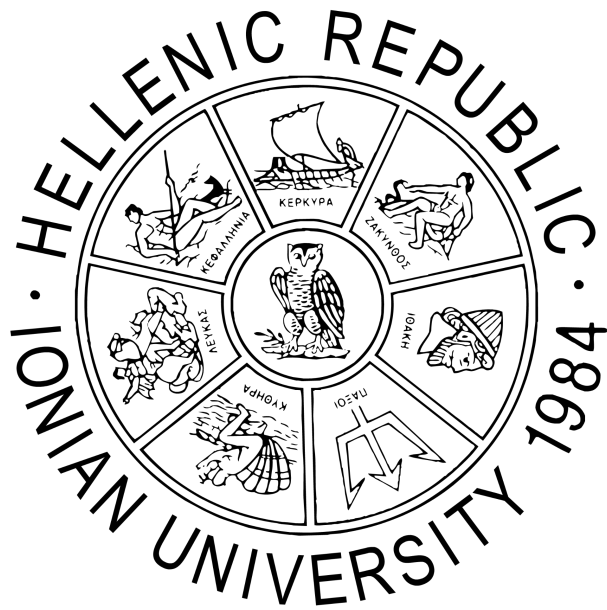

Το πρόβλημα των κρυπτογράφων που δειπνούν Dining cryptographers problem

Πτυχιακή Εργασία



Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής Τμήμα
Πληροφορικής Ιόνιο Πανεπιστήμιο

Καρανάνου Περιστέρα

Στοιχεία Φοιτητή:

Καρανάνου
Περιστέρα
Π2018171

Επιβλέπων καθηγητής:

Θεόδωρος
Ανδρόνικος

Επιτροπή:

Μιχαήλ
Στεφανιδάκης

Εμμανουήλ
Μάγκος



Περιεχόμενα

Λέξεις κλειδιά/ Συντομογραφίες.....	3
Περιεχόμενα εικόνων.....	5
Περιεχόμενα πινάκων.....	6
Πρόλογος.....	7
Abstract.....	8
Ευχαριστίες.....	9
Κεφάλαιο 1ο.....	1
1.1 Εισαγωγή.....	1
1.2 Ιστορική αναδρομή.....	2
1.3 Το πρόβλημα.....	4
1.4 Παράδειγμα.....	7
1.5 Μειονεκτήματα.....	12
1.5.1 Συγκρούσεις.....	14
1.5.2 Επιθέσεις.....	15
1.6 Πλεονεκτήματα.....	16
Κεφάλαιο 2ο.....	18
2.1 Αλγόριθμοι εμπνευσμένοι από το DCP.....	18
2.2 Dining cryptographers network.....	19
2.3 Κρυπτογραφία κατωφλίου με DC-Nets.....	20
2.4 Εφαρμογή τοπολογία δακτυλίου.....	23
Κεφάλαιο 3ο.....	25
3.1 Εισαγωγή στον κβαντικό κόσμο.....	25
3.2 Εντροπία.....	29
3.3 EPR, GHZ.....	31
3.4 Κβαντικά πρωτόκολλα του DCP.....	32
Κεφάλαιο 4ο.....	35
4.1 Το νέο πρωτόκολλο.....	35
4.2 The Scalable quantum protocol for the Dining Cryptographers Problem.....	37
4.3 Εκτέλεση του πρωτοκόλλου SQDCP.....	41
4.4 Παράδειγμα.....	47
Κεφάλαιο 5ο.....	54
5.1 Συμπεράσματα.....	54
Πηγές και βιβλιογραφία.....	56

Λέξεις κλειδιά/ Συντομογραφίες

Ασφαλεια, Ιδιωτικότητα, Ανωνυμία, Κρυπτογραφικό πρωτόκολλο, Δίκτυα, Κυβερνοασφάλεια, πολυμερής υπολογισμός

DC: Dining cryptographers

DCP: Dining cryptographers protocol

A,B,C: Alice, Bob, Charlie

K: Κοινό κλειδί

K_{AB} : Κοινό κλειδί μεταξύ A και B

A_A : Αποκάλυψη του A

$\oplus$: XOR

n : κβαντικοί καταχωρητές

m : qubits ανα καταχωρητή σε κατάσταση $|GHZ_n\rangle$

AIR: κβαντικός καταχωρητής εισόδου της Alice

IR_i : κβαντικός καταχωρητής εισόδου του C_i , $0 \leq i \leq n - 2$

AOR: κβαντικός καταχωρητής εξόδου της Alice

OR_i : κβαντικός καταχωρητής εξόδου του C_i , $0 \leq i \leq n - 2$

U_{fA} : ενιαίος μετασχηματισμός της Alice

U_{fi} : ενιαίος μετασχηματισμός του C_i , $0 \leq i \leq n - 2$

$H^{\otimes m}$: μετασχηματισμός Hadamard

fA, fi : ιδιωτικές μυστικές συναρτήσεις

p : πληροφορία

QKD: Διανομή κβαντικού κλειδιού

QAV: κβαντικό ανώνυμα βέτο

AQC: Ανώνυμη κβαντική επικοινωνία

NESA: Non-maximally entanglement state analysis

MTAS: Message transfer with anonymous sender

SQDCP: Scalable quantum protocol for the Dining Cryptographers Problem

Περιεχόμενα εικόνων

Εικόνα 1: XOR.....	6
Εικόνα 2: Σχεδιάγραμμα τριών κόμβων.....	7
Εικόνα 3: Σχεδιάγραμμα τριών κόμβων.....	8
Εικόνα 4: Σχεδιάγραμμα τεσσάρων κόμβων, πλήρως συνδεδεμένη τοπολογία.....	9
Εικόνα 5: Σχεδιάγραμμα τεσσάρων κόμβων, τοπολογία δακτυλίου.....	11
Εικόνα 6: Σχεδιάγραμμα τριών κόμβων με 3 και 2 συνδεδεμένους κόμβους.....	19
Εικόνα 7: Τοπολογία δακτυλίου.....	23
Εικόνα 8: Διαφορά μεταξύ bit, qbit.....	26
Εικόνα 9: $ GHZ_n\rangle$	37
Εικόνα 10: Τέσσερις κρυπτογράφοι.....	39
Εικόνα 11: Κβαντικό κύκλωμα.....	43
Εικόνα 12: Περίπτωση που η Alice πλήρωσε το δείπνο.....	48
Εικόνα 13: Περίπτωση που η Alice πλήρωσε το δείπνο μερικές από τις πιθανές μετρήσεις και τις αντίστοιχες πιθανότητες για το κύκλωμα.....	49
Εικόνα 14: Περίπτωση που κανένας κρυπτογράφος δε πλήρωσε το δείπνο.....	51
Εικόνα 15: Περίπτωση που κανένας κρυπτογράφος δε πλήρωσε το δείπνο μερικές από τις πιθανές μετρήσεις και τις αντίστοιχες πιθανότητες για το κύκλωμα.....	52

Περιεχόμενα πινάκων

Πίνακας 1: XOR.....	6
Πίνακας 2: Υπολογισμός.....	7
Πίνακας 3: Υπολογισμός.....	8
Πίνακας 4: Υπολογισμός με $n = 4$	10
Πίνακας 5: Υπολογισμός με $n = 4$	11
Πίνακας 6: Υπολογισμός με $K = 6$ bits.....	12
Πίνακας 7: Αριθμός κόμβων και κλειδιών.....	23

Πρόλογος

Η παρούσα πτυχιακή εργασία συγγράφηκε κατά το ακαδημαϊκό έτος 2023/2024. Το αντικείμενο της αφορά το πρόβλημα των κρυπτογράφων που δειπνούν. Το συγκεκριμένο πρόβλημα εστιάζει στον τρόπο εκτέλεσης ενός ασφαλούς υπολογισμού πολλαπλών μερών. Η θεωρία παιγνίων μπορεί να μας βοηθήσει να λύσουμε διάφορα κοινωνικά και πρακτικά προβλήματα και να συμβάλουμε όσο το δυνατόν περισσότερο στην ανάπτυξη πιο βιώσιμων κοινοτήτων. Μέσω της θεωρίας παιγνίων επίσης έχουμε την ικανότητα να προβάλλουμε ιδέες καθιερώνοντας ταυτόχρονα τις θεμελιώδεις αρχές που διέπουν την ανθρώπινη και γενικότερα την κοινωνική συμπεριφορά. Στην εποχή που ζούμε η ανωνυμία είναι απαραίτητη για πολλές εργασίες διατήρησης του απορρήτου στη δικτυακή επικοινωνία. Επικοινωνίες υψηλής ασφάλειας δεν μπορούν να επιτευχθούν μόνο με ασφαλή διανομή κλειδιού. Είναι συχνά απαραίτητο να κρυφτείς από έναν εχθρό που στέλνει μηνύματα ή που επιδιώκει να αποσπάσει πληροφορίες από τα δικά σου μηνύματα. Έτσι ο David Chaum ανέπτυξε μία μέθοδο για ανώνυμη δημοσίευση μηνυμάτων. Επέλεξα αυτό το θέμα καθώς θεωρώ πως η ανωνυμία και η ιδιωτικότητα ανέκαθεν ήταν και εξακολουθεί να είναι ένα από τα σημαντικότερα ζητήματα στις επικοινωνίες. Στις μέρες μας, το φάσμα της επικοινωνίας συνεχώς διευρύνεται ενώ τα όρια της ανωνυμίας και της ιδιωτικότητας σταδιακά μειώνονται. Είναι ιδιαίτερα σημαντική η διατήρησή της ιδιωτικότητας στον διασυνδεδεμένο κόσμο που έχουμε χτίσει. Ο σκοπός της παρούσας εργασίας είναι η όσο το δυνατόν περισσότερο σφαιρική και λεπτομερής επεξήγηση του προβλήματος, καθώς και μία τροποποίηση του προβλήματος σε κβαντικό επίπεδο. Εξίσου σημαντική όμως είναι και η ενημέρωση, η κατανόηση της χρησιμότητας αλλά και της αναγκαίας διατήρησης της ανωνυμίας και της ιδιωτικότητας. Τέλος προτείνονται προτείνεται ένα νέο κβαντικό πρωτόκολλο, με σκοπό την επίλυση του κλασικού προβλήματος σε κβαντικό επίπεδο.

Abstract

The present thesis was written during the academic year 2023/2024. Its subject concerns the problem of cryptographers dining. This particular problem focuses on the execution of secure multi-party computation. Game theory can help us solve various social and practical problems and contribute as much as possible to the development of more sustainable communities. Through game theory, we also have the ability to project ideas and ideology while simultaneously establishing the fundamental principles that govern human and, more broadly, social behavior. In the era we live in, anonymity is essential for many tasks in maintaining privacy in online communication. High-security communications cannot be achieved solely through secure key distribution. It is often necessary to hide from an adversary sending messages or seeking to extract information from your own messages. Thus, David Chaum developed a method for anonymous message publishing. I chose this topic because I believe that anonymity and privacy have always been and continue to be one of the most important issues in communication. Nowadays, the spectrum of communication is constantly expanding while the boundaries of anonymity and privacy are gradually diminishing. It is particularly important to maintain privacy in the interconnected world we have built. The purpose of this thesis is to provide as spherical and detailed an explanation as possible of the problem, as well as to modify the problem at a quantum level. Equally important, however, is the dissemination of information, understanding of the usefulness, and necessary maintenance of anonymity and privacy. Finally, a new quantum protocol is proposed to solve the classical problem at a quantum level.

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον καθηγητή και επιβλέποντά μου κ. Θεόδωρο Ανδρόνικο, για το ενδιαφέρον και την καθοδήγηση του κατά τη δύσκολη απόφαση της επιλογής του θέματος της πτυχιακής μου εργασίας αλλά και για τις πολύ εποικοδομητικές παρατηρήσεις και συστάσεις του. Καθώς και για την καθοδήγηση του κατά στην εκπόνηση της παρακάτω εργασίας. Μου έδωσε τη δυνατότητα να ασχοληθώ με ένα πολύ ενδιαφέρον και διαχρονικό θέμα, το πρόβλημα των κρυπτογράφων που δειπνούν. Παράλληλα, με την συνεχή του καθοδήγηση και υποστήριξη δημιουργήθηκε από κοινού ένα καινοτόμο κβαντικό πρωτόκολλο για την επίλυση του κλασικού προβλήματος, The Scalable quantum protocol for the Dining Cryptographers Problem. Και τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου που στάθηκε αρωγός και συνεχίζει μέχρι και σήμερα να στηρίζει τις επιλογές μου πάντα δίπλα στο πλευρό μου. Όπως επίσης και τους φίλους μου που ήταν δίπλα μου κατά τη διάρκεια όλων των φοιτητικών μου χρόνων, με υπομονή και διάθεση να προσφέρουν την πολύτιμη βοήθεια τους όποτε κι αν την χρειάστηκα. Τους ευχαριστώ όλους πραγματικά μέσα από την καρδιά μου.

Κεφάλαιο 1^ο

1.1 Εισαγωγή

Η παρούσα πτυχιακή εργασία έχει ως στόχο την έρευνα και την εξέλιξη του προβλήματος των κρυπτογράφων που δειπνούν. Παράλληλος σκοπός είναι να τονιστεί η ανάγκη για ασφαλή και ανώνυμη επικοινωνία. Η κυβερνοασφάλεια είναι τώρα πιο σημαντική από ποτέ. Στην ταχέως αναπτυσσόμενη ψηφιακή εποχή μας, η τεχνολογία ενσωματώνεται απρόσκοπτα σε κάθε μέρος και πτυχή της ζωής μας. Καθώς διαπραγματευόμαστε την πολυπλοκότητα των ψηφιακών συνόρων, βρισκόμαστε εμπλεκόμενοι σε έναν κόσμο όπου υπάρχουν απρόβλεπτες απειλές, ενώ παράλληλα η γνώση ανταλλάσσεται ελεύθερα. Η έννοια της ιδιωτικής ζωής έχει εξελιχθεί αποτελούμενη από κρίσιμα σημεία ατομικής ελευθερίας και ασφάλειας σε μια εποχή που χαρακτηρίζεται από γρήγορες τεχνολογικές ανακαλύψεις και ψηφιακά συνδεδεμένα πεδία. Σε μία τέτοια εποχή, το απόρρητο αναφέρεται στην ικανότητα ενός ατόμου να διαχειρίζεται τις προσωπικές του πληροφορίες και να επιλέγει το πώς αλλά και το αν θα συλλέγονται. Να έχει την δυνατότητα να επιλέξει το αν και το πώς θα χρησιμοποιηθούν καθώς και το αν θα κοινοποιούνται. Πλέον το φάσμα θεμάτων όπου το απόρρητο θεωρείται αναγκαίο είναι πολύ ευρύ, από τις ιδιωτικές επικοινωνίες και τις οικονομικές συναλλαγές έως τις ιδιωτικές πληροφορίες υγείας. Ζητήματα σχετικά με το απόρρητο έχουν γίνει πιο περίπλοκα καθώς οι ψηφιακές πλατφόρμες και οι έξυπνες τεχνολογίες έχουν ενσωματωθεί πολύ περισσότερο στην καθημερινή μας ζωή. Τα μέσα κοινωνικής δικτύωσης, οι υπηρεσίες διαδικτύου και οι τεχνολογίες που βασίζονται σε δεδομένα έχουν επιφέρει ένα πρωτοφανές επίπεδο ευκολίας, έχοντας επίσης πυροδοτήσει επείγουσες ανησυχίες σχετικά με το απόρρητο των ατόμων. Η σύγκρουση μεταξύ της ανάγκης για καινοτομία και της απαίτησης προστασίας των προσωπικών δεδομένων έχει αναδειχθεί ως κύριο θέμα συζήτησης τα τελευταία χρόνια.

Η κυβερνοασφάλεια είναι αλληλένδετη με την προστασία των δεδομένων μας, του απορρήτου και του δικτυωμένου πολιτισμού μας. Η κυβερνοασφάλεια είναι υπεύθυνη για την προστασία των ψηφιακών συστημάτων, δικτύων και συσκευών από διάφορες απειλές στον κυβερνοχώρο. Αυτοί οι κίνδυνοι, κυμαίνονται από επιθέσεις ransomware και εξελιγμένη κατασκοπεία έως ιούς υπολογιστών και παραβιάσεις δεδομένων, όχι μόνο παρουσιάζουν οικονομικούς κινδύνους αλλά και θέτουν σε κίνδυνο ολόκληρο το θεμέλιο της εμπιστοσύνης στο Διαδίκτυο. Πλέον με την εξέλιξη που επικρατεί διαкиβέβεται μέχρι και η ανθρώπινη ζωή. Η ανάπτυξη του διαδικτύου και η ευρεία χρήση έξυπνων gadgets έχουν αλλάξει τον τρόπο που εργαζόμαστε, επικοινωνούμε, ψωνίζουμε και περνάμε τον ελεύθερο χρόνο μας. Ωστόσο, η ψηφιακή επανάσταση έχει αυξήσει την επιφάνεια επίθεσης που μπορούν να χρησιμοποιήσουν οι κυβερνοεγκληματίες προς όφελός τους. Ως αποτέλεσμα, η κυβερνοασφάλεια είναι ένας τομέας που αναπτύσσεται διαρκώς για να κρατηθεί μπροστά από αυτούς τους κινδύνους. Δίπλα από την εξέλιξη του software αλλά και του hardware οφείλει να εξελίσσεται και η ασφάλειά τους θωρακίζοντας το εκάστοτε

σύστημα από τις νέες επιθέσεις. Αυτό το επιτυγχάνετε συνδυάζοντας τεχνολογικές προόδους, κανονισμούς και ανθρώπινες δεξιότητες. Καθώς διασχίζουμε τον κόσμο της κυβερνοασφάλειας, γίνεται σαφές ότι η διαφύλαξη του ψηφιακού μας μέλλοντος περιλαμβάνει περισσότερα από την απλή προστασία δεδομένων. Η κατανόηση και η εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας είναι το κλειδί για μια ασφαλέστερη, πιο ανθεκτική ψηφιακή κοινωνία.

Το κρυπτογραφικό πρωτόκολλο που ονομάζεται The Dining Cryptographers Problem (Το πρόβλημα των κρυπτογράφων που δειπνούν) διερευνά την ιδέα της ανώνυμης επικοινωνίας σε ένα κοινωνικό πλαίσιο. Ο David Chaum το πρότεινε για πρώτη φορά το 1988 ως ένα πείραμα σκέψης για να δείξει τις δυνατότητες για ιδιωτική και ασφαλή επικοινωνία μεταξύ των συμμετεχόντων. Δίνεται ιδιαίτερη έμφαση στην διατήρηση του απορρήτου και της ανωνυμίας κάθε συμμετέχοντα για την επίτευξη του στόχου η οποία είναι η ανταλλαγή μηνυμάτων. Προκειμένου να αποτραπεί η αποκάλυψη μεμονωμένων συνεισφορών, το πρωτόκολλο χρησιμοποιεί κρυπτογραφικές τεχνικές για να βεβαιωθεί ότι οι πληροφορίες που αποστέλλονται μεταξύ των κρυπτογράφων αποκαλύπτουν μόνο το προ-συμφωνημένο αποτέλεσμα (0/1). Το σενάριο βασίζεται σε πραγματικές συνθήκες στις οποίες οι άνθρωποι επιθυμούν να μοιραστούν πληροφορίες με άλλους, διατηρώντας παράλληλα το απόρρητό τους και το απόρρητο των μηνυμάτων τους. Εκτός από θεωρητική έννοια λοιπόν, το Dining Cryptographers Problem παρέχει επίσης μια βάση για συζητήσεις και προόδους στα πρωτόκολλα επικοινωνίας με ασφαλή υπολογισμό πολλών μερών και διατήρηση της ιδιωτικής ζωής. Παρέχοντας πληροφορίες σχετικά με τον τρόπο χρήσης κρυπτογραφικών τεχνικών για την παροχή ασφαλούς επικοινωνίας σε διαφορετικά περιβάλλοντα, ενώ παράλληλα οι λύσεις αυτού του προβλήματος συμβάλλουν στο ευρύτερο πεδίο της κρυπτογραφίας. Το πρωτόκολλο Dining Cryptographers είναι θεμελιωδώς διαφορετικό από άλλα σχετικά πρωτόκολλα ασφαλείας ελέγχου μοντέλων, επειδή δεν χρησιμοποιεί κρυπτογράφηση και επειδή οι προδιαγραφές του εστιάζουν φυσικά στο τι γνωρίζουν οι κρυπτογράφοι του συστήματος και όχι στο τι είναι. Η φράση ‘Dining Cryptographers’ αναφέρεται σε μια μεταφορική κατάσταση στην οποία 3 κρυπτογράφοι τρώνε μαζί σε ένα εστιατόριο και ανταλλάσσουν ανώνυμα πληροφορίες. Οι προδιαγραφές του πρωτοκόλλου ορίζουν ότι οι κρυπτογράφοι έχουν καθορίσει πληροφορίες όπου πρέπει να γνωρίζουν πριν αλλά και μετά την εκτέλεση του πρωτοκόλλου. Οι ιδέες, οι μέθοδοι κρυπτογράφησης και οι πρακτικές εφαρμογές που καθιστούν τα πρωτόκολλα και τα δίκτυα Dining Cryptographers ένα πολύ ενδιαφέρον πεδίο έρευνας που στοχεύει στην αναζήτηση της ιδιωτικής ζωής και της ασφαλούς επικοινωνίας.

1.2 Ιστορική αναδρομή

Σε έναν κόσμο όπου οποιαδήποτε μεταφορά μπορούσε να ανιχνευθεί η πηγή της, έμοιαζε αδύνατο να μείνει απόρρητο το ποιος μεταδίδει καθώς και ποιά μηνύματα. Ανεξάρτητα με το αν βασίζεται κανείς σε δημόσια κλειδιά ή ιδιωτικά κλειδιά, η μέθοδος που πρόσφερε ο David Chaum είναι κρυπτογραφικά αλλά και άνευ όρων ασφαλής.

Ταυτόχρονα, αυτή η μέθοδος μπορεί να τροποποιηθεί για να αντιμετωπίσει αποτελεσματικά ένα ευρύ φάσμα πρακτικών ζητημάτων. Το κίνητρο πίσω από το πρόβλημα των Dining Cryptographers ήταν η διερεύνηση τρόπων για την επίτευξη ανώνυμης επικοινωνίας, η δημιουργία ενός μέσου για συμμετοχή σε ηλεκτρονικές συναλλαγές χωρίς οι συμμετέχοντες να αποκαλύπτουν την ταυτότητά τους, ειδικά στο πλαίσιο της ηλεκτρονικής ψηφοφορίας. Ο David Chaum τη δεκαετία του 1980, παρουσίασε ένα νέο πρωτοποριακό πρωτόκολλο ανώνυμης επικοινωνίας [1].

Η βασική ιδέα πίσω από τα DC-Nets είναι η επικοινωνία με τέτοιο τρόπο ώστε να καθίσταται υπολογιστικά αδύνατο να προσδιοριστεί ποιος έστειλε ένα συγκεκριμένο μήνυμα. Αυτή η καινοτομία έθεσε τα θεμέλια για τις σύγχρονες τεχνικές διατήρησης της ιδιωτικής ζωής στην ψηφιακή εποχή καθώς πυροδότησε σημαντικό ενδιαφέρον στους τομείς της κρυπτογραφίας αλλά και γενικότερα στην επιστήμη των υπολογιστών. Με την πάροδο των χρόνων, μέσω της έρευνας και της τεχνολογικής εξέλιξης, οι τεχνολογίες απορρήτου έχουν επεκταθεί περαιτέρω από τις αρχές των δικτύων DC, οδηγώντας σε πιο εξελιγμένα και αποτελεσματικά πρωτόκολλα για την επίτευξη ανώνυμης επικοινωνίας. Τα DC-Nets αντιπροσωπεύουν ένα σημαντικό ορόσημο στην εξέλιξη των κρυπτογραφικών πρωτοκόλλων για τη διασφάλιση της ανώνυμης επικοινωνίας μεταξύ μιας ομάδας συμμετεχόντων. Οι αποδείξεις μηδενικής γνώσης, ο ασφαλής υπολογισμός πολλών μερών και τα ασφαλή συστήματα ανταλλαγής μηνυμάτων είναι μερικές από τις εξελίξεις που αντλούν έμπνευση από το αρχικό πρόβλημα του Dining Cryptographers. Το πρόβλημα των κρυπτογράφων που δειπνούν παραμένει μια θεμελιώδης ιδέα στον τομέα της ιδιωτικότητας και της κρυπτογραφίας, επηρεάζοντας τον σχεδιασμό και την εφαρμογή διαφόρων πρωτοκόλλων διατήρησης της ιδιωτικής ζωής. Παρόλο που το αρχικό πρόβλημα που έθεσε ο David Chaum ήταν θεωρητικό, το αντίκτυπο του ήταν εκτεταμένο, συμβάλλοντας στην ανάπτυξη πρακτικών λύσεων για την προστασία της ιδιωτικής ζωής των ατόμων στην ψηφιακή εποχή. Η ιδέα ήταν να επιτραπεί στους συμμετέχοντες να συνεισφέρουν τις εισροές τους σε μια κοινή ομάδα χωρίς να αποκαλύπτουν τα μεμονωμένα στοιχεία τους, καθιστώντας έτσι δύσκολο για τους εξωτερικούς παρατηρητές να εντοπίσουν την πηγή κάθε συνεισφοράς.

Συγκεκριμένα οι συμμετέχοντες μπορούν να στέλνουν μηνύματα ασφαλή κρυπτογραφικά και μη ιχνηλατήσιμα. Για την απλούστευση αλλά και την καλύτερη κατανόηση του πρωτοκόλλου του, χρησιμοποίησε ως παράδειγμα το πρόβλημα των κρυπτογράφων. Σύμφωνα με αυτό το πρόβλημα υπάρχουν 3 κρυπτογράφοι οι οποίοι δειπνούν και επιδιώκουν να επικοινωνήσουν μεταξύ τους με πλήρη ανωνυμία. Έπειτα τα Dining Cryptographer Networks ή DC-nets αναπτύχθηκαν γενικεύοντας το πρόβλημα των κρυπτογράφων που δειπνούν απλουστεύοντας την ανώνυμη δημοσίευση μηνυμάτων. Τα δίκτυα DC τροποποιούνται εύκολα για να υποστηρίξουν μεταδόσεις πολλαπλών bit σε κάθε γύρο, αλλά και σε σενάρια με περισσότερους από τρεις συμμετέχοντες και αυθαίρετα "αλφάβητα" εκτός από τα δυαδικά ψηφία 0 και 1. Με άλλα λόγια η ανιχνευσιμότητα όχι μόνο του αποστολέα και του παραλήπτη αλλά και του ίδιου του μηνύματος καθιστάται αδύνατη. Δυστυχώς όμως, αυτές οι ισχυρές διαβεβαιώσεις ανωνυμίας έχουν το κόστος της κακής απόδοσης [3], της επεκτασιμότητας καθώς και μιας σειράς άλλων προβλημάτων που κάνουν την εφαρμογή της δύσκολη στην πραγματικότητα [2]. Ωστόσο το πρόβλημα των κρυπτογράφων που δειπνούν έχει χρησιμοποιηθεί σε διάφορες εφαρμογές, όπως η ασφαλής

επικοινωνία, η ανώνυμη ψηφοφορία και τα ηλεκτρονικά μετρητά. Το πρόβλημα του Dining Cryptographers ανέδειξε την ανάγκη για κρυπτογραφικά πρωτόκολλα, τονίζοντας τη σημασία της ιδιωτικότητας και της ανωνυμίας. Θέτει τα θεμέλια για διάφορα μετέπειτα κρυπτογραφικά πρωτόκολλα και τεχνικές που επικεντρώνονται στην επίτευξη ιδιωτικότητας και ανωνυμίας στα συστήματα επικοινωνίας. Οι συνεισφορές του David Chaum έχουν επηρεάσει σημαντικά την ανάπτυξη ανώνυμων ψηφιακών νομισμάτων, ανώνυμων συστημάτων ψηφοφορίας και των τεχνολογιών ενίσχυσης της ιδιωτικής ζωής. Οι εφαρμογές τους επεκτάθηκαν σε τομείς όπως ο ασφαλής πολυμερής υπολογισμός, τα ανώνυμα συστήματα ψηφοφορίας και η ανάλυση δεδομένων για τη διατήρηση της ιδιωτικής ζωής. Ακόμη και σήμερα, τα DC-Nets συνεχίζουν να αποτελούν αντικείμενο ακαδημαϊκής έρευνας αλλά και πειραματισμού. Οι ερευνητές έχουν εργαστεί για τη βελτίωση της ασφάλειας, της επεκτασιμότητας και της πρακτικότητας των DC-Nets για να ανταποκριθούν στην αυξανόμενη ζήτηση για ασφαλή και ιδιωτική επικοινωνία σε έναν όλο και πιο ψηφιακό κόσμο. Παρά τη θεωρητική τους κομψότητα, οι προκλήσεις και τα τρωτά σημεία εξακολουθούν να υφίστανται και η αντιμετώπισή τους παραμένει μια συνεχής επιδίωξη στον τομέα της κρυπτογραφίας και της ασφάλειας των υπολογιστών.

1.3 Το πρόβλημα

Το πρόβλημα αρχικά προτάθηκε σε θεωρητικό επίπεδο για τη διατήρηση της ανώνυμης επικοινωνίας μεταξύ μιας ομάδας συμμετεχόντων. Στόχος του ήταν να αντιμετωπίσει την πρόκληση της ασφαλούς και ιδιωτικής επικοινωνίας με παρουσία πιθανών υποκλοπών. Το σενάριο με τρεις κρυπτογράφους να δειπνούν μαζί σε ένα εστιατόριο χρησιμοποιήθηκε ως μεταφορά, τονίζοντας και απλουστεύοντας το πρόβλημα. Οι κρυπτογράφοι ήθελαν να προσδιορίσουν εάν το γεύμα έχει πληρωθεί από έναν από αυτούς ή όχι, χωρίς να αποκαλυφθεί η κατάσταση πληρωμής οποιουδήποτε μεμονωμένου κρυπτογράφου, ο ένας στον άλλον ή σε κάποιο πιθανό κακόβουλο κρυφογράφο. Σκοπός ενός κρυφογράφου σε κάθε πρόβλημα είναι η απόσπαση πληροφοριών, για να πετύχει τον στόχο του ακούει την συζήτηση που έχουν οι κρυπτογράφοι στο τραπέζι. Το συγκεκριμένο πρόβλημα αναδεικνύει μία μέθοδο που θα μπορούσαν να επιτρέψουν στους συμμετέχοντες να ανταλλάσσουν πληροφορίες χωρίς να διακυβεύεται το απόρρητό τους. Στην ουσία του, το πρόβλημα των κρυπτογράφων που δειπνούν είναι μια μεταφορική έννοια για ανώνυμη και ανεξιχνίαστη μετάδοση πληροφοριών.

Το δείπνο σερβίρεται σε τρεις κρυπτογράφους, οι οποίοι πήγαν να δειπνήσουν σε κάποιο εστιατόριο. Κάποια στιγμή ο σερβιτόρος τους αποκαλύπτει πως έχει πληρωθεί κρυφά ο λογαριασμός. Το δείπνο μπορεί να έχει πληρωθεί από έναν από τους κρυπτογράφους ή από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA). Οι τρεις κρυπτογράφοι αναγνωρίζουν και κατανοούν ο ένας το δικαίωμα του άλλου να κάνει μια ανώνυμη πληρωμή, αλλά αναρωτιούνται αν το έχει πληρώσει η Υπηρεσία Εθνικής Ασφάλειας. Αποφάσισαν λοιπόν, να βρουν έναν τρόπο με τον οποίο να δημοσιοποιούνται τα μηνύματα χωρίς να αφήνουν ίχνη, με σκοπό να ανακαλύψουν αν ένας εξ αυτών έχει

πληρώσει. Έτσι στο τέλος του δείπνου τους, βρίσκουν μια μέθοδο για να το πετύχουν. Η μέθοδος αυτή ισχύει και για κάθε πρόταση και κάθε μήνυμα οποιουδήποτε μήκους. Αυτή η διαδικασία επαναλαμβάνεται όποτε το επιθυμεί ένας κρυπτογράφος. Ακολουθούν το παρακάτω πρωτόκολλο για να επιλύσουν δίκαια την απορία τους για το ποιος τελικά έχει πληρώσει το δείπνο:

1. Κάθε κρυπτογράφος βγάζει ένα νόμισμα και το γυρίζει ανάμεσα στον ίδιο και τον κρυπτογράφο που κάθεται στα δεξιά του. Για να μην γνωρίζουν οι υπόλοιποι το αποτέλεσμα της ρίψης αποφασίζουν να γυρίσουν το νόμισμα πίσω από το μενού. Με αυτόν τον τρόπο μόνο οι δυο τους μπορούν να δουν το αποτέλεσμα και έτσι έχει εδραιωθεί το κοινό μυστικό κλειδί. Κάθε ρίψη του κέρματος αποτελεί ένα μοναδικό συμμετρικό κλειδί.
2. Στη συνέχεια, κάθε κρυπτογράφος δηλώνει φωναχτά αν τα δύο νομίσματα (το ένα που γύρισε ο ίδιος και αυτό που γύρισε ο αριστερός συνάδελφός του) έπεσαν από διαφορετική ή από την ίδια πλευρά. Με εξαίρεση τον κρυπτογράφο που έχει πληρώσει εάν υπάρχει.

Εάν έχει πληρώσει κάποιος από τους κρυπτογράφους, ισχυρίζεται ότι αυτό που πραγματικά παρατηρεί είναι το αντίθετο. Δηλαδή, δηλώνει το αντίθετο από αυτό που είδε. Εάν στο σύνολο υπάρχει ο περιττός αριθμός 1 που δηλώνονται στο τραπέζι, σημαίνει πως ένας από τους κρυπτογράφους έχει πληρώσει. Ενώ, αν υπάρχει ο αριθμός 0 έχει πληρώσει η NSA. Βασική υπόθεση είναι το νόμισμα να είναι αμερόληπτο, δηλαδή να υπάρχει ίση πιθανότητα να έρθει κορώνα ή γράμματα (50/50). Ένας ακόμη περιορισμός είναι ότι το γεύμα έχει πληρωθεί μόνο μία φορά και τέλος πως όλοι οι κρυπτογράφοι είναι ειλικρινείς και έμπιστοι. Εάν πάψει να ισχύει ένας από αυτούς τους περιορισμούς το πρωτόκολλο καθίσταται αναξιόπιστο καθώς θέτει σε κίνδυνο την ταυτότητα και την ανωνυμία.

Με αυτή τη μέθοδο εάν ένας κρυπτογράφος έχει πληρώσει, κανένας από τους υπόλοιπους κρυπτογράφους δεν μπορεί να συμπεράνει τίποτα για την ταυτότητά του. Σε περίπτωση που υπάρχουν μόνο δύο κρυπτογράφοι τότε οι μη συμμετέχοντες ακροατές δεν μπορούν να κάνουν διάκριση μεταξύ των δύο πιθανών αποστολέων, παρόλο που μεταξύ τους γνωρίζουν. Αυτό το πρωτόκολλο είναι απολύτως ασφαλές εάν ακολουθηθεί κατά γράμμα. Το δίλημμα που αντιμετωπίζει ένας κρυπτογράφος που δεν έχει πληρώσει είναι πως θέλει να μάθει ποιος είναι ο κρυπτογράφος που έχει πληρώσει, κάτι το οποίο δεν μπορεί να επιτευχθεί. Κάθε κρυπτογράφος ανακοινώνει το αποτέλεσμα που προκύπτει από την κοινή πράξη των δύο ρήψεων. Σε περίπτωση που έχει πληρώσει η NSA, δεν υπάρχει θέμα με την ανωνυμία. Άρα εμπλέκονται δύο υποθέσεις. Ένας από τους κρυπτογράφους να δήλωσε "ψέματα" στο σενάριο, ενώ ο άλλος απάντησε "το πραγματικό", υποδεικνύοντας ότι τα δύο νομίσματα που βλέπει ο παρατηρητής είναι ίδια. Σε κάθε κρυμμένο νόμισμα και οι δύο υποθέσεις έχουν ίσες πιθανότητες να συμβούν. Δηλαδή πως το κέρμα είναι αμερόληπτο. Με αυτόν τον τρόπο ο κρυπτογράφος που δεν έχει πληρώσει δεν μπορεί να γνωρίζει ποιος από τους υπόλοιπους κρυπτογράφους πληρώνει σε κάθε υποπερίπτωση.

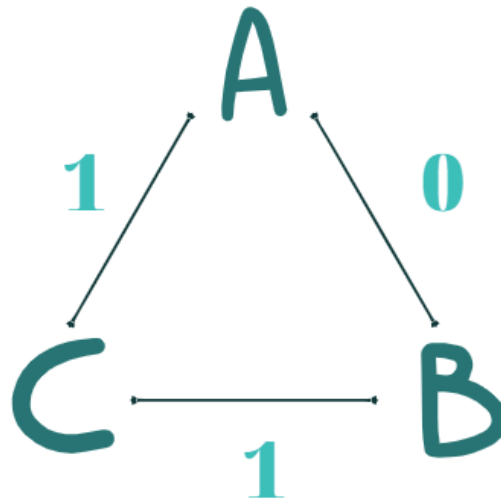


Εικόνα 1: XOR

A	B	Αποτέλεσμα
0	0	0
0	1	1
1	0	1
1	1	0

Πίνακας 1: XOR

1.4 Παράδειγμα



Εικόνα 2: Σχεδιάγραμμα τριών κόμβων

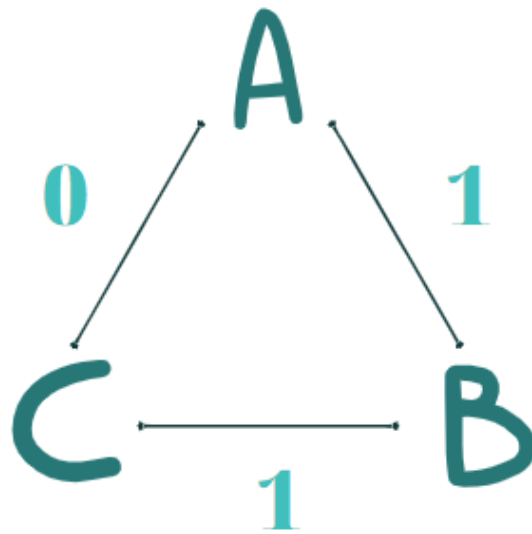
Στην παραπάνω εικόνα βλέπουμε τους τρεις κρυπτογράφους Alice, Bob, Charlie (A, B, C) και τα αποτελέσματα των ρίψεων. Σε κάθε περίπτωση το νόμισμα υποθέτουμε πως είναι δίκαιο. Υπάρχουν δηλαδή ίσες πιθανότητες να έρθει κορώνα ή γράμματα (1 ή 0). Σε περίπτωση που δεν έχει έχει πληρώσει κάποιος από αυτούς τον λογαριασμό ισχύει το πινακάκι.

Ποιός	Υπολογίζει	Αποκαλύπτει
A	$AB \text{ XOR } AC = 0 \text{ XOR } 1 = 1$	1
B	$BC \text{ XOR } BA = 1 \text{ XOR } 0 = 1$	1
C	$CA \text{ XOR } CB = 1 \text{ XOR } 1 = 0$	0

Πίνακας 2: Υπολογισμός

Και οι τρεις κρυπτογράφοι αρχικά υπολογίζουν την XOR πράξη μεταξύ των δύο ρίψεων που γνωρίζουν. Στην συνέχεια αποκαλύπτουν την τελευταία στήλη του πίνακα που δηλώνει το αποτέλεσμα αυτής της πράξης. Τέλος για να μάθουν αν έχει πληρώσει κάποιος από αυτούς ή όχι κάνουν XOR τα στοιχεία της τελευταίας στήλης. Επομένως $A_A \text{ XOR } A_B \text{ XOR } A_C = 1 \text{ XOR } 1 \text{ XOR } 0 = 0 \text{ XOR } 0 = 0$, όπου A η τρίτη στήλη (π.χ. A_A η αποκάλυψη της Alice). Όταν το αποτέλεσμα ισούται με 0 οι κρυπτογράφοι μπορούν να είναι σίγουροι πως το δείπνο είναι πληρωμένο από την NSA.

Σε μία αντίθετη περίπτωση, δηλαδή στην περίπτωση που κάποιος από τους κρυπτογράφους έχει πληρώσει το XOR αποτέλεσμα των αποκάλυψεων θα ισούται με 1.



Εικόνα 3: Σχεδιάγραμμα τριών κόμβων

Σε μία τέτοια περίπτωση, που ο λογαριασμός έχει πληρωθεί από κάποιον κρυπτογράφο, το μόνο που αλλάζει είναι η τρίτη στήλη του κρυπτογράφου που έχει πληρώσει. Έστω ότι έχει πληρώσει ο Bob, στην τρίτη στήλη θα αποκαλύψει το αντίθετο αποτέλεσμα των πράξεων.

Ποιός	Υπολογίζει	Αποκαλύπτει
A	$AB \text{ XOR } AC = 1 \text{ XOR } 0 = 1$	1
B	$BC \text{ XOR } BA = 1 \text{ XOR } 1 = 0$	1
C	$CA \text{ XOR } CB = 0 \text{ XOR } 1 = 1$	1

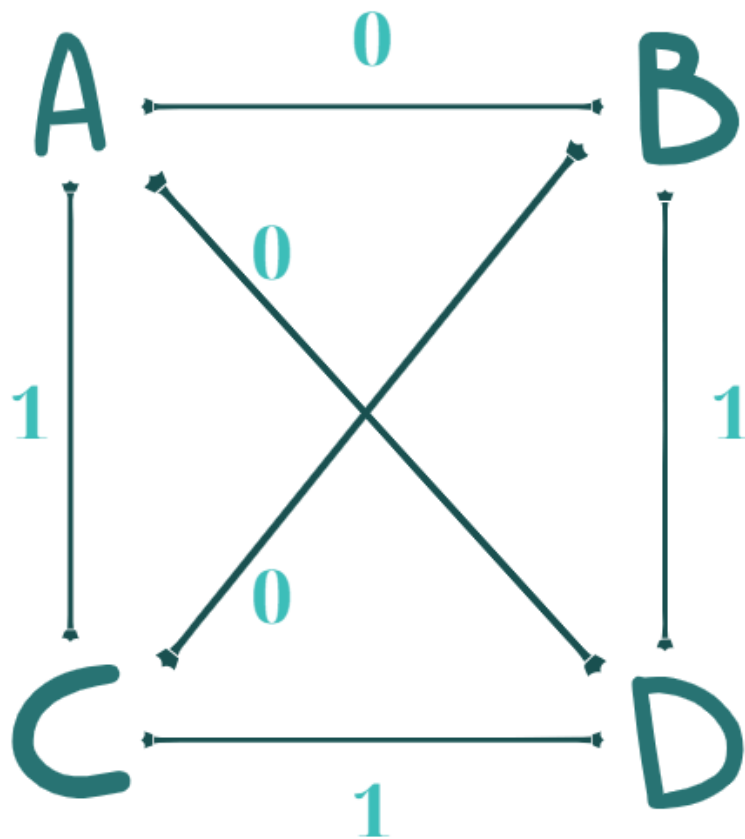
Πίνακας 3: Υπολογισμός

Υπολογίζοντας την πράξη $A_A \text{ XOR } A_B \text{ XOR } A_C = 1 \text{ XOR } 1 \text{ XOR } 1 = 1$ μπορούν πλέον να είναι σίγουροι πως κάποιος από αυτούς έχει πληρώσει. Με αυτόν τον τρόπο λειτουργούν τα DC-net. Το πρωτόκολλο διασφαλίζει ότι όταν ένας συμμετέχων εκπέμπει το bit του, οι άλλοι συμμετέχοντες μπορούν να μάθουν το άθροισμα όλων των bit αλλά δεν μπορούν να καθορίσουν την ατομική συνεισφορά κάθε κρυπτογράφου.

Σε μία διαφορετική περίπτωση όπου στο τραπέζι κάθονται περισσότεροι κρυπτογράφοι, το πρωτόκολλο εξακολουθεί να ισχύει. Για παράδειγμα εάν το $n = 4$, δηλαδή έχουμε 4 κρυπτογράφους και μία πλήρη τοπολογία:

Κλειδιά:

1. $K_{AB} = 0$
2. $K_{AC} = 1$
3. $K_{AD} = 0$
4. $K_{BC} = 0$
5. $K_{BD} = 1$
6. $K_{CD} = 1$



Εικόνα 4: Σχεδιάγραμμα τεσσάρων κόμβων, πλήρως συνδεδεμένη τοπολογία

Ποιός	Υπολογίζει	Αποκαλύπτει
A	$K_{AB} \oplus K_{AC} \oplus K_{AD} = 0 \oplus 1 \oplus 0$	1
B	$K_{AB} \oplus K_{BC} \oplus K_{BD} = 0 \oplus 0 \oplus 1$	1
C	$K_{AC} \oplus K_{BC} \oplus K_{CD} = 1 \oplus 0 \oplus 1$	0
D	$K_{AD} \oplus K_{BD} \oplus K_{CD} = 0 \oplus 1 \oplus 1$	0

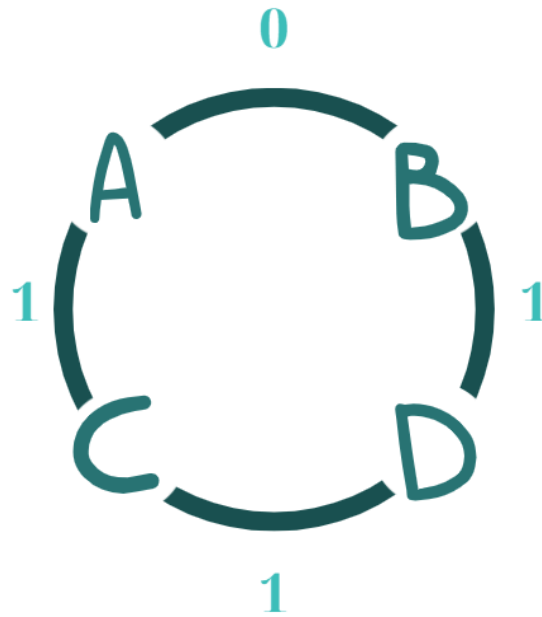
Πίνακας 4: Υπολογισμός με $n = 4$

Όπως λοιπόν και στα προηγούμενα υπολογίζοντας την πράξη $A_A \text{ XOR } A_B \text{ XOR } A_C \text{ XOR } A_D = 1 \text{ XOR } 1 \text{ XOR } 0 \text{ XOR } 0 = 0$ μπορούν πλέον να είναι σίγουροι πως κανένας από αυτούς δεν έχει πληρώσει.

Μία διαφορετική προσέγγιση είναι χρήση τοπολογίας δακτυλίου. Όταν το $n = 3$ δεν υπάρχει καμία διαφορά αλλά όσο το n αυξάνεται τότε η πολυπλοκότητα μειώνεται ραγδαία, καθώς μειώνονται οι υπολογιστικοί πόροι. Συγκριτικά πάντα με μία πλήρη τοπολογία. Σε μία τέτοια περίπτωση το παραπάνω γράφημα διαμορφώνεται ως εξής:

Κλειδιά:

1. $K_{AB} = 0$
2. $K_{AC} = 1$
3. $K_{BD} = 1$
4. $K_{CD} = 1$



Εικόνα 5: Σχεδιάγραμμα τεσσάρων κόμβων, τοπολογία δακτυλίου

Παίχτης	Υπολογίζει	Αποκαλύπτει
A	$K_{AB} \oplus K_{AC} = 0 \oplus 1$	1
B	$K_{AB} \oplus K_{BD} = 0 \oplus 1$	1
C	$K_{AC} \oplus K_{CD} = 1 \oplus 1$	0
D	$K_{BD} \oplus K_{CD} = 1 \oplus 1$	0

Πίνακας 5: Υπολογισμός με $n = 4$

Παρατηρούμε πως η τρίτη στήλη του πίνακα είναι ίδια, ως εκ τούτου $A_A \text{ XOR } A_B \text{ XOR } A_C \text{ XOR } A_D = 1 \text{ XOR } 1 \text{ XOR } 0 \text{ XOR } 0 = 0$. Μία τέτοια τοπολογία απλοποιεί την διαδικασία τόσο στο στάδιο δημιουργίας των κλειδιών όσο και στο στάδιο υπολογισμού. Ως αποτέλεσμα να απαιτούνται λιγότεροι υπολογιστικοί πόροι αλλά και λιγότερος χρόνος.

Γενικεύοντας λοιπόν το πρόβλημα, συμπεριλαμβανομένων τριών συμμετεχόντων και ανταλλάσσουν αυτή τη φορά μηνύματα μεγέθους 6 bit. Κάθε συμμετέχων γνωρίζει δύο μοναδικά συμμετρικά κλειδιά, τα οποία μοιράζεται με τους υπόλοιπους. Ας υποθέσουμε ότι η Alice επιθυμεί να επικοινωνήσει με τους υπόλοιπους. Χρησιμοποιεί όλα τα κλειδιά που μοιράζεται με τους άλλους συμμετέχοντες για να γράψει το μήνυμά της. Το αποτέλεσμα είναι μια έξοδος που η Alice διανέμει σε κάθε χρήστη του δικτύου DC. Την ίδια τεχνική ακολουθούν και οι υπόλοιποι συμμετέχοντες, εκτός από το ότι αντικαθιστούν τα μηνύματά τους με μηδενικά. Λόγω του ότι τα κλειδιά ακυρώνουν το ένα το άλλο, όλες οι έξοδοι των

συμμετεχόντων συνδυάζονται για να εμφανίσουν το σημαντικό μήνυμα της Alice. Αυτό συμβαίνει γιατί κάθε συμμετρικό κλειδί χρησιμοποιείται δύο φορές [2]. Για παράδειγμα:

Κλειδιά:

1. $K_{AB} = 111001$
2. $K_{AC} = 101001$
3. $K_{BC} = 010010$

Ποιός	Μήνυμα		K_{AB}		K_{AC}		K_{BC}		Έξοδος
A	010011	$\oplus$	111001	$\oplus$	101001	$\oplus$	-	=	000011
B	000000	$\oplus$	111001	$\oplus$	-	$\oplus$	010010	=	101011
C	000000	$\oplus$	-	$\oplus$	101001	$\oplus$	010010	=	111011

Πίνακας 6: Υπολογισμός με $K = 6$ bits

Τέλος υπολογίζουν την XOR πράξη από της εξόδους για μπορέσουν να διαβάσουν το μήνυμα. **000011 XOR 101011 XOR 111011 = 010011** που ισούται με το αρχικό μήνυμα της Alice. Σε κάθε περίπτωση η ταυτότητα του ομιλητή παραμένει άγνωστη όχι μόνο στους υπόλοιπους κρυπτογράφους αλλά και σε οποιοδήποτε κακόβουλο και μη έχει ακούσει το μήνυμα [2].

Είναι σημαντικό να τονίσουμε πως κάθε κλειδί πρέπει να χρησιμοποιείται μία μόνο φορά. Στην αρχή κάθε νέου γύρου πρέπει να δημιουργούνται και νέα κλειδιά, δηλαδή να γίνονται καινούργιες ρίψεις και να εδραιώνονται για την διασφάλιση της σωστής λειτουργίας του πρωτοκόλλου [1]. Επίσης είναι πολύ σημαντικό σε κάθε γύρο να μεταδίδει μόνο ένας για την αποφυγή συγκρούσεων.

1.5 Μειονεκτήματα

Το πρωτόκολλο έχει ορισμένα ειδικά πλεονεκτήματα όσον αφορά την ανωνυμία και το απόρρητο, αλλά έχει και ορισμένα μειονεκτήματα. Σε αυτό το σημείο, θα διερευνήσουμε τα μειονεκτήματα και τις δυσκολίες του Πρωτοκόλλου Dining Cryptographers. Είναι σημαντικό λοιπόν να εξετάσουμε τα μειονεκτήματά του, τα οποία κυμαίνονται από προβλήματα επεκτασιμότητας και αποτελεσματικότητας έως πιθανές ευπάθειες σε συγκεκριμένες καταστάσεις. Το πρωτόκολλο DC-net είναι ασφαλές ακριβώς επειδή βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών και προσφέρει μερικά μοναδικά πλεονεκτήματα για την επίτευξη ανώνυμης επικοινωνίας. Έχει όμως μερικούς κινδύνους και περιορισμούς. Εάν ένας εισβολέας μπορούσε να συνυπολογίσει το άθροισμα των τυχαίων αριθμών των κρυπτογράφων, τότε θα μπορούσε να συμπεράνει ποιος κρυπτογράφος πλήρωσε για το γεύμα. Ωστόσο, η παραγοντοποίηση μεγάλων αριθμών είναι ένα υπολογιστικά δύσκολο πρόβλημα, επομένως αυτό δεν είναι εφικτό.

Ένα από τα ελαττώματα του αλγορίθμου είναι ο χρόνος, όσο περισσότεροι οι συμμετέχοντες τόσο μεγαλύτερη καθυστέρηση του αλγορίθμου. Καθώς η ανάγκη για ασφαλή επικοινωνία μεταξύ μελών δημιουργεί επιπλέον κόστος επηρεάζοντας έτσι και την ομαλή λειτουργία του αλγορίθμου. Το πρόβλημα των κρυπτογράφων που δειπνούν απαιτεί συχνά πολλαπλούς γύρους επικοινωνίας μεταξύ των κρυπτογράφων, γεγονός που μπορεί να οδηγήσει σε αυξημένα έξοδα επικοινωνίας, ειδικά όταν πρόκειται για μεγάλες ομάδες. Αυτό συμβαίνει επειδή το πρωτόκολλο χρησιμοποιεί μια τεχνική που ονομάζεται μυστική κοινή χρήση. Η συγκεκριμένη τεχνική απαιτεί την ανταλλαγή μεγάλου αριθμού μηνυμάτων, των οποίων τόσο η επεξεργασία τους όσο και η ανταλλαγή τους απαιτεί χρόνο. Πρακτικά κάθε κρυπτογράφος ακόμη και αν δεν έχει κάποιο μήνυμα να επικοινωνήσει οφείλει να στείλει ένα “κενό” μήνυμα για να επιτευχθεί το πρωτόκολλο. Καθώς αυξάνεται ο αριθμός των κρυπτογράφων, αυξάνεται και η πολυπλοκότητα της επίτευξης ανωνυμής επικοινωνίας. Αυτό μπορεί να καταστήσει δύσκολη την αποτελεσματική κλίμακα της λύσης για μεγάλο αριθμό συμμετεχόντων. Το πρωτόκολλο απαιτεί μεγάλο αριθμό μηνυμάτων που πρέπει να ανταλλάσσονται μεταξύ των συμμετεχόντων, έτσι το κόστος της επικοινωνίας αυξάνεται. Η επεκτασιμότητα του συγκεκριμένου προβλήματος αυξάνει το κόστος επικοινωνίας καθώς και τη πολυπλοκότητα του πρωτοκόλλου. Καθώς αυξάνεται ο αριθμός των συμμετεχόντων, αυξάνεται επίσης η πολυπλοκότητα της διατήρησης της ανωνυμίας και του συγχρονισμού. Η επίτευξη επεκτασιμότητας διατηρώντας παράλληλα την ανωνυμία είναι μια πρόκληση καθώς ο αλγόριθμος απαιτεί ολοένα και περισσότερους πόρους. Προκλήσεις όπως η επίτευξη συγχρονισμού μεταξύ των συμμετεχόντων και η αντιμετώπιση τρωτών σημείων όπως οι επιθέσεις Sybil ήταν τομείς ενεργού έρευνας.

Ένα από τα βασικότερα προβλήματα των DCP είναι η αυξημένη ευπάθεια σε επιθέσεις. Ανάλογα με το κάθε πρωτόκολλο που χρησιμοποιείται για την επίλυση του προβλήματος των κρυπτογράφων τραπεζαρίας, ενδέχεται να υπάρχουν ευπάθειες που μπορούν να εκμεταλλευτούν οι αντίπαλοι και να θέσει σε κίνδυνο την ανωνυμία των συμμετεχόντων. Αυτή η ευπάθεια προκύπτει λόγω της φύσης του αλγορίθμου και πιο συγκεκριμένα από την επίτευξη της τέλει ανωνυμίας σε ένα κατανομημένο και δυνητικά αντίθετο περιβάλλον. Κατά συνέπεια ο αλγόριθμος γίνεται επιρρεπής σε μία σειρά διάφορων επιθέσεων. Επίσης ο συγχρονισμός των μηνυμάτων είναι απαραίτητος. Ο αλγόριθμος απαιτεί προσεκτικό συγχρονισμό μεταξύ των συμμετεχόντων για να διασφαλιστεί ότι το πρωτόκολλο προχωρά σωστά. Εάν τα ρολόγια των συμμετεχόντων δεν είναι καλά συγχρονισμένα, μπορεί να οδηγήσει σε αποτυχίες πρωτοκόλλου ή λανθασμένα αποτελέσματα ακόμη και σε συγκρούσεις [14]. Το πρωτόκολλο επίσης, προϋποθέτει ότι όλοι οι συμμετέχοντες ακολουθούν το πρωτόκολλο με ειλικρίνεια και δεν συνεργάζονται για να υπονομεύσουν την ασφάλειά των συμμετεχόντων αλλά και του μηνύματος. Εάν οποιοσδήποτε συμμετέχων παρεκκλίνει από το πρωτόκολλο ή ενεργεί με κακόβουλο τρόπο, οι εγγυήσεις απορρήτου που παρέχονται από τον DCP ενδέχεται να τεθούν σε κίνδυνο. Σύμφωνα με το πρωτόκολλο η εμπιστοσύνη μεταξύ μελών καθίσταται απαραίτητη για την ασφαλή λειτουργία του. Επίσης, σε περίπτωση που ένας συμμετέχων δεν ακολουθήσει το πρωτόκολλο και αποκαλύψει το δικό του τυχαίο bit, θα μπορούσε να θέσει σε κίνδυνο το απόρρητό του αλλά και των άλλων. Όπως συμβαίνει με οποιαδήποτε κρυπτογραφικό πρωτόκολλο άλλωστε, τα σφάλματα υλοποίησης μπορεί να οδηγήσουν σε κενά ασφαλείας. Η ασφάλεια του πρωτοκόλλου θα μπορούσε να τεθεί σε κίνδυνο, για παράδειγμα, εάν η

λειτουργία XOR δεν εκτελεστεί σωστά ή εάν η τυχαία δημιουργία κλειδιών, η ρίψη νομίσματος στην συγκεκριμένη περίπτωση έχει ελαττώματα.

Λόγω του συγκεκριμένου σχεδιασμού και των περιορισμών του, το DCP ενδέχεται να μην είναι κατάλληλο για όλες τις απαιτήσεις απορρήτου ή ανωνυμίας. Διαφορετικά πρωτόκολλα κρυπτογράφησης ή τεχνολογίες ενίσχυσης της ιδιωτικής ζωής μπορεί να είναι πιο κατάλληλα για αρκετά σενάρια. Μια τέτοια θεωρητική κατασκευή ενδέχεται να μην έχει άμεσες πρακτικές εφαρμογές. Ενώ η ανώνυμη επικοινωνία είναι μια ενδιαφέρουσα έννοια, οι εφαρμογές του πραγματικού κόσμου συχνά περιλαμβάνουν πρόσθετες σκέψεις που υπερβαίνουν το πεδίο αυτού του προβλήματος. Ωστόσο χρησιμοποιείται κυρίως ως θεωρητικό κατασκεύασμα για τη μελέτη κρυπτογραφικών πρωτοκόλλων και αποτελεί έμπνευση για ερευνητές. Το DCP λειτουργεί ως θεωρητικό πλαίσιο για την έρευνα των θεμελιωδών αρχών και των περιορισμών της ανώνυμης επικοινωνίας. Τα συστήματα πραγματικού κόσμου που το απαιτούν συνδυάζουν συχνά κρυπτογραφικές μεθόδους, συσκότιση της κυκλοφορίας και αυστηρές διαδικασίες ασφαλείας για τη μείωση των τρωτών σημείων. Κατά τη χρήση, τα κρυπτογραφικά πρωτόκολλα και τα συστήματα ανωνυμίας υποβάλλονται σε εις βάθος εξέταση ασφαλείας και τα σχέδιά τους ενημερώνονται συχνά για την αντιμετώπιση τυχόν αδυναμιών και την αποτροπή επιθέσεων όσο το δυνατόν περισσότερο. Ωστόσο, η επίτευξη πλήρους επωνυμίας σε ένα εχθρικό περιβάλλον εξακολουθεί να είναι ένα δύσκολο ερευνητικό θέμα στους τομείς της ασφάλειας των υπολογιστών και της κρυπτογραφίας.

1.5.1 Συγκρούσεις

Δυστυχώς ενδέχεται να προκύψουν διάφορες διενέξεις εάν έστω και ένας συμμετέχων αποκλίνει από το πρωτόκολλο ή εάν το πρωτόκολλο δεν εκτελεστεί σωστά. Σε περίπτωση για παράδειγμα, που σταλούν δύο ή και περισσότερα μηνύματα στον ίδιο γύρο θα συγκρουστούν και θα γίνουν άχρηστα, δηλαδή δε θα μπορούν να διαβαστούν [14]. Ένα από τα κύρια προβλήματα με το πρωτόκολλο DC είναι η ευπάθειά του σε επιθέσεις ανάλυσης κυκλοφορίας. Αυτό μπορεί να συμβεί είτε τυχαία είτε σκόπιμα. Για παράδειγμα, εάν ένα κακόβουλο μέρος παρεμβαίνει στην επικοινωνία στέλνοντας είτε λανθασμένα είτε μη έγκυρα μηνύματα με σκοπό να την εμποδίσει. Με αυτό τον τρόπο εμποδίζεται η ροή των μηνυμάτων και τελικά οι συμμετέχοντες δεν καταφέρνουν να επικοινωνήσουν.

Συνεπώς το DCP είναι ευάλωτο σε επιθέσεις παρεμβολής, καθώς και συνολικά δεν είναι τόσο αποτελεσματικό όσο κάποια άλλα κρυπτογραφικά πρωτόκολλα. Αυτό δημιουργεί το εξής ερώτημα: Πώς γνωρίζει κάθε συμμετέχων πότε είναι η σειρά του να στείλει; Θα πρέπει να γνωρίζουμε πως πρωτόκολλα κράτησης χρονοθυρίδων (slot reservation protocols), όπως αυτά που χρησιμοποιούνται σε δίκτυα TDMA (πολλαπλής πρόσβασης δυναμικής διαίρεσης χρόνου), δεν είναι κατάλληλα, καθώς θα έθεταν σε κίνδυνο την ανωνυμία [2]. Η επιλογή ενός χρονοδιαγράμματος αποστολής, είναι καθήκον της κράτησης υποδοχής στο DC-net, ώστε κάθε συμμετέχων να γνωρίζει πότε να στείλει, ενώ παράλληλα να μην γνωρίζει ποιος στέλνει κατά τη διάρκεια των άλλων χρονοθυρίδων. Υπάρχουν

συνήθως τρεις τρόποι χειρισμού αυτού του προβλήματος. Η πρώτη στρατηγική αποτελείται από τεχνικές γνωστές ως τεχνική κράτησης-χάρτης (reservation-map). Αυτές οι τεχνικές χρησιμοποιούν ένα διάνυσμα προγραμματισμού που αποτελείται από υποδοχές. Κάθε υποδοχή αντιστοιχεί σε έναν μελλοντικό γύρο με έναν σχετικό αριθμό ευρητηρίου. Ένας συμμετέχων μπορεί να κρατήσει έναν γύρο σημειώνοντας το αντίστοιχο διάστημα όπως λαμβάνεται στο διάνυσμα προγραμματισμού. Η δεύτερη στρατηγική για την επίλυση των συγκρούσεων είναι η χρήση διαφόρων αλγορίθμων. Ενώ η τρίτη μέθοδος περιλαμβάνει τη χρήση ασφαλούς υπολογισμού πολλαπλών μερών για τη δημιουργία μιας μυστικής ανταλλαγής που κατανέμει τους συμμετέχοντες σε γύρους. Μία τρίτη λύση θα μπορούσε να είναι η εισαγωγή επιπρόσθετων μέτρων όπως padding. Η χρήση padding είναι εξαιρετικά ωφέλιμη όταν χρειάζεται να διαχωρίσουμε με πλαίσια διατηρώντας τα ευθυγραμμισμένα. Ωστόσο, η εφαρμογή τέτοιων μέτρων μπορεί να είναι δύσκολη και να δημιουργήσει επιπλέον πολυπλοκότητες.

Ο David Chaum για πρόληψη συγκρούσεων προτείνει την αναμετάδοση του μηνύματος [1]. Όταν δηλαδή ανακαλύπτεται μια σύγκρουση να μεταδίδεται ξανά το ίδιο μήνυμα, αν και το έγγραφο δεν προσδιορίζει τον τρόπο ρύθμισης της αναμετάδοσης. Ο αλγόριθμος Dining Cryptographers επιτρέπει στους συμμετέχοντες να στέλνουν μηνύματα με τέτοιο τρόπο που να διασφαλίζεται ότι δεν μπορούν να εντοπιστούν. Μια τέτοια ανωνυμία αποστολέα, ωστόσο, δημιουργεί νέα προβλήματα. Κάποιοι συμμετέχοντες μπορούν να στείλουν πολλά μηνύματα ενώ άλλοι μπορεί να μην στείλουν και κανένα. Και τότε έχουμε αναστάτωση. Μια θεωρητική λύση παρουσιάζει ο Chaum, η οποία καθίσταται αδύνατη, καθώς ο αριθμός των συμμετεχόντων είναι τετραγωνικός. Αντίστοιχα δίνουν μία λύση οι Jurjen Bos και Bert den Boer [14].

1.5.2 Επιθέσεις

Όπως προείπαμε το πρωτόκολλο είναι πέρα ως πέρα ασφαλές εάν εκτελεστεί σωστά, σε τι είδους επιθέσεις όμως υπόκειται; Σε περίπτωση που κάποιος παρατηρήσει τα μοτίβα ανταλλαγής μηνυμάτων και τα εξετάσει μπορεί να αποσπάσει πληροφορίες για τη ταυτότητα των συνομιλητών ακόμη και αν το μήνυμα είναι κρυπτογραφημένο. Αυτή η επίθεση ονομάζεται traffic analysis attack, περιλαμβάνει την παρατήρηση και την ανάλυση των προτύπων ανταλλαγής μηνυμάτων και χωρίς απαραίτητα να αποκρυπτογραφείται το περιεχόμενό τους. Παρόλο που το περιεχόμενο είναι κρυπτογραφημένο, ο χρόνος, η συχνότητα και το μέγεθος των μηνυμάτων μπορούν να παρέχουν ενδείξεις για το ποιος επικοινωνεί με ποιον. Τεχνικές όπως οι επιθέσεις συσχέτισης κυκλοφορίας στοχεύουν στην εκμετάλλευση αυτών των μοτίβων με σκοπό να αντλήσουν την παραμικρή πληροφορία [19]. Τα DC-Nets συνήθως απαιτούν από τους συμμετέχοντες να στέλνουν "εικονικά" μηνύματα ή "0" μαζί με τα πραγματικά τους μηνύματα για να διατηρηθεί η ανωνυμία. Εάν ένας εισβολέας μπορεί να συμπεράνει το μέγεθος αυτών των ψευδών μηνυμάτων, μπορεί να είναι σε θέση να τα συσχετίσει με πραγματικά μηνύματα. Αυτή η επίθεση ονομάζεται Message Size Analysis. Μια διαφορετική επίθεση είναι η Sybil attack, σύμφωνα με την

οποία κάποιος κακόβουλος δημιουργεί πολλαπλές πλαστές ταυτότητες [20]. Στο DCP, μία τέτοια επίθεση θα μπορούσε να περιλαμβάνει τη δημιουργία πολλαπλών εικονικών κρυπτογράφων οι οποίοι είτε απλά παρακολουθούν είτε συμμετέχουν προσπαθώντας να αποσπάσουν πληροφορίες ή να διαταράξουν τη λειτουργία του πρωτοκόλλου. Τα DC-Nets προϋποθέτουν ότι υπάρχει ένας σταθερός και γνωστός αριθμός συμμετεχόντων. Επιθέσεις τύπου Sybil συμβαίνουν όταν ένας αντίπαλος δημιουργεί πολλαπλές πλαστές ταυτότητες, κάποιες φορές ξεπερνώντας τους ειλικρινείς συμμετέχοντες. Αυτό μπορεί να διαταράξει τις εγγυήσεις ανωνυμίας του πρωτοκόλλου, καθώς ο εισβολέας έχει μεγαλύτερη παρουσία στο δίκτυο. Αυτές οι ταυτότητες θα μπορούσαν να έχουν την μορφή κόμβων ή κρυπτογράφων στην περίπτωση του DCP. Αντίστοιχα σε επιθέσεις Denial of Service, στοχεύουν να διαταράξουν το πρωτόκολλο [22]. Γνωστή ως DoS, προσπαθεί να παραβιάσει το πρωτόκολλο βομβαρδίζοντάς το με υπερβολική κίνηση ή αιτήματα. Όπως ακριβώς είχε συμβεί το 2000 στις μεγαλύτερες εταιρείες eBay, Amazon, CNN, Dell και Yahoo [21]. Αυτό μπορεί να δυσκολέψει τους νόμιμους κρυπτογράφους να επικοινωνήσουν ξεκάθαρα ή να καταλήξουν σε κάποια συμφωνία. Οι εισβολείς ενδέχεται να παραβιάσουν μηνύματα είτε στέλνοντας τα δικά τους μηνύματα είτε επαναλαμβάνοντας κάποιο προηγούμενο μήνυμα. Αυτό μπορεί να οδηγήσει σε σύγχυση μεταξύ των συμμετεχόντων. Εάν ένας εισβολέας επίσης, μπορεί να πλημμυρίσει το δίκτυο με μεγάλο αριθμό μηνυμάτων. Τα δίκτυα DC συχνά περιλαμβάνουν σημαντικό όγκο πλεονάζουσας επικοινωνίας, αφού απαιτούνται εικονικά μηνύματα. Ο αλγόριθμος από μόνος του έχει πολύ αυξημένες δαπάνες επικοινωνίας και μία τέτοια επίθεση μπορεί πολύ γρήγορα να εξαντλήσει τους πόρους του συστήματος, να διαταράξει τη σωστή λειτουργία του πρωτοκόλλου, να προκαλέσει συμφόρηση ή να δυσκολέψει την επικοινωνία των ειλικρινών συμμετεχόντων.

Για την αποφυγή τέτοιου είδους επιθέσεων είναι σημαντικό να χρησιμοποιείται ισχυρή κρυπτογράφηση για τη διασφάλιση των μηνυμάτων. Έτσι εμποδίζεται για κάποιο κακόβουλο μέρος, η κατανόηση των μηνυμάτων ακόμα κι αν καταφέρει να αναλύσει τα μοτίβα κυκλοφορίας. Η κρυπτογράφηση από άκρο σε άκρο (end-to-end encryption) διασφαλίζουν ότι μόνο ο προβλεπόμενος παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα.

1.6 Πλεονεκτήματα

Το πρωτόκολλο Dining Cryptographers Protocol είναι ένα πρωτόκολλο μηδενικής γνώσης που έχει σχεδιαστεί για να επιτρέπει σε μια ομάδα συμμετεχόντων να συμφωνήσουν σε μια κοινή πορεία χωρίς να αποκαλύπτουν μεμονωμένες πληροφορίες. Ένα από τα μεγαλύτερα και σημαντικότερα πλεονεκτήματα του πρωτοκόλλου είναι η διατήρηση του απορρήτου. Αποτελεί και τον σκοπό άλλωστε, η ικανότητά του να επιτρέπει στους συμμετέχοντες να μοιράζονται πληροφορίες με τρόπο που διατηρεί το απόρρητο. Δίνεται η δυνατότητα να ανταλλάσσουν μηνύματα χωρίς να αποκαλυφθεί ούτε η ταυτότητα του μηνύματος αλλά ούτε και του αποστολέα. Οι πληροφορίες που αποστέλλονται ενδέχεται να είναι ευαίσθητες ή εμπιστευτικές, το DCP επιτυγχάνει τη διατήρηση της ιδιωτικής ζωής

μέσω της έννοιας της ανώνυμης μετάδοσης και των αποδείξεων μηδενικής γνώσης. Το πρωτόκολλο διασφαλίζει ότι όταν ένας συμμετέχων εκπέμπει το μήνυμά του, οι άλλοι συμμετέχοντες μπορούν να μάθουν το άθροισμα όλων των μηνυμάτων αλλά δεν μπορούν να καθορίσουν την ατομική συνεισφορά κάθε συμμετέχοντα. Σε μία πιθανή παρουσία κάποιου κακόβουλου κρυφογράφου όπως η Eve για παράδειγμα, δεν διακυβεύονται τα προσωπικά δεδομένα των συμμετεχόντων αλλά ούτε και το μήνυμα. Εξαίρεση βέβαια αποτελεί η συνεργασία της Eve με κάποιους από τους συμμετέχοντες, έτσι η Eve θα καταφέρει να αποσπάσει πληροφορίες. Αυτό όμως δεν είναι εφικτό, καθώς μία απαραίτητη προϋπόθεση για την ομαλή λειτουργία του πρωτοκόλλου όπως προείπαμε, αποτελεί πως όλοι οι κρυπτογράφοι είναι ειλικρινής και έμπιστοι. Άρα κανένας τους δεν θα συνεργαζόταν με κάποιον κακόβουλο.

Με τη χρήση αποδείξεων μηδενικής γνώσης (zero-knowledge), ένα μέρος μπορεί να αποδείξει σε ένα τρίτο μέρος ότι γνωρίζει μια συγκεκριμένη πληροφορία χωρίς στην πραγματικότητα να την αποκαλύψει. Δηλαδή, στο πρωτόκολλο DC οι κρυπογράφοι μπορούν να αποδείξουν πως πως έχουν μεταδώσει ένα μήνυμα χωρίς να αποκαλύψουν το περιεχόμενο του μηνύματος. Ως αποτέλεσμα, οι υπόλοιποι κρυπτογράφοι μπορούν να υπολογίσουν το σύνολο των μηνυμάτων, δεν είναι σε θέση να γνωρίζουν ποιος κρυπογράφος μετέδωσε ποιο μήνυμα. Οι αποδείξεις μηδενικής γνώσης χρησιμοποιούνται συχνά στο πλαίσιο του απορρήτου και της ανωνυμίας για να δείξουν ότι κάποιος γνωρίζει ένα μυστικό κλειδί ή άλλες σχετικές πληροφορίες χωρίς στην πραγματικότητα να αποκαλύψει το κλειδί αλλά ούτε και το μήνυμα. Άρα μπορούμε να εγγυηθούμε πως οι συνομιλίες και οι αλληλεπιδράσεις μπορούν να πραγματοποιηθούν με ασφάλεια χωρίς να αποκαλυφθούν οποιαδήποτε δεδομένα. Οι αποδείξεις μηδενικής γνώσης χρησιμοποιείται στα δίκτυα DC για να αυξηθεί η διατήρηση της ιδιωτικότητας. Οι συμμετέχοντες στο δίκτυο DC μπορούν να αποδείξουν ότι ακολούθησαν σωστά το πρωτόκολλο και πως έστειλαν ένα έγκυρο μήνυμα χωρίς να αποκαλύπτουν το ίδιο το μήνυμα χρησιμοποιώντας αποδείξεις μηδενικής γνώσης. Σε κάποια πιθανή ύπαρξη ενός αλλά και περισσότερων κακόβουλων μελών, δεν μπορούν να αποσπάσουν καμία πληροφορία ούτε για το περιεχόμενο του μηνύματος αλλά ούτε και για την ταυτότητα του αποστολέα του. Με άλλα λόγια δεν μπορεί κάποιος εξωτερικός παρατηρητής να συνδέσει ένα μήνυμα με τον κρυπτογράφο που το έστειλε. Το πρωτόκολλο των κρυπτογράφων που δειπνούν καθιστά υπολογιστικά αδύνατο για έναν ξένο να συνδέσει τη δραστηριότητα ενός συμμετέχοντα με τα δεδομένα που παραδίδονται.

Από τη φύση του το πρωτόκολλο είναι αδιαπέραστο σε ακροατές. Αυτό σημαίνει πως ακόμα κι αν ένα τρίτο μέρος ακούσει τη συνομιλία, δεν θα μπορεί να προσδιορίσει τις ατομικές συνεισφορές των συμμετεχόντων. Επίσης διασφαλίζεται πως οι συμμετέχοντες μπορούν να επικοινωνούν με ασφάλεια. Εμποδίζει τους ξένους ή τους κρυφογράφους να μάθουν για τις αποφάσεις που έλαβαν οι συμμετέχοντες. Το πρωτόκολλο προσφέρει αδιαπέραστη ιδιωτικότητα αλλά υπό όρους. Κάτι που σημαίνει ότι με βάση συγκεκριμένα κρυπτογραφικά τεκμήρια και προϋποθέσεις, το απόρρητο των συμμετεχόντων προστατεύεται.

Κεφάλαιο 2^ο

2.1 Αλγόριθμοι εμπνευσμένοι από το DCP

Αξίζει να σημειωθεί ότι το Πρόβλημα των Κρυπτογράφων Τραπεζαρίας χρησιμοποιείται κυρίως ως θεωρητικό κατασκεύασμα για τη μελέτη κρυπτογραφικών πρωτοκόλλων και της ιδιωτικής ζωής αντί να είναι άμεσα εφαρμόσιμο σε πρακτικά σενάρια. Οι ερευνητές το χρησιμοποιούν ως σημείο εκκίνησης για να αναπτύξουν πιο εξελιγμένες και περισσότερο πρακτικές λύσεις ανωνυμίας. Αν και το ίδιο το DCP μπορεί να μην εφαρμόζεται άμεσα σε σενάρια πραγματικού κόσμου, έχει επηρεάσει τη δημιουργία μιας σειράς άλλων πρωτοκόλλων που σχετίζονται με το απόρρητο και την κρυπτογραφία. Σε αυτά τα πρωτόκολλα συχνά εμπεριέχουν διάφορα είδη ανώνυμης και ασφαλούς επικοινωνίας. Το πρόβλημα που παρουσίασε ο David Chaum αποτέλεσε έμπνευση καθώς τόνιζε τη σημασία και τη σημαντικότητα της ανωνυμίας και της ασφαλούς επικοινωνίας. Μερικοί αλγόριθμοι που επηρεάστηκαν από το DCP και συχνά επεκτείνουν και προσαρμόζουν αυτές τις ιδέες για να αντιμετωπίσουν συγκεκριμένες περιπτώσεις χρήσης και τεχνολογικές προκλήσεις στον σύγχρονο κόσμο:

1. Onion Routing (Tor)
2. Mix Networks
3. Oblivious Transfer
4. Private Information Retrieval
5. Privacy-Preserving Cryptocurrencies
6. Privacy-Preserving Machine Learning
7. Zero-Knowledge Proofs
8. Anonymous Voting Protocols
9. Secure Multi-Party Computation
10. Cryptocurrency Privacy Features
11. Homomorphic Encryption

Στον Onion Routing για παράδειγμα Για να επιτευχθεί η ανώνυμη επικοινωνία στο διαδίκτυο, χρησιμοποιείται μια παραλλαγή της δρομολόγησης onion [15]. Τα δεδομένα κρυπτογραφούνται σε επίπεδα με δρομολόγηση κρεμμυδιού, με κάθε στρώμα να αποκωδικοποιείται σε ξεχωριστό κόμβο δικτύου. Η ιδέα του συνδυασμού και της τυφλής πληροφορίας που περιγράφεται στο DCP χρησίμευσε ως ένα είδος έμπνευσης για αυτή τη διαδικασία. Οι αποδείξεις μηδενικής γνώσης επιτρέπουν σε ένα άτομο να αποδείξει σε ένα άλλο ότι γνωρίζει κάποιες πληροφορίες χωρίς να αποκαλύψει αυτές τις πληροφορίες. Πολλά κρυπτογραφικά πρωτόκολλα, όπως τα zk-SNARK του Zcash, τα οποία επηρεάστηκαν από την έρευνα απορρήτου του Chaum, χρησιμοποιούν αυτήν την ιδέα [16].

2.2 Dining cryptographers network

Τα DC-nets (Dining cryptographers network) επικεντρώνονται στη δημιουργία ενός ιδιωτικού και ασφαλούς δικτύου για την επικοινωνία των συμμετεχόντων. Τα δίκτυα DC βασίζονται στην καθιέρωση των μυστικών κλειδιών μεταξύ κάθε ζεύγους των μερών. Οι συμμετέχοντες προσπαθούν να υποβάλουν μηνύματα με ανώνυμο τρόπο και να λάβουν ομαδική έξοδο χωρίς να αποκαλύπτουν τις ατομικές εισροές τους. Αυτό επιτυγχάνεται αποκρύπτοντας την προέλευση του μηνύματος κάθε συμμετέχοντα χρησιμοποιώντας μια σειρά από κρυπτογραφικές διαδικασίες και τεχνικές. Από τότε τα δίκτυα DC έχουν χρησιμοποιηθεί ως ένας από τους πιθανούς τρόπους υλοποίησης της ανώνυμης μετάδοσης των μηνυμάτων [3]. Οι χρήστες τους μπορούν να μεταδίδουν αλλά και να λαμβάνουν μηνύματα με πλήρη ανωνυμία. Με τα Dc-nets κάθε συμμετέχων γνωρίζει συγκεκριμένα τα bit του χρονοδιαγράμματος που αντιστοιχούν στη συγκεκριμένη θυρίδα μετάδοσης του, ενώ ταυτόχρονα δεν γνωρίζει σε ποιον ανήκουν υπόλοιπες θυρίδες μετάδοσης.



Εικόνα 6: Σχεδιάγραμμα τριών κόμβων με 3 και 2 συνδεδεμένους κόμβους

Με αυτό τον τρόπο κάθε μέλος γνωρίζει πότε μπορεί να μεταδώσει χωρίς να έχει καμία εικόνα για τη σειρά μετάδοσης. Το πρωτόκολλο μπορεί να εκτελεστεί και με λιγότερο από πλήρως συνδεδεμένα γραφήματα. Αν οι συνδεδεμένοι παίκτες που συνομιλούν μπορούν να χωρίσουν το γράφημα κοινής μυστικής χρήσης σε διαφορετικά συνδεδεμένα στοιχεία, η ανωνυμία μπορεί να μειωθεί. Ωστόσο, η εκτέλεση του πρωτοκόλλου με λιγότερο από πλήρως συνδεδεμένα γραφήματα κοινής χρήσης μυστικών μπορεί να αυξήσει την αποτελεσματικότητα και την επεκτασιμότητα των πραγματικών υλοποιήσεων του δικτύου DC. Το κλασικό πρόβλημα των κρυπτογράφων που δειπνούν είναι ένα δίκτυο με τοπολογία δακτυλίου/δαχτυλίδι και $n = 3$ συμμετέχοντες, οι οποίοι είναι πλήρως συνδεδεμένοι μεταξύ τους. Ωστόσο, εάν η Alice και ο Charlie είναι στην πραγματικότητα κακόβουλοι που κάθονται δεξιά και αριστερά του Bob, που είναι αθώος, και αν η Alice και ο Charlie συνεννοηθούν κρυφά για να αποκαλύψουν τα μυστικά τους ο ένας στον άλλο, τότε μπορούν να γνωρίζουν με βεβαιότητα αν ο Bob ήταν ή όχι ο αποστολέας ενός μηνύματος σε μια εκτέλεση DC-net, ανεξαρτήτως από τον αριθμό των συμμετεχόντων που υπάρχουν συνολικά. Αυτό οφείλεται στο γεγονός ότι η Alice και ο Charlie ουσιαστικά έσπασαν το γράφημα χωρίζοντάς το σε δύο ξεχωριστά αποσυνδεδεμένα στοιχεία, το ένα περιέχει μόνο τον Bob, το άλλο περιέχει την Alice και τον Charlie.

Το βασικό πρωτόκολλο δικτύων DC γενικεύεται σε οποιοδήποτε τελεστή αλφάβητου και συνδυασμού κατάλληλου για κρυπτογράφηση ηλεκτρολογίου μίας χρήσης, παρόλο που το απλό πρωτόκολλο δικτύων DC χρησιμοποιεί δυαδικά ψηφία ως αλφάβητο μετάδοσης και τον τελεστή XOR για να συνδυάζει κρυπτογραφημένα κείμενα. Επίσης ένα πολύ σημαντικό πλεονέκτημα των DC-net δικτύων είναι ότι παρέχει πλήρη ανωνυμία σε αποστολέα και παραλήπτη χωρίς να βασίζεται σε κάποιο έμπιστο τρίτο μέρος. Το γεγονός ότι τα μυστικά που κοινοποιούνται από τα διάφορα ζεύγη συμμετεχόντων είναι στην πραγματικότητα, μόνο One-time pad (σημειωματάριο μιας χρήσης) που συνδέονται συμμετρικά σε έναν μόνο γύρο δικτύου DC και οδηγεί σε αυτήν την ευελιξία. Το One-time pad (OTP) είναι μια μέθοδος κρυπτογράφησης χωρίς δυνατότητα διάρρηξης. Στην ουσία, χρησιμοποιεί ένα πρώην-κοινόχρηστο κλειδί μιας χρήσης που δεν μπορεί να είναι μικρότερο από το μήνυμα που αποστέλλεται. Αυτή η μέθοδος συνδυάζει ένα απλό κείμενο με ένα μυστικό κλειδί που επιλέγεται τυχαία. Στη συνέχεια κάθε bit ή χαρακτήρας του απλού κειμένου συνδυάζεται με το αντίστοιχο bit ή χαρακτήρα από το pad για να δημιουργηθεί το νέο κρυπτογραφημένο μήνυμα.

2.3 Κρυπτογραφία κατωφλίου με DC-Nets

Μία ιδέα για επιπλέον ασφάλεια και εχεμύθεια μπορούμε να επιτύχουμε κρυπτογραφώντας το μήνυμα με χρήση περισσότερων αλγορίθμων. Δυστυχώς όμως αυξάνεται και η πολυπλοκότητα αλλά και οι απαιτούμενοι υπολογιστικοί πόροι, με αποτέλεσμα να χρειάζεται πολύ χρόνο. Η χρήση κοινού μυστικού (secret sharing) ή η παραλλαγή της k -out-of- n είναι μία κρυπτογραφική τεχνική, χρησιμοποιείται για τον διαμοιρασμό ενός μυστικού μεταξύ πολλών ατόμων. Το μυστικό μπορεί να ανακατασκευαστεί μόνο όταν ένας προκαθορισμένος αριθμός συμμετεχόντων συγκεντρωθεί. Ο κάθε συμμετέχων συνεισφέρει το μερίδιό του στο μυστικό. Είναι ένα ασφαλές σύστημα κοινής χρήσης πληροφοριών με εχεμύθεια [11]. Αποτελεί ένα από τα πιο δημοφιλή και ευρέως χρησιμοποιούμενα συστήματα. Βασική ιδέα πίσω από την κοινή χρήση μυστικών αποτελεί ο πλεονασμός και να αποτρέπει οποιονδήποτε μεμονωμένο μέρος από το να έχει πλήρη και μη γνώση του εκάστοτε μυστικού. Με αυτό τον τρόπο το επίπεδο ασφάλειας είναι αρκετά υψηλό ενώ ταυτόχρονα διασφαλίζει ότι το μυστικό παραμένει ασφαλές ακόμα κι αν ορισμένοι συμμετέχοντες είναι σε κίνδυνο. Ένας ορισμός είναι: Ένα σύστημα k -out-of- n απαρτίζεται από n στοιχεία τα οποία αρχίζουν να λειτουργούν ταυτόχρονα. Ο αλγόριθμος λειτουργεί όσο λειτουργούν τα k στοιχεία και πέφτει όταν $n-k+1$. Τα παράλληλα και τα σειριακά συστήματα είναι συγκεκριμένες περιπτώσεις k -out-of- n και αντιστοιχούν σε $k = 1$ και $k = n$, αντίστοιχα [12]. Τουλάχιστον K συμμετέχοντες πρέπει να συγκεντρωθούν και να συνδυάσουν τις γνώσεις τους για να αποκαλύψουν το μυστικό, αλλά λιγότεροι από K συμμετέχοντες δεν μπορούν να παρέχουν πληροφορίες σχετικά με το μυστικό. Με άλλα λόγια πρέπει όλοι οι συμμετέχοντες να

παρευρίσκονται για να επιτύχουν την αποκρυπτογράφηση του μυστικού. Εάν οι συμμετέχοντες, δηλαδή το K είναι σε υψηλή τιμή αυξάνει την ασφάλεια, καθώς απαιτούνται περισσότεροι συμμετέχοντες για την αποκρυπτογράφηση του μυστικού, αλλά μπορεί επίσης να καταστήσει πολύ πιο δύσκολο τόσο στον συντονισμό όσο και στην ανακατασκευή του μυστικού.

Από τη μία αυτή η ιδιότητα είναι χρήσιμη σε σενάρια όπου πολλά άτομα ή οντότητες μπορεί να χρειαστεί να συνεργαστούν για να εκτελέσουν κρίσιμες λειτουργίες, όπως ανάκτηση δεδομένων, διαχείριση κρυπτογραφικού κλειδιού ή πρόσβαση σε ευαίσθητες πληροφορίες. Παρέχει έναν τρόπο διανομής της εμπιστοσύνης και του ελέγχου μεταξύ διαφορετικών συμμετεχόντων, διασφαλίζοντας παράλληλα ότι το μυστικό παραμένει ασφαλές όσο ο αριθμός των συμμετεχόντων που έχουν παραβιαστεί είναι μικρότερος από το όριο K .

Συνδυάζοντας τις τεχνικές του k -out-of- n και των DC-Nets δημιουργείται ένα σύστημα στο οποίο ισχύουν τα πλεονεκτήματα και τα μειονεκτήματα κι των δύο αυτών τεχνικών. Το σύστημα αυτό παρέχει πλήρη ανωνυμία αλλά και ασφάλεια σε ένα πλαίσιο συγκεκριμένων συμμετεχόντων. Πως μπορούμε να το πετύχουμε αυτό; Αντλούμε από το k -out-of- n ένα μυστικό ή κρυπτογραφικό κλειδί το οποίο διαιρείται σε έναν αριθμό μετοχών, στο σύνολο των κρυπτογράφων που είναι συμμετέχοντες στο δείπνο στη συγκεκριμένη περίπτωση. Με αυτό τον τρόπο έχει οριστεί ένας ορισμένος αριθμός συμμετεχόντων (k από n) ο οποίος είναι απαραίτητος για την ανασύσταση του αρχικού μυστικού. Αυτό διασφαλίζει ότι κανείς δεν μπορεί να ανακαλύψει το μυστικό μόνος του, ούτε και με ένα μέρος των συμμετεχόντων. Από τα DC-Nets αντλούμε την κεντρική ιδέα. Οποιοσδήποτε μπορεί να μεταδώσει ένα μήνυμα, καθιστώντας υπολογιστικά αδύνατο να προσδιοριστεί η πηγή οποιουδήποτε δεδομένου μηνύματος. Η ιδέα της ανάμειξης μηνυμάτων μεταξύ των συμμετεχόντων είναι κεντρική στα DC-nets για να ενεργοποιηθεί η ανώνυμη επικοινωνία της ομάδας συμμετεχόντων. Χρησιμοποιώντας λοιπόν, ένα σύστημα k -out-of- n για την διανομή κλειδιών που θα μπορούσαν να χρησιμοποιηθούν για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων μέσα σε ένα δίκτυο DC. Με τη χρήση ενός συστήματος κρυπτογράφησης k -out-of- n (κατωφλίου), για παράδειγμα το κλειδί πρέπει να ανακατασκευαστεί από τουλάχιστον k συμμετέχοντες από n . Η διανομή κλειδιού είναι αναμφίβολα ένα κρίσιμο σημείο πολλών κρυπτογραφικών συστημάτων, προκειμένου να κρυπτογραφηθούν και να αποκρυπτογραφηθούν τα μηνύματα. Παράλληλα θα πρέπει να προστατεύεται το απόρρητο και η ακεραιότητα αυτών των κλειδιών αλλά και η ανωνυμία των συμμετεχόντων.

Η διανομή κλειδιών με DKG περιλαμβάνει την ασφαλή διανομή κρυπτογραφικών κλειδιών στους συμμετέχοντες. Ένα πρωτόκολλο δημιουργίας κατανεμημένου κλειδιού (DKG) χρησιμοποιείται συχνά για την παραγωγή των κρυπτογραφικών κλειδιών στην κρυπτογραφία κατωφλίου. Σε αυτό το σημείο, το DKG θα χρησιμοποιηθεί για τη δημιουργία και τη διανομή των κλειδιών που απαιτούνται τόσο για την κρυπτογράφηση κατωφλίου όσο και για τα δίκτυα DC. Με τη βοήθεια αυτού του συστήματος, ελαχιστοποιείται το μέγεθος με αποτέλεσμα να μειώνεται σημαντικά ο χρόνος από $O(n^2)$ σε $O(n \log n)$ [23], με n τον αριθμό των συμμετεχόντων. Πολλοί συμμετέχοντες μπορούν να δημιουργήσουν μαζί ένα κρυπτογραφικό κλειδί χωρίς κανένας από αυτούς να γνωρίζει το

πλήρες κλειδί. Αντίθετα, ο καθένας τους έχει ένα τμήμα του κλειδιού και απαιτείται ένας ορισμένος αριθμός παικτών (k από n) για να ανακατασκευαστεί ολόκληρο το κλειδί. Οι συμμετέχοντες πρέπει να έχουν εμπιστοσύνη στην εκτέλεση του πρωτοκόλλου δημιουργίας κλειδιού κατωφλίου και στην ασφάλεια της διανομής μεριδίου κλειδιού. Για να διευκολυνθεί η διανομή κλειδιών, τα μέρη μπορεί περιστασιακά να χρειαστεί να έχουν εμπιστοσύνη σε έναν αξιόπιστο αντιπρόσωπο ή αρχή. Αυτό συμβαίνει τις περισσότερες φορές όταν πρόκειται για διαμοιρασμό κοινών κλειδιών. Το κανάλι εδραίωσης των κλειδιών θα πρέπει να είναι ασφαλές όπως και το κανάλι επικοινωνίας. Ένας συγκεκριμένος αριθμός ατόμων, όπως προείπαμε, πρέπει να συνεργαστεί για να ξαναχτίσει ολόκληρο το κλειδί προτού μπορέσει να χρησιμοποιηθεί για κρυπτογράφηση ή αποκρυπτογράφηση. Αυτή η διαδικασία διασφαλίζει ότι κανένα άτομο δεν μπορεί να θέσει σε κίνδυνο το κλειδί από μόνο του ενώ παράλληλα διασφαλίζεται πως το μήνυμα παραμένει κρυφό.

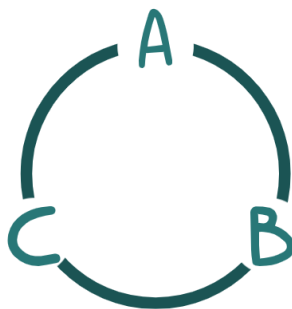
Οι συμμετέχοντες δημιουργούν επίσης κρυπτογραφικά κλειδιά για λειτουργίες DC-net. Αυτά τα κλειδιά διασφαλίζουν πως τα μηνύματα που ανταλλάσσονται εντός του δικτύου DC είναι ανώνυμα και δεν μπορούν να συνδεθούν με τους αποστολείς τους. Με αυτό τον τρόπο η ασφάλεια του κλειδιού και του μηνύματος δεν επηρεάζεται ακόμη και αν ένα υποσύνολο συμμετεχόντων διακυβεύεται. Οι συμμετέχοντες στο DC-net χρησιμοποιούν τα κλειδιά τους για να κρυπτογραφήσουν τα μηνύματα. Τα μηνύματα κρυπτογραφούνται περαιτέρω χρησιμοποιώντας τα κλειδιά κρυπτογράφησης κατωφλίου. Αυτή η διπλή κρυπτογράφηση παρέχει ένα πρόσθετο επίπεδο ασφάλειας και διασφαλίζει ότι μόνο πολύ συγκεκριμένες ομάδες συμμετεχόντων (k από n) μπορούν να αποκρυπτογραφήσουν και να έχουν πρόσβαση στα μηνύματα. Η κρυπτογράφηση διασφαλίζει ότι ακόμα κι αν κάποιος κακόβουλος παραβιάσει έναν ή ακόμη και περισσότερους συμμετέχοντες, δεν μπορεί να αποκρυπτογραφήσει τα μηνύματα. Με αυτόν τον τρόπο, διασφαλίζουμε πως είναι υπολογιστικά ανέφικτος ο προσδιορισμός του αποστολέα ενός συγκεκριμένου μηνύματος, διατηρώντας την ανωνυμία. Στη συνέχεια, τα μηνύματα αποστέλλονται μέσω του δικτύου DC. Οι ιδιότητες του DC-net καθιστούν δύσκολο τον προσδιορισμό του αποστολέα οποιουδήποτε μηνύματος, προσθέτοντας ένα επιπλέον επίπεδο απορρήτου.

Για την αποκρυπτογράφηση ενός μηνύματος, ένα όριο συμμετεχόντων (k από n) πρέπει να συνεργαστούν για την ανακατασκευή του κλειδιού αποκρυπτογράφησης. Αυτό επιτυγχάνεται χρησιμοποιώντας τα κοινόχρηστά τους κλειδιά, διασφαλίζοντας ότι κανένας μόνος συμμετέχων δεν μπορεί να αποκρυπτογραφήσει μηνύματα μόνος του, προσθέτοντας ένα επίπεδο ασφάλειας. Αφού ανακατασκευαστεί το κλειδί αποκρυπτογράφησης κατωφλίου, οι συμμετέχοντες μπορούν να το χρησιμοποιήσουν για να αποκρυπτογραφήσουν μηνύματα εντός του δικτύου DC, αποκαλύπτοντας το αρχικό περιεχόμενο διατηρώντας παράλληλα την ανωνυμία του αποστολέα.

Ο συνδυασμός κρυπτογραφίας κατωφλίου με δίκτυα DC μπορεί να προσφέρει ένα σύστημα όπου οι συμμετέχοντες μπορούν να επικοινωνούν ανώνυμα, διασφαλίζοντας παράλληλα ότι ένας ελάχιστος αριθμός συμμετεχόντων πρέπει να συνεργάζεται για πρόσβαση. Για ευαίσθητες πληροφορίες ή αποκρυπτογράφηση μηνυμάτων με έναν τέτοιο συνδυασμό επιτυγχάνεται τόσο η ασφαλή επικοινωνία (μέσω κρυπτογραφίας κατωφλίου) όσο και η ανωνυμία (μέσω δικτύων DC) σε ένα κατανεμημένο και συνεργατικό περιβάλλον. Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο σε σενάρια όπου τόσο το απόρρητο όσο και η ασφάλεια είναι κρίσιμα, όπως η ασφαλής ομαδική επικοινωνία ή τα συστήματα ψηφοφορίας

που διατηρούν το απόρρητο. Ωστόσο, η εφαρμογή ενός τέτοιου συστήματος είναι εξαιρετικά πολύπλοκη και η ανάπτυξη του στον πραγματικό κόσμο θα πρέπει να λάβει υπόψη διάφορα θέματα όπως η επεκτασιμότητα, η απόδοση, οι υπολογιστικοί πόροι.

2.4 Εφαρμογή τοπολογία δακτυλίου



Εικόνα 7: Τοπολογία δακτυλίου

Μία άλλη ιδέα με σκοπό τη μείωση της πολυπλοκότητας αλλά και την εξάλειψη των συγκρούσεων είναι η χρήση τοπολογίας δακτυλίου (ring topology). Με αυτή τη μέθοδο ο εκάστοτε κρυπτογράφος θα έχει την δυνατότητα να επικοινωνεί μόνο με τον δεξιά του. Επιπλέον σε δίκτυα με $n > 3$, δηλαδή με περισσότερους από 3 κρυπτογράφους το πρόβλημα απλοποιείται κατά πολύ καθώς δε θα απαιτείται η σύνδεση όλων των κόμβων και η δημιουργία τόσων κλειδιών. Σε μία πλήρη τοπολογία n κόμβων ο κάθε συμμετέχων θα έχει στην κατοχή του $n - 1$ κλειδιά και θα χρειαστεί να κάνει περαιτέρω πράξεις στο

στάδιο του υπολογισμού. Σε ένα δίκτυο με $n = 3$ θα χρειαστούμε 3 ρίψεις, δηλαδή 3 κοινόχρηστα κλειδιά, σε ένα δίκτυο με $n = 4$ θα χρειαστούμε 6 κλειδιά και αν $n = 5$ θα χρειαστούμε 10. Παρατηρούμε πως ο αριθμός των κλειδιών αυξάνεται απότομα. Πιο συγκεκριμένα εάν $n = \text{κόμβους/συμμετέχοντες}$ και $k = \text{κλειδιά}$ μπορούμε να παρατηρήσουμε την ταχύτητα με την οποία αυξάνεται ο αριθμός των κλειδιών.

n	k
2	1
3	4
4	6
5	10
6	15
7	21

Πίνακας 7: Αριθμός κόμβων και κλειδιών

Αντίθετα εάν η τοπολογία είναι ring, η πολυπλοκότητα μειώνεται ραγδαία καθώς ο αριθμός των κόμβων θα ισούται με τον αριθμό των κλειδιών. Επίσης ο κάθε συμμετέχων θα γνωρίζει 2 μονο κλειδιά αντίθετα με την πλήρη τοπολογία όπου θα γνωρίζει $n - 1$. Αντίστοιχα μειώνεται και το υπολογιστικό κόστος αλλά και οι ενδεχόμενες συγκρούσεις. Δυστυχώς ο αλγόριθμος γίνεται πιο ευάλωτος σε επιθέσεις, βέβαια εάν το πρωτόκολλο ακολουθηθεί κατά γράμμα δεν διακυβεύεται το απόρρητο κανενός.

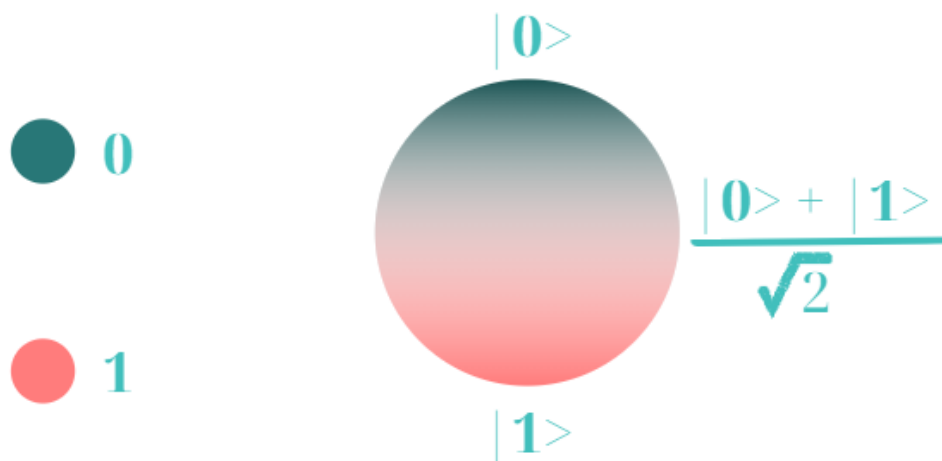
Κεφάλαιο 3^ο

3.1 Εισαγωγή στον κβαντικό κόσμο

Σε αυτό το σημείο θα εξετάσουμε μία ενδεχόμενη μετατροπή του αλγορίθμου DC σε κβαντικό επίπεδο. Αρχικά θα χρειαστεί να κάνουμε μία ιστορική αναδρομή με σκοπό να μάθουμε τι δουλειά έχει γίνει μέχρι στιγμής αλλά και να κατανοήσουμε κάποιες βασικές έννοιες του κβαντικού υπολογισμού. Για να συμβεί αυτό θα πρέπει να κατανοήσουμε κάποια πεδία της κβαντικής φυσικής. Η κβαντική φυσική, χρησιμοποιεί μια καινοτόμα θεωρία για να περιγράψει τη συμπεριφορά των σωμάτων σε πολύ μικρές κλίμακες. Αυτή η θεωρία αντικαθιστά την κλασική μηχανική του Νεύτωνα σε αυτό το επίπεδο.

Στην κβαντική φυσική, τα σωματίδια όπως τα ηλεκτρόνια και τα φωτόνια μπορούν να βρίσκονται σε κβαντικές καταστάσεις, οι οποίες περιγράφονται από κβαντικούς αριθμούς και συναρτήσεις κύματος. Αντίθετα από την κλασική φυσική σύμφωνα με την οποία η θέση αλλά και η ταχύτητα ενός σωματιδίου είναι ορισμένες. Τα σωματίδια λοιπόν, μπορούν να βρίσκονται ταυτόχρονα σε πολλές καταστάσεις, με αυτές τις καταστάσεις να αλληλεπιδρούν μεταξύ τους στο φαινόμενο της υπέρθεσης (superposition). Αυτό είναι μια βασική αρχή της κβαντικής μηχανικής. Στον κόσμο της κβαντικής φυσικής, κάτι που βρίσκεται σε κβαντική υπερθέση αντιπροσωπεύει ένα σύνολο καταστάσεων που είναι όλα παράλληλα υπαρκτά και όχι μόνο μία συγκεκριμένη κατάσταση. Αντίθετα στην κλασική μηχανική, αντικείμενα ή σωματίδια μπορούν να βρίσκονται σε μία συγκεκριμένη κατάσταση την οποία μπορούμε να περιγράψουμε με συγκεκριμένες τιμές που δεν αλλάζουν όπως ο τόπος, η ταχύτητα και η ενέργεια. Στην κβαντική φυσική, όμως, τα σωματίδια μπορούν να βρίσκονται σε υπερθέσεις, δηλαδή να έχουν ταυτόχρονα πολλές διαφορετικές καταστάσεις. Για παράδειγμα, ένα bit σε έναν κλασικό υπολογιστή μπορεί να είναι είτε 0 είτε 1, ενώ ένα bit σε έναν κβαντικό υπολογιστή μπορεί να βρίσκεται σε κατάσταση υπερθέσης όπου είναι ταυτόχρονα 0 και 1. Αυτό το φαινόμενο επιτρέπει στους κβαντικούς υπολογιστές να εκτελούν παράλληλη επεξεργασία πολλαπλών καταστάσεων ταυτόχρονα, προσφέροντας δυνατότητες υπολογισμού που είναι αδύνατο να πραγματοποιηθούν με χρήση κλασικών υπολογιστικών συστημάτων. Η ικανότητά τους να επεξεργάζονται ταυτόχρονα πολλές καταστάσεις, χρησιμοποιώντας την αρχή της υπέρθεσης. Αυτή τους η ικανότητά, δίνει την ταυτόχρονης επεξεργασίας πολλαπλών καταστάσεων, χρησιμοποιώντας την αρχή της υπέρθεσης. Αυτό τους καθιστά ιδιαίτερα ισχυρούς στον τομέα της επίλυσης προβλημάτων που είναι δύσκολα για τους κλασικούς υπολογιστές. Οι κβαντικοί υπολογιστές χρησιμοποιούν qubits αντί για τα κλασικά bits και μπορούν να εκτελούν παράλληλα πολλούς υπολογισμούς χάρη στην υπέρθεση, καθιστώντας τους πολύ ισχυρούς σε ορισμένες εφαρμογές. Η κβαντική υπερθέση αποτελεί βασικό στοιχείο της κβαντικής μηχανικής και επιτρέπει τη δημιουργία νέων και προηγμένων τεχνολογιών, όπως οι κβαντικοί υπολογιστές και η κβαντική κρυπτογραφία. Επίσης, έχουν την ιδιότητα της σύμπλεξης (entanglement), που επιτρέπει τη συσχέτιση τους με άλλα qubits, ακόμη και αν αυτά βρίσκονται σε μεγάλες αποστάσεις. Όπως βλέπουμε και στην παραπάνω εικόνα ένα κλασικό Bit (αριστερά) μπορεί

να πάρει την τιμή 1 ή 0. Αντίθετα ένα Qbit (δεξιά) μπορεί να πάρει την τιμή $|1\rangle$ ή $|0\rangle$ αλλά μπορεί να πάρει και οποιαδήποτε ενδιάμεση τιμή.



Εικόνα 8: Διαφορά μεταξύ bit, qbit

Οι ενδιάμεσες κβαντικές καταστάσεις αντιπροσωπεύουν κβαντικές καταστάσεις των σωμάτων που βρίσκονται μεταξύ των αρχικών και των τελικών καταστάσεων. Συχνά χρησιμοποιούνται για να περιγράψουν την εξέλιξη καθώς και την αλληλεπίδραση των σωμάτων κατά τη διάρκεια κβαντικών μεταβάσεων. Αυτές οι καταστάσεις αποτελούν ένα κρίσιμο πεδίο για την κατανόηση της επικοινωνίας αλλά και του συντονισμού σε κβαντικά συστήματα. Κατά τη διάρκεια μιας κβαντικής μετάβασης από μια αρχική στην τελική κατάσταση, το σύστημα περνά από διάφορες ενδιάμεσες καταστάσεις. Αυτές οι καταστάσεις επηρεάζουν την τελική κατάσταση και την πιθανότητα ενός συγκεκριμένου αποτελέσματος. Στον κβαντικό υπολογισμό, οι ενδιάμεσες καταστάσεις χρησιμοποιούνται για να αναπαραστήσουν τα κβαντικά κυκλώματα και να εκτελέσουν κβαντικούς αλγορίθμους. Οι μεταβάσεις μεταξύ αυτών των καταστάσεων αντιπροσωπεύουν την εκτέλεση υπολογισμών ενώ παράλληλα περιέχουν πολλές πληροφορίες σχετικά με την εξέλιξη του συστήματος. Η κατανόηση αυτών των καταστάσεων είναι σημαντική για την πρόβλεψη της συμπεριφοράς του κβαντικού συστήματος.

Σύμφωνα με την κβαντική φυσική, είναι αδύνατο να γνωρίζουμε ταυτόχρονα με ακρίβεια τη θέση και την ταχύτητα ενός σωματιδίου σε κβαντικό επίπεδο. Πιο αναλυτικά πρόκειται για την αβεβαιότητα Heisenberg γνωστή και ως αρχή της αβεβαιότητας του Heisenberg. Αποτελεί ένα βασικό χαρακτηριστικό της κβαντικής μηχανικής και αναφέρεται στην αδυναμία να μετρήσουμε ταυτόχρονα με απόλυτη ακρίβεια δύο συζευγμένες μεταβλητές του κβαντικού συστήματος, όπως η θέση και η ταχύτητα ενός σωματιδίου. Αυτό το φαινόμενο προτάθηκε από τον Γερμανό φυσικό Werner Heisenberg το 1927 και αποτελεί μία από τις βασικές αρχές της κβαντικής μηχανικής [25]. Η ακρίβεια με την οποία μπορούμε να μετρήσουμε τη θέση ενός σωματιδίου και την ορμή του (συνήθως ταχύτητα) είναι περιορισμένη. Πιο συγκεκριμένα, αν προσπαθήσουμε να μετρήσουμε τη θέση ενός σωματιδίου με αυξημένη ακρίβεια, τότε η αβεβαιότητα στη μέτρηση της ορμής του

αυξάνεται, και αν προσπαθήσουμε να μετρήσουμε την ορμή με μεγαλύτερη ακρίβεια, τότε η αβεβαιότητα στη μέτρηση της θέσης του αυξάνεται. Αυτό δεν είναι απλώς έλλειψη τεχνολογικής ακρίβειας, αλλά αποτελεί μια φυσική περιοριστική αρχή που αφορά την φύση της πραγματικότητας στην κβαντική κλίμακα. Με άλλα λόγια όσο προσπαθούμε να μετρήσουμε την θέση μιας μεταβλητής χάνουμε την ορμή της και αντίστροφα. Η αρχή της αβεβαιότητας του Heisenberg εκφράζεται μαθηματικά μέσω της ανισότητας Heisenberg, η οποία περιορίζει τη ταυτόχρονη μέτρηση της θέσης και της ορμής ενός σωματιδίου. Αυτή η αρχή έχει σημαντικές επιπτώσεις στην κβαντική μηχανική και αντικατοπτρίζει την αντίληψη ότι η φύση στην κβαντική κλίμακα είναι θεμελιωδώς πιθανοτική και συνάμα αβέβαιη.

Η κβαντική ασφάλεια, ιδιαίτερα στο πλαίσιο της κρυπτογραφίας και της προστασίας δεδομένων, εμφανίστηκε ως απάντηση στην πιθανή απειλή που θέτουν οι κβαντικοί υπολογιστές, με τις τρέχουσες μεθόδους κρυπτογράφησης. Η παραδοσιακή κρυπτογράφηση βασίζεται σε μαθηματικά προβλήματα που είναι δύσκολο να επιλυθούν από τους κλασικούς υπολογιστές, αποτελώντας την ασφαλή επικοινωνία αλλά και την αποθήκευση δεδομένων. Ωστόσο, οι κβαντικοί υπολογιστές έχουν τη δυνατότητα να λύσουν αυτά τα προβλήματα πολύ πιο γρήγορα χρησιμοποιώντας αλγόριθμους όπως ο αλγόριθμος του Shor, ο οποίος θα μπορούσε να καταστήσει ευάλωτες τις τρέχουσες μεθόδους κρυπτογράφησης. Η ιδέα της κβαντικής-ανθεκτικής (quantum-resistant) ή της κβαντικής ασφαλούς κρυπτογραφίας άρχισε να κερδίζει την προσοχή στα τέλη του 20ου αιώνα, καθώς οι ερευνητές άρχισαν να εξερευνούν τις επιπτώσεις του κβαντικού υπολογισμού για την ασφάλεια των πληροφοριών. Οι αλγόριθμοι που αντιστέκονται στις προσπάθειες των κβαντικών υπολογιστών να σπάσουν τους κώδικες αναφέρονται ως κβαντικοί ανθεκτικοί. Επιστήμονες όπως ο Peter Shor μεταξύ άλλων έθεσαν τις βάσεις αποδεικνύοντας ότι οι κβαντικοί υπολογιστές θα μπορούσαν θεωρητικά να σπάσουν τα ευρέως χρησιμοποιούμενα σχήματα κρυπτογράφησης. Έτσι, οι προσπάθειες για την ανάπτυξη μεθόδων κρυπτογράφησης ανθεκτικές στις κβαντικές επιθέσεις άρχισαν να αποκτούν δυναμική. Οι κρυπτογράφοι ξεκίνησαν να εξερευνούν αλγόριθμους ανθεκτικούς στα κβαντικά συστήματα, όπως κρυπτογραφία βασισμένη σε πλέγμα, κρυπτογραφία βασισμένη σε κατακερματισμό, κρυπτογραφία με βάση κώδικα, που πιστεύεται ότι είναι ασφαλείς έναντι επιθέσεων τόσο από κλασικούς όσο και από κβαντικούς υπολογιστές. Πολλές εταιρείες αλλά και ερευνητικά ιδρύματα από τότε επενδύουν στην ανάπτυξη κρυπτογραφικών πρωτοκόλλων ανθεκτικών σε κβαντικά για να εξασφαλίσουν την ασφάλεια των δεδομένων και των επικοινωνιών σε ένα μέλλον όπου οι κβαντικοί υπολογιστές ενδέχεται να είναι σε θέση να παραβιάζουν τα τρέχοντα πρότυπα κρυπτογράφησης. Όπως προείπαμε ένα κβαντικό υπολογιστικό σύστημα υπολογίζει πολύ πιο γρήγορα και αποδοτικά συγκριτικά με έναν συμβατό υπολογιστή. Έτσι τα τρένωντα ασφαλές συστήματα σε μία κβαντική συνθήκη υπόκεινται σε διάφορους κινδύνους. Η αναζήτηση για την κβαντική ασφάλεια βρίσκεται σε εξέλιξη, που περιλαμβάνει τόσο τη θεωρητική έρευνα όσο και την πρακτική εφαρμογή για να διασφαλιστεί ότι τα δεδομένα παραμένουν ασφαλή στην εποχή του κβαντικού υπολογισμού. Αυτά τα στάδια είναι αναγκαία για να διασφαλίσουμε την διατήρηση της ανωνυμίας αλλά και της ιδιωτικότητας.

Οι φυσικοί Charles H. Bennett [26] και Stephen Wiesner πρότειναν για πρώτη φορά την κβαντική κρυπτογραφία [27], ένα υποπεδίο της επιστήμης της κβαντικής πληροφορίας. Και κάπως έτσι ξεκίνησε ένα κύμα πρώιμων ιδεών για τη διανομή κβαντικών κλειδιών, μια

τεχνική που κρυπτογραφεί τις επικοινωνίες χρησιμοποιώντας την κβαντική μηχανική. Στη συνέχεια, στις δεκαετίες του 1980 και του 1990, επιστήμονες όπως ο Gilles Brassard, ο Artur Ekert, ο Charles Bennett μεταξύ άλλων έκαναν σημαντικές προόδους στη θεωρητική βάση και τις πραγματικές χρήσεις της κβαντικής κρυπτογραφίας. Τα κβαντικά ασφαλή πρωτόκολλα επικοινωνίας κατέστησαν δυνατά χάρη σε αυτά τα θεμελιώδη επιτεύγματα. Ο φυσικός Stephen Wiesner πρότεινε για πρώτη φορά την κβαντική κρυπτογραφία, ένα υποπεδίο της επιστήμης της κβαντικής πληροφορίας, στις αρχές της δεκαετίας του 1980. Αλλά η έννοια της ασφαλούς επικοινωνίας μέσω της κβαντικής μηχανικής ξεκίνησε στην πραγματικότητα τη δεκαετία του 1970, όταν ο φυσικός Stephen L. Braunstein και άλλοι ξεχωριστά πρότειναν τη χρήση κβαντικών καταστάσεων στην επικοινωνία.

Ο Wiesner δημιούργησε την ιδέα του κβαντικού χρήματος στα τέλη της δεκαετίας του 1970-1980. Αυτός ο τύπος κβαντικών πληροφοριών βοήθησε στην ανάπτυξη της κβαντικής κρυπτογραφίας. Η έννοια της διανομής κβαντικού κλειδιού (QKD) και η ιδέα της αξιοποίησης των κβαντικών χαρακτηριστικών για τη δημιουργία ασφαλούς επικοινωνίας έγιναν δυνατές από το έργο του Wiesner. Στη δεκαετία του 1980, ο David Deutsch και ο Richard Jozsa έκαναν επίσης σημαντικές θεωρητικές προόδους στον τομέα της επιστήμης της κβαντικής πληροφορίας βελτιώνοντας την κατανόησή μας για την κβαντική επεξεργασία και τους κβαντικούς αλγόριθμους. Το 1984, ο David Deutsch πρότεινε την έννοια του κβαντικού υπολογιστή. Ο φυσικός Τσαρλς Μπένετ και οι συνεργάτες του παρουσίασαν την ιδέα της διανομής κβαντικών κλειδιών το 1989, θέτοντας τα θεμέλια για την κβαντική κρυπτογραφία. Ακόμη και εκείνη την εποχή κατανοούσαν την συμμετοχή της ασφαλούς επικοινωνίας και πολλοί μελετητές αφιερώθηκαν σε αυτό για την αποφυγή κινδύνων. Αυτές οι πρώτες ανακαλύψεις άνοιξαν το δρόμο για την ανάπτυξη της διανομής κβαντικών κλειδιών και της κβαντικής κρυπτογραφίας ως ενεργά ερευνητικά πεδία, με άλλους ερευνητές να συνεισφέρουν σημαντικά στο θέμα με την πάροδο του χρόνου.

Η κβαντική ασφάλεια, είναι η χρήση κβαντικών υπολογιστών για την υπεράσπιση δεδομένων από επιτιθέμενους. Οι συμβατικές τεχνικές κρυπτογράφησης βασίζονται στην επίλυση μαθηματικών γρίφων. Δηλαδή, οι παραδοσιακές μέθοδοι κρυπτογράφησης βασίζονται σε μαθηματικά προβλήματα που είναι δύσκολο να επιλύσουν οι κλασικοί υπολογιστές. Ωστόσο, οι τρέχουσες τεχνικές κρυπτογράφησης κινδυνεύουν επειδή οι κβαντικοί υπολογιστές μπορεί να είναι σε θέση να αντιμετωπίσουν αυτά τα ζητήματα πολύ πιο γρήγορα. Για την ανάπτυξη τεχνικών κρυπτογράφησης που αποτρέπουν τις επιθέσεις από κβαντικούς υπολογιστές, η κβαντική ασφάλεια βασίζεται σε ιδέες από την κβαντική φυσική. Η διανομή κβαντικού κλειδιού (QKD) αποτελεί μία από αυτές τις τεχνικές. Με τη χρήση της κβαντικής φυσικής, το QKD δημιουργεί ένα ασφαλές κλειδί που μοιράζεται μόνο μεταξύ δύο μερών. Προκειμένου να διασφαλιστεί ότι ευαίσθητα δεδομένα και πληροφορίες είναι ασφαλή ακόμη και στην εποχή των ισχυρών κβαντικών υπολογιστών, δημιουργούνται πρόσθετοι αλγόριθμοι ανθεκτικοί σε κβαντικό υπολογισμό, έτσι ώστε να αντικατασταθούν τα υπάρχοντα κρυπτογραφικά πρότυπα. Για να συμβαδίσουν με τις ταχέως αναπτυσσόμενες δυνατότητες του κβαντικού υπολογισμού, επιστήμονες και ερευνητές από όλο τον κόσμο προσπαθούν συνεχώς να προωθήσουν μέτρα κβαντικής ασφάλειας.

Σε κάθε περίπτωση, πτυχές της κβαντικής φυσικής αποκαλύπτονται, πέρα από τα όρια της συμβατικής φυσικής και της κοινής λογικής. Η διαπλοκή/σύμπλεξη (entanglement) είναι ένα από αυτά τα απίστευτα περιστατικά που όχι μόνο μας μπερδεύει, αλλά

παρουσιάζει και εξαιρετικές ευκαιρίες για να ολοκληρώσουμε δραστηριότητες που είναι περίπλοκες ή ίσως ανέφικτες στον παραδοσιακό κόσμο. Τα σύνθετα κβαντικά συστήματα, τα οποία αποτελούνται συνήθως από δύο ή περισσότερα υποσυστήματα που είναι συχνά διασκορπισμένα, είναι εκεί όπου προκύπτει διαπλοκή. Όταν η κατάσταση ενός σύνθετου συστήματος δεν μπορεί να εκφραστεί ως το απλό γινόμενο δύο ή περισσότερων καταστάσεων υποσυστήματος, μαθηματικά λέγεται ότι είναι ένα σύστημα συμπλοκής. Το γεγονός ότι όταν μετράται ένα qubit ενός συμπλεγμένου ζεύγους ή πλειάδας, το άλλο qubit συμπτύσσεται αμέσως στην αντίστοιχη κατάσταση βάσης είναι ένα από τα εκπληκτικά πλεονεκτήματα της κβαντικής σύμπλεξης. Αντίστοιχα ισχύει και αν αυτό το qubit είναι συνδεδεμένο με περισσότερα qubits και αυτό αποτελεί έναν από τους λόγους που η κβαντική σύμπλεξη είναι χρήσιμη για διάφορα πρωτόκολλα κρυπτογράφησης κβαντικής, όπως μεταξύ άλλων η διανομή κλειδιού και ο κοινός κρυπτογραφικός καταμερισμός.

3.2 Εντροπία

Για να μπορέσουμε να προχωρήσουμε παρακάτω είναι σημαντικό να εξηγήσουμε τι είναι η εντροπία. Με την ευρύτερη έννοια, η εντροπία είναι μια βασική έννοια η οποία εντάσσεται σε πολλούς κλάδους, συμπεριλαμβανομένης της θεωρίας της πληροφορίας, της φυσικής, ακόμη και των κοινωνικών επιστημών. Η εντροπία είναι ένα μέτρο της αταξίας ή της μη προβλεψιμότητας ενός συστήματος. Στη φυσική, εκφράζει το επίπεδο αταξίας ή ασάφειας σε ένα σύστημα, ειδικά στη θερμοδυναμική. Συχνά συνδέεται με τον δεύτερο κανόνα της θερμοδυναμικής, ο οποίος δηλώνει ότι όταν η εντροπία αυξάνεται σε ένα κλειστό σύστημα με την πάροδο του χρόνου, η διαταραχή ή η τυχαιότητα τείνει επίσης να αυξάνεται. Αυτή η ιδέα προέκυψε ως μέσο κατανόησης της πορείας των φυσικών διεργασιών, τονίζοντας την τάση των συστημάτων να γίνονται πιο άτακτα.

Η εντροπία είναι ένας όρος που χρησιμοποιείται στη θεωρία πληροφοριών για να περιγράψει τη μέση ποσότητα πληροφοριών που περιλαμβάνεται σε ένα μήνυμα ή σύνολο δεδομένων. Η υψηλότερη εντροπία υποδηλώνει μεγαλύτερη απρόβλεπτη ικανότητα. Ποσοτικοποιεί την αβεβαιότητα ή το απρόβλεπτο των πληροφοριών. Για παράδειγμα, μια σειρά τυχαίων ακεραίων αριθμών έχει περισσότερη εντροπία από μια σειρά που έχει ένα ξεχωριστό μοτίβο. Η εντροπία είναι απαραίτητη στην κρυπτογραφία για την παροχή ασφαλών κλειδιών κρυπτογράφησης. Η ισχυρή κρυπτογράφηση που είναι διαπεράσιμη από επιθέσεις απαιτεί μεγάλο βαθμό απρόβλεπτου και τυχαίου, που είναι αυτό που προορίζεται να επιτευχθεί μέσω της εντροπίας. Ο Boltzmann έδωσε μια λειτουργική μορφή της εντροπίας και την εξέφρασε ως: $S = k_b \ln \Omega$ [28]. Πλέον γνωστή και ως Boltzmann entropy, όπου Ω είναι ο αριθμός των μικροκαταστάσεων που είναι συμβατές με τα παρατηρήσιμα χαρακτηριστικά της μακροκατάστασης ή το στατιστικό βάρος, k είναι μία σταθερά Boltzmann. Προκειμένου να εξηγήσει τις παρατηρήσιμες ιδιότητες του συστήματος, ο Boltzmann πρόσθεσε πως κάθε κατάσταση είναι εξίσου πιθανό να συμβεί και πως μεγιστοποιείται στην ισορροπία. Ο δεύτερος νόμος της θερμοδυναμικής, που λέει

ότι η εντροπία τείνει να αυξάνεται με το χρόνο σε ένα απομονωμένο σύστημα, απαιτεί γνώση αυτής της ιδέας. Υποδηλώνει ότι τα συστήματα εγγενώς πηγαίνουν προς πιο διαταραγμένες ή τυχαίες καταστάσεις, ή σε καταστάσεις με αυξημένη εντροπία, που έχει ως αποτέλεσμα μια κατεύθυνση προς στις φυσικές διαδικασίες.

Ο Shannon έδωσε την δική του μορφή για την εντροπία καταγράφει το απρόβλεπτο ή τη διαταραχή μέσα σε ένα σύστημα. Μαθηματικά την εξέφρασε ως:

$$H(X) = - \sum_{x_i} p(X = x_i) \log_2 p(X = x_i), \text{ όπου το } H(X) \text{ αντιπροσωπεύει την εντροπία του}$$

συστήματος ενώ το $p(X = x_i)$ είναι η πιθανότητά του και το $\log_2$ υποδηλώνει την βάση του λογαρίθμου σε 2 αποδίδοντας την εντροπία σε bit. Όσο μικρότερη είναι η εντροπία τόσο μεγαλύτερη προβλεψιμότητα ή τάξη στα δεδομένα, ενώ υψηλότερα επίπεδα εντροπίας σημαίνει μεγαλύτερη αβεβαιότητα ή χάος. Όταν ένα σύστημα ή ένα σύνολο δεδομένων έχει χαμηλή εντροπία, υποδηλώνει ότι ορισμένα αποτελέσματα είναι πιο πιθανά από κάποια άλλα, γεγονός που μειώνει την αβεβαιότητα που το περιβάλλει. Ο Landauer υποστήριξε πως όταν οι πληροφορίες διαγράφονται, δημιουργείται μια αναπόφευκτη αύξηση της εντροπίας στο περιβάλλον. Με αφορμή αυτό ο Bennett συνδέει αυτή τη διαδικασία διαγραφής με τους θεμελιώδεις νόμους της θερμοδυναμικής, συγκεκριμένα τον δεύτερο νόμο, ο οποίος υπογορεύει ότι η εντροπία τείνει να αυξάνεται σε ένα κλειστό σύστημα. Εξέτασε ένα πείραμα το οποίο περιλάμβανε ένα σύστημα με δύο διακριτές καταστάσεις που αντιπροσωπεύουν τις διαγραμμένες και μη διαγραμμένες πληροφορίες. Έδειξε ότι μια λογικά μη αναστρέψιμη λειτουργία όπως η διαγραφή πληροφοριών, μπορεί να πραγματοποιηθεί μόνο με μια θερμοδυναμικά μη αναστρέψιμη διαδικασία που αυξάνει την εντροπία. Τέλος, αφού το $S = k_b \ln 2H$ και $\Delta H = -1$ ισχύει:

$$\Delta S - \frac{Q}{T} \geq 0$$

$$- k_b \ln 2 H - \frac{Q}{T} \geq 0$$

$$- Q \geq k_b T \ln 2$$

Όλα αυτά όμως ισχύουν στην μηχανική και στην θεωρία της πληροφορίας. Τι συμβαίνει όμως όταν αυτές οι καταστάσεις είναι κβαντικές; Σύμφωνα με τον Schrodinger $i\hbar \frac{\partial \psi}{\partial t} = H\psi$, με H Hamiltonian του συστήματος, δηλαδή οποιοδήποτε διάνυσμα στο χώρο Hilbert που ενεργεί Hamiltonian. $|\psi(t)\rangle = U(t)|\psi(0)\rangle$ και μέσω αυτού δημιουργείται $\frac{\partial U}{\partial t} = \frac{-i}{\hbar} H U \Rightarrow U(0) = I$ και $\frac{\partial (U^\dagger U)}{\partial t} = 0 \Rightarrow U(t)^\dagger U(t) = I$ το οποίο ορίζει την ενότητα. Επομένως, όλη η εξέλιξη στην κβαντική μηχανική είναι μοναδιαία, άρα ο ορισμός της ενότητας. Επομένως, όλη η εξέλιξη στην κβαντική μηχανική είναι μοναδιαία [28]. Ο περιορισμός της εντροπίας μας επιτρέπει να θέσουμε όρια στο πόση πληροφορία μπορούν να λάβουν μετρήσεις από μια πηγή κβαντικής φύσης.

3.3 EPR, GHZ

Το ζεύγος Einstein-Podolsky-Rosen (EPR), η πιο βασική μέγιστη εμπλεκόμενη κατάσταση δύο qubit, αναφέρεται συχνά ως bell states [40]. Ένα ζεύγος EPR είναι ένα ζεύγος qubits που βρίσκονται σε μια μέγιστα μπλεγμένη κατάσταση, είναι ένα ζεύγος δύο σωματιδίων που έχουν αλληλεπίδραση μεταξύ τους. Αποτελεί μια ειδική κατάσταση που οι ιδιότητες των σωματιδίων εξαρτώνται η μία από την άλλη, ακόμη και αν βρίσκονται σε μεγάλη απόσταση. Τα ζεύγη αυτά αποτελούν σημαντικό εφόδιο για την επίτευξη της κβαντικής επικοινωνίας καθώς και του κβαντικού υπολογισμού, όπως για παράδειγμα η κβαντική τηλεμεταφορά. Αυτό σημαίνει ότι η μέτρηση ενός qubit επηρεάζει άμεσα την κατάσταση του άλλου, ακόμη και αν βρίσκονται σε μεγάλη απόσταση όπως προαναφέρθηκε. Τα ζεύγη κοινών EPR επηρεάζονται μεταξύ τους και αυτό το φαινόμενο οδηγεί στην κβαντική συνδεσιμότητα η οποία αποτελεί μια από τις πιο παράξενες και ενδιαφέρουσες ιδιότητες της κβαντικής μηχανικής. Το ζεύγος EPR πήρε το όνομά του από το παράδοξο EPR (Einstein-Podolsky-Rosen), ένα πείραμα σκέψης που διατύπωσαν οι Αϊνστάιν, Ποντόλσκι και Ρόζεν το 1935 [41].

Το πείραμα αυτό επιχειρεί να δείξει ότι η κβαντική μηχανική δεν είναι αποτελεσματική, καθώς δεν παρέχει μια πλήρη περιγραφή της πραγματικότητας. Ένα ζεύγος σωματιδίων, παράγονται σε ένα κοινό σημείο και στη συνέχεια διαχωρίζονται σε μεγάλες αποστάσεις. Σύμφωνα με την κβαντική μηχανική, τα σωματίδια αυτά παραμένουν συνδεδεμένα, ακόμα και μετά το διαχωρισμό τους. Έτσι, η μέτρηση μιας ιδιότητας ενός σωματιδίου έχει άμεσο αντίκτυπο στην ιδιότητα του άλλου σωματιδίου, ανεξάρτητα από την απόσταση που τα χωρίζει. Στην ουσία, τα σωματίδια είναι συνδεδεμένα και η μέτρηση μιας ιδιότητας ενός σωματιδίου καθορίζει την ιδιότητα του άλλου σωματιδίου. Σύμφωνα με το παράδοξο EPR, η κβαντική συνδεσιμότητα οδηγεί σε μη τοπικές συσχετίσεις μεταξύ των μετρήσεων, που φαίνονται να παραβιάζουν την αρχή της τοπικότητας (δύο συμβάντα σε απομακρυσμένα μέρη δεν μπορούν να επηρεάσουν το ένα το άλλο άμεσα, αλλά μόνο μέσω μιας μετρήσιμης αλληλεπίδρασης) και τη θεωρία της σχετικότητας ενώ παράλληλα δεν επιτρέπει τη μεταφορά πληροφορίας με υπερφωτεινή ταχύτητα, καθώς η μέτρηση ενός qubit είναι τυχαία και απρόβλεπτη. Αποτελεί μια αναγκαία προϋπόθεση για την υλοποίηση των κβαντικών υπολογιστών, των κβαντικών κρυπτογραφικών πρωτοκόλλων καθώς και των κβαντικών τηλεμετρήσεων. Το παράδοξο EPR είναι ένα σημαντικό πείραμα σκέψης που έχει ασκήσει μεγάλη επιρροή στην ανάπτυξη της φυσικής. Το αποτέλεσμα του πειράματος εξακολουθεί να αποτελεί αντικείμενο συζήτησης και έρευνας.

Το Greenberger-Horne-Zeilinger (GHZ) είναι ένα παράδοξο που χρησιμοποιείται για τη δημιουργία κβαντικών καταστάσεων που είναι διεμπλεγμένες. Συγκεκριμένα, οι κβαντικές καταστάσεις που παράγονται από το πρωτόκολλο GHZ είναι τέτοιες ώστε τα qubits που τις αποτελούν είναι διεμπλεγμένα μεταξύ τους. Αυτό σημαίνει ότι η κατάσταση του ενός qubit επηρεάζει την κατάσταση των υπόλοιπων. Συγκεκριμένα, το πρωτόκολλο GHZ μπορεί να χρησιμοποιηθεί για τη δημιουργία κρυπτογραφημένων μηνυμάτων μεταξύ τριών ή περισσότερων συστημάτων qubits. Η χρησιμότητα του GHZ στην κβαντική κρυπτογράφηση έγκειται στο γεγονός ότι μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα κοινό μυστικό μεταξύ δύο ή περισσότερων ατόμων. Αυτό το κοινό μυστικό μπορεί στη συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση μηνυμάτων ή άλλων πληροφοριών.

Αυτό το παράδοξο συγκριτικά με τη μη τοπικότητα του Bell (Bell's nonlocality) διακατέχεται από κβαντική μη τοπικότητα (quantum nonlocality), γνωστή ως μη τοπικότητα GHZ. Το παράδοξο GHZ έχει πολλές χρήσεις, συμπεριλαμβανομένων κβαντικών πρωτοκόλλων που μειώνουν την πολυπλοκότητα επικοινωνίας [42]. Ίσως, η πιο διαδεδομένη μορφή μέγιστης εμπλοκής που βρίσκεται σε σύνθετα συστήματα n qubits, όπου $n \geq 3$, είναι η κατάσταση $|GHZ_n\rangle$. Σε μία τέτοια περίπτωση, ένα σύνθετο κβαντικό σύστημα αποτελείται από n ξεχωριστά qubits, όπου κάθε υποσύστημα είναι μόνο ένα qubit. Τα συμπλεγμένα qubits μπορούν κάλλιστα να διαχωριστούν χωρικά, κάτι που οδηγεί σε ενδιαφέρουσες δυνατότητες, όπως η κβαντική τηλεμεταφορά μεταξύ άλλων. Το παράδοξο GHZ είναι σημαντικό για την κβαντική κρυπτογραφία και την κβαντική επικοινωνία.

3.4 Κβαντικά πρωτόκολλα του DCP

Ο Boykin το 2002, πρότεινε ένα κβαντικό πρωτόκολλο στο οποίο οι συμμετέχοντες διανέμουν ζεύγη κοινών EPR, τα οποία στη συνέχεια χρησιμοποιούν για να λάβουν bits κλειδιών [28]. Ένα ζεύγος EPR είναι ένα ζεύγος qubits που βρίσκονται σε μια μέγιστα μπλεγμένη κατάσταση. Τα ζεύγη αυτά βρίσκονται αποτελούν σημαντικό εφόδιο για την επίτευξη της κβαντικής επικοινωνίας καθώς και του κβαντικού υπολογισμού, όπως για παράδειγμα η κβαντική τηλεμεταφορά όπως αναλύσαμε προηγουμένως. Το σύστημα του Boykin, επιτρέπει την ανώνυμη μετάδοση συμβατικών πληροφοριών βασισμένο στην κβαντική τηλεμεταφορά. Σε περίπτωση θορύβου ή επιθέσεων κβαντικού καναλιού, το πρωτόκολλο αυτό είναι ασφαλές. Ένας χρήστης θα στείλει μισή κατάσταση Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Κάθε μέλος ελέγχει αυτά τα δύο bits, Αν τα υπολογίσει θα πρέπει να καταμετρηθεί στην βάση x , αλλιώς εκτελεί μια μέτρηση Bell στα δύο bit. Το πρωτόκολλο που πρότεινε ο Boykin αποτελεί το πρώτο πρωτόκολλο κβαντικής ασφάλειας καταφέρνει να διαχειριστεί περισσότερους από δύο συμμετέχοντες.

Μετέπειτα, οι Christandl και Wehner δημιούργησαν ένα νέο πρωτόκολλο για την ανώνυμη διανομή qbits [29]. Δεδομένου ότι το μόνο που χρειάζεται για το ανώνυμο πρωτόκολλο αποστολής qubit είναι να ανακτήσει ο παραλήπτης το απεσταλμένο qubit, δεν παρέχει ένα παράδειγμα γενικού κβαντικού ασφαλούς υπολογισμού πολλαπλών μερών. Οι υπόλοιποι παίκτες δεν μοιράζονται αυτή την κατάσταση και ο παραλήπτης της θα οφείλει να παραμείνει κρυφός. Αντίθετα με το κλασικό πρωτόκολλο, δεν απαιτείται όλοι οι ειλικρινείς παίκτες να έχουν στην κατοχή τους το ίδιο qubit στο τέλος, καθώς κάτι τέτοιο θα ερχόταν σε σύγκρουση με την ιδιότητα της μη κλωνοποίησης των κβαντικών καταστάσεων. Το πρωτόκολλο αυτό εστιάζει στη χρήση EPR με σκοπό να σταλεί ένα κβαντικό νόμισμα $|\varphi\rangle$ μέσω τηλεμεταφοράς.

Λίγα χρόνια αργότερα οι Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, S'ébastien Gambs1 και Alain Tapp έδωσαν την δική τους εκδοχή [30]. Σύμφωνα με αυτή η αποστολέας μπορεί να στείλει ένα βαντικό μήνυμα με πλήρη ανωνυμία ακόμη και αν κάποιοι από τους συμμετέχοντες είναι 'διεφθαρμένοι', όπως οι ίδιοι τονίζουν. Εισάγουν την

έννοια της αποτυχημένης-ασφαλούς τηλεμεταφοράς (fail-safe teleportation), όπου σε περίπτωση της κβαντικής τηλεμεταφοράς, ένα σύστημα που είναι "fail-safe" ακόμη και αν προκύψουν σφάλματα ή διαταραχές κατά τη μετάδοση της κβαντικής κατάστασης, η πληροφορία θα φτάσει στον προορισμό της με τη μεγαλύτερη δυνατή ακρίβεια και ασφάλεια. Μετέπειτα, οι Ronghua Shi, Qian Su, Ying Guo και Moon Ho Lee παρουσίασαν μέθοδο για την υλοποίηση κβαντικής ανώνυμης επικοινωνίας σε ένα μοντέλο δημόσιου δέκτη που χρησιμοποιεί το χαρακτηριστικό ανωνυμίας των DC-Nets και των μη μέγιστα (non-maximally) κβαντικών καναλιών [32]. Το QSDC ενός μη μεγιστου συνδεδεμένου καναλιού χρησιμοποιείται για αξιόπιστη μεταφορά κβαντικών πληροφοριών αλλά και για τους τυχαίους αριθμούς που μπορούν να αξιοποιηθούν σε κάποιο ανώνυμο πρωτόκολλο ασφάλειας. Ένα μόνο ζεύγος qubit που δεν είναι το μέγιστο μπορεί να επικοινωνήσει δύο bit πληροφοριών: το bit μηνύματος μπορεί να εκτελέσει τη μέθοδο ανακοίνωσης και το τυχαίο bit μπορεί να αντικαταστήσει τη διαδικασία ρίψης νομίσματος στην συγκεκριμένη περίπτωση. Οι Q Wang, K Zhang ανάλυσαν τα κενά αλλά και πρότειναν κάποιες αλλαγές στα παραπάνω πρωτόκολλα. Τόνισαν την περίπτωση κάποιου κακόβουλου μέλους εξηγώντας πως κάτι τέτοιο θέτει σε κίνδυνο την ανωνυμία του αποστολέα [34].

Το 2015 οι Ramij Rahaman και Guruprasad Kar παρουσίασαν δύο κβαντικά πρωτόκολλα για το πρόβλημα των Dining Cryptographers καθώς και για το πρόβλημα Ανώνυμου βέτο (AV). Αυτά τα πρωτόκολλα βασίζονται στο παράδοξο GHZ και στις ιδιότητες της συσχέτισης GHZ. Στο πρόβλημα των κρυπτογράφων που δειπνούν, με $n \leq 3$ μπορούν να εντοπιστούν πολλαπλές πληρωμές. Τέλος γενίκευσαν το πρόβλημα για $n > 3$, δηλαδή για περισσότερους από 3 συμμετέχοντες, με σκοπό την εύρεση μιας απλής λύσης στο πρόβλημα του ανώνυμου βέτο. Απαραίτητη προϋπόθεση αποτελεί, ο λογαριασμός να έχει πληρωθεί μόνο μία φορά [35]. Αργότερα, οι Alley Hameedi, Breno Marques, Sadiq Muhammad, Marcin Wiesniak, Mohamed Bourennane πρότειναν μία νέα κβαντική λύση σε αυτό το πρόβλημα με τη χρήση ενός μονόδρομου διαδοχικού πρωτοκόλλου (one-way sequential protocol) καθώς και την επέκταση στο πρόβλημα του ανώνυμου βέτο. Η χαρακτηριστική ιδιότητα του πρωτοκόλλου είναι ότι βασίζεται σε ένα μόνο qbit, με χρήση καταστάσεων GHZ λόγω της υψηλής συμμετρίας. Στην ουσία σε ένα πρωτόκολλο με $n = 3$, κάθε μέρος εκτελεί μια τοπική μοναδιαία λειτουργία στην κοινή κατάσταση GHZ σε περίπτωση πληρωμής. Για n ψηφοφόρους, το πρωτόκολλο θα απαιτούσε χώρο Hilbert διαστάσεων $(n + 1)^n$ [36].

Έπειτα, οι Jan Bouda και Josef Sprojcar παρουσίασαν ένα πρωτόκολλο για την ανώνυμη κοινή χρήση κβαντικών δεδομένων [37]. Σύμφωνα με τους ίδιους αυτό το πρωτόκολλο μπορεί να αξιοποιηθεί για την υλοποίηση ανώνυμων καναλιών αποστολέα και παραλήπτη, με τέτοιο τρόπο ώστε να διασφαλίζεται το απόρρητο και η ανωνυμία των μηνυμάτων. Αυτό το πρωτόκολλο έχει την δυνατότητα αντοχής της διακοπής του, αλλά η κβαντική δέσμευση Gilbert-Varshamov (quantum Gilbert-Varshamov bound) πρέπει να ικανοποιηθεί από έναν πεπερασμένο αριθμό διαταρακτών. Με άλλα λόγια ο αριθμός των διαταρακτών πρέπει να περιορίζεται από το κβαντικό όριο Gilbert-Varshamov.

Στα πρωτόκολλα που βασίζονται σε κβαντικές καταστάσεις ενός μόνο σωματιδίου, η ανίχνευση της ασφάλειας των μεταδιδόμενων κβαντικών πόρων είναι κρίσιμη. Στα υπάρχοντα πρωτόκολλα, πρέπει να πραγματοποιείται ανίχνευση μετά από κάθε

ολοκληρωμένη μετάδοση για να διασφαλιστεί η ασφάλεια του καναλιού. Το πρωτόκολλο πραγματοποιεί πάρα πολλές επαναλαμβανόμενες λειτουργίες όταν ο αριθμός των συμμετεχόντων είναι μεγάλος. Η σταδιακή ανίχνευση έχει ενσωματωμένα ελαττώματα στο κόστος των κβαντικών πόρων. Έτσι οι Yuancheng Li, Chaohang Yu, QingleWang και Jiangshan Liu, το 2021 παρουσίασαν ένα ανώνυμο πρωτόκολλο μετάδοσης που χρησιμοποιεί καταστάσεις ενός σωματιδίου με συλλογική ανίχνευση [38]. Σε αντίθεση με προηγούμενες μελέτες και πρωτόκολλα που χρησιμοποιούν τις καταστάσεις GHZ και τις ζεύξεις EPR, αντίστοιχα. Με τη συλλογική ανίχνευση κατάφεραν να μειώσουν σημαντικά τον αριθμό των απαραίτητων γύρων ως αποτέλεσμα να μειωθεί το απαιτούμενο κόστος. Παράλληλα η αποτελεσματικότητα της μέτρησης, αποδίδει καλύτερα συγκριτικά με τις μεθόδους που αναφερθήκαμε προηγουμένως.

Τέλος, το 2022 οι S Mishra, K Thapliyal, A Parakh και A Pathak δημοσίευσαν μία σειρά πρωτοκόλλων QAV, δηλαδή κβαντικά πρωτόκολλα του ανώνυμου βέτο [39]. Τα πρωτόκολλα αυτά εμπίπτουν σε 3 κατηγορίες ντετερμινιστικά, επαναληπτικά και πιθανολογικά ενώ βασίζονται σε ένα μόνο φωτόνιο, διμερείς και πολυμερείς εμπλεκόμενες καταστάσεις, ορθογώνια κατάσταση και συζευγμένη κωδικοποίηση. Έτσι κατά τη δημιουργία νέων πρωτοκόλλων, διερευνώνται επίσης οι εγγενείς σχέσεις μεταξύ του ανώνυμου βέτο και των κρυπτογραφικών που δειπνούν. Το πρωτόκολλο που περιγράφεται είναι δομημένο παρόμοια με το πρωτόκολλο DC, καθώς όλα τα ζεύγη ψηφοφόρων πρέπει πρώτα να δημιουργήσουν συμμετρικά κλειδιά για να αρχίσουν οι συμμετέχοντες να ψηφίζουν. Έχουν ερευνήσει τις εγγενείς συνδέσεις μεταξύ DC και AV πρωτοκόλλων αλλά δεν προτείνουν κάποια κβαντική εκδοχή του DC.

Κεφάλαιο 4^ο

4.1 Το νέο πρωτόκολλο

Αυτό το πρωτόκολλο στοχεύει στην κλιμάκωση όσον αφορά τόσο τον αριθμό των κρυπτογράφων n όσο και την ποσότητα των ανώνυμων πληροφοριών που μεταφέρονται, που αντιπροσωπεύονται από τον αριθμό των qubits m εντός κάθε κβαντικού καταχωρητή. Πιο αναλυτικά το πρωτόκολλο υποστηρίζει έναν τυχαίο αριθμό κρυπτογράφων n , επιτρέποντας την κλιμάκωση τόσο στον αριθμό των συμμετεχόντων όσο και στον όγκο των ανώνυμων πληροφοριών που μεταδίδονται. Το προτεινόμενο πρωτόκολλο επιτρέπει στο m (τον αριθμό των qubits σε κάθε καταχωρητή) να είναι οποιοσδήποτε τυχαία μεγάλος θετικός ακέραιος, κάτι που αντιτίθεται στο αρχικό πρόβλημα του Dining Cryptographers καθώς επικεντρώθηκε σε μία μόνο πληροφορία. Αυτό συμβαίνει γιατί από την φύση του το πρωτόκολλο προϋποθέτει το δείπνο να έχει πληρωθεί μία μόνο φορά. Το συγκεκριμένο πρωτόκολλο διευρύνει την ευελιξία του στην προσαρμογή τόσο των τοπικών όσο και των κατανεμημένων εκδόσεων του προβλήματος DC. Το τοπικό σενάριο περιλαμβάνει όλους τους κρυπτογράφους που συγκεντρώνονται με φυσική παρουσία στον ίδιο τόπο, όπως ένα εστιατόριο, ταυτόχρονα, σε αντίθεση ένα κατανεμημένο σενάριο έχει την δυνατότητα να φιλοξενήσει κρυπτογράφους που βρίσκονται σε διαφορετικά μέρη, οι οποίοι συμμετέχουν σε ένα εικονικό δείπνο ταυτόχρονα. Τέλος, όσον αφορά την υλοποίηση, το πρωτόκολλο διασφαλίζει την ομοιομορφία, καθώς απαιτείται από όλους τους κρυπτογράφους να χρησιμοποιούν πανομοιότυπα ιδιωτικά κβαντικά κυκλώματα. Επιπλέον, κάθε ιδιωτικό κβαντικό κύκλωμα χρησιμοποιεί αποκλειστικά τις ευρέως χρησιμοποιούμενες κβαντικές πύλες Hadamard και CNOT, διευκολύνοντας την υλοποίηση σε σύγχρονους κβαντικούς υπολογιστές.

Σε προηγούμενο κεφάλαιο αναφερθήκαμε σε καταστάσεις GHZ. Η κατάσταση $|GHZ_n\rangle$ αποτελεί μια κατάσταση με μέγιστης εμπλοκής, κάτι που σημαίνει πως η εμπλοκή μεταξύ των n qubits είναι όσο το δυνατόν πιο ισχυρή. Μαθηματικά, η κατάσταση αυτή μπορεί να εκφραστεί ως: $|GHZ_n\rangle = \frac{|0\rangle_{n-1}|0\rangle_{n-2}\dots|0\rangle_0 + |1\rangle_{n-1}|1\rangle_{n-2}\dots|1\rangle_0}{\sqrt{2}}$, όπου $i, 0 \leq i \leq n - 1$ δηλώνει το i -οστό qubit.

Αυτή τη στιγμή, οι σύγχρονοι κβαντικοί υπολογιστές μπορούν να δημιουργήσουν αυθαίρετες καταστάσεις GHZ χρησιμοποιώντας πρότυπα κβαντικές πύλες όπως οι πύλες Hadamard και CNOT. Επιπλέον, τα κυκλώματα που είναι υπεύθυνα για την παραγωγή αυτών των καταστάσεων επιτυγχάνουν υψηλή αποδοτικότητα, απαιτώντας μόνο $\lg_n$ βήματα για την κατάσταση $|GHZ_n\rangle$ [43]. Για το συγκεκριμένο πρωτόκολλο απαιτείται ένα πιο περίπλοκο και ευέλικτο κβαντικό σύστημα όπου κάθε υποσύστημα είναι ένας κβαντικός καταχωρητής r_i , $0 \leq i \leq n - 1$, που περιέχει m qubits. Με αυτόν τον τρόπο τα αντίστοιχα qubits σε όλους τους καταχωρητές n μπλέκονται στην κατάσταση $|GHZ_n\rangle$. Το

$SBEDS_{n,m}$ είναι το σχέδιο κατανομής συμμετρικής εμπλοκής δυαδικών ψηφίων των (n,m) , Symmetric Bitwise Entanglement Distribution Scheme, όπου:

1. υπάρχουν n κβαντικοί καταχωρητές $r_0, r_1, \dots, r_{n-1}$
2. κάθε καταχωρητής περιέχει m qubits
3. τα n qubit στη θέση j , $0 \leq j \leq m - 1$, σε κάθε καταχωρητή μπλέκονται στην κατάσταση $|GHZ_n\rangle$

Το σύστημα των n κβαντικών καταχωρητών μπορεί να είναι είτε τοπικό, είτε χωρικά κατανεμημένο, κάτι που εξαρτάται από το αν οι καταχωρητές βρίσκονται στην ίδια ή σε διαφορετικές γεωγραφικές τοποθεσίες στο χώρο. Σε κάθε περίπτωση, η συνολική κατάσταση του σύνθετου συστήματος [44] (n, m) Symmetric Bitwise Entanglement Distribution Scheme:

$$|GHZ_n\rangle^{\otimes m} = \frac{1}{\sqrt{2^m}} \sum_{x \in B^m} |x\rangle_{n-1} \dots |x\rangle_0$$

1. το B είναι το δυαδικό σύνολο $\{0, 1\}$
2. $x \in B^m$, διάνυσμα x μήκους m είναι μια συντομογραφία μιας ακολουθίας από m bits: $x = x_{m-1} \dots x_0$. Στην ειδική περίπτωση όπου όλα τα bit είναι μηδέν, το διάνυσμα bit μηδέν συμβολίζεται με $\mathbf{0}$
3. $x \in B^m$, Το m αντιπροσωπεύει τη δυαδική αναπαράσταση ενός από τα 2^m βασικά kets που αποτελούν την υπολογιστική βάση του διαθέσιμου χώρου Hilbert
4. i , $0 \leq i \leq n - 1$ για να τονίσουμε ότι $|x\rangle_i$ είναι η κατάσταση του i -οστού κβαντικού καταχωρητή

Εκτός από την κατάσταση $|GHZ_n\rangle$, χρησιμοποιείται επίσης $|-\rangle$:

$$|-\rangle = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Ο μετασχηματισμός Hadamard μιας αυθαίρετης βάσης ket φαίνεται παρακάτω:

$$H^{\otimes m}|x\rangle = \frac{1}{\sqrt{2^m}} \sum_{z \in B^m} (-1)^{z \cdot x} |z\rangle$$

όπου $x \cdot y$ υποδηλώνει τη λειτουργία του εσωτερικού γινομένου modulo 2. Το εσωτερικό γινόμενο modulo 2 λαμβάνει ως είσοδο δύο δυαδικούς διανυσματικούς χώρους όπου $x, y \in B^m$ και εξάγει το εσωτερικό τους γινόμενο. Πιο συγκεκριμένα, αν $x = x_{m-1} \dots x_0$ και $y = y_{m-1} \dots y_0$ τότε $x \cdot y = x_{m-1}y_{m-1} \oplus \dots \oplus x_0y_0$, όπου $\oplus$ η πρόσθεση modulo 2. Η λειτουργία εσωτερικού γινομένου modulo 2 χαρακτηρίζεται από μια βασική ιδιότητα η οποία είναι κεντρική σε πολλούς κβαντικούς αλγορίθμους. Αν λάβουμε οποιοδήποτε σταθερό στοιχείο c από το B^m , αν το $c \neq 0$, τότε για το μισό των στοιχείων

$x \in B^m$, το αποτέλεσμα της λειτουργίας $c \cdot x$ είναι 0, και για το υπόλοιπο μισό, το αποτέλεσμα της λειτουργίας $c \cdot x$ είναι 1. Η εξαίρεση του 0 δικαιολογείται επειδή όταν $c = 0$, τότε για όλα τα $x \in B^m$, $c \cdot x = 0$. Με άλλα λόγια αν το $c = 0$, τότε $c \cdot x = 0$ αλλά αν το $c \neq 0$, τότε $c \cdot x = 0$ ή $c \cdot x = 1$.



Εικόνα 9: $|GHZ_n\rangle$

Στο παραπάνω σχήμα μπορούμε να διακρίνουμε το σύνολο mn qubits, με n τους κβαντικούς καταχωρητές όπου ο καθένα τους περιέχει m qubits. Είναι σημαντικό να τονίσουμε πως δεν έχει σημασία οι n πλειάδες βρίσκονται στην ίδια τοποθεσία ή όχι.

4.2 The Scalable quantum protocol for the Dining Cryptographers Problem

Το κλιμακούμενο κβαντικό πρωτόκολλο για το πρόβλημα των κρυπτογράφων που δειπνούν/ The Scalable quantum protocol for the Dining Cryptographers Problem ή πρωτόκολλο SQDCP για συντομία. Αυτό το παιχνίδι παίζεται από n κρυπτογράφους, η Alice έχει οργανώσει ένα επίσημο δείπνο για τον εαυτό της και τους $n - 1$ συναδέλφους της. Στο παράδειγμα που θα ακολουθήσει θα συμμετέχει ο Bob, ο Charlie ο Dave και φυσικά η Alice. Το δείπνο σερβίρεται σε τέσσερις κρυπτογράφους, οι οποίοι πήγαν να δειπνήσουν σε κάποιο εστιατόριο. Κάποια στιγμή ο σερβιτόρος τους αποκαλύπτει πως έχει πληρωθεί

κρυφά ο λογαριασμός. Το δείπνο μπορεί να έχει πληρωθεί από έναν από τους κρυπτογράφους ή να το έχει πληρώσει ο εργοδότης τους. Οι κρυπτογράφοι αναγνωρίζουν και κατανοούν ο ένας το δικαίωμα του άλλου να κάνει μια ανώνυμη πληρωμή, αλλά αναρωτιούνται αν το έχει πληρώσει ο εργοδότης τους. Το πρωτόκολλο SQDCP φέρνει τρεις κύριες καινοτομίες:

1. **Scalability/ Κλιμακωσιμότητα:** η έννοια της κλιμακωσιμότητας περιλαμβάνει και τις παραμέτρους n και m . Ο αριθμός των κρυπτογράφων n μπορεί να είναι οποιοσδήποτε αυθαίρετα μεγάλος θετικός ακέραιος, ενώ παράλληλα μπορεί ανεμπόδιστα να κλιμακωθεί όσον αφορά το ποσό των ανώνυμων πληροφοριών που μεταφέρει. Σε αντίθεση με το κλασικό πρωτόκολλο το οποίο αφορούσε μόνο ένα bit πληροφοριών, δηλαδή εάν κάποιος από τους κρυπτογράφους πλήρωσε ή όχι για το δείπνο. Στο πρωτόκολλο SQDCP, ο αριθμός m των qubits σε κάθε καταχωρητή μπορεί επίσης να είναι ένας μεγάλος θετικός ακέραιος, αντικατοπτρίζει τον όγκο των πληροφοριών που μπορούν να μεταδοθούν. Για παράδειγμα, ο κρυπτογράφος που πραγματικά πλήρωσε το λογαριασμό μπορεί επίσης να αποκαλύψει πόσο κόστισε ή πότε έγινε η συναλλαγή.
2. **Local and Distribute Mode/ Τοπική και Κατανεμημένη Λειτουργία:** το δείπνο των κρυπτογράφων ήταν ένα τοπικό γεγονός, υπο την έννοια πως όλοι οι κρυπτογράφοι ήταν μαζί στην ίδια χωρική τοποθεσία αλλά και σε ένα συγκεκριμένο χρονικό σημείο. ο πρωτόκολλο που εισάγεται σε αυτήν την εργασία μπορεί να αντιμετωπίσει όχι μόνο αυτήν την τοπική κατάσταση αλλά και μια κατανεμημένη έκδοση του προβλήματος.
3. **Uniformity and Ease of Implementation/ Ομοιομορφία και Ευκολία Εφαρμογής:** Όλοι οι κρυπτογράφοι χρησιμοποιούν ίδια κβαντικά κυκλώματα. η κβαντική υλοποίηση είναι διαμορφωμένη έτσι ώστε όλες οι ενότητες να είναι το ίδιο. Επιπλέον, κάθε κβαντικό κύκλωμα μπορεί να εφαρμοστεί εύκολα από ένα σύγχρονο κβαντικό υπολογιστή επειδή χρησιμοποιεί μόνο τις ευρέως διαδεδομένες κβαντικές πύλες Hadamard και CNOT.



Εικόνα 10: Τέσσερις κρυπτογράφοι

Αρχικά, η Alice συγκεντρώνεται μαζί με τους $n - 1$ συναδέλφους της κρυπτογράφους $C_0, \dots, C_{n-2}$ για μια φιλική βραδιά σε ένα κοντινό εστιατόριο. Για όλους τους παίκτες n , το δείπνο λαμβάνει χώρα ταυτόχρονα και στον ίδιο χώρο. Κάθε παίκτης χρησιμοποιεί ένα κβαντικό κύκλωμα όπου κρυφά ενσωματώνει τις επιθυμητές πληροφορίες, δηλαδή εάν πλήρωσε ή όχι για το δείπνο. Μετά τη μέτρηση των κβαντικών τους καταχωρητών και τη δημόσια συνδυασμό των αποτελεσμάτων που έχουν προκύψει, όλοι οι παίκτες γνωρίζουν αμέσως αν το δείπνο πληρώθηκε από έναν από αυτούς ή από τον εργοδότη τους, και, ενδεχομένως, κάποιες επιπλέον πληροφορίες, όπως η τιμή του δείπνου ή η ημερομηνία της πληρωμής, κπλ. Η ταυτότητα αυτού που πλήρωσε το λογαριασμό πρέπει να παραμείνει άγνωστη σε όλους τους άλλους κρυπτογράφους. Τα διεμπλεγμένα μεταξύ τους υποσυστήματα είναι αλληλένδετα παρόλο που είναι χωρικά διαχωρισμένα. Αυτό είναι το κλειδί που επιτρέπει την αποτελεσματική λειτουργία πολλών κατανεμημένων κβαντικών πρωτοκόλλων. Το πρωτόκολλο SQDCP επίσης εκμεταλλεύεται το entanglement με σκοπό να επιτύχει το επιθυμητό αποτέλεσμα σε ένα εντελώς κατανεμημένο περιβάλλον.

Η Alice συγκεντρώνεται μαζί με τους συναδέλφους της $C_0, \dots, C_{n-2}$ για μια φιλική βραδιά σε ένα κοντινό εστιατόριο. Υπάρχει όμως μια επιπλοκή τώρα σε σύγκριση με την προηγούμενη περίπτωση, καθώς όλοι οι n παίκτες κατοικούν σε διαφορετικές γεωγραφικές τοποθεσίες. Παρ' όλα αυτά, είναι αποφασισμένοι να δειπνήσουν ταυτόχρονα, αν και σε διαφορετικά εστιατόρια, και να είναι σε συνεχή ηχητική και οπτική επαφή μέσω τηλεδιάσκεψης. Κάθε παίκτης χρησιμοποιεί ένα τοπικό κβαντικό κύκλωμα το οποίο ενσωματώνει κρυφά τις επιθυμητές πληροφορίες, δηλαδή εάν πλήρωσε ή όχι για το δείπνο. Κατά τη μέτρηση των κβαντικών τους καταχωρητών, ανταλλάσσουν δημόσια τις μετρήσεις τους μέσω κλασικών καναλιών. Στη συνέχεια, κάθε παίκτης συνδυάζει τα αποτελέσματα και γνωρίζει αμέσως εάν το δείπνο πληρώθηκε από κάποιον από αυτούς ή από τον εργοδότη τους, και, πιθανώς, κάποιες πρόσθετες πληροφορίες.

Για να προχωρήσουμε, θα χρειαστεί να κάνουμε κάποιους περιορισμούς. Παρόλο που δεν υπάρχει θεωρητικός περιορισμός στον αριθμό n των κρυπτογράφων που μπορεί να είναι ένας αυθαίρετα μεγάλος ακέραιος αριθμός, σύγχρονα κβαντικά μηχανήματα μπορεί να επιβάλλουν περιορισμούς στην παραγωγή των συνόλων $|GHZ_n\rangle$, όπου το n υπερβαίνει κάποιο κατώφλι. Επίσης, υποθέτουμε πως πριν από την εκτέλεση του πρωτοκόλλου SQDCP, έχουν ληφθεί ορισμένες διατάξεις μεταξύ των κρυπτογράφων σχετικά με την ποσότητα και τη φύση των επιθυμητών πληροφοριών. Αυτό είναι απαραίτητο για τον καθορισμό του αριθμού m , που αντιστοιχεί στην ποσότητα της πληροφορίας, και τη σωστή ερμηνεία του αποτελέσματος. Στην κατανεμημένη έκδοση, υποθέτουμε επίσης την ύπαρξη αυθεντικών καναλιών κατά ζεύγη που επιτρέπουν τη μετάδοση κλασικών πληροφοριών.

Η Alice, ο Bob, ο Charlie και ο Dave δείπνουν τόσο στο τοπικοποιημένο όσο και στο κατανεμημένο σενάριο. Κοινό και στα δύο σενάρια είναι το γεγονός ότι οι κβαντικοί καταχωρητές εισόδου τους μπλέκονται σύμφωνα με το (n, m) Symmetric Bitwise Entanglement Distribution Scheme. Έχουμε άρα μία ειδική περίπτωση στην οποία το $n = 4$ αν υποθέσουμε ότι η επιθυμητή πληροφορία περιλαμβάνει επίσης το ποσό των χρημάτων που πληρώθηκε για το δείπνο, μπορούμε επίσης να θεωρήσουμε το $m = 4$. Με αυτόν τον τρόπο το τελικό αποτέλεσμα του πρωτοκόλλου θα είναι m bits που εκφράζουν τη δυαδική

αναπαράσταση του κόστους του δείπνου, π.χ. σε ευρώ €. Ένα τέτοιο παράδειγμα μικρής κλίμακας απαιτεί $4 |GHZ_4\rangle$ ομοιόμορφα κατανεμημένα μεταξύ των 4 παικτών. Όταν το δείπνο λαμβάνει χώρα στο ίδιο εστιατόριο την ίδια ώρα και για τους τέσσερις κρυπτογράφους, έχουμε την τυπική έκδοση του προβλήματος και το αναφέρουμε ως εντοπισμένο σενάριο (localized scenario).

Εκτός από την τυπική προσέγγιση, το γεγονός ότι οι κβαντικοί καταχωρητές είναι μπερδεμένοι ανοίγει το δυνατότητα υλοποίησης του πρωτοκόλλου SQDCP ακόμη και στην περίπτωση που οι κρυπτογράφοι βρίσκονται σε διαφορετικές τοποθεσίες. Σε ένα τέτοιο σενάριο, τρώνε ένα εικονικό δείπνο ταυτόχρονα, αλλά τώρα ο καθένας τους βρίσκεται σε διαφορετική τοποθεσία.

4.3 Εκτέλεση του πρωτοκόλλου SQDCP

Πριν ξεκινήσουμε, ας επισημάνουμε ότι το πρωτόκολλό μας δεν παραβιάζει το θεώρημα της μη κλωνοποίησης [45]. Η κατάσταση $|GHZ_n\rangle$ είναι γνωστή σε όλους τους κρυπτογράφους που συμμετέχουν στο πρωτόκολλο προτού ξεκινήσει. Σε πρώτη φάση, ένας από τους κρυπτογράφους ενσωματώνει τις ιδιωτικές πληροφορίες στην κατανεμημένη μπερδεμένη κατάσταση του συστήματος. Η φάση της μπλεγμένης διαμονής (Entanglement distribution phase). Στην επακόλουθη ανάλυση, ορίζεται ο αριθμός qubits σε κάθε κβαντικό καταχωρητή εισόδου από το m . Αυτός ο αριθμός θεωρείται πως είναι ένας κατάλληλα επιλεγμένος μεγάλος θετικός ακέραιος, ικανός να μεταφέρει την επιθυμητή ποσότητα πληροφοριών. Ένα έμπιστο μέλλος, δημιουργεί μια ακολουθία από $m |GHZ_n\rangle$ ζεύγη δηλαδή, mn qubits συνολικά τα οποία αποτελούν απαραίτητη προϋπόθεση για την εκτέλεση του πρωτοκόλλου και την ιδιωτική μετάδοση των απαιτούμενων πληροφοριών. Αυτά τα ζεύγη, δημιουργούνται και διανέμονται αξιόπιστα μεταξύ των κρυπτογράφων. Για λόγους ευκολίας, ας υποθέσουμε ότι σε κάθε σύνολο $|GHZ_n\rangle$, τα κβιτς αριθμούνται από 0 έως $n-1$. Η κατανομή αυτών των πλειάδων ακολουθεί το παρακάτω πρότυπο, το οποίο εξασφαλίζει την ομοιόμορφη και ισότιμη κατανομή της συγκάλυψης μεταξύ των κρυπτογράφων.

1. Η Alice αποθηκεύει στον καταχωρητή εισόδου της, που συμβολίζεται με AIR το $(n - 1)$ -οστό qubit από κάθε μία $|GHZ_n\rangle$ πλειάδα.
2. Ο κρυπτογράφος C_i , $0 \leq i \leq n - 2$, αποθηκεύει στον καταχωρητή εισόδου του, που συμβολίζεται με IR_i , το i -οστό qubit από κάθε πλειάδας $|GHZ_n\rangle$

Εκτός από τον καταχωρητή εισόδου της, η Alice χρησιμοποιεί έναν καταχωρητή εξόδου ενός bit που ορίζεται από AOR , το οποίο αρχικοποιείται στην κατάσταση $|-\rangle$. Επίσης, όλοι οι συνάδελφοί της κρυπτογράφοι C_i , $0 \leq i \leq n - 2$ διαθέτουν παρόμοιο καταχωρητή εξόδου ενός bit που συμβολίζεται με OR_i . Αυτοί οι καταχωρητές εξόδου παίζουν κρίσιμο

ρόλο στην ενσωμάτωση ιδιωτικών πληροφοριών στην πλεγμένη κατάσταση του σύνθετου κυκλώματος. Όλοι οι κρυπτογράφοι λειτουργούν ιδιωτικά και μυστικά στα δικά τους κβαντικά κυκλώματα, ακριβώς όπως και στο κλασικό σενάριο. Όλα αυτά τα κυκλώματα είναι πανομοιότυπα. Επίσης, είναι σημαντικό να επισημαίνουμε ότι ολόκληρος ο αλγόριθμος εξαρτάται από την ύπαρξη διεμπλοκής, ως εκ τούτου, είναι πολύ σημαντικό να επαληθευτεί ότι όλοι οι κβαντικοί καταχωρητές των κρυπτογράφων είναι κατάλληλα μπλεγμένοι.

Προχωράμε στην επόμενη φάση, κατά την οποία γίνεται η ενσωμάτωσης ιδιωτικών πληροφοριών. Ο κρυπτογράφος που πραγματικά πλήρωσε για το δείπνο, υποθέτοντας ότι αυτό ήταν πράγματι το σενάριο, είναι σε θέση να ενσωματώσει ιδιωτικά και μυστικά αυτήν την πληροφορία, ίσως μαζί με οποιαδήποτε επιπλέον σχετική πληροφορία. Συγκεκριμένα, αν ήταν η Alice που κρυφά πλήρωσε για το δείπνο, και η δυαδική αναπαράσταση του ποσού που πλήρωσε είναι P_A σε ευρώ €, τότε θα εισάγει το P_A στην μπλεγμένη κατάσταση του κυκλώματος μέσω του ιδιωτικού ενιαίου μετασχηματισμού της U_{fA} . Το U_{fA} το γνωρίζει μόνο η ίδια έτσι, οι απαιτούμενες πληροφορίες θα ενσωματωθούν κρυφά και κανείς δεν θα μπορεί να τα εντοπίσει πίσω στην Alice. Αν η Alice δεν πλήρωσε για το δείπνο, τότε χρησιμοποιεί το μηδενικό διάνυσμα bit 0 στο U_{fA} , η οποία ουσιαστικά αφήνει αναλλοίωτη την κατάσταση του συστήματος στην καθολική κατάσταση και δεν ενσωματώνει καμία νέα πληροφορία.

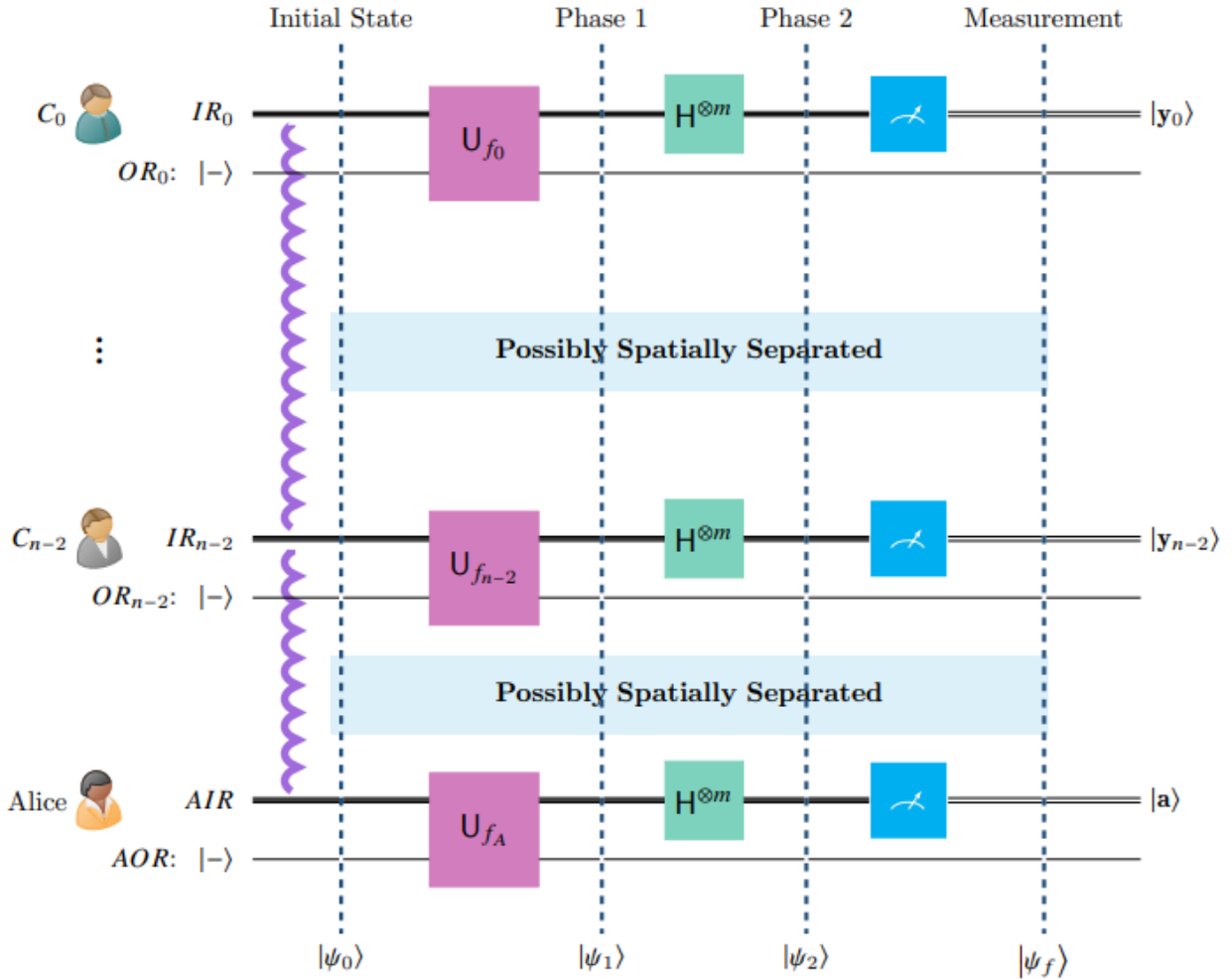
Αν ο κρυπτογράφος C_i , $0 \leq i \leq n - 2$, πλήρωσε για το δείπνο και η δυαδική αναπαράσταση του ποσού που καταβλήθηκε είναι P_i , τότε θα το κάνει εισάγει μπερδεμένη κατάσταση του κυκλώματος μέσω του ιδιωτικού μοναδικού μετασχηματισμού U_{fi} . Καθώς το U_{fi} είναι γνωστό μόνο στον κρυπτογράφο C_i , αυτή η πληροφορία θα ενσωματωθεί κρυφά και ιδιωτικά, και κανείς δεν θα μπορεί να την εντοπίσει στον C_i . Αν ο κρυπτογράφος C_i δεν πλήρωσε για το δείπνο, τότε χρησιμοποιεί το μηδενικό διάνυσμα bit 0 στο U_{fi} και έτσι μένει αναλλοίωτη η κατάσταση του συστήματος στην καθολική κατάσταση και δεν ενσωματώνει καμία νέα πληροφορία.

Το κβαντικό μέρος του πρωτοκόλλου ολοκληρώνεται όταν οι κρυπτογράφοι μετρήσουν τους δικούς τους καταχωρητές εισόδου. Οι λαμβανόμενες μετρήσεις προστίθενται μεταξύ τους, χρησιμοποιώντας το modulo 2. Δηλαδή προκύπτει το σύνολο των XOR. Το τελικό αποτέλεσμα p παρέχει την επιθυμητή πληροφορία.

1. Αν $p \neq 0$, το δείπνο πληρώθηκε από έναν από τους κρυπτογράφους. Ανακαλύπτουμε επίσης πόσο κοστίζει το δείπνο, επειδή το p είναι η δυαδική αναπαράσταση του κόστους σε €.
2. Αν $p = 0$ ή bit 0, το δείπνο πληρώθηκε από τον εργοδότη τους

Το πρωτόκολλο SQDCP θα λειτουργήσει ακόμα και αν όλοι οι συμμετέχοντες βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες. Αυτό συμβαίνει επειδή ακόμα και αν οι κβαντικοί καταχωρητές εισόδου είναι χωρισμένοι χωρικά, αυτοί εξακολουθούν να αποτελούν ένα σύνθετο καταναμημένο κβαντικό σύστημα λόγω των ισχυρών συσχετισμών μεταξύ των qubit τους που προέρχονται από την εμπλοκή $|GHZ_n\rangle$. Η μόνη διαφορά στην περίπτωση της

κατανεμημένης αναφοράς είναι ότι κάθε κρυπτογράφος πρέπει να κοινοποιεί τις μετρήσεις χρησιμοποιώντας κλασικά κανάλια με έλεγχο ταυτότητας κατά ζεύγη.



Εικόνα 11: Κβαντικό κύκλωμα

Η παραπάνω εικόνα απεικονίζει το σύνθετο κβαντικό κύκλωμα που χρησιμοποιείται από τους κρυπτογράφους τραπέζαρίας. Φαίνεται το ατομικό τοπικό κύκλωμα της Alice και κάθε ένας από τους συναδέλφους της. Τα διανύσματα κατάστασης $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$ και $|\psi_f\rangle$ περιγράφουν την εξέλιξη αυτού του σύνθετου συστήματος. Όπως προείπαμε ο κβαντικός καταχωρητής εισόδου της Alice συμβολίζεται με AIR . Το IR_i είναι ο καταχωρητής εισόδου του κρυπτογράφου C_i , $0 \leq i \leq n - 2$. Συνολικά υπάρχουν καταχωρητές εισόδου n , καθένας από τους οποίους περιέχει m qubits. Τα αντίστοιχα qubits σε καθένα από τους καταχωρητές n είναι μπλεγμένα στην κατάσταση $|GHZ_n\rangle$. Με AOR συμβολίζεται ο καταχωρητής εξόδου της Alice. Το OR_i είναι ο καταχωρητής εξόδου του κρυπτογράφου C_i ,

$0 \leq i \leq n - 2$. Όλοι οι καταχωρητές εξόδου περιέχουν μόνο ένα qubit στην κατάσταση $|-\rangle$. Το U_{fA} συμβολίζει τον ιδιωτικό ενιαίο μετασχηματισμό της Alice και U_{fi} ο ενιαίος μετασχηματισμός του κρυπτογράφου C_i , $0 \leq i \leq n - 2$. Το $H^{\otimes m}$ είναι ο μετασχηματισμός Hadamard. Η αρχική κατάσταση του κατανεμημένου κβαντικού κυκλώματος του $|\psi_0\rangle$ μπορεί να γραφτεί ως:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in B^m} |-\rangle_A |x\rangle_A |-\rangle_{n-2} |x\rangle_{n-2} \cdots |-\rangle_0 |x\rangle_0$$

Η Alice και οι υπόλοιποι κρυπτογράφοι ξεκινούν την εκτέλεση του πρωτοκόλλου SQDCP ενεργώντας σύμφωνα με τα μεμονωμένα κβαντικά κυκλώματα μέσω των ιδιωτικών ενιαίων μετασχηματισμών τους U_{fA} και U_{fi} . Με αυτόν τον τρόπο, ο καθένας από αυτούς μπορεί να ενσωματώσει τις απαιτούμενες ιδιωτικές πληροφορίες στην μπερδεμένη κατάσταση του σύνθετου συστήματος. Οποιοσδήποτε από αυτούς, χρησιμοποιώντας το ατομικό του, και τοπικό στο κατανεμημένο σενάριο, κβαντικό κύκλωμα, θα κωδικοποιήσει αυτές τις ιδιωτικές πληροφορίες που πρέπει να κοινοποιηθούν στους υπόλοιπους παίκτες, στους μπλεγμένους καταχωρητές εισόδου του κυκλώματος. Επί της ουσίας τα U_{fA} και U_{fi} βασίζονται σε ιδιωτικές και μυστικές συναρτήσεις f_A και f_i , $0 \leq i \leq n - 2$ τα οποία είναι γνωστά μόνο στον αντίστοιχο κρυπτογράφο. Ο ορισμός τους: $f_A(x) = p_A \bullet x$, όπου p_A τα χρήματα που πλήρωσε η Alice για το δείπνο ή 0 αν η Alice δεν πλήρωσε για το δείπνο. Και αντίστοιχα $f_i(x) = p_i \bullet x$ όπου p_i τα χρήματα που πλήρωσε ο κρυπτογράφος C_i για το δείπνο ή 0 αν ο κρυπτογράφος C_i δεν πλήρωσε για το δείπνο. Οι ενιαίοι μετασχηματισμοί $U_f: |x\rangle |y\rangle \rightarrow |y \oplus f(x)\rangle |x\rangle$ και σύμφωνα με τα προηγούμενα μπορούν να γραφτούν ως:

$$U_{fA}: |-\rangle_A |x\rangle_A \rightarrow (-1)^{p_A \bullet x} |-\rangle_A |x\rangle_A$$

$$U_{fi}: |-\rangle_i |x\rangle_i \rightarrow (-1)^{p_i \bullet x} |-\rangle_i |x\rangle_i, 0 \leq i \leq n - 2$$

Η συνδυασμένη επίδραση των ενιαίων μετασχηματισμών έχει ως αποτέλεσμα το σύστημα να μπει στην κατάσταση $|\psi_1\rangle$:

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2^m}} \sum_{x \in B^m} (U_{fA} |-\rangle_A |x\rangle_A) (U_{fn-2} |-\rangle_{n-2} |x\rangle_{n-2}) \cdots (U_{f0} |-\rangle_0 |x\rangle_0) \\ &= \frac{1}{\sqrt{2^m}} \sum_{x \in B^m} (-1)^{p_A \bullet x} |-\rangle_A |x\rangle_A (-1)^{p_{n-2} \bullet x} |-\rangle_{n-2} |x\rangle_{n-2} \cdots (-1)^{p_0 \bullet x} |-\rangle_0 |x\rangle_0 \\ &= \frac{1}{\sqrt{2^m}} \sum_{x \in B^m} (-1)^{(p_A \oplus p_{n-2} \oplus \cdots \oplus p_0) \bullet x} |-\rangle_A |x\rangle_A |-\rangle_{n-2} |x\rangle_{n-2} \cdots |-\rangle_0 |x\rangle_0 \end{aligned}$$

Επομένως, στο τέλος της πρώτης φάσης, ο κρυπτογράφος που πλήρωσε για το δείπνο έχει ενσωματώσει τις πληροφορίες που είναι γνωστές μόνο σε αυτόν με ανεξιχνίαστο τρόπο στη μπερδεμένη κατάσταση $|\psi_1\rangle$ του κυκλώματος. Σε αυτή τη φάση, απομένει να αποκρυπτογραφηθούν αυτές οι πληροφορίες, ώστε να γίνουν γνωστές σε όλους τους άλλους κρυπτογράφους. Για να αποκρυπτογραφήσουν τις ενσωματωμένες ιδιωτικές πληροφορίες, η Alice και οι υπόλοιποι κρυπτογράφοι εφαρμόζουν τον μετασχηματισμό Hadamard m στους καταχωρητές εισόδου τους. Ως αποτέλεσμα, στο τέλος της Φάσης 2, η κατάσταση του συστήματος έχει γίνει $|\psi_2\rangle$.

$$|\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in B^m} (-1)^{(p_A \oplus p_{n-2} \oplus \dots \oplus p_0) \cdot x} |-\rangle_A H^{\otimes m} |x\rangle_A |-\rangle_{n-2} H^{\otimes m} |x\rangle_{n-2} \dots |-\rangle_0 H^{\otimes m} |x\rangle_0$$

Αναλύοντας περεταίρω αυτή την σχέση:

$$H^{\otimes m} |x\rangle_A = \frac{1}{\sqrt{2^m}} \sum_{a \in B^m} (-1)^{a \cdot x} |a\rangle_A$$

$$H^{\otimes m} |x\rangle_{n-2} = \frac{1}{\sqrt{2^m}} \sum_{c_{n-2} \in B^m} (-1)^{c_{n-2} \cdot x} |c_{n-2}\rangle_{n-2}$$

$$H^{\otimes m} |x\rangle_0 = \frac{1}{\sqrt{2^m}} \sum_{c_0 \in B^m} (-1)^{c_0 \cdot x} |c_0\rangle_0$$

Κάνοντας κάποιες αντικαταστάσεις:

$$|\psi_2\rangle = \frac{1}{(\sqrt{2^m})^{n+1}} \sum_{a \in B^m} \sum_{c_{n-2} \in B^m} \dots \sum_{c_0 \in B^m} \sum_{x \in B^m} (-1)^{(p_A \oplus p_{n-2} \oplus \dots \oplus p_0 \oplus a \oplus c_{n-2}) \cdot x} |-\rangle_A |a\rangle_A |-\rangle_{n-2} |c_{n-2}\rangle_{n-2} \dots |-\rangle_0 |c_0\rangle_0$$

$$|\psi_2\rangle = \frac{1}{(\sqrt{2^m})^{n+1}} \sum_{a \in B^m} \sum_{c_{n-2} \in B^m} \dots \sum_{c_0 \in B^m} |-\rangle_A |a\rangle_A |-\rangle_{n-2} |c_{n-2}\rangle_{n-2} \dots |-\rangle_0 |c_0\rangle_0,$$

όπου $a \oplus c_{n-2} \oplus \dots \oplus c_0 = p_A \oplus p_{n-2} \oplus \dots \oplus p_0$ αναφερόμαστε στη σχέση ως θεμελιώδη ιδιότητα συσχέτισης που διαπλέκει τους καταχωρητές εισόδου των κρυπτογράφων τραπεζαρίας. Αυτή η σχέση είναι η συνέπεια της αρχικής εμπλοκής μεταξύ όλων των καταχωρητών εισόδου. Στο τέλος αυτής της φάσης ο κρυπτογράφος που πλήρωσε για το δείπνο έχει ενσωματώσει τις σχετικές ιδιωτικές πληροφορίες στη γενική κατάσταση του σύνθετου κβαντικού κυκλώματος. Το κβαντικό μέρος του πρωτοκόλλου SQDCP έχει τελειώσει όταν οι κρυπτογράφοι μετρήσουν τις εισόδους των καταχωρητών τους. Με αυτή την ενέργεια, η κατάσταση του σύνθετου συστήματος καταρρέει στην τελική κατάσταση, η οποία έχει την ακόλουθη μορφή:

$$|\psi_f\rangle = |-\rangle_A |a\rangle_A |-\rangle_{n-2} |c_{n-2}\rangle_{n-2} \dots |-\rangle_0 |c_0\rangle_0,$$

$$\text{όπου } a \oplus c_{n-2} \oplus \dots \oplus c_0 = p_A \oplus p_{n-2} \oplus \dots \oplus p_0$$

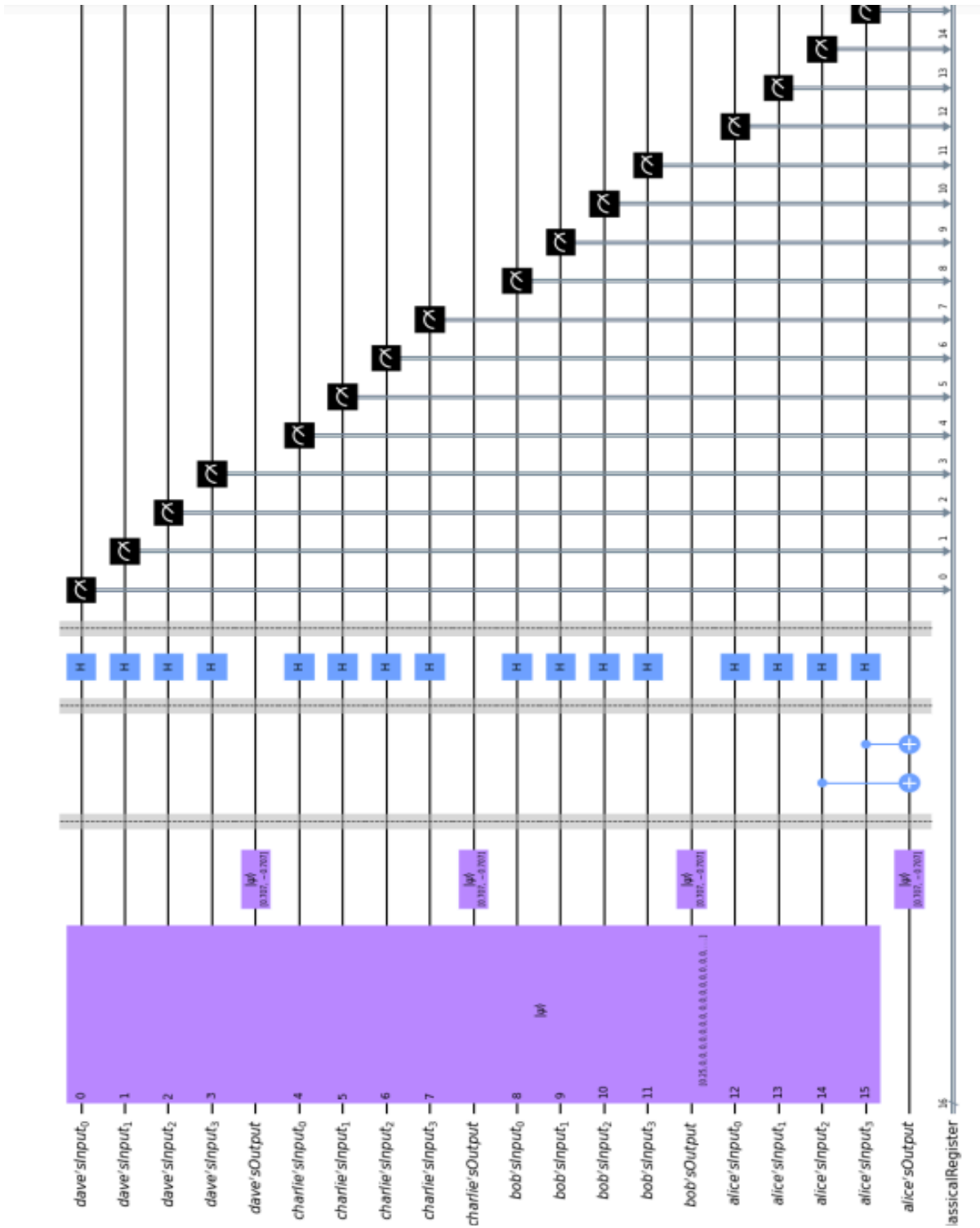
Όλες οι παραπάνω εξισώσεις ισχύουν τόσο στις τοπικές όσο και στις κατανεμημένες εκδοχές του πρωτοκόλλου SQDCP, διότι η εγκυρότητά τους πηγάζει από την αρχική διαπλοκή μεταξύ όλων των εισόδων. Όσο υπάρχει διαπλοκή, η απόσταση μεταξύ των dining cryptographers δεν παίζει κανέναν ρόλο. Το πρωτόκολλο ολοκληρώνεται αφού κάθε κρυπτογράφος κοινοποιεί με κάθε άλλον κρυπτογράφο τα μετρημένα περιεχόμενα του καταχωρητή εισόδου του. Η Alice στέλνει a στους $n - 1$ συναδέλφους κρυπτογράφους. Αντίστοιχα και οι υπόλοιποι, κάθε C_i , $0 \leq i \leq n - 2$ στέλνει c_i στην Alice και στους υπόλοιπους συναδέλφους κρυπτογράφους. Σε ένα τοπικοποιημένο περιβάλλον, αυτό το βήμα είναι αρκετά απλό. Σε ένα κατανεμημένο περιβάλλον, είναι επίσης εφικτό, καθώς απαιτεί μόνο τη χρήση κλασικών καναλιών επικοινωνίας με έλεγχο ταυτότητας κατά ζεύγη. Σε αυτό το σημείο, κάθε παίκτης γνωρίζει όλα τα διανύσματα bit $a \ c_{n-2} \dots c_0$. Αυτό επιτρέπει σε κάθε κρυπτογράφο να υπολογίσει το άθροισμα του υπολοίπου της διαίρεσης modulo 2 $a \oplus c_{n-2} \oplus \dots \oplus c_0$ το οποίο, παράγει το άθροισμα του υπολοίπου της διαίρεσης modulo 2 $p_A \oplus p_{n-2} \oplus \dots \oplus p_0$ όπως είδαμε παραπάνω. Έτσι μεταδίδεται η πληροφορία που οι κρυπτογράφοι επιθυμούσαν να αποκαλύψουν αρχικά και αυτό συμβαίνει γιατί:

1. Σε περίπτωση που κανένας από τους κρυπτογράφους δεν πλήρωσε το δείπνο, $p_A = p_{n-2} = \dots = p_0 = 0$ και κατα συνέπεια το άθροισμα του modulo 2 τους είναι 0. Το οποίο συνεπάγεται με το άθροισμα του modulo 2 $a \ c_{n-2} \dots c_0$ που είναι επίσης ίσο με 0. Και έτσι οι κρυπτογράφοι συμπεραίνουν ότι το δείπνο πληρώθηκε από τον εργοδότη τους.
2. Στην αντίθετη περίπτωση που C_i , $0 \leq i \leq n - 2$, πλήρωσε ένα συγκεκριμένο ποσό για το δείπνο, τότε, p_i η δυαδική αναπαράσταση αυτού του ποσού, είναι μη μηδενική, ενώ το p_A και όλα τα άλλα p_j , με $j \neq i$, είναι 0. Με τη σειρά τους, το modulo 2 άθροισμά τους είναι 0, που σημαίνει ότι το υπολογισμένο modulo 2 άθροισμα $a \ c_{n-2} \dots c_0$ είναι p_i . Επομένως, οι κρυπτογράφοι συμπεραίνουν πως ένας από αυτούς που πλήρωσε για το δείπνο και γνωρίζουν επίσης πόσο κόστισε το δείπνο. Ενώ το ίδιο επιχείρημα ισχύει αυτολεξεί σε περίπτωση που ήταν η Alice που πλήρωσε το δείπνο.

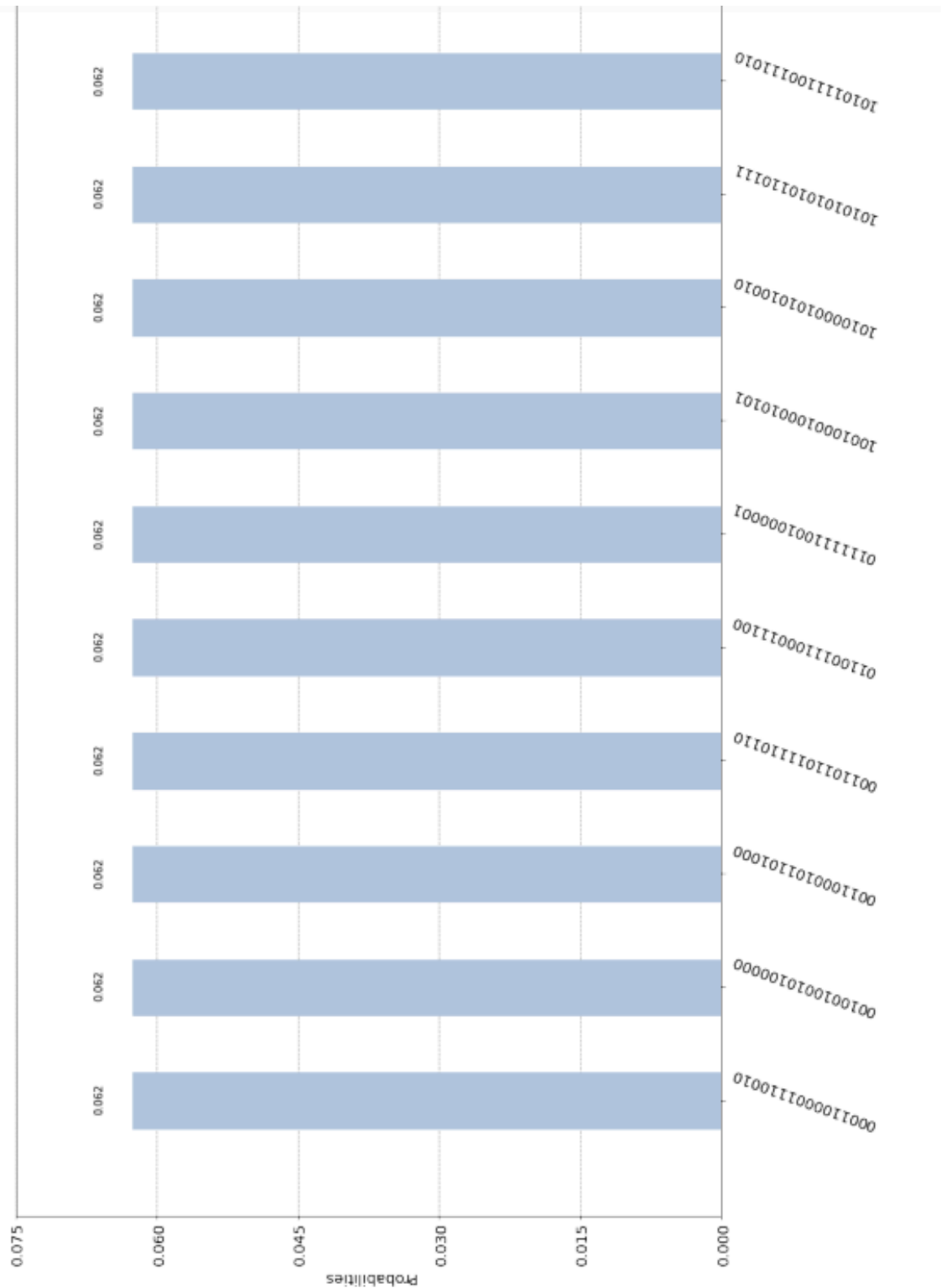
Με αυτόν τον τρόπο βλέπουμε επίσης ότι η αρχική πηγή των πληροφοριών παραμένει άγνωστη και ανεξιχνίαστη. Οι ιδιωτικές πληροφορίες, είτε είναι p_A είτε p_i έχουν απορροφηθεί στο άθροισμα $p_A \oplus p_{n-2} \oplus \dots \oplus p_0$ και δεν υπάρχει τρόπος να ανακτηθούν.

4.4 Παράδειγμα

Δεν έχει σημασία εάν βρίσκονται φυσικά μαζί στον ίδιο τραπέζι, ή αν βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες και δείπνουνται εικονικά καθώς το πρωτόκολλο SQDCP θα πραγματοποιηθεί σε κάθε περίπτωση. Οι κβαντικοί καταχωρητές εισόδου περιέχουν 4 qubits, ο καθένας. Τα αντίστοιχα qubits στους 4 κβαντικούς καταχωρητές σχηματίζουν ένα τετράπτυχο μπλεγμένο στο $|GHZ_4\rangle$, δηλαδή το $n = 4$. Αρχικά, ας εξετάσουμε την περίπτωση όπου ένας από τους κρυπτογράφους, η Alice, πλήρωσε για το δείπνο. Εάν η Alice πλήρωσε, ας πούμε, 12 €, τότε ενσωματώνει τη δυαδική αναπαράσταση του 12. Έτσι το $p_A = 1100$ ενσωματώνεται στην περιπλεγμένη κατάσταση του σύνθετου κυκλώματος. Αυτό επιτυγχάνεται εύκολα μέσω πυλών CNOT. Αν εφαρμόσουμε το γενικό κβαντικό κύκλωμα που φαίνεται στην Εικόνα 11 στο Qiskit καταλήγουμε στη συγκεκριμένη υλοποίηση που απεικονίζεται στην Εικόνα 12 παρακάτω. Μετρώντας τους καταχωρητές εισόδου τους, η Alice, ο Bob, ο Charlie και ο Dave λαμβάνουν μία από τις $2^{16} = 65536$ ισοπίθανες εξόδους.



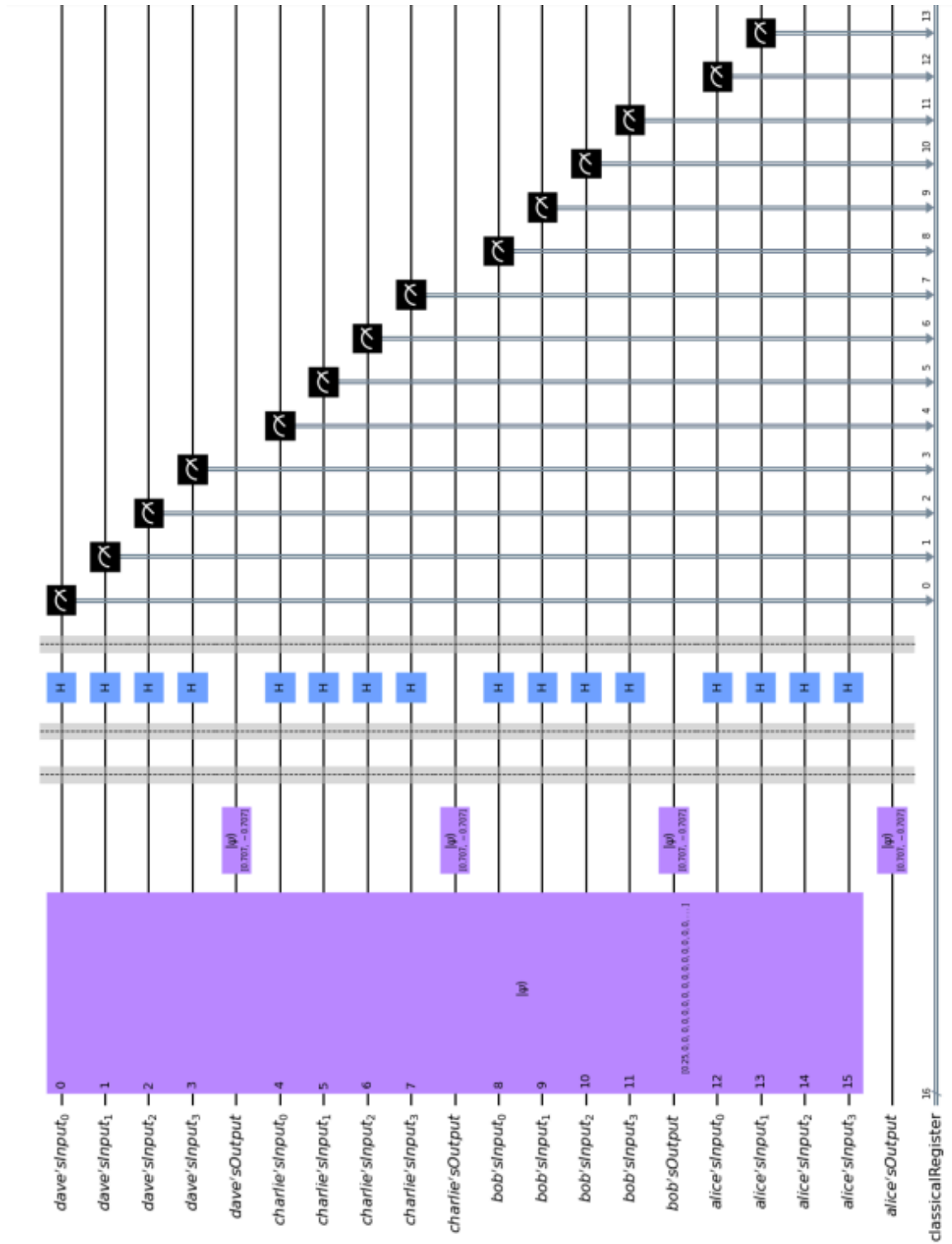
Εικόνα 12: Περίπτωση που η Alice πλήρωσε το δείπνο



Εικόνα 13: Περίπτωση που η Alice πλήρωσε το δείπνο μερικές από τις πιθανές μετρήσεις και τις αντίστοιχες πιθανότητες για το κύκλωμα

Για προφανείς τεχνικούς περιορισμούς, δεν μπορούμε να δείξουμε όλα αυτά τα αποτελέσματα. Είναι απλό όμως να ελεγχθεί ότι κάθε δυνατό αποτέλεσμα ικανοποιεί τη θεμελιώδη ιδιότητα της συσχέτισης και επαληθεύει τις εξισώσεις. Για παράδειγμα, μπορούμε να εξετάσουμε την ετικέτα της πρώτης μπάρας του ιστογράμματος, η οποία είναι 0001 1000 0111 0010. Αυτό σημαίνει ότι μετά τη μέτρηση τα περιεχόμενα του καταχωρητή εισόδου της Alice, του Bob, του Charlie και του Dave είναι $a = 0001$, $b = 1000$, $c = 0111$ και $d = 0010$ αντίστοιχα. Αυτά τα περιεχόμενα μοιράζονται μεταξύ των τεσσάρων κρυπτογράφων και τα γνωρίζουν όλοι. Τέλος, υπολογίζουν τα XOR μαζί για να αποκαλύψουν τις μυστικές πληροφορίες $p = a \oplus b \oplus c \oplus d = 0001 \oplus 1000 \oplus 0111 \oplus 0010 = 1100$. Έτσι οι κρυπτογράφοι μπορούν να εικάσουν ότι κάποιος από αυτούς πλήρωσε 12 € για το δείπνο. Το κρίσιμο είναι ότι ούτε τα μετρημένα περιεχόμενα a , b , c , d των καταχωρητών εισόδου αλλά ούτε οι τελικές ιδιωτικές πληροφορίες p μπορούν να αποκαλύψουν την ταυτότητα του κρυπτογράφου που πλήρωσε το λογαριασμό.

Ας εξετάσουμε επίσης εν συντομία την περίπτωση όπου κανένας από τους κρυπτογράφους δεν πλήρωσε το δείπνο. Σε τέτοια μια κατάσταση που όλοι οι κρυπτογράφοι ενσωματώνουν το διάνυσμα μηδενικών μπιτ στην κατάσταση εμπλοκής του σύνθετου κυκλώματος. Σε αυτή τη περίπτωση $p_A = p_B = p_C = p_D = 0000$. Το κβαντικό κύκλωμα και σε αυτή την περίπτωση είναι πολύ εύκολο να εξακριβωθεί ότι κάθε πιθανό αποτέλεσμα ικανοποιεί την ιδιότητα θεμελιώδη συσχέτιση και επαληθεύει τις εξισώσεις. Για παράδειγμα, μπορούμε να εξετάσουμε την ετικέτα της τρίτης γραμμής του ιστογράμματος, το οποίο είναι 0001 1100 1001 0100. Αυτό σημαίνει ότι τα περιεχόμενα των Alice, Bob, Charlie και ο καταχωρητής εισόδου του Dave είναι $a = 0001$, $b = 1100$, $c = 1001$ και $d = 0100$. Υπολογίζοντας $p = a \oplus b \oplus c \oplus d = 0001 \oplus 1100 \oplus 1001 \oplus 0100 = 0000$. Έτσι μπορούν να καταλήξουν πως κανένας από αυτούς δεν πλήρωσε για το δείπνο, οπότε πρέπει να ήταν ο εργοδότης τους.



Εικόνα 14: Περίπτωση που κανένας κρυπτογράφος δε πλήρωσε το δείπνο



Εικόνα 15: Περίπτωση που κανένας κρυπτογράφος δε πλήρωσε το δείπνο μερικές από τις πιθανές μετρήσεις και τις αντίστοιχες πιθανότητες για το κύκλωμα

Κεφάλαιο 5^ο

5.1 Συμπεράσματα

Η εργασία που προηγήθηκε, πραγματεύεται το πρόβλημα των κρυπτογράφων που δειπνούν. Έγινε αρχικά μία σφαιρική και λεπτομερής επεξήγηση του προβλήματος, τονίζοντας την σημαντικότητα και ανάγκη για ασφάλεια και ανωνυμία. Παρατηρήθηκαν οι δυνατότητες του αλγορίθμου και τέλος δημιουργήθηκε ένα κβαντικό πρωτόκολλο. Το συγκεκριμένο πρόβλημα εστιάζει στον τρόπο εκτέλεσης ενός ασφαλούς υπολογισμού πολλαπλών μερών. Η θεωρία παιγνίων μπορεί να μας βοηθήσει να λύσουμε διάφορα κοινωνικά και πρακτικά προβλήματα και να συμβάλουμε όσο το δυνατόν περισσότερο στην ανάπτυξη πιο βιώσιμων κοινοτήτων όπως προείπαμε. Σήμερα, περισσότερο από ποτέ η ανωνυμία είναι απαραίτητη για πολλές εργασίες διατήρησης του απορρήτου στη δικτυακή επικοινωνία. Επικοινωνίες υψηλής ασφάλειας δεν μπορούν να επιτευχθούν μόνο με ασφαλή διανομή κλειδιού. Έτσι ο David Chaum ανέπτυξε μία μέθοδο για ανώνυμη δημοσίευση μηνυμάτων. Το φάσμα της επικοινωνίας συνεχώς διευρύνεται ενώ τα όρια της ανωνυμίας και της ιδιωτικότητας σταδιακά μειώνονται. Είναι ιδιαίτερα σημαντική η διατήρησή της ιδιωτικότητας στον διασυνδεδεμένο κόσμο που ζούμε σήμερα. Εξίσου σημαντική όμως είναι και η ενημέρωση, η κατανόηση της χρησιμότητας αλλά και της αναγκαίας διατήρησης της ανωνυμίας και της ιδιωτικότητας.

Αυτή η εργασία παρουσιάζει ένα νέο πρωτόκολλο βασισμένο στην κβαντική διεμπλοκή για την επίλυση του προβλήματος των Dining Cryptographers. Το προτεινόμενο πρωτόκολλο βασίζεται σε μέγιστα μπλεγμένες πλειάδες $|GHZ_n\rangle$ για να πετύχει τον στόχο του. Το κύριο κίνητρο ήταν η προσφορά κλιμάκωσης τόσο του αριθμού των κρυπτογράφων n όσο και σε της ποσότητας της ανώνυμης πληροφορίας που μεταφέρει, μετρημένη από τον αριθμό m των κουμπιών κβαντικών που περιέχονται σε κάθε κβαντικό καταχώριση. Ο αριθμός των κρυπτογράφων n μπορεί να είναι οποιοσδήποτε αυθαίρετα μεγάλος θετικός ακέραιος. Εκτός από την κλιμάκωση στον αριθμό των συμμετεχόντων, το πρωτόκολλο SQDCP μπορεί εύκολα να κλιμακωθεί και σε όρους της ποσότητας της ανώνυμης πληροφορίας που μεταφέρει.

Αρχικά, το πρόβλημα των Dining Cryptographers αφορούσε μόνο ένα bit πληροφοριών, δηλαδή εάν ένας από τους κρυπτογράφους πλήρωσε για το δείπνο. Στο προτεινόμενο πρωτόκολλο SQDCP, ο αριθμός m των qubits που περιέχονται σε κάθε κβαντικό καταχωρητή μπορεί επίσης να είναι οποιοσδήποτε αυθαίρετα μεγάλος θετικός ακέραιος. Αυτός ο αριθμός αντικατοπτρίζει την ποσότητα των πληροφοριών που μπορεί να μεταδοθεί. Όπως για παράδειγμα, ο κρυπτογράφος που πραγματικά πλήρωσε το λογαριασμό μπορεί επίσης να αποκαλύψει πόσο κόστισε ή πότε έγινε η συναλλαγή κ.λπ. Μια ακόμη σημαντική λειτουργία του πρωτοκόλλου που παρουσιάζεται σε αυτήν την εργασία είναι η ικανότητά του να αντιμετωπίσει τόσο μια τοπικοποιημένη όσο και μια κατανεμημένη έκδοση του προβλήματος των κρυπτογράφων που δειπνούν. Ένα τοπικό σενάριο περιλαμβάνει όλους τους κρυπτογράφους να βρίσκονται μαζί στην ίδια χωρική θέση,

δηλαδή, στον ίδιο εστιατόριο, σε ένα συγκεκριμένο σημείο στον χρόνο. Το κατανεμημένο σενάριο περιλαμβάνει τους κρυπτογράφους να βρίσκονται σε διαφορετικές χωρικές θέσεις, αλλά να δειπνούν εικονικά ταυτόχρονα.

Τέλος, όσον αφορά την ουσιαστική εφαρμογή του πρωτοκόλλου, επισημαίνουμε ότι όλοι οι κρυπτογράφοι χρησιμοποιούν ιδιωτικά κβαντικά κυκλώματα που είναι πανομοιότυπα. Με αυτόν τον τρόπο επιτυγχάνεται ένα εντελώς αρθρωτό κβαντικό σύστημα, με όλα τα διακριτά μέρη να είναι ίδια. Επιπλέον, κάθε ιδιωτικό κβαντικό κύκλωμα χρησιμοποιεί μόνο τις πύλες κβαντικής τεχνολογίας Hadamard και CNOT, κάνοντάς τα εύκολα υλοποιήσιμα σε σύγχρονους κβαντικούς υπολογιστές.

Οι συνεισφορές του David Chaum έχουν επηρεάσει σημαντικά την ανάπτυξη ανώνυμων ψηφιακών νομισμάτων, ανώνυμων συστημάτων ψηφοφορίας και των τεχνολογιών ενίσχυσης της ιδιωτικής ζωής. Οι εφαρμογές τους επεκτάθηκαν σε τομείς όπως ο ασφαλής πολυμερής υπολογισμός, τα ανώνυμα συστήματα ψηφοφορίας και η ανάλυση δεδομένων για τη διατήρηση της ιδιωτικής ζωής. Ακόμη και σήμερα, τα DC-Nets συνεχίζουν να αποτελούν αντικείμενο ακαδημαϊκής έρευνας αλλά και πειραματισμού. Οι ερευνητές έχουν εργαστεί για τη βελτίωση της ασφάλειας, της επεκτασιμότητας και της πρακτικότητας των DC-Nets για να ανταποκριθούν στην αυξανόμενη ζήτηση για ασφαλή και ιδιωτική επικοινωνία σε έναν ολοένα και πιο ψηφιακό κόσμο. Παρά τη θεωρητική τους κομψότητα, οι προκλήσεις και τα τρωτά σημεία εξακολουθούν να υφίστανται και η αντιμετώπισή τους παραμένει μια συνεχής επιδίωξη στον τομέα της κρυπτογραφίας και της ασφάλειας των υπολογιστών.

Οι κβαντικοί υπολογιστές έχουν τη δυνατότητα να επιλύουν ορισμένα προβλήματα που είναι δύσκολο ή αδύνατο να επιλυθούν από τους κλασικούς υπολογιστές, όπως για παράδειγμα προβλήματα βασισμένα στην παράλληλη αναζήτηση και στον προσδιορισμό των καλύτερων λύσεων μέσα από έναν τεράστιο χώρο αναζήτησης. Παρόλο που οι κβαντικοί υπολογιστές βρίσκονται σε στάδιο ανάπτυξης, υπάρχει μεγάλο ενδιαφέρον από την επιστημονική κοινότητα για τις δυνατότητές τους στην επίλυση προβλημάτων που υπερβαίνουν την ικανότητα των κλασικών υπολογιστών. Η τεχνολογία συνεχώς εξελίσσεται, όπως και ο κόσμος μας. Κατανοώντας την σημαντικότητα και ανάγκη για ιδιωτικότητα και η ανωνυμία, κρατάμε στα χέρια μας το κλειδί για την διασφάλιση τους.

Πηγές και βιβλιογραφία

1. The dining cryptographers problem, Journal of Cryptology volume 1, pages 65–75 , David Chaum 1988
2. Footprint scheduling for Dining-Cryptographer networks, Paper 2015/1213, Anna Krasnova, Moritz Neikes, and Peter Schwabe
3. Πρωτόκολλα Ανώνυμης Επικοινωνίας: Μελέτη περίπτωσης-Το πρωτόκολλο BAR και επεκτάσεις του πρωτοκόλλου Anonymous Communication Protocols: A case study of the BAR protocol and some extensions, Μεταπτυχιακή Διατριβή, Μανδαλενάκη Μαρία-Ευφραιμία Μάρτιος 2016
4. Program Semantics and a Verification Technique for Knowledge-Based Multi-Agent Systems, Francesco Belardinelli, Ioana Boureanu, Vadim Malvone, Solofomampionona Fortunat Rajaona, Jun 2022
5. Network Protocols ANDREW S. TANENBAUM ACM Computing Surveys Volume 13 Issue 4, pp 453–489, 1981
6. GHZ correlation provides secure Anonymous Veto Protocol, Ramij Rahaman, Guruprasad Kar, 2015
7. Implementation of quantum secret sharing and quantum binary voting protocol in the IBM quantum computer, Dintomon Joy, M. Sabir, Bikash K. Behera, Prasanta K. Panigrahi, Quantum Information Processing volume 19, Article number: 33, 2020
8. Quantum-based anonymity and secure veto, Qingle Wang, Yuancheng Li, Chaohang Yu, Runhua Shi, Zhichao Zhang Quantum Information Processing volume 20, Article number: 85, 2021
9. Quantum anonymous veto: a set of new protocols Sandeep Mishra, Kishore Thapliyal, Abhishek Parakh, Anirban Pathak, Mishra et al. EPJ Quantum Technology, 2022
10. Κβαντομηχανική ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ ΚΑΙ ΜΕΘΟΔΟΙ, ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ, Στέφανος Λ. Τραχανάς, Πανεπιστημιακές εκδόσεις Κρήτης, μέρος 'Α, κεφ 5, 2019
11. Space efficient secret sharing for implicit data security, ScienceDirect, Information Sciences, Volume 181, Issue 2, 15 January 2011, Pages 335-341
12. Ch. 12. Sequential k-out-of-n systems - ScienceDirect, Handbook of Statistics, Volume 20, 2001, Pages 301-372
13. The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability, Michael Waidner, Birgit Pfizmann Universität Karlsruhe, Postfach 6980 D-7500 Karlsruhe 1, F. R. Germany, 1989
14. Detection of Disrupters in the DC Protocol, Jurjen Bos, Bert den Boer Centrum voor Wiskunde en Informatica, Amsterdam, 1990
15. Anonymous Connections and Onion Routing Paul F. Syverson, David M. Goldschlag, and Michael G. Reed Naval Research Laboratory, May 1997
16. Zero knowledge proofs of identity, Uriel Feige, Amos Fiat* and Adi Shamir Department of Applied Mathematics The Weizmann Institute of Science, 1987
17. Untraceable electronic mail, return addresses, and digital pseudonyms, David L. Chaum University of California, Berkeley, 1988

18. Mix Networks, Claudia Diaz KU Leuven, Leuven, Belgium
19. A Web Traffic Analysis Attack Using Only Timing Information, Saman Feghhi and Douglas J. Leith, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 8, AUGUST 2016
20. The Sybil Attack, John R. Douceur Microsoft Research, JR Douceur - International workshop on peer-to-peer systems, 2002
21. Understanding DDoS Attack & Its Effect In Cloud Environment Rashmi V. Deshmukha , Kailas K. Devadkar, 2015
22. Distributed Denial of Service Attack, Felix Lau, Stuart H. Rubin, Michael H. Smith, Ljiljana Trajković , 2000
23. Aggregatable Distributed Key Generation, Kobi Gurkan, Philipp Jovanovic, Mary Maller, Sarah Meiklejohn, Gilad Stern, Alin Tomescu, 2021
24. Symbolic Model Checking the Knowledge of the Dining Cryptographers, Ron van der Meyden National ICT Australia & School of Computer Science and Engineering University of New South Wales, Kaile Su† Institute of Logic and Cognition, Zhongshan University, 2004
25. Werner Heisenberg, 1901-1976, Nevill Francis Mott and Rudolf Ernst Peierls, Biographical Memoirs of Fellows of the Royal Society Volume 23, Issue 23, 1977
26. PROGRESS IN ATOMIC PHYSICS NEUTRINOS AND GRAVITATION, Charles H. Bennett, Gilles Brassard and Artur K. Ekert, JOURNAL ARTICLE, Vol. 267, No. 4, 1992
27. Cryptology Column 25 Years of Quantum Cryptography, Gilles Brassard, Claude Crépeau, ACM SIGACT News, volume 27 Issue 3, 1996
28. Information Security and Quantum Mechanics: Security of Quantum Protocols, P. Boykin, PhD thesis, University of California, 2002
29. Quantum Anonymous Transmissions, M Christandl, S Wehner, Advances in Cryptology, ASIACRYPT, pp 217–235, 2005
30. Anonymous quantum communication, Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, Alain Tapp, 2007
31. Security, probability and nearly fair coins in the Cryptographers' Cafe, Annabelle McIver , Larissa Meinicke , and Carroll Morgan, Netherlands, 2009
32. Quantum Secure Communication Based on Non Maximally Entangled Qubit Pair and Dining Cryptographers Problem, Ronghua Shi, Qian Su, Ying Guo, Moon Ho Lee, International Joint Conference of IEEE, 2011
33. The Dining Cryptographer Problem-Based Anonymous Quantum Communication via Non-maximally Entanglement State Analysis | SpringerLink, Ronghua Shi, Qian Su, Ying Guo & Dazu Huang International Journal of Theoretical Physics volume 52, pages 376–384, 2013
34. Security analysis and improvement of the dining cryptographer problem-based anonymous quantum communication via non-maximally entanglement state analysis, SpringerLink, Q Wang, K Zhang - International Journal of Theoretical Physics, 2015
35. Quantum Anonymous VSecurity analysis and improvement of the dining cryptographer problem-based anonymous quantum communication via non-maximally entanglement state analysis | SpringerLinketo protocol, Ramij Rahaman, Guruprasad Kar, 2015
36. Single Photon Sources and Single Quantum System enabled Communication, Muhammad Alley Hameedi Department of Physics, Stockholm University, p. 122, 2017
37. Anonymous Transmission of Quantum Information, J Bouda, J Sprojcar, IEEE, 2018

38. Quantum communication for sender anonymity based on single-particle with collective detection, Yuancheng Li, Chaohang Yu, QingleWang and Jiangshan Liu, *Physica Scripta*, 2021
39. Quantum anonymous veto: a set of new protocols, S Mishra, K Thapliyal, A Parakh, A Pathak - *EPJ Quantum Technology*, 2022
40. Colloquium: The Einstein-Podolsky-Rosen paradox: From concepts to applications M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, G. Leuchs, volume 81 Issue 4, *American Physical Society*, 2009
41. On the einstein podolsky rosen paradox, J. S. BELL, Department of Physics, University of Wisconsin, 1964
42. Multisetting Greenberger-Horne-Zeilinger theorem, Junghee Ryu, Changhyoup Lee, Zhi Yin, Ramij Rahaman, Dimitris G. Angelakis, Jinhyoung Lee, and Marek Żukowski *Phys. Rev. A* 89, 024103, 2014
43. Efficient Quantum Algorithms for GHZ and W States, and Implementation on the IBM Quantum Computer, Diogo Cruz, Romain Fournier, Fabien Gremion, Alix Jeannerot, Kenichi Komagata, Tara Tosić, Jarla Thiesbrummel, Chun Lam Chan, Nicolas Macris, Marc-André Dupertuis, Clément Javerzac-Galy, *Advanced Quantum Technologies*, Volume 2, Issue 5-6, 2019
44. Quantum Secret Aggregation Utilizing a Network of Agents, Michael Ampatzis, Theodore Andronikos, 2023
45. A single quantum cannot be cloned, W. K. Wootters, W. H. Zurek, *Nature* 299, 1982