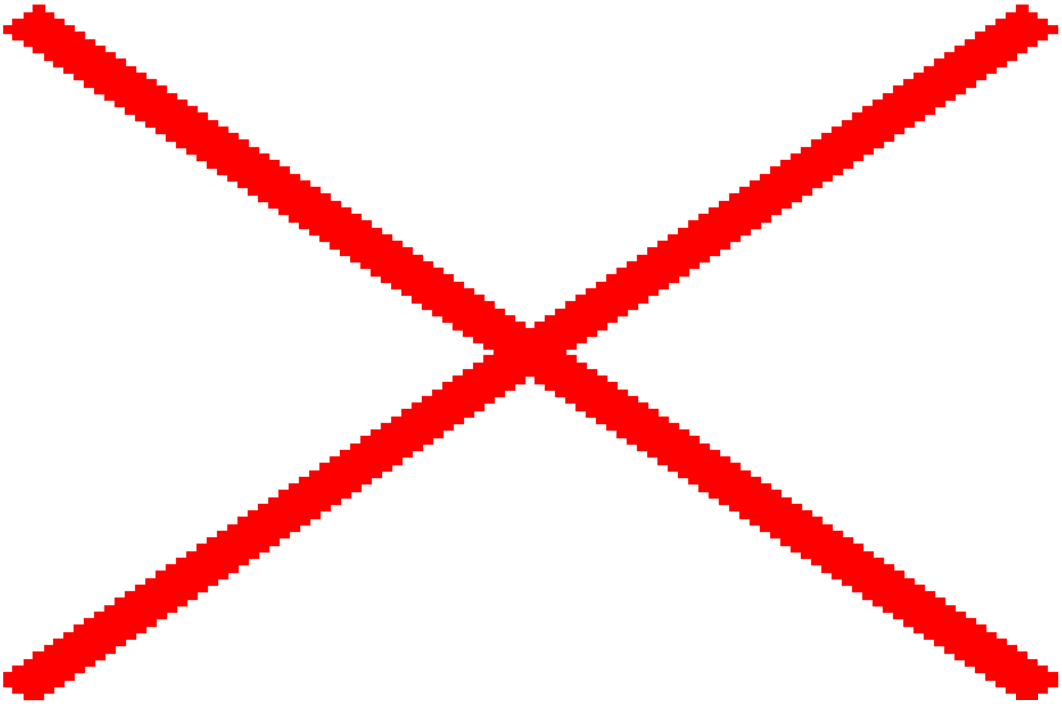
Και στις δύο περιπτώσεις λοιπόν προέκυψαν τα ίδια πολυώνυμα.

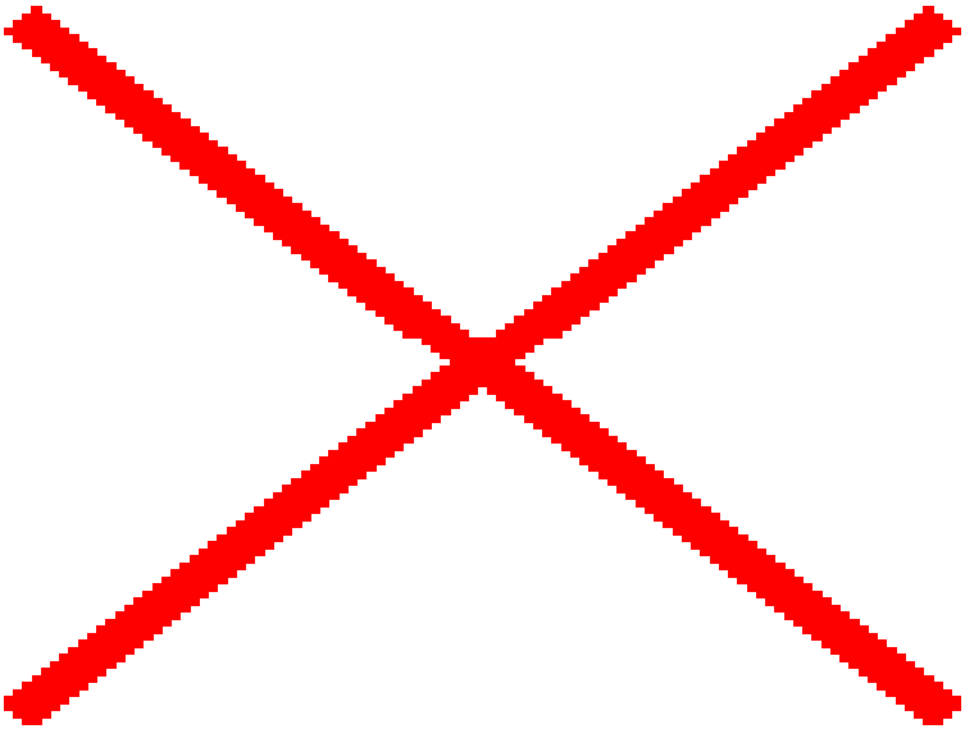
7.2.3.2 Πρόσθεση Ενός Νέου Αγνώστου Σημείου

Στην περίπτωση που παρουσιάζεται στην συγκεκριμένη ενότητα, και συνεχίζοντας το παράδειγμα με το μυστικό D=(1234), ας γίνει η υπόθεση ότι θα χρησιμοποιηθεί ακόμα ένα σημείο για την επανάκτηση του αρχικού μηνύματος, σημείο όμως που είναι άγνωστο (δηλαδή τυχαίο, που δεν ανήκει στην υπάρχουσα συνάρτηση, και άρα αυτή θα πρέπει να επαναϋπολογιστεί). Θα χρησιμοποιηθούν δηλαδή τα σημεία $(x_0, y_0)=(2, 1942)$, $(x_1, y_1)=(4, 3402)$, $(x_2, y_2)=(5, 4414)$ και το $(x_3, y_3) = (8,2)$.

Προκειμένου να γίνει αυτό με την μέθοδο Lagrange, θα πρέπει να γίνουν τις εξής πράξεις :

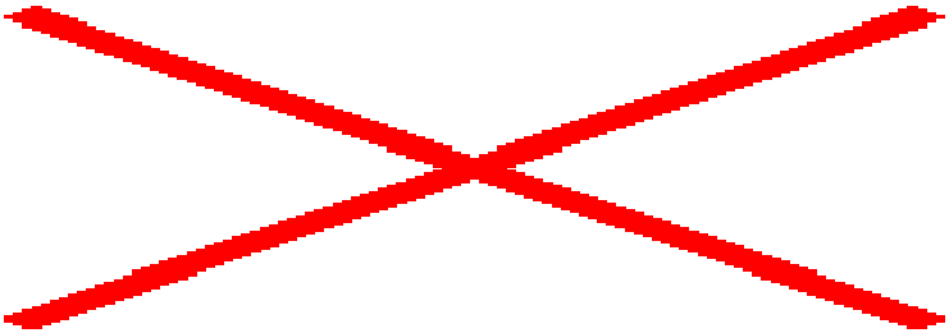


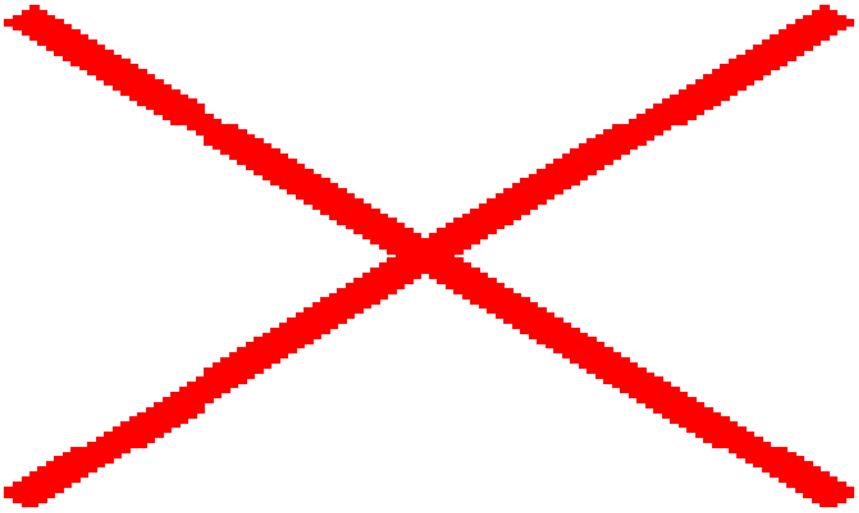




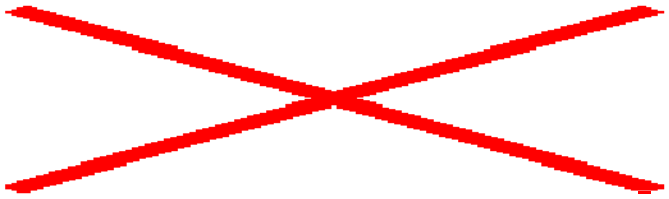
Ακολουθούμε τώρα τη διαδικασία επανάκτησης του αρχικού μηνύματος, με τη φόρμουλα παρεμβολής του Newton.

Προκειμένου να πραγματοποιηθεί αυτό με την μέθοδο Newton, αρκεί όπως φαίνεται και από τον τύπο, να υπολογισθεί το κομμάτι  και να προστεθεί στους προηγούμενους υπολογισμούς. Έτσι λοιπόν, θα πρέπει να γίνουν οι εξής πράξεις :



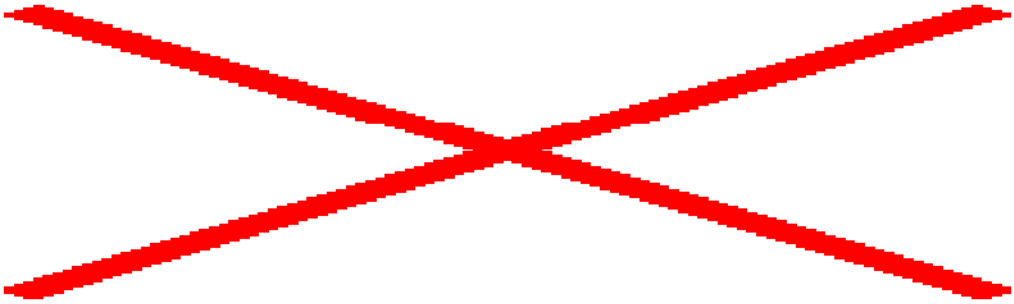


και



Επομένως προκύπτει ότι :

Άρα χρησιμοποιώντας και τους προηγούμενους υπολογισμούς, η σχέση μετασχηματίζεται ως εξής :



Επομένως προκύπτει το ίδιο πολυώνυμο και από τις δύο φόρμουλες παρεμβολής.

7.2.3.3 Συμπεράσματα από Πρόσθεση Ενός Νέου Σημείου

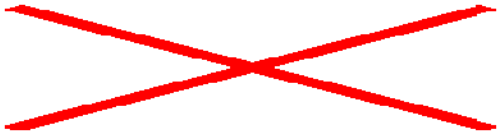
Στη συνέχεια, θα παρουσιαστούν ορισμένα συμπεράσματα που ισχύουν και για τις δύο περιπτώσεις που παρουσιάζονται στις υποενότητες 7.2.3.1. και 7.2.3.2.

Αρχικά, η πρώτη παρατήρηση που προκύπτει είναι ότι και οι δύο φόρμουλες παρεμβολής, Lagrange και Newton είναι το ίδιο αποτελεσματικές. Αυτό πρακτικά σημαίνει ότι και δύο μέθοδοι, εφόσον χρησιμοποιηθούν τα ίδια σημεία, καταλήγουν στο ίδιο πολυώνυμο παρεμβολής, και επομένως στο ίδιο αποτέλεσμα.

Η βασική τους διαφορά έγκειται στους υπολογισμούς που χρειάζεται να γίνουν σε κάθε μία περίπτωση. Πιο συγκεκριμένα, στην φόρμουλα παρεμβολής Lagrange είναι απαραίτητο να γίνουν όλοι οι υπολογισμοί από τον αρχή όταν επιθυμούμε να προσθέσουμε ακόμα ένα σημείο, το οποίο επηρεάζει και ουσιαστικά διαφοροποιεί τον τύπο για τον υπολογισμό του πολυωνύμου. Από την άλλη μεριά, στην φόρμουλα παρεμβολής Newton, δεν απαιτείται η επανάληψη και η εκτέλεση των πράξεων από την αρχή, καθώς δεν επηρεάζονται τα προηγούμενα τμήματα του τύπου, παρά μόνο να προστεθεί στο τέλος το γινόμενο, όπως στα παραπάνω παραδείγματα το $K_3 * n_3 (x)$. Μάλιστα σε γενικές γραμμές προκύπτει ότι για τον υπολογισμό του πολυωνύμου Lagrange απαιτούνται περίπου n^2 στο πλήθος προσθέσεις και πολλαπλασιασμοί, ενώ στην περίπτωση της φόρμουλας Newton, μόνο $n^2/2$, αριθμός κατά πολύ μικρότερος (Bezzateev et al., 2020). Συνεπώς, εύκολα προκύπτει το συμπέρασμα ότι είναι προτιμότερη η εφαρμογή της φόρμουλας παρεμβολής του Newton, λόγω του μικρότερου πλήθους υπολογισμών.

Αξίζει να γίνει αναφορά στο γεγονός ότι εκτός από το πλήθος των υπολογισμών, υπήρξαν και διαφορές ανάμεσα στις δύο φόρμουλες και ως προς την δυσκολία των υπολογισμών. Πιο συγκεκριμένα, αυτό σημαίνει ότι οι υπολογισμοί στην περίπτωση της φόρμουλας παρεμβολής Newton ήταν πιο εύκολοι, με πιο εύκολες και απλές πράξεις, σε αντίθεση με τους πιο μεγάλους και περίπλοκους της φόρμουλας Lagrange, γεγονός που αποτελεί σημαντικό πλεονέκτημα της φόρμουλας Newton.

Από την άλλη μεριά, πρέπει να αναφερθεί και ένα σημαντικό πλεονέκτημα της φόρμουλας παρεμβολής Lagrange έναντι αυτής του Newton. Πιο συγκεκριμένα, υπάρχει οι δυνατότητα να χρησιμοποιηθούν κάποιοι προηγούμενοι υπολογισμοί, για τον υπολογισμό του πολυωνύμου παρεμβολής Lagrange, γεγονός το οποίο μπορεί να οδηγήσει σε μικρότερο πλήθος υπολογισμών, και κατά συνέπεια σε υπολογισμό του αρχικού μηνύματος με μεγαλύτερη ευκολία (Bezzateev et al., 2020).Μάλιστα, δεδομένου του γεγονότος ότι ουσιαστικά αυτό που ενδιαφέρει περισσότερο είναι ο υπολογισμός της τιμής L(0), καθώς έτσι θα προκύψει και το αρχικό μήνυμα, αξίζει να αναφερθεί ένα χαρακτηριστικό παράδειγμα, το οποίο περιλαμβάνει πρόταση για υπολογισμό του L(0) χρησιμοποιώντας τον μεταποιημένο τύπο (Stack Exchange, n.d.):



Παρόλα αυτά, η παρατήρηση αυτή δεν ισχύει στην περίπτωση που προστεθεί κάποιο καινούριο σημείο, καθώς στη συγκεκριμένη περίπτωση δεν μπορούν να γίνουν αυτές οι απλοποιήσεις και ως αποτέλεσμα, πρέπει να επαναληφθούν οι υπολογισμοί από την αρχή. (Bezzateev et al., 2020)

Συνοψίζοντας λοιπόν τις παρατηρήσεις αυτές, προκύπτει το συμπέρασμα ότι η φόρμουλα παρεμβολής Newton, είναι πιο εύχρηστη σε σχέση με τη φόρμουλα παρεμβολής Lagrange, καθώς παρέχει τη

δυνατότητα για ταχύτερους υπολογισμούς, με μεγαλύτερη ευκολία στην εκτέλεση τους, ακόμα και με την πρόσθεση νέων σημείων για τον υπολογισμό των πολυωνύμων και κατά συνέπεια για την ανακατασκευή του αρχικού μηνύματος. Μόνο στην περίπτωση που δεν υπάρχει πρόσθεση επιπλέον σημείων, θα μπορούσε να χρησιμοποιηθεί με απλοποιήσεις η φόρμουλα του Lagrange, παρέχοντας κάποιο πλεονέκτημα, και πιο συγκεκριμένα αυτό των πιο απλοποιημένων υπολογισμών. Αν όμως υπάρχει γενικότερα η ανάγκη να παρουσιαστεί γενικά το πολυώνυμο L(x) και να υπολογιστούν και επιπλέον τιμές, εκτός από την τιμή L(0), τότε η φόρμουλα παρεμβολής του Newton θα είναι πιο αποδοτική.

Κεφάλαιο 8

Τεχνική διαμοιρασμού μυστικού του Shamir και ψευδωνυμοποίηση

Όπως αναφέρθηκε και σε προηγούμενα κεφάλαια, η τεχνική Shamir Secret Sharing, και πιο συγκεκριμένα η δυνατότητα που παρέχει για διαχωρισμό ενός μηνύματος σε πολλά τμήματα και η ανακατασκευή του με τη χρήση ενός αριθμού από αυτά, παρέχει τη δυνατότητα για χρησιμοποίηση της σε πλήθος εφαρμογών. Μία χαρακτηριστική περίπτωση, η οποία διερευνάται στο παρόν κεφάλαιο, αποτελεί η χρησιμοποίησή της στη διαδικασία της ψευδωνυμοποίησης, κάτι το οποίο μπορεί να επιφέρει πολλές σημαντικές λύσεις σε απαιτήσεις νομοθεσίας ως προς την προστασία προσωπικών δεδομένων.

Για παράδειγμα, ας αναλογιστούμε αρχεία καταγραφής ενεργειών τα οποία παράγονται στο πλαίσιο ενός μηχανισμού τύπου Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System – IDS). Πιο συγκεκριμένα, ας γίνει η υπόθεση ότι το προαναφερθέν Σύστημα Ανίχνευσης Εντολών, προκειμένου να ανιχνεύσει έγκαιρα οποιαδήποτε επιθετική δραστηριότητα, διατηρεί αρχεία καταγραφής (log files). Τα συγκεκριμένα αρχεία καταγραφής χρησιμοποιούνται για την καταγραφή οποιασδήποτε δραστηριότητας – συναλλαγής πραγματοποιείται ανάμεσα στο σύστημα και σε άλλους εξωτερικούς χρήστες – οντότητες. Ουσιαστικά προχωράει στην καταγραφή όλων των IP διευθύνσεων με τις οποίες παρατηρείται ότι υπάρχει κάποια δραστηριότητα ή/και, αναλόγως την περίπτωση, άλλων αναγνωριστικών (identifiers) του χρήστη (ας ανακαλέσουμε στο σημείο αυτό ότι, όπως περιγράφηκε στο Κεφάλαιο 3, κάθε αναγνωριστικό συσκευής που αντιστοιχεί σε φυσικό πρόσωπο, συμπεριλαμβανομένης της IP διεύθυνσης, αποτελεί προσωπικό δεδομένο).

Το πρόβλημα που δημιουργείται στην περίπτωση της καταγραφής όλων των δραστηριοτήτων, είναι το γεγονός ότι, αν δεν λαμβάνονται εχέγγυα για την προστασία των προσωπικών δεδομένων, ενδέχεται να εγείρονται ζητήματα ως προς την ιδιωτικότητα των χρηστών. Για παράδειγμα, αν καταγράφονται ενέργειες νόμιμων χρηστών (συμπεριλαμβανομένων των εσωτερικών χρηστών/υπαλλήλων), και επί αυτών, αν και πρόκειται "αθώες" ενέργειες που δεν εγείρουν ζήτημα ασφάλειας, γίνεται περαιτέρω επεξεργασία για άλλους σκοπούς (π.χ. εξαγωγή συμπερασμάτων για τη συμπεριφορά του χρήστη, δημιουργία προφίλ συμπεριφοράς/προσωπικότητας κτλ.), τότε τίθενται ζητήματα ως προς τη νομιμότητα της επεξεργασίας. Από την άλλη πλευρά βέβαια, η ασφάλεια των δεδομένων/συστημάτων αποτελεί σαφώς πτυχή και της προστασίας προσωπικών δεδομένων, οπότε και ο ρόλος ενός μηχανισμού καταγραφής ενεργειών χρηστών για τη ανίχνευση/αποτροπή/διερεύνηση περιστατικών παραβίασης είναι ουσιαστικός, ενώ ταυτόχρονα πολλές φορές μία ενέργεια χρήστη από μόνη της δεν καθιστά σαφές αν πρόκειται για επίθεση ή όχι και πρέπει να διερευνηθεί περαιτέρω, συνδυαστικά με άλλες συναφείς ενέργειες. Έτσι λοιπόν προκύπτει το συμπέρασμα ότι ένας μηχανισμός καταγραφής ενεργειών στο πλαίσιο ανίχνευσης εισβολών ιδανικά δεν θα πρέπει να συλλέγει δεδομένα τα οποία δεν είναι απαραίτητα για την πραγματοποίηση των βασικών διεργασιών του ή, ισοδύναμα, δεν θα πρέπει να επιτρέπει τη συλλογή υπέρμετρων δεδομένων εν όψει του σκοπού επεξεργασίας. Αντίθετα, κατά τη διάρκεια εκτέλεσης της συλλογής των δεδομένων, θα πρέπει να γίνεται ένας διαχωρισμός, και τα δεδομένα που δε είναι απαραίτητα για τις βασικές δραστηριότητες, να απορρίπτονται. Φυσικά, η δυσκολία επίτευξης αυτού είναι εξαιρετικά μεγάλη.

8.1 Η Χρήση της Ψευδωνυμοποίησης

Στο σημείο αυτό εμφανίζεται η τεχνική της ψευδωνυμοποίησης. Όπως αναφέρεται και στον Γενικό Κανονισμό Προστασίας των Δεδομένων (βλ. Και Κεφάλαιο 3), η ψευδωνυμοποίηση αναφέρεται ως "η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο

υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (Δρ. Κωνσταντίνος Λιμνιώτης & Ιωάννης Μαυρίδης, 2019).

Η ψευδωνυμοποίηση μπορεί να χρησιμοποιηθεί επομένως στις περιπτώσεις όπου χρειάζεται να διασφαλιστούν (Δρ. Κωνσταντίνος Λιμνιώτης, 2018):

- Η ασφάλεια, δεδομένου ότι μπορεί να αποτελέσει ένα πολύ σημαντικό μέσο για την απόκρυψη των αληθινών ταυτοτήτων των χρηστών.

- Η ιδιωτικότητα, δεδομένου ότι αποτελεί ένα αναφαίρετο δικαίωμα των χρηστών, οι οποίοι μπορούν να επιλέγουν και να αποφασίζουν από μόνοι τους για το ποιες από τις προσωπικές τους πληροφορίες-δεδομένα, επιθυμούν να αποτελέσουν αντικείμενο επεξεργασίας.

Υπάρχουν διάφορες κατηγορίες ψευδωνύμων, τα οποία χρησιμοποιούνται για την επίτευξη μεγαλύτερου βαθμού ανωνυμίας, οι σημαντικότερες από τις οποίες είναι οι εξής (Biskup & Flegel, 2000):

- Τα ψευδώνυμα τα οποία βασίζονται στις οντότητες. Τα ψευδώνυμα αυτά μπορεί να χρησιμοποιηθούν σε διάφορες περιπτώσεις “συναλλαγών” των οντοτήτων. Η συχνή χρησιμοποίηση τους μπορεί να συνεπάγεται την αύξηση του ρίσκου της επανα-αναγνώρισης τους. Επιπλέον, μπορεί να χρησιμοποιηθούν για το χαρακτηρισμό μιας ομάδας οντοτήτων, προκειμένου να αποφευχθεί η απόδοση κάποιων γεγονότων σε συγκεκριμένες οντότητες. Τέλος, τα ψευδώνυμα αυτής της κατηγορίας μπορούν να χωριστούν σε τρεις υπό-κατηγορίες, ανάλογα με το ποιος μπορεί να έχει πρόσβαση στην ταυτότητα των οντοτήτων. Πρόκειται δηλαδή για

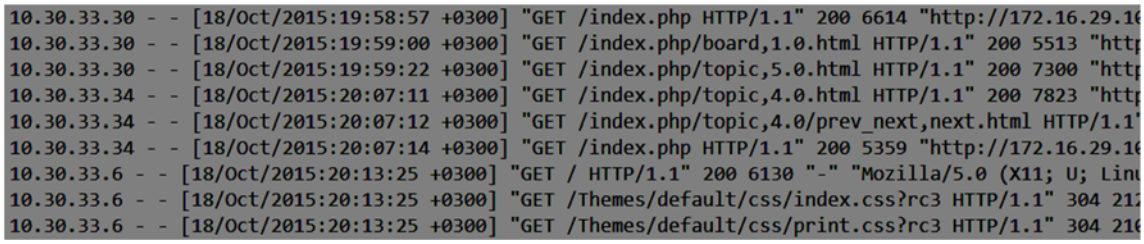
τα δημόσια, που μπορούν όλοι να έχουν πρόσβαση, τα μη-δημόσια, στα οποία έχουν πρόσβαση κάποιες συγκεκριμένες οντότητες και τα ανώνυμα, στα οποία έχουν πρόσβαση μόνο οι οντότητες αυτές καθ' αυτές.

⑩ Τα ψευδώνυμα τα οποία βασίζονται στους ρόλους των οντοτήτων. Όπως και στην προηγούμενη κατηγορία, εγκυμονεί και εδώ ο κίνδυνος της επανα-αναγνώρισης των ταυτοτήτων των οντοτήτων. Μπορούν να χωριστούν σε δύο υπό-κατηγορίες, ανάλογα με τον αριθμό των συναλλαγών στις οποίες χρησιμοποιούνται τα ψευδώνυμα από τις οντότητες. Πρόκειται δηλαδή για τα ψευδώνυμα που μπορούν να χρησιμοποιηθούν σε πολλές περιπτώσεις, οι οποίες σχετίζονται μεταξύ τους, καθώς και τα ψευδώνυμα που μπορούν να χρησιμοποιηθούν μία φορά σε μία και μόνο συναλλαγή.

8.2 Πρακτική Εφαρμογή της Τεχνικής του Shamir για Επίτευξη Ψευδωνυμοποίησης

Στη συνέχεια, θα παρουσιαστεί μία περίπτωση ψευδωνυμοποίησης, η οποία θα βασίζεται στην τεχνική διαμοιρασμού μυστικού του Shamir και η οποία έχει συγκεκριμένα πλεονεκτήματα, τα οποία επιτρέπουν την αξιοποίηση της σε περιπτώσεις όπου εγείρονται ζητήματα όπως αυτά που περιγράφηκαν ανωτέρω και σχετίζονται με αρχεία καταγραφής ενεργειών χρηστών.

Έστω ότι έχουμε ένα αρχείο καταγραφής ενεργειών των χρηστών, στο οποίο καταγράφονται όλες οι IP διευθύνσεις, με τις οποίες πραγματοποιήθηκαν και συνεχίζουν να πραγματοποιούνται συναλλαγές, είτε αυτές είναι καλόβουλες είτε κακόβουλες. Όλες αυτές οι διευθύνσεις καταγράφονται σε ένα αρχείο (log file) με μορφή όπως φαίνεται παρακάτω (για την περίπτωση αρχείου καταγραφής ενεργειών που τηρεί ένα Apache web server):



Εικόνα 6: Τμήμα αρχείου καταγραφής δραστηριοτήτων (log file)

Από το συγκεκριμένο τμήμα του αρχείου καταγραφής, μπορεί εύκολα να γίνει η παρατήρηση ότι έχει υπάρξει επικοινωνία με τις διευθύνσεις 10.30.33.30 , 10.30.33.34 και 10.30.33.6.

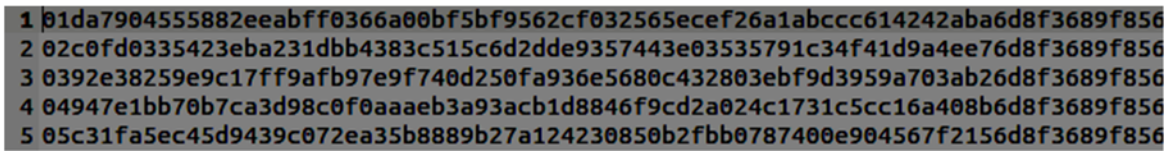
Στη συνέχεια, μπορεί να χρησιμοποιηθεί η τεχνική του Shamir με σκοπό να "σπάσει" κάθε διεύθυνση σε πολλά τμήματα – shares, κάθε ένα εκ των οποίων, όπως θα δούμε, θα αποτελεί "ψευδώνυμο" του αρχικού αναγνωριστικού (IP διεύθυνση). Θα μπορούσε να οριστεί για παράδειγμα, ότι κάθε IP διεύθυνση που υπάρχει μέσα στο αρχείο καταγραφής, θα χωρίζεται σε 5 τμήματα, από τα οποία χρειάζεται να είναι γνωστά τα 4, προκειμένου να γίνει ανακατασκευή τους.

Με τον τρόπο που περιγράφηκε νωρίτερα στο Κεφάλαιο 7, προκύπτει ότι οι τρεις παραπάνω διευθύνσεις μπορούν να χωριστούν, με τη χρήση της εντολής **echo "IP pou spaei" | secret-share-split -n 5 -t 4 > arxeioapothikeusis.txt** στα εξής κομμάτια, τμήματα των οποίων φαίνονται παρακάτω :

- Για την διεύθυνση 10.30.33.30 :

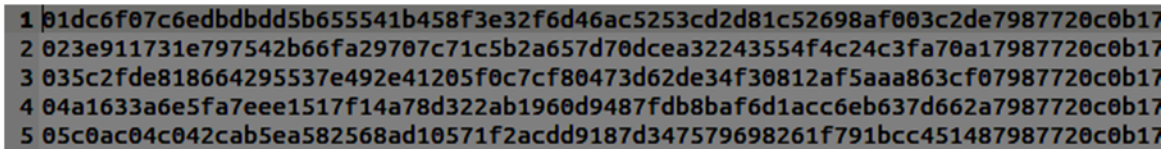
Εικόνα 7: Τμήμα των shares που δημιουργήθηκαν για την IP διεύθυνση 10.30.33.30

- Για την διεύθυνση 10.30.33.34 :



Εικόνα 8: Τμήμα των shares που δημιουργήθηκαν για την IP διεύθυνση 10.30.33.34

❿ Για την διεύθυνση 10.30.33.6 :



Εικόνα 9: Τμήμα των shares που δημιουργήθηκαν για την IP διεύθυνση 10.30.33.6

Από την παραπάνω διαδικασία φαίνεται ότι κάθε μυστικό, όπως στη συγκεκριμένη περίπτωση μια διεύθυνση IP, μπορεί εύκολα να σπάσει σε πολλά κομμάτια με τη χρήση της τεχνικής του Shamir. Τι κερδίζουμε όμως από έναν τέτοιο "διαχωρισμό" μίας IP διεύθυνσης σε πολλά επιμέρους ψευδώνυμα; Προκειμένου να υπάρξει μεγαλύτερη ασφάλεια και να θεωρηθεί η παραπάνω διαδικασία σαν καλή ψευδωνυμοποίηση, θα πρέπει να ακολουθηθεί μια λίγο πιο περίπλοκη διαδικασία.

Ουσιαστικά, μία πιο ολοκληρωμένη προσέγγιση που έχει προταθεί σε αυτήν την κατεύθυνση (Biskup & Flegel, 2000) είναι η ακόλουθη, και η οποία είναι προσανατολισμένη ακριβώς σε μηχανισμούς ανίχνευσης εισβολών. Κάθε διεύθυνση IP, που αποτελεί το βασικό μυστικό, συνδέεται-αντιστοιχίζεται με μία ταυτότητα. Αυτά τα ζευγάρια δημιουργούνται για κάθε περίπτωση επικοινωνίας με κάποια διεύθυνση IP. Υπάρχουν κάποιες οντότητες, που μπορούν να έχουν πρόσβαση σε αυτές τις ταυτότητες, οι οποίες οντότητες μπορούν να χαρακτηριστούν ως οντότητες επαναταυτοποίησης. Κάθε μία από αυτές τις οντότητες, όπως επίσης και οι οντότητες που παράγουν τα ψευδώνυμα, γνωρίζει ποιες είναι οι αντιστοιχήσεις, δηλαδή ποιες είναι οι πραγματικές ταυτότητες που αντιστοιχίζονται σε μία περίπτωση συναλλαγής. Στη συνέχεια, το κάθε

ζεύγος μυστικού-ταυτότητας, μπορεί εύκολα με τη χρήση της τεχνικής του Shamir να "σπάσει" σε πολλά κομμάτια-shares: ο διαχωρισμός αυτός γίνεται από άλλη οντότητα. Ταυτόχρονα, μπορεί οι οντότητες επαναταυτοποίησης να γνωρίζουν τις αντιστοιχήσεις των διευθύνσεων IP με τις ταυτότητες, αλλά τα μυστικά αυτά καθ' αυτά που έχουν προκύψει δεν τους παρέχουν καμία απολύτως πληροφορία για το ποια από αυτά μπορούν να συνδυαστούν για να ανακατασκευαστεί μία διεύθυνση IP. Αν συνέβαινε το αντίθετο, τότε δεν θα μπορούσαν να θεωρηθούν αυτά τα ψευδώνυμα έγκυρα. Το μόνο που μπορούν να κάνουν είναι να κάνουν τυχαίους συνδυασμούς, κάτι που είναι όμως σχεδόν απίθανο να τους οδηγήσει σε σωστό συνδυασμό.

Δεδομένου ότι η παραπάνω διαδικασία μπορεί να πραγματοποιηθεί για οποιαδήποτε διεύθυνση IP υπάρχει στο αρχείο καταγραφής, προκύπτει το συμπέρασμα ότι μπορούν αυτές να σπάσουν σε πολλά κομμάτια, καθένα από τα οποία έχει μία μορφή, που δεν προδίδει κανένα στοιχείο για την αρχική διεύθυνση IP. Αυτό σημαίνει δηλαδή ότι, ακόμα και αν κάποιο από αυτά τα κομμάτια έρθει στα χέρια ενός αντιπάλου, τότε δεν θα μπορεί με κανένα τρόπο να ανακτήσει την αρχική διεύθυνση IP. Πρόκειται δηλαδή για μία περίπτωση ψευδωνυμοποίησης.

Για να φανεί αυτό στην πράξη, έστω ότι οι τρεις παραπάνω διευθύνσεις έχουν συνδεθεί με τις εξής ταυτότητες:

1 → 10.30.33.30	2 → 10.30.33.34	3 → 10.30.33.6

Πίνακας 12: Δημιουργία ταυτοτήτων για κάθε διεύθυνση

Τη συγκεκριμένη αντιστοίχιση την γνωρίζουν τόσο οι οντότητες επαναταυτοποίησης, όσο και αυτές που κατασκευάζουν τα ψευδώνυμα.

Στη συνέχεια κάθε μία από αυτές τις ταυτότητες, σπάει, με τη χρήση της εντολής **echo "tautotita->IP" | secret-share-split -n 10 -t 8 > arxeioapothikeusis.txt** με τυχαία επιλογή αριθμών στο συγκεκριμένο παράδειγμα, σε 10 κομμάτια, τμήματα των οποίων φαίνονται στις παρακάτω εικόνες :

Εικόνα 10: Δημιουργία shares για την ταυτότητα της IP διεύθυνσης 10.30.33.30

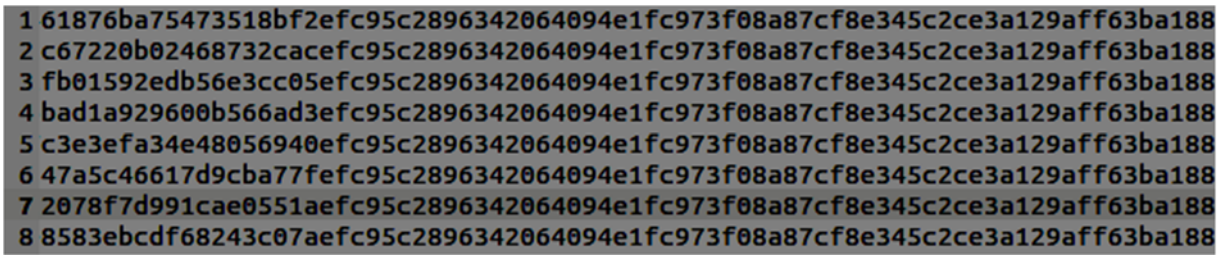
Εικόνα 11: Δημιουργία shares για την ταυτότητα της IP διεύθυνσης 10.30.33.34

Εικόνα 12: Δημιουργία shares για την ταυτότητα της IP διεύθυνσης 10.30.33.6

Στη συνέχεια, εφόσον συνεχίζεται η παραγωγή αυτή των shares, και αυτά αποθηκεύονται με τυχαία σειρά, δεν μπορεί κανείς να γνωρίζει πια από αυτά αποτελούν κομμάτια μιας IP διεύθυνσης που μπορούν να χρησιμοποιηθούν για την ανακατασκευή τους, καθώς δεν παρέχουν καμία πληροφορία. Δημιουργείται έτσι μια περίπτωση ψευδωνυμοποίησης.

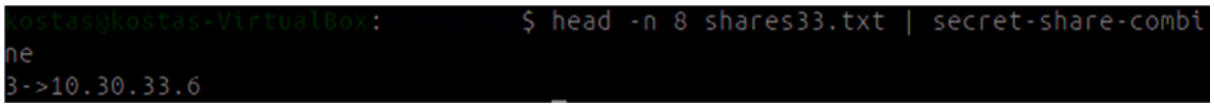
Μετά την δημιουργία των παραπάνω shares, και σε περίπτωση που υπάρξει κάποιος σημαντικός λόγος, όπως για παράδειγμα υποψία ότι κάποια IP διεύθυνση ανήκει σε μια οντότητα με ύποπτη δραστηριότητα, τότε ανάλογα και με το κατώφλι που έχει οριστεί, μπορούν να χρησιμοποιηθούν τα shares αυτά για να γίνει ανάκληση της ύποπτης διεύθυνσης IP.

Έτσι στο παράδειγμα, αν γίνει η υπόθεση ότι παρατηρήθηκε μια ύποπτη δραστηριότητα, σχετικά με την διεύθυνση 10.30.33.6, τότε μπορούν να χρησιμοποιηθούν,μετά από συνεννόηση των κατόχων τους, τα εξής 8 τουλάχιστον shares :



Εικόνα 13: Τμήμα των shares που χρησιμοποιούνται για ανακατασκευή της ταυτότητας της IP διεύθυνησης 10.30.33.6

Τέλος, με τη χρήση του εργαλείου που παρουσιάστηκε στην αρχή του κεφαλαίου, και πιο συγκεκριμένα με τη χρήση της ακόλουθης εντολής, μπορεί να ανακατασκευαστεί η αντιστοίχιση που έγινε νωρίτερα και κατά συνέπεια η “επικίνδυνη” διεύθυνση IP.



Εικόνα 14: Αποτέλεσμα ανακατασκευής της ταυτότητας της IP διεύθυνσης 10.30.33.6

Ουσιαστικά, το πλεονέκτημα αυτής της μεθόδου, όπως αναφέρεται και στο (Biskup & Flegel, 2000), είναι ότι ο μηχανισμός παρακολούθησης των αρχείων καταγραφής μπορεί να "βλέπει" αρχικώς ψευδώνυμα και όχι τις πραγματικές IP διευθύνσεις: με αυτόν τον τρόπο προστατεύεται η ιδιωτικότητα των απλών χρηστών: σημειώνεται ότι οι ερευνητές στο (Biskup & Flegel, 2000) θεωρούν ως μοντέλο ασφάλειας την περίπτωση όπου ενδέχεται να είναι κακόβουλος αυτός που ελέγχει τα αρχεία καταγραφής και να κάνει και άλλη επεξεργασία από αυτή που πρέπει – ενώ επίσης η προτεινόμενη τεχνική καλύπτει και περίπτωση διαρροής του αρχείου καταγραφής σε κακόβουλο τρίτο, αφού κατά τον προτεινόμενο τρόπο δεν θα περιέχει πληροφορίες που θα ταυτοποιούν χρήστες. Από την άλλη πλευρά, αν για κάποια "ψευδωνυμοποιημένη" IP διεύθυνση διαφαίνεται ενδεχόμενο ύποπτης συμπεριφοράς, τότε ενεργοποιείται διαφανώς κατάλληλη διαδικασία εσωτερικά στον οργανισμό έτσι ώστε να συνδυάσουν τις πληροφορίες τους k οντότητες που κατέχουν k ψευδώνυμα (shares) για να ανακτήσουν την αρχική IP διεύθυνση. Σημειώνεται δε ότι η οντότητα που μπορεί να κάνει επαναταυτοποίηση δεν χρειάζεται να έχει προσβάσεις στα αρχεία καταγραφής. Με αυτόν τον τρόπο, η δυνατότητα ανάλυσης ενεργειών, για δημιουργία π.χ. προφίλ συμπεριφοράς, καλόβουλων χρηστών εξαλείφεται (Biskup & Flegel, 2000).

Αξίζει να αναφερθεί ότι η παραπάνω διαδικασία, θα μπορούσε να εφαρμοστεί όχι μόνο για ολόκληρες τις διευθύνσεις IP, αλλά ακόμα και για το τελευταίο τμήμα αυτών. Η ανάθεση δηλαδή ταυτοτήτων μπορεί να γίνει για τα τελευταία 2 κομμάτια των διευθύνσεων αυτών. Στη συνέχεια θα μπορούσαν να δημιουργηθούν με την ίδια ακριβώς μέθοδο τα shares, τα οποία να περιέχουν την ταυτότητα των τμημάτων των διευθύνσεων IP, και εφόσον κριθεί αναγκαίο, να πραγματοποιηθεί ανακατασκευή τους.

8.3 Νέες Κατευθύνσεις Συμβολής της Τεχνικής του Shamir

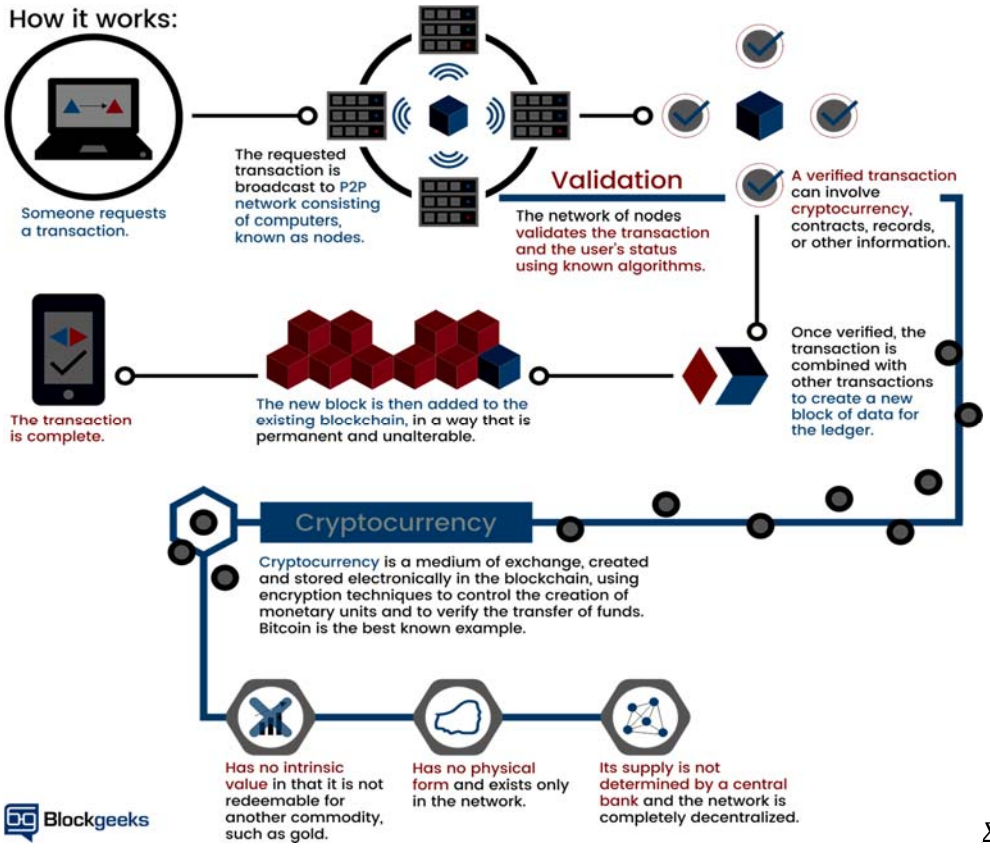
Στο παρόν τελευταίο τμήμα της μεταπτυχιακής διατριβής, θα γίνει μια παρουσίαση ορισμένων προτάσεων, για νέες κατευθύνσεις στις οποίες μπορεί να στραφεί κανείς με τη χρήση της τεχνικής του Shamir. Στόχος μας είναι να αναδείξουμε πώς η ως άνω τεχνική, εφαρμοζόμενη στον τομέα της ψευδωνυμοποίησης προσωπικών δεδομένων, μπορεί να δώσει λύσεις σε σημερινές σύνθετες εφαρμογές, παρέχοντας κατά αυτόν τον τρόπο συνεισφορά στην απάντηση σημερινών ερευνητικών ερωτημάτων. Ειδικότερα, τα τελευταία έτη υπάρχει πολύ έντονη ερευνητική δραστηριότητα ως προς την αξιοποίηση τεχνολογιών blockchain για την υποστήριξη υπηρεσιών ασφάλειας , αφού τα blockchain αποτελούν ένα κατάλληλο μέσο για την καταγραφή συμβάντων/αναφορών σε ένα σύστημα. Από την άλλη πλευρά, εκ της φύσης τους οι τεχνολογίες blockchain εγείρουν ζητήματα ως προς την προστασία προσωπικών δεδομένων, για αυτό και αποτελεί τρέχουσα ερευνητική δραστηριότητα η αντιμετώπιση των ζητημάτων αυτών (Brotsis et al., 2019; Kolokotronis et al., 2019; Minoli & Occhiogrosso, 2018; Reyna et al., 2018).

Στην παρούσα ενότητα, θα προταθεί ένα καινούριο και ταυτόχρονα ρεαλιστικό σενάριο εφαρμογής της τεχνικής διαμοιρασμού μυστικού του Shamir, στο οποίο θα μπορεί να χρησιμοποιηθεί η πρόσφατη παραλλαγή αυτής η οποία βασίζεται στη φόρμουλα παρεμβολής του Newton, το οποίο θα αποσκοπεί στην ψευδωνυμοποίηση προσωπικών δεδομένων (κατά τρόπο ανάλογο με αυτόν που παρουσιάστηκε στην προηγούμενη ενότητα) τα οποία αποθηκεύονται σε δομές blockchain.,

8.3.1 Σύντομη Παρουσίαση του Blockchain

Ο όρος Blockchain, αναφέρεται σε μια βάση δεδομένων, η οποία είναι κατανεμημένη σε διάφορα γεωγραφικά μέρη. Η βάση αυτή των δεδομένων, αποτελείται από ένα σύνολο πολλών blocks, τα οποία έχουν μία συγκεκριμένη δομή. Τα blocks αυτά συνδέονται

μεταξύ τους με μία χρονική ακολουθία και με μία αναφορά στο προηγούμενο block, δημιουργώντας έτσι μια αλυσίδα (Δρ. Κωνσταντίνος Λιμνιώτης, 2019). Η αλυσίδα Blockchain, χρησιμοποιείται για την περιγραφή διάφορων συναλλαγών που έχουν πραγματοποιηθεί καθώς και για την αποθήκευση διαφόρου είδους ψηφιακών αγαθών με έναν ασφαλή και διαφανή τρόπο. Η κάθε συναλλαγή υπογράφεται ψηφιακά με το ιδιωτικό κλειδί του ιδιοκτήτη και στη συνέχεια επικυρώνεται με το δημόσιο κλειδί. (Kolokotronis et al., 2019) Ακόμη, το Blockchain αποτελεί έναν μηχανισμό που επιτρέπει την επικύρωση των συναλλαγών που συμβαίνουν και παρέχει πρόσβαση σε συναλλαγές που έχουν συμβεί στο παρελθόν, με ακριβής πληροφορίες για τη χρονική στιγμή που αυτές πραγματοποιήθηκαν. (Reyna et al., 2018).

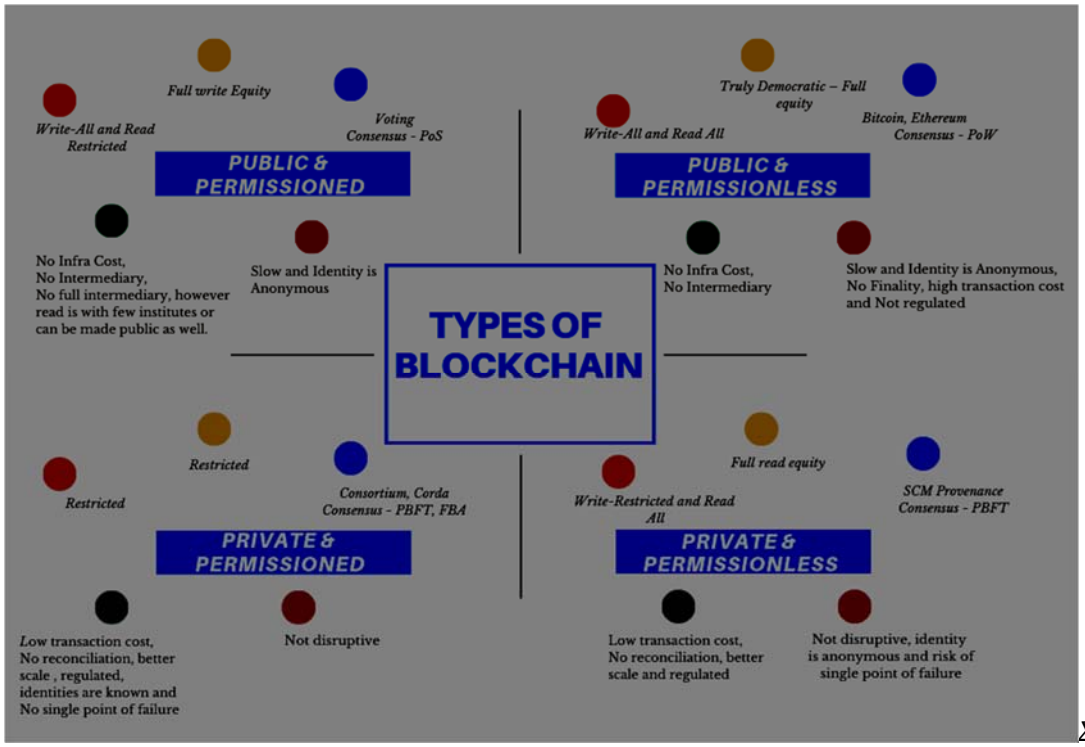


Σχήμα 8:

Περιγραφή λειτουργίας Blockchain ,

Πηγή : " Blockchain Technology Explained to Understand it " , (Techloyce.com, 2017)

Ένα Blockchain μπορεί να ανήκει σε μία από δύο κατηγορίες, δημόσιο και ιδιωτικό (Gwyneth Iredale, 2021). Η βασική διαφορά έγκειται στο γεγονός ότι στην πρώτη περίπτωση η αλυσίδα είναι ανοιχτή για οποιονδήποτε επιθυμεί να έχει πρόσβαση σε αυτή. Αντίθετα, στη δεύτερη περίπτωση, πρόσβαση μπορούν να έχουν μόνο συγκεκριμένες οντότητες που ανήκουν σε έναν οργανισμό. Ένας ακόμη διαχωρισμός μπορεί να είναι σε permissioned και permissionless blockchain. Η βασική τους διαφορά είναι ότι στα permissionless blockchains δεν χρειάζεται κάποια ειδική άδεια για να μπορεί κάποιος να συμμετέχει ή να αλληλεπιδρά, και μπορεί επομένως ο οποιοσδήποτε να συμμετέχει και να επικυρώσει μία συναλλαγή. Κάτι τέτοιο δεν συμβαίνει στα permissioned blockchains, όπου δεν μπορεί να συμμετέχει ο οποιοσδήποτε και την επικύρωση μιας συναλλαγής την πραγματοποιεί ένα επιλεγμένο σύνολο ατόμων, που έχει επιλεγεί με την συγκατάθεση του ιδιοκτήτη του blockchain (Permissioned vs Permissionless Blockchains, 2020)



Σχήμα 9: Κατηγορίες Blockchain ,

Πηγή : " Types of blockchain networks " , (Vivek Acharya et al., 2019)

8.3.2 Γενικά Χαρακτηριστικά Τεχνολογίας Blockchain

Στην παρούσα υποενότητα, θα γίνει παρουσίαση των γενικών χαρακτηριστικών που διαθέτει η τεχνολογία του Blockchain. Πιο συγκεκριμένα (Chakray.com, n.d.; Fabiano, 2017; Joshi et al., 2018; Kolokotronis et al., 2019; Minoli & Occhiogrosso, 2018; Oksiiuk & Dmyrieva, 2020; Reyna et al., 2018):

- Ο μηχανισμός Blockchain, παρέχει τη δυνατότητα σε οντότητες να μπορούν να δουν τα blocks ανάλογα με την εφαρμογή. Υπάρχουν περιπτώσεις που παρέχεται η δυνατότητα σε κάποιον να δει τις συναλλαγές, αλλά χρησιμοποιούνται ψευδώνυμα και δεν μπορεί να δει αυτούς που τις εκτελούν (π.χ. Bitcoin). Υπάρχουν και περιπτώσεις που το περιεχόμενο δεν είναι προσβάσιμο, αφού μπορεί να χρησιμοποιούνται κρυπτογραφικοί μηχανισμοί, και πιο συγκεκριμένα ιδιωτικά κλειδιά. Βέβαια, υπάρχει πάντα το ενδεχόμενο, σε περίπτωση που αποκαλυφθεί ο χρήστης ενός κλειδιού, δημόσιου ή ιδιωτικού, τότε αυτό να οδηγήσει σε σύνδεση και αποκάλυψη άλλων ενεργειών που έγιναν από τον συγκεκριμένο χρήστη, καθώς και πληροφοριών για εκείνον.

- Στην περίπτωση που ο μηχανισμός είναι δημόσιος, δεδομένου ότι αποτελεί μία κατανεμημένη βάση δεδομένων, όπως αναφέρθηκε και προηγουμένως, τα δεδομένα αυτά βρίσκονται διασκορπισμένα και αποθηκευμένα σε διάφορες γεωγραφικές τοποθεσίες. Ακόμα όμως και στην περίπτωση που είναι ιδιωτικός, πρόκειται για μια μερικώς κατανεμημένη βάση δεδομένων, που παρέχει παρόλα αυτά κάποια επίπεδα εμπιστοσύνης.

- "Ότι γράφει δεν ξεγράφει". Οποιαδήποτε συναλλαγή και γενικότερα πληροφορία αποθηκεύεται στο Blockchain, παραμένει εκεί αμετάβλητη. Εφόσον κάποιος θελήσει να τροποποιήσει κάποια καταγραφή, τότε το κόστος για να το

πραγματοποιήσει αυτό είναι τεράστιο, γεγονός που ουσιαστικά αποτρέπει οποιαδήποτε τέτοιου είδους ενέργεια. Το γεγονός αυτό όμως μπορεί να αποτελέσει μειονέκτημα για οποιαδήποτε χρήστη μετανιώσει και θέλει να αναιρέσει οποιαδήποτε πληροφορία πρόσθεσε στο Blockchain.

- Χρησιμοποιούνται timestamps. Αυτό πρακτικά σημαίνει ότι κάθε block που προστίθεται στην αλυσίδα, περιέχει ακριβείς πληροφορίες για τον ακριβή χρόνο που αυτές πραγματοποιήθηκαν και προστέθηκαν στην αλυσίδα, τηρώντας μία χρονική ακολουθία των "συμβάντων" (συναλλαγών) που καταγράφονται στο Blockchain.

- Προκειμένου να μπορεί μια οντότητα να εγκρίνει μια συναλλαγή, πρέπει να αποκτήσει μέσω κάποιου μηχανισμού κοινής συμφωνίας (consensus mechanism), ομοφωνία αυτή την ιδιότητα. Υπάρχουν διάφορα πρωτόκολλα κοινής συμφωνίας (π.χ. Proof-of-Work, Proof-of-Stake κ.α.)

- Σε περίπτωση που κάποια πληροφορία έχει προστεθεί στην αλυσίδα, τότε κανείς δεν μπορεί να αμφισβητήσει την ύπαρξη της.

8.3.3 Χρήση Blockchain για Ασφάλεια σε IoT Περιβάλλοντα

Αποτελεί πραγματικότητα το γεγονός ότι, η αλυσίδα Blockchain μπορεί να συμβάλλει στην ενίσχυση της ασφάλειας και να παρέχει λύσεις σε ζητήματα που έχουν να κάνουν με την ασφάλεια και το πως μπορεί αυτή να επιτευχθεί στα περιβάλλοντα του Διαδικτύου των Πραγμάτων (Internet of Things – IoT). Πιο συγκεκριμένα, οι πληροφορίες και οι διαφόρου είδους επικοινωνίες που γίνονται μέσω των IoT συσκευών, μπορούν να αποθηκεύονται σαν συναλλαγές στο Blockchain (Brotsis et al., 2019; Kolokotronis et al., 2019; Minoli & Occhiogrosso, 2018; Reyna et al., 2018). Χαρακτηριστικά μπορεί το Blockchain να προσφέρει τις εξής λύσεις :

- Σχετικά με την προστασία των ταυτοτήτων, το Blockchain μπλοκάρει πιθανές προσπάθειες κλοπής τους, ψεύτικων πιστοποιητικών δημοσίων κλειδιών και επιθέσεων man-in-the-middle. Αυτό συμβαίνει λόγω του ότι το blockchain παρέχει τη δυνατότητα για αναγνώριση οποιασδήποτε ταυτότητας μιας συσκευής καθώς επίσης και έμπιστων μεθόδων αυθεντικοποίησης.

- Σχετικά με την ασφάλεια της επικοινωνίας μεταξύ των IoT συσκευών, το Blockchain χρησιμοποιεί μία ποικιλία κρυπτογραφικών μηχανισμών, δημιουργώντας υψηλά επίπεδα ασφάλειας.

- Σχετικά με την ασφάλεια στις πληροφορίες που ανταλλάσσονται μεταξύ των IoT συσκευών, το Blockchain παρέχει τη δυνατότητα παροχής ασφάλειας τους, αποθηκεύοντας τα σαν συναλλαγές, που επικυρώνονται μέσω της χρήσης έξυπνων συμβολαίων. Επιπλέον, παρέχει ασφάλεια, σταματώντας DDoS επιθέσεις και προστατεύοντας τις υποδομές των σημαντικών πληροφοριών.

- Σχετικά με την ασφάλεια των δεδομένων των IoT συσκευών, που αποθηκεύονται στο Blockchain, όπως αναφέρθηκε και νωρίτερα, παραμένουν εκεί αμετάβλητα τόσο αυτά όσο και η χρόνοι που αυτά συλλέχθηκαν και αποθηκεύτηκαν.

- Δεδομένου ότι το Blockchain αποτελεί μια αποκεντροποιημένη βάση δεδομένων, μπορεί να αποτρέψει πιθανές επιθέσεις αντιπάλων στις πληροφορίες των IoT συσκευών, καθώς είναι αδύνατο να επιτεθούν ταυτόχρονα και με επιτυχία σε πολλά διαφορετικά μέρη και συστήματα.

Από την άλλη μεριά, προκύπτουν ορισμένα ζητήματα σχετικά με την ασφάλεια και την ιδιωτικότητα, τα οποία εγείρουν αμφιβολίες σχετικά με την καταλληλότητα εφαρμογής της αλυσίδας Blockchain στο Διαδίκτυο των Πραγμάτων, σε διάφορες περιπτώσεις, είτε

είναι αυτή δημόσια είτε ιδιωτική (Brotsis et al., 2019; CyfRA, n.d.; Kolokotronis et al., 2019; Minoli & Occhiogrosso, 2018; Reyna et al., 2018).

- Μπορεί να δημιουργηθεί πρόβλημα σχετικά με την αξιοπιστία των δεδομένων. Ο μηχανισμός του Blockchain μπορεί να διασφαλίσει ότι τα δεδομένα μέσα στην αλυσίδα παραμένουν εκεί αμετάβλητα, αν όμως προστεθούν δεδομένα μη γνήσια ή ανακριβή ή κακόβουλα ("ξεγελώντας" το μηχανισμό κοινής συμφωνίας που έχει υιοθετηθεί) δεν θα μπορεί κανείς να ελέγξει την αξιοπιστία τους, με αποτέλεσμα να παραμείνουν σε αυτή τη μορφή

- Εφόσον τα δεδομένα που συλλέγονται μέσω των IoT συσκευών, μπορεί να είναι πολλές φορές ευαίσθητα δεδομένα που συνδέονται με την ταυτότητα ορισμένων ανθρώπων, θα πρέπει να μπορεί να διασφαλιστεί η ανωνυμία αυτών των ατόμων καθώς επίσης και η ιδιωτικότητα των δεδομένων.

- Δεδομένου ότι τα δεδομένα που εισάγονται στο Blockchain παραμένουν εκεί αμετάβλητα, θα πρέπει, εφόσον αυτά αναφέρονται σε προσωπικά στοιχεία των χρηστών ενός IoT περιβάλλοντος και αν εκείνος το επιθυμεί οποιαδήποτε στιγμή, να μπορούν να αφαιρεθούν.

- Αναφέρθηκε προηγουμένως ότι τα δεδομένα που εισάγονται στο Blockchain είναι προσβάσιμα είτε σε οποιονδήποτε (δημόσιο Blockchain) είτε στις οντότητες ενός οργανισμού (ιδιωτικό Blockchain). Μπορεί όμως να προκύψουν θέματα ιδιωτικότητας, όταν τα δεδομένα αυτά περιέχουν ευαίσθητες πληροφορίες, οι οποίες, σύμφωνα και με την νομοθεσία που υπάρχει σχετικά με την προστασία των προσωπικών δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR), γίνονται γνωστά σε περισσότερες οντότητες, χωρίς να υπάρχει συγκατάθεση ή άλλη επαρκής νομική βάση. Για παράδειγμα, ακόμα και στην περίπτωση ενός ιδιωτικού Blockchain, στο οποίο αποθηκεύονται οι διευθύνσεις IP ενός συστήματος, παρόλο που μπορούν μόνο συγκεκριμένες οντότητες να

έχουν πρόσβαση σε αυτές, εξακολουθεί να υφίσταται το ίδιο πρόβλημα (βλ. την ανάλυση της προηγούμενης ενότητας για ζητήματα προστασίας προσωπικών δεδομένων που εγείρονται από “υπερσυλλογή” προσωπικών δεδομένων που μπορούν να χρησιμοποιηθούν και για διαφορετικούς, από τους αρχικούς, σκοπούς).

8.3.4 Εφαρμογή της Τεχνικής του Shamir στη Δομή του Blockchain

Όπως αναφέρθηκε και νωρίτερα στην ενότητα 6.4.2, η δομή του Blockchain διαθέτει αρκετά πλεονεκτήματα, αλλά ταυτόχρονα εγείρονται και πολλά ζητήματα σχετικά με την ασφάλεια και την ιδιωτικότητα. Προκειμένου να αντιμετωπιστούν τα παραπάνω ζητήματα, στο σημείο αυτό προτείνουμε τη χρήση Πρωτοκόλλων Ασφαλών Υπολογισμών Πολλών Συμμετεχόντων, και πιο συγκεκριμένα η τεχνική Shamir Secret Sharing.

Έστω ότι υπάρχει μία περίπτωση ενός Συστήματος Καταγραφής Συμβάντων , όπως αναφέρθηκε και νωρίτερα, το οποίο καταγράφει κάθε συναλλαγή-επικοινωνία σε ένα σύστημα (π.χ. ένα IoT περιβάλλον, όπως π.χ. ένα “έξυπνο” σπίτι), οι οποίες συναλλαγές αφορούν οντότητες που “αναγνωρίζονται” μέσω των διευθύνσεων IP (προφανώς, οποιοαδήποτε αναγνωριστικό (identifier), εκτός από διεύθυνση IP, θα μπορούσε να χρησιμοποιηθεί αντίστοιχα). Επιπλέον, ας γίνει η υπόθεση ότι χρησιμοποιούνται οι δομές του Blockchain για την καταγραφή και αποθήκευση αυτών των ενεργειών, οι οποίες συσχετίζονται με διευθύνσεις IP. Εφόσον επιλεγεί το να γίνει αποθήκευση των διευθύνσεων IP αυτών καθ’ αυτών στην αλυσίδα του Blockchain για σκοπούς διαφανούς ιχνηλάτησης (tracking) ενεργειών των διαφόρων χρηστών, τότε δημιουργούνται πολλά προβλήματα τα οποία έχουν άμεση σχέση με την ιδιωτικότητα και τα ζητήματα που

αναφέρθηκαν στην υποενότητα 6.4.2. Πιο συγκεκριμένα, εγείρονται θέματα σχετικά με την προστασία προσωπικών δεδομένων, αφού για παράδειγμα οι διευθύνσεις αυτές μπορεί από τη μία να μην είναι δημόσια ανοιχτές και προσβάσιμες στον οποιονδήποτε (αφού τα blockchains που χρησιμοποιούνται σε αυτήν την περίπτωση πρέπει να είναι ιδιωτικά και όχι δημόσια), αλλά παρόλα αυτά είναι ορατές στους χρήστες του οργανισμού που μπορούν να έχουν πρόσβαση στην αλυσίδα, χωρίς να υπάρχει σχετική παροχή έγκρισης για την γνωστοποίηση σε όλες αυτές τις οντότητες (για παράδειγμα, για την περίπτωση "'εξυπνου" σπιτιού, στο blockchain μπορεί να αποθηκεύεται και πληροφορία σχετικά με τις διαδικτυακές ενέργειες που πραγματοποιούν οι συσκευές του χρήστη, οπότε και η επεξεργασία αυτών των πληροφοριών μπορεί να οδηγήσει σε εξαγωγή συμπερασμάτων για την καθημερινότητα του χρήστη και τις συνήθειές του, χωρίς αυτός να το γνωρίζει). Γενικότερα, το πρόβλημα αυτό μπορεί να γενικευτεί σε οποιαδήποτε προσπάθεια γίνει να αποθηκευτούν συμβάντα, παρόμοια με την περίπτωση των διευθύνσεων IP, τα οποία περιέχουν πληροφορίες και προσωπικά δεδομένα, στην αλυσίδα ενός ιδιωτικού Blockchain.

Στο σημείο αυτό, θα μπορούσε να αξιοποιηθεί κατάλληλα η περίπτωση που αναφέρθηκε νωρίτερα στην ενότητα 8.2, για ψευδωνυμοποίηση με τη χρήση της τεχνικής του Shamir. Πιο συγκεκριμένα, μπορεί να χρησιμοποιηθεί η δημιουργία των shares από τις ταυτότητες των δεδομένων, που έχουν δημιουργηθεί όπως ακριβώς αναφέρθηκε στην ενότητα 6.3, όπου τα δεδομένα στη συγκεκριμένη περίπτωση ήταν οι διευθύνσεις IP από ένα αρχείο καταγραφών.

Προκειμένου λοιπόν να επιτευχθεί ο στόχος της αποθήκευσης γεγονότων, όπως για παράδειγμα των IP διευθύνσεων, χωρίς να προκύπτουν τα παραπάνω προβλήματα ιδιωτικότητας, μπορεί να χρησιμοποιηθεί η αλυσίδα του Blockchain σε συνδυασμό με την τεχνική του Shamir για καλή ψευδωνυμοποίηση. Πιο συγκεκριμένα, προκειμένου να επιτευχθεί αυτός ο στόχος, αρκεί να ακολουθηθεί η ακόλουθη διαδικασία, που περιλαμβάνει τα εξής δύο βήματα:

- Το πρώτο βήμα, περιλαμβάνει ουσιαστικά την δημιουργία των ψευδωνύμων με τη χρήση της τεχνικής του Shamir. Ουσιαστικά, αρκεί να δημιουργηθούν οι ταυτότητες των δεδομένων, για παράδειγμα των IP διευθύνσεων, και στη συνέχεια n στον αριθμό shares των ταυτοτήτων αυτών με τη χρήση της τεχνικής του Shamir. Μία οντότητα εντός του οργανισμού θα πραγματοποιεί αυτό το διαχωρισμό (παραγωγή ψευδωνύμων για κάθε αναγνωριστικό χρήστη/συσκευής όπως η IP διεύθυνση, ενέργεια του οποίου/οποίας πρόκειται να εγγραφεί στο blockchain), η οποία οντότητα όμως δεν θα πρέπει να έχει η ίδια πρόσβαση στο blockchain (το οποίο, προφανώς, θα είναι τύπου "permissioned"). Στο σημείο αυτό, αξίζει να τονιστεί ότι η ψευδωνυμοποίηση θα μπορούσε να πραγματοποιηθεί με τη χρήση της φόρμουλας παρεμβολής του Newton – δηλαδή όχι με την κλασική υλοποίηση του Shamir. Ο λόγος για τον οποίο προτείνεται η συγκεκριμένη φόρμουλα παρεμβολής, σε σχέση με αυτή του Lagrange, είναι το γεγονός ότι η συγκεκριμένη φόρμουλα παρέχει ένα πολύ σημαντικό πλεονέκτημα, όπως αναφέρθηκε και νωρίτερα στην υποενότητα 7.2.3. Πρόκειται ουσιαστικά για το γεγονός ότι ακόμα και αν χρειασθεί να προστεθεί κάποια καινούρια πληροφορία, δεν χρειάζεται να τροποποιηθούν οι ήδη υπάρχοντες υπολογισμοί, παρά μόνο να γίνουν αυτοί που αφορούν την καινούρια πληροφορία και να προστεθούν στους προηγούμενους. Με αυτό τον τρόπο, παραμένουν αμετάβλητοι οι υπολογισμοί και γενικότερα οι πληροφορίες που έχουν προστεθεί μέχρι εκείνη τη στιγμή, παρέχοντας μεγαλύτερη ευελιξία αν τυχόν χρειαστεί για οποιοδήποτε λόγο να "προστεθούν σημεία" στο πολυώνυμο υπολογισμού.

- Το δεύτερο βήμα, είναι αυτό που έρχεται να συνδέσει την ψευδωνυμοποίηση μέσω της τεχνικής του Shamir, με τις δομές του Blockchain. Σε αυτό το βήμα, και εφόσον το κάθε ψευδώνυμο έχει "σπάσει" σε n κομμάτια, από τα οποία αρκεί να είναι γνωστά τα k προκειμένου να γίνει η ανακατασκευή του, τοποθετούνται στην αλυσίδα του Blockchain κατά μέγιστο τα k-1 από αυτά, ίσως και λιγότερα. Ουσιαστικά δηλαδή θα πρέπει να υπάρχει στο Blockchain το μεγαλύτερο ποσοστό από αυτά, δηλαδή η βασική πληροφορία, σε τέτοιο μέγεθος που αν κάποιος αποκτήσει πρόσβαση σε αυτά τα k-1, να μην μπορεί να προχωρήσει στην ανάκτηση του αρχικού ψευδωνύμου και να αποκαλυφθεί έτσι κάποια

πληροφορία που πρέπει να μείνει μυστική. Η χρήσιμη λοιπόν πληροφορία, αυτή δηλαδή που σε συνδυασμό με τις k-1 θα δώσει το μυστικό, παραμένει εκτός αλυσίδας Blockchain, και μόνο στην περίπτωση που συντρέχει σημαντικός λόγος μπορεί να χρησιμοποιηθεί. Για παράδειγμα, στην περίπτωση με τις διευθύνσεις IP, αποθηκεύονται στο Blockchain τα k-1 (κατά μέγιστο) τμήματα των αναγνωριστικών τους (ψευδώνυμα), με αποτέλεσμα κανένας από αυτούς που έχουν πρόσβαση στο Blockchain να μην μπορεί να ανακτήσει και να μάθει τις διευθύνσεις IP αυτές καθ' αυτές. Αυτό μπορεί να συμβεί μόνο σε περίπτωση που υπάρξει κάποιο περιστατικό ασφαλείας, όπως για παράδειγμα αν υπάρχει μία υπόνοια ότι κάποια ψευδωνυμοποιημένη διεύθυνση IP ανήκει σε κάποιον κακόβουλο αντίπαλο ή πρόκειται για συσκευή "μολυσμένη" που, υπό την καθοδήγηση εξωτερικού εισβολέα, πραγματοποιεί κακόβουλες ενέργειες. Με αυτόν τον τρόπο, επιτυγχάνονται τα εξής:

- Οι χρήστες που είναι εξουσιοδοτημένοι να έχουν πρόσβαση στο blockchain για έλεγχο συμβάντων ασφάλειας, δεν είναι σε θέση να εξάγουν πληροφορίες σχετικά με τα προφίλ ενεργειών καλόβουλων χρηστών ούτε να κάνουν άλλη περαιτέρω επεξεργασία η οποία θα έθετε σε αμφιβολία τη συμμόρφωση με το νομικό πλαίσιο προστασίας δεδομένων.

- Ανίχνευση "ύποπτων" ενεργειών είναι εφικτή, απλά οι πηγές των ενεργειών αυτών είναι ψευδωνυμοποιημένες. Σε αυτήν την περίπτωση όμως, με κατάλληλη εσωτερική διαδικασία του οργανισμού ενεργοποιείται η άρση της ψευδωνυμοποίησης για αυτές τις περιπτώσεις, προκειμένου να γίνει περαιτέρω ανάλυση επί των πραγματικών δεδομένων.

- Η ψευδωνυμοποιημένη πληροφορία που υπάρχει στο blockchain επιτρέπει στην διεκπεραίωση τυχόν στατιστικών ή άλλου τύπου επιστημονικών αναλύσεων, χωρίς αποκάλυψη στοιχείων που μπορούν να ταυτοποιούν τους χρήστες.

Με την παραπάνω διαδικασία μπορεί έτσι να επιτευχθεί ο στόχος της καλής ψευδωνυμοποίησης με τη χρήση της τεχνικής του Shamir, χρησιμοποιώντας την φόρμουλα παρεμβολής του Newton, προκειμένου να μπορούν να αποθηκεύονται στο εσωτερικό της αλυσίδας Blockchain κρίσιμες πληροφορίες και γενικότερα γεγονότα από αρχεία καταγραφής, για να ενισχύεται η ασφάλεια, προασπίζοντας ταυτόχρονα την ιδιωτικότητα και την προστασία των ευαίσθητων δεδομένων. Προφανώς, η επιλογή των κατάλληλων παραμέτρων k, n χρήζει διερεύνησης και μελέτης (για παράδειγμα, ενδεχομένως και χαμηλές τιμές τους να είναι επαρκείς, ενώ διαφαίνεται ότι η αποθήκευση λιγότερων από k-1 ψευδωνύμων στο blockchain είναι μάλλον επιθυμητή, προκειμένου να ελαχιστοποιείται ακόμα περισσότερο η δυνατότητα άρσης της ψευδωνυμοποίησης από κάποιον τρίτο που δεν θα έπρεπε να είναι σε θέση να την κάνει. Επισημαίνεται ότι η εσωτερική διαδικασία του οργανισμού προκειμένου να αρθεί η ψευδωνυμοποίηση μπορεί να στηρίζεται στο ότι θα πρέπει να συναινέσουν συγκεκριμένες, καλά προσδιορισμένες, οντότητες εντός αυτού που η κάθε μία κατέχει ένα “ψευδώνυμο”, έτσι ώστε στο πλήθος τους να είναι k.

Κεφάλαιο 9

Επίλογος

Στο πλαίσιο της παραπάνω μεταπτυχιακής διατριβής, πραγματοποιήθηκε μία γενική παρουσίαση της έννοιας των πρωτοκόλλων ασφαλών υπολογισμών πολλών συμμετεχόντων. Πιο συγκεκριμένα αναφέρθηκαν οι σημαντικότεροι λόγοι για τους οποίους είναι απαραίτητη η χρήση των συγκεκριμένων πρωτοκόλλων. Δεδομένης της χρησιμοποίησης ορισμένων εννοιών που συνδέονται άμεσα με τα πρωτόκολλα SMC, παρουσιάστηκαν και οι σημαντικότεροι ορισμοί και νομικές βάσεις που συνδέονται με τα πρωτόκολλα SMC, όπως αυτά περιγράφονται στον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR). Ακολούθως έγινε αναφορά στην ασφάλεια των SMC πρωτοκόλλων και στους παράγοντες που την διαμορφώνουν, τόσο στον πραγματικό όσο και στον ιδεατό κόσμο. Στη συνέχεια, παρουσιάστηκαν οι σημαντικότερες τεχνικές που χρησιμοποιούνται στα πρωτόκολλα ασφαλών υπολογισμών πολλών συμμετεχόντων καθώς και οι σημαντικότερες εφαρμογές που αυτές μπορεί να τυγχάνουν.

Η μεταπτυχιακή αυτή διατριβή, εστίασε στη συνέχεια σε μία συγκεκριμένη τεχνική, και πιο συγκεκριμένα σε αυτή του διαμοιρασμού μυστικού του Shamir. Αρχικά, μέσα από

μετρήσεις που έγιναν σε εικονικά περιβάλλοντα, και με τη χρήση ενός εργαλείου, έγινε προσπάθεια να καταγραφούν οι χρόνοι που χρειάζονται τόσο για την δημιουργία των μυστικών (shares), όσο και για την ανακατασκευή του αρχικού μηνύματος. Από τις παραπάνω μετρήσεις προέκυψε το συμπέρασμα ότι ο αριθμός των shares, είτε που επιλέγεται να δημιουργηθούν είτε που συνδυάζονται για την ανακατασκευή του αρχικού μηνύματος, καθώς και το μέγεθος του αρχικού μυστικού, επηρεάζουν τον χρόνο εκτέλεσης των εντολών.

Σε επόμενο βήμα, πραγματοποιήθηκε μία σύγκριση ανάμεσα στις φόρμουλες παρεμβολής του Lagrange και του Newton, καθώς και του πως αυτές συμπεριφέρονται με την προσθήκη ενός νέου σημείου. Από την μελέτη αυτή προέκυψε το συμπέρασμα ότι φόρμουλα παρεμβολής Newton, είναι πιο εύχρηστη σε σχέση με τη φόρμουλα παρεμβολής Lagrange, καθώς παρέχει τη δυνατότητα για ταχύτερους υπολογισμούς, με μεγαλύτερη ευκολία στην εκτέλεση τους, ακόμα και με την πρόσθεση νέων σημείων για τον υπολογισμό των πολυωνύμων και κατά συνέπεια για την ανακατασκευή του αρχικού μηνύματος. Μόνο στην περίπτωση που δεν υπάρχει πρόσθεση επιπλέον σημείων, θα μπορούσε να χρησιμοποιηθεί με απλοποιήσεις η φόρμουλα του Lagrange, παρέχοντας κάποιο πλεονέκτημα, και πιο συγκεκριμένα αυτό των πιο απλοποιημένων υπολογισμών.

Στο τελευταίο κομμάτι της διατριβής, παρουσιάστηκε η ιδέα για χρήση της τεχνικής του Shamir, με σκοπό την επίτευξη καλής ψευδωνυμοποίησης. Πιο συγκεκριμένα, παρουσιάστηκε ένα παράδειγμα με χρήση των διευθύνσεων IP που καταγράφονται σε ένα αρχείο καταγραφής (log file). Προέκυψε ότι η χρήση της τεχνικής του Shamir για αυτό τον σκοπό, παρέχει το πλεονέκτημα ότι ο μηχανισμός παρακολούθησης των αρχείων καταγραφής μπορεί να "βλέπει" αρχικώς ψευδώνυμα και όχι τις πραγματικές IP διευθύνσεις και αν για κάποια "ψευδωνυμοποιημένη" IP διεύθυνση διαφαίνεται ενδεχόμενο ύποπτης συμπεριφοράς, τότε ενεργοποιείται διαφανώς κατάλληλη διαδικασία, για να ανακτηθεί η αρχική IP διεύθυνση, με τον συνδυασμό των k στον αριθμό μυστικών, όπως ορίζει η τεχνική του Shamir.

Την ίδια στιγμή, στο τελευταίο αυτό κεφάλαιο, μετά από μια σύντομη παρουσίαση του blockchain και διάφορων ζητημάτων ασφάλειας και ιδιωτικότητας που προκύπτουν από τη χρησιμοποίηση του σε περιβάλλοντα του Διαδικτύου των Πραγμάτων, δόθηκε και μία νέα κατεύθυνση, προκειμένου να ερευνηθεί μελλοντικά και να υλοποιηθεί ένα ρεαλιστικό σενάριο εφαρμογής της τεχνικής

διαμοιρασμού μυστικού του Shamir, στο οποίο θα μπορεί να χρησιμοποιηθεί η συγκεκριμένη τεχνική, βασιζόμενη στη νέα μορφή της με τη χρήση της φόρμουλας παρεμβολής του Newton, το οποίο θα αποσκοπεί στην ψευδωνυμοποίηση προσωπικών δεδομένων τα οποία θα αποθηκεύονται σε δομές blockchain.

Βιβλιογραφία

Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, L. (2014). Secure Multiparty Computations on Bitcoin. *Communications of the ACM*, *59*, 443–458. https://doi.org/10.1109/SP.2014.35

Anli Chen. (2004, November 17). *Yao's Millionaires Problem*.

Arampatzis, A. (2020). *What Is Homomorphic Encryption [& How It Is Used] | Venafi*. https://www.venafi.com/blog/homomorphic-encryption-what-it-and-how-it-used

Archer, D., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J., Smart, N., & Wright, R. (2018). From Keys to Databases—Real-World Applications of Secure Multi-Party Computation. *Computer Journal*, *61*, 1749–1771. https://doi.org/10.1093/comjnl/bxy090

Bayatbabolghani, F., & Blanton, M. (2018). Secure Multi-Party Computation. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2157–2159. https://doi.org/10.1145/3243734.3264419

Bezzateev, S., Davydov, V., & Ometov, A. (2020). On Secret Sharing with Newton's Polynomial for Multi-Factor Authentication. *Cryptography*, *4*, 1–11. https://doi.org/10.3390/cryptography4040034

Bhushan Sonawane. (n.d.). *How to Exchange Secrets With Oblivious Transfer*.

Biskup, J., & Flegel, U. (2000). *On Pseudonymization of Audit Data for Intrusion Detection*. *2009*, 161–180. https://doi.org/10.1007/3-540-44702-4_10

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J. D., Nielsen, J. B., Nielsen, K., Pagter, J., Schwartzbach, M., & Toft, T. (2009). Secure Multiparty Computation Goes Live. In R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security* (Vol. 5628, pp. 325–343). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03549-4_20

Bringer, J., Chabanne, H., & Patey, A. (2013). Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends. *IEEE Signal Process. Mag.*, *30*, 42–52. https://doi.org/10.1109/MSP.2012.2230218

Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavué, C. (2019). Blockchain Solutions for Forensic Evidence Preservation in IoT Environments. *2019 IEEE Conference on Network Softwarization (NetSoft)*, 110–114. https://doi.org/10.1109/NETSOFT.2019.8806675

Canetti, R. (2001). Universally composable security: A new paradigm for cryptographic protocols. *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, 136–145. https://doi.org/10.1109/SFCS.2001.959888

Canetti, Ran. (2000). Security and Composition of Multiparty Cryptographic Protocols. *Journal of Cryptology*, *13*(1), 143–202. https://doi.org/10.1007/s001459910006

Canetti, Ran, Feige, U., Goldreich, O., & Naor, M. (2001). Adaptively Secure Multi-party Computation. *Proc. 28th STOC*. https://doi.org/10.1145/237814.238015

Chakray.com. (n.d.). *Https://www.chakray.com/blockchain-iot-security/*.

Chase, M., & Miao, P. (2020). Private Set Intersection in the Internet Setting from Lightweight Oblivious PRF. In D. Micciancio & T. Ristenpart (Eds.), *Advances in Cryptology – CRYPTO 2020* (Vol. 12172, pp. 34–63). Springer International Publishing. https://doi.org/10.1007/978-3-030-56877-1_2

Christina-Angeliki Toli, Abdelrahaman Aly, & Bart Preneel. (n.d.). *Privacy-Preserving Multibiometric Authenticationin Cloud with Untrusted Database Providers*.

Cohen, R., & Lindell, Y. (2016). Fairness Versus Guaranteed Output Delivery in Secure Multiparty Computation. *Journal of Cryptology*, *30*. https://doi.org/10.1007/s00145-016-9245-5

Covington, J., & Golbek, M. (2015). *SECURE MULTIPARTY COMPUTATION*. 11.

Crépeau, C. (1995). Equivalence Between Two Flavours of Oblivious Transfers. *LNCS*, *293*, 350–354. https://doi.org/10.1007/3-540-48184-2_30

Crypto Wiki. (n.d.). *Https://cryptography.fandom.com/wiki/Shamir%27s_Secret_Sharing*.

CyfRA. (n.d.). *Blockchain as a security measure for IoT systems*.

Demir, L., Kumar, A., Cunche, M., & Lauradoux, C. (2018). The Pitfalls of Hashing for Privacy. *IEEE Communications Surveys & Tutorials*, *20 no.1*, 551–565. https://doi.org/10.1109/COMST.2017.2747598

Du, W., & Atallah, M. (2002). Secure Multi-Party Computation Problems and Their Applications: A Review And Open Problems. *Proceedings New Security Paradigms Workshop*, 10. https://doi.org/10.1145/508171.508174

Dugan, T., & Zou, X. (2016). *A Survey of Secure Multiparty Computation Protocols for Privacy Preserving Genetic Tests*. 173–182. https://doi.org/10.1109/CHASE.2016.71

Evans, D., Kolesnikov, V., & Rosulek, M. (2018). *A Pragmatic Introduction to Secure Multi-Party Computation*. *2*, 70–246. https://doi.org/10.1561/3300000019

Even, S., Goldreich, O., & Lempel, A. (1982). A Randomized Protocol for Signing Contracts. *Communications of the ACM*, *28*, 205–210. https://doi.org/10.1145/3812.3818

Fabiano, N. (2017). Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard. *2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 727–734. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112

Facebook Security. (2013). *Custom Audiences: Data Security Overview*. https://3qdigital.com/wp-content/uploads/2016/06/facebook_audiences_data_security_overview.pdf

Goldreich, O., Micali, S., & Wigderson, A. (1987). How to Play ANY Mental Game. *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, 218–229. https://doi.org/10.1145/28395.28420

Goldwasser, S. (1997). Multi party computations: Past and present. *Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing - PODC '97*, 1–6. https://doi.org/10.1145/259380.259405

Guo, X., Zhang, S., & Li, Y. (2013). Key Technologies and Applications of Secure Multiparty Computation. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *11*. https://doi.org/10.11591/telkomnika.v11i7.2827

Gwyneth Iredale. (2021, January 10). *Public Vs Private Blockchain: How Do They Differ?*

Ion, M., Kreuter, B., Nergiz, E., Patel, S., Saxena, S., Seth, K., Shanahan, D., & Yung, M. (2017). Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions. *IACR Cryptol. EPrint Arch.*, *2017*, 738.

Ishai, Y., Katz, J., Kushilevitz, E., Lindell, Y., & Petrank, E. (2011). On Achieving the "Best of Both Worlds" in Secure Multiparty Computation. *SIAM J. Comput.*, *40*, 122–141.

Ishai, Y., Kushilevitz, E., Lindell, Y., & Petrank, E. (2006). On Combining Privacy with Guaranteed Output Delivery in Secure Multiparty Computation. In C. Dwork (Ed.), *Advances in Cryptology—CRYPTO 2006* (pp. 483–500). Springer. https://doi.org/10.1007/11818175_29

Joshi, A., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*, 121–147. https://doi.org/10.3934/mfc.2018007

Kelong Cong. (2020a, May 4). *C06GC: Introduction to Garbled Circuit*. https://www.esat.kuleuven.be/cosic/blog/introduction-to-garbled-circuit/

Kelong Cong. (2020b, October 20). *Co6GC: Introduction to Oblivious Transfer*. https://www.esat.kuleuven.be/cosic/blog/co6gc-introduction-to-oblivious-transfer/

Kolesnikov, V., Kumaresan, R., Rosulek, M., & Trieu, N. (2016). *Efficient Batched Oblivious PRF with Applications to Private Set Intersection*. 818–829. https://doi.org/10.1145/2976749.2978381

Kolokotronis, N., Limniotis, K., Shiaeles, S., & Griffiths, R. (2019). Secured by Blockchain: Safeguarding Internet of Things Devices. *IEEE Consumer Electronics Magazine*, *8*, 28–34.

Konstantinos Gkikas. (2014, October 23). *Yao's Garbled Circuit*.

Kshemkalyani, A., & Singhal, M. (2008). Distributed Computing: Principles, Algorithms, and Systems. *Distributed Computing: Principles, Algorithms, and Systems*. https://doi.org/10.1017/CBO9780511805318

Lindell, Y. (2020). *Secure Multiparty Computation (MPC)*. 15.

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1–2*, 1–13. https://doi.org/10.1016/j.iot.2018.05.002

Naidu, P., Kharat, R., Tekade, R., Mendhe, P., & Magade, V. (2016). *E-voting system using visual cryptography & secure multi-party computation*. 1–4. https://doi.org/10.1109/ICCUBEA.2016.7860062

Ni Trieu. (n.d.). *Privacy Preserving analytics Private Set Intersection (PSI)*.

Oksiiuk, O., & Dmyrieva, I. (2020). Security and privacy issues of blockchain technology. *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 1–5. https://doi.org/10.1109/TCSET49122.2020.235489

Peeter Laud & Liina Kamm. (2015). *Applications of Secure Multiparty Computations* (Vol. 13).

Permissioned vs Permissionless Blockchains. (2020, May 28).

Pinkas, B., Schneider, T., & Segev, G. (2015). Phasing: Private set intersection using permutation-based hashing. *Proceedings of the 24th Conference on USENIX Security Symposium*, *15*, 515–530.

Pinkas, B., Schneider, T., & Zohner, M. (2018). Faster private set intersection based on OT extension. *ACM Transactions on Privacy and Security*, *21*, 797–812. https://doi.org/10.1145/3154794

Rabin, M. O. (1981). *How to Exchange Secrets with Oblivious Transfer*. 26.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Robin Roehm, Ayoub Benaissa, Sabrina Steinert, & Michael Hoeh. (2020, April 29). *A PRIVACY-PRESERVING WAY TO FIND THE INTERSECTION OF TWO DATASETS*.

Shamir, A. (1979). How to Share a Secret. *Commun. ACM*, *22*(11), 612–613. https://doi.org/10.1145/359168.359176

Snyder, P. (2014). *Yao's Garbled Circuits: Recent Directions and Implementations*. 12.

Stack Exchange. (n.d.). *Https://crypto.stackexchange.com/questions/17871/how-come-shamir-secret-sharing-uses-lagrange-interpolation*.

Techloyce.com. (2017, December 22). *Blockchain Technology Explained to Understand it*.

Tso, R., Liu, Z.-Y., & Hsiao, J.-H. (2019). Distributed E-Voting and E-Bidding Systems Based on Smart Contract. *Electronics*, *8*, 422. https://doi.org/10.3390/electronics8040422

Vivek Acharya, Anand Eswararao Yerrapati, & Nimesh Prakash. (2019). *Oracle Blockchain Quick Start Guide* (1st ed.). Packt Publishing.

von Maltitz, M., & Carle, G. (2018). Leveraging Secure Multiparty Computation in the Internet of Things. *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, 508–510. https://doi.org/10.1145/3210240.3223569

Weerasooriya W.A.A.C.P. (2014). *Homomorphic Encryption for Secure Multi-Party Computation*.

William J Buchanan. (n.d.). *Threshold scheme with ECC*.

Yakoubov, S. (2017). *A Gentle Introduction to Yao's Garbled Circuits*. 12.

Yang, Y., Wei, L., Wu, J., & Long, C. (2020). *Block-SMPC: A Blockchain-based Secure Multi-party Computation for Privacy-Protected Data Sharing*. 46–51. https://doi.org/10.1145/3390566.3391664

Yao, A. C. (1982). Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, 160–164.

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & yu-an, T. (2018). Secure Multi-Party Computation: Theory, Practice and Applications. *Information Sciences*, *476*. https://doi.org/10.1016/j.ins.2018.10.024

Δρ. Κωνσταντίνος Λιμνιώτης. (2018, November 22). *Η ψευδωνυμοποίηση στον Γενικό Κανονισμό Προστασίας Δεδομένων*.

Δρ. Κωνσταντίνος Λιμνιώτης. (2019, 2020). *Διαφάνειες Θ.Ε. Κρυπτογραφία*.

Δρ. Κωνσταντίνος Λιμνιώτης & Ιωάννης Μαυρίδης. (2019, 2020). *Διαφάνειες Θ.Ε. Διαχείριση Κινδύνων Ασφαλείας Πληροφοριακών και Επικοινωνιακών Συστημάτων*.

Ευρωπαϊκό Κοινοβούλιο. (2016). *ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/ 679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ - GDPR*. 88.

Ευστάθιος Ζάχος, Αριστείδης Παγουρτζής, & Παναγιώτης Γροντάς. (2015). *Υπολογιστική Κρυπτογραφία*.

Πληροφορίες για την κωδικοποίηση στοιχείων πελατών με hash. (n.d.). Κέντρο βοήθειας του Facebook Business. Retrieved April 13, 2021, from https://el-gr.facebook.com/business/help/112061095610075