

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

185,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



# Overlay Security: Quantum-Safe Communication over the Internet Infrastructure

*Shlomi Dolev*

## Abstract

The need for a quantum-safe Internet is emerging, and this is a great opportunity to re-examine the legacy of public key infrastructure. There is a need for perspective on the evolution of cryptography over the years, including the perfect information-theoretical secure schemes and the computationally secure schemes, in particular. There is also a need to examine the evolving Internet infrastructure to identify efficient design and secure cryptographic schemes over the existing Internet infrastructure. A combination of overlay security, blockchain, and Merkle trees with Lamport's signatures offers just such an easily implementable quantum-safe Internet.

**Keywords:** public key infrastructure, post-quantum cryptography, secret sharing, blockchain, Lamport signatures

## 1. Introduction

Securing the digital world is essential as critical infrastructures are based on communicating with remote computers. The trust in the computer network is based on having a secure and authenticated communication. The change in social activity, where the big four companies Google, Amazon, Facebook, and Apple (GAFA) influence many aspects in modern society implies the need for secure computer and network infrastructures. The past interest in quantum cryptography has grown significantly in recent years. National Institute of Standards and Technology (NIST) authors wrote an overview on the subjects in 2009 [25], and the activity expanded dramatically, having dedicated conferences on the subject [27]. The most challenging component of Internet security that needs to be considered is the replacement of the existing asymmetric encryption scheme, namely, to replace an RSA [29]. For this there are several candidates: lattice-based cryptography (e.g., shortest vector problem, closest vector problem), code-based cryptography (e.g., McEliece, Niederreiter), and more (see, e.g., [24]). The second challenging task is a replacement for signature scheme; here hash-based Lamport's one-time signature together with the Merkle tree is believed to address that need (see [39] for an overview). The integration of the post-quantum cryptographic ingredients into a complete infrastructure is also challenging (as we detail in the sequel).

We present a design for quantum-safe communication over the existing Internet infrastructure. No hardware changes are required, only software updates over the

heterogeneous Internet architecture. Different aspects of the solution are presented in the sequel.

## **2. Quantum computing today**

The emergence of quantum computers is a fact [12]; beyond the commercial non-universal commercial quantum computer of several thousand qubits (quantum bits) of D-Wave [10], IBM commercializes 50 qubits quantum computers [18]. The quantum computer race leads to exponential growth in the number of qubits, where in 2018 Intel presented 49 qubits quantum computer [19] and Google announced 72 qubits computers [16]. In addition, several startups including Rigetti announced a 36 qubits quantum computer [28] and a quantum processing unit (QPU) (see also Ion Q [20] and QCI [32]).

Many quantum computers restrict the qubits that participate as inputs for quantum gate operations and employ qubit teleportation to allow quantum gate operations over non-neighboring quantum bits, e.g., [36, 8]. The advance in techniques for producing entangled qubits and teleportation [37, 38] may assist in using several quantum computers to cooperate on a task by teleporting qubits from one to another, thus building a virtual quantum computer with the needed qubits for the task. In particular, for breaking the asymmetric encryption schemes in use almost immediately, much earlier than estimated.

## **3. Quantum algorithms**

Shor's algorithm [35], designed for quantum computers, changed the way modern cryptography and Internet security are captured. New algorithms for quantum computers are frequently invented [31, 4].

Computationally secure cryptography is based on the unproven assumption of the existence of one-way function, a function that can be computed easily but is hard to be inverted. The risk that an algorithm that breaks a considered one-way function will be found always exists, e.g., [1]. Even one-way functions proposed for post-quantum cryptosystems are at risk of the discovery of new efficient inverse algorithms. One famous example of an open problem for decades is the primality test that had no polynomial deterministic algorithm, until just such an algorithm was found [2].

## **4. Perspective on encryption**

The asymmetric encryption schemes, proposed by Merkle [23], Diffie and Hellman [9], and Rivest et al. [29], revolutionized cryptography. The idea to use computational tasks in order to establish a symmetric key started with the suggestion of Merkle to use computation puzzles. Merkle's puzzle scheme started with Alice choosing at random many computation puzzles, possibly hashed random numbers (with tuned lengths) each concatenated with a sequence number, such that Bob is able to randomly choose one of the puzzles and reverse this number in reasonable time. Then, Bob sends a few of the bits of the revealed random number back to Alice, identifying the puzzle Bob decided to solve. Both Alice and Bob will be using the unrevealed bits of the solved puzzle as their symmetric key. Eve on the other hand will not know which of the puzzles was chosen by Bob, will likely have to solve many puzzles before identifying the puzzle randomly chosen by Bob, and

revealing the symmetric key they use. Later Diffie and Helman and then Rivest, Shamir and Adelman suggested more efficient schemes based on number theory assumptions.

Asymmetric encryption enabled the creation of a symmetric key among communicating parties over tapped communication links [23, 9] and is even able to identify the intervention of malicious parties in the communication [29]. The identification of such malicious parties was due to the capability of [29] to sign certificates that monolithically associated a public key with the entity identity description to which the public key belongs. The signature was issued by a trusted third party, the certificate authority. This public key infrastructure is the de facto security infrastructure today, securing Internet activity, including military, governmental, social, financial, and, in fact, all activities in the Internet.

Thus, the appearance of quantum computers and fitting quantum algorithms, which may break the basic mathematical foundations of [9, 29], has great implications. Post-quantum cryptosystems [26] are examined, e.g., [15], replacing the believed to be one-way functions that are currently used by other functions, which are also believed to be one-way functions. Provable perfect encryption does exist, namely, encryption based on the classical one-time pad [34], as long as the one-time pad is a true random sequence. True random sequences are possibly produced by the use of quantum effects, e.g., [17].

Another difficulty in using one-time pad is the need to share the one-time pad prior to communication. The one-time pad can be shared prior to communication by physically delivering a copy of the one-time pad. Distribution of a one-time pad to many users may risk the loss or duplication of one copy of the one-time pad, nullifying the secrecy of the encryption.

Quantum key distribution [3] suggests using quantum bits superposition for detecting a tapper in the communication of random bits; however this scheme can only be used in direct links of at most 100 km. Recently, [22, 30] succeeded in using satellites and quantum bits entanglement to share a key over longer distances. This key can be viewed as a short one-time pad, as the rate of the received random bits is limited. One difficulty is the need to mobilize the symmetric key received from the satellite in one satellite receiver to the actual place the key should be used and the fact that the key authenticates the satellite receiver, but may not yield the identification of other users.

## 5. Overlay security

Occasionally, one needs to send a credit number electronically, sending one email with the first digits of the credit card and then another email with the rest. Still, the email servers and the Internet server providers may act as a man in the middle and tap in, capturing part or all of the digits of the credit card. It is possible to send a random string (one-time pad) via WhatsApp (owned by Facebook) and the bitwise x-or of the credit card with the random string via Gmail. On one hand, this resembles sending entangled bits in two channels. On the other hand, just like content distribution networks (CDN), e.g., Akamai, that uses overlay network of the Internet ISPs as their source for extra reliability and services, *overlay security* uses the accumulated secrecy, authenticity, and identification of the diverse capabilities of the communication channels, applications, and protocols.

The maturity and evolvment of the Internet technology enabled the CDN company to use the Internet infrastructure as a playground for delivering contents at will. In the last decades, more and more communication channels identify, authenticate, and secure the communication between entities. Email, SMS, push

notifications, and messengers (WhatsApp, Facebook Messenger, Skype, Snapchat, LINE, LinkedIn, Telegram, Weibo, Slack, etc.) form logical secured channels. Each of the channels, even if they use the same physical channel, implies already built trust in the identification and authentication of the entity communicated through the channel. Moreover, the maintenance and repair of the security of each channel are guaranteed by the channel supplier. Still, each channel may act as a man-in-the-middle accumulating the communications transmitted through the channel servers. The use of a random one-time pad over channels nullifies information accumulated by the server of each channel.

This is the current playground suggested to be used by the overlay security concept, to create a symmetric key based on perfectly secure information-theoretical secure scheme, namely, quantum-safe replacements for asymmetric encryption. In addition, the security of new channels can be obtained inductively by the security of existing channels, employing them to create a random shared key for the new channel.

## **6. Redundancy and secret sharing**

Overlay security uses several channels and random numbers to obtain a high level of confidence in identification, authentication, and secrecy, a level implied by all the used channels. However, if one of the channels, say Android push notification, is not available (possibly in China), then the communication is blocked. Secret sharing [33, 5] schemes imply a tunable threshold for the number of channels needed to reconstruct the secret. Shamir secret sharing is based on polynomials over a finite field, where each participant, in our case channel, receives one point of the polynomial and the secret is the free coefficient of the polynomial. For example, if the polynomial is a random linear function with the secret being the free coefficient, any two participants/channels can reveal the secret, but a single participant/channel has absolutely no information on the secret. Polynomials with greater degrees used over many channels may imply more trust in the aggregated identification, authentication, and secrecy while allowing several of the channels to be blocked or even to corrupt the information conveyed through them.

## **7. Authentication bay**

Identifying and authenticating an entity in the physical world by the digital world are the biggest challenges in information security. Having secured robust and reliable identification and authentication of a person, an institute, a company, or a device are the first chain in securing digital representation and processing of information. For example, a bank client needs to be identified and authenticated for performing digital operations on their account. The linkage between the physical entity and the digital representation of an entity allows processing of digital and physical assets in the computers and the Internet.

The need for identification and authentication of an entity started before computers exist. Certificates signed by trusted authorities were used by governments to monitor the activity of the society, to enable law and order. Certificates used to authenticate entities were and are part of business infrastructure. The procedures used to authenticate an entity were and are defined by societies. A newborn child does not need a certificate to be born, obviously when the child is born at home. Moreover, a newborn may not have a certificate with identifying details, including identifying number, without enforcing society's regulations. Some societies pay



parents of newborns when they register the child, an attractive payment that almost ensures that newborn will be registered.

In the scope of people, biometric identifications, by using fingerprints, face recognition, iris, and palm, are becoming standard. The identification starts with the registration process in which there is a need to identify and link the person with the biometric information recorded during the registration process. This is an error-prone process that encapsulates the challenge in the authentication bay. There is a need for a trusted authority (e.g., government, banks) or trusted manufacturer (e.g., Apple, Samsung) to collect biometric samples while authenticating the person by other means (e.g., driving license, passport) and digitally link them in a digital record. The actual biometric sampling would be better stored in a form of one-way hash, just like passwords; otherwise, they can be copied and used without the actual involvement of the biometric identification device (e.g., fingerprint reader, camera). Keeping the biometric database private and secure is another challenging task, as once a biometric data is leaked to untrusted entities, the search for confusing biometric data to fake identification can be feasible.

Moreover, current technologies for identifying a person biometrically are not perfect. Biometric identifications have false positives, when a non-authorized person is identified as another authorized person and performs an action they are not allowed to perform. Biometric identifications also have false negatives, when a person is not correctly identified as the person registered and cannot perform actions they are authorized to take. DNA identification will also be possible in the near future; still identical twins share the same DNA.

Having unique attributes is only one facet of the identification and authentication process, as there should be trust in the digital identification and authorization process. For example, consider a program identifying a person having DNA linked to the registered digital record of a person with a certain identity number, and then send an approval on the check. There are several questions to ask on the program actions. Does the program have the means to verify that the input device (e.g., fingerprint, camera) observed the person, or is it a mock-up? Were the input device compromised and a replay attack performed? Another question is whether the program verified the collected data from the input device against the right registration record or was maybe hacked to output approval with no actual checking. This chain of trust is yielded from the trust in the biometric device producer.

In the framework of the Internet of Things (IoT), the identification of things is even more challenging, as devices and items tend to be produced identically. Vehicle networking is now emerging, and the means to identify a car (by another car) is one of the basic ingredients that the trust vehicles have in inter-vehicle communication. Recent works suggested to monolithically sign the car description (e.g., driving license, color, and brand) and the public key associated with the car description in one monolithically signed certificate. The signing authority can be the governmental vehicle registration [10]. The car description should allow for a unique identification by means of an out-of-band channel such as a camera. Note that the identity of a device can be challenging; for example, consider two cars of the same model; if one exchanges the doors of these cars, does that alter the identity of the car? What about changing the engine? And so on.

Another possibility for identifying IoT devices requires trust in the producer, which embeds a unique serial identification number. A unique identifying numbers in unaltered barcode, QR code, RFID, and ROM that can be used as part of the identification and authentication process.

The cloud and blockchain infrastructures enable a new opportunity for representing each person, entity, and organization by a digital avatar. The avatar, being a digital historical record of events, digital assets, and procedures/functions defined

to be executed upon given events. The identity linkage between the avatar and the physical entity accumulates trust over time, letting the physical entity monitor the possibility of identity theft, as recorded actions for the avatar can be examined by the actual entity represented by the avatar.

Fake avatars already exist, and they are represented by profiles in social networks, Facebook, LinkedIn, etc., and may interact with persons as bots do. This is one light form of identity theft where there may be no real entity linked to the avatar. Identity theft has been a trust problem in societies from the years of the bible where Jacob represented himself as Esav to Itzhak. Nowadays, the remote actions enabled in the digital interaction make the identity theft phenomena a major concern.

In some cases, e.g., cryptocurrency, anonymity is an important aspect, as cash money, or digital money, appearing in an account had better not carry its history. Thus every coin or bill having an identical value. Blockchain associates an account with a public key, where the matching private key is held by the owner of a wallet. This somewhat anonymous linkage between an entity and digital assets is only by the means of the private key. The vulnerability of such a solution erases the famous cases of lost/stolen private keys.

Private keys are also a means to sign transactions binding the holder (even in court) to the transaction; thus, the way to secure the private key, possibly in enclaved memory, is very important. Moreover, having a quantum-safe signature is a must, as the bidding is a very important aspect of the trust infrastructure, and if the bidding is broken, deniability of actions is possible. A client that transferred a million dollars from their account may rightly claim that someone else preformed the transfer to this account on their behalf, with no permission.

Another aspect of the authentication bay is the usage of passwords. The illusion that passwords can contribute to the security of the communication is misleading. Many of the passwords are subject to dictionary attacks. Users tend to forget and manage passwords in vulnerable storage, leading to many password lists being sold on the black net. The typical password renewal procedure involves password reset invocation and a temporal password sent through email. Such single channel security is another weak chain in the security infrastructure, a weak chain that may dramatically benefit using the multichannel security and authenticity yielded from the overlay security concept.

## **8. Distributed trust, blockchain, beyond social identity**

Certificate authorities are a major source of trust for the public key infrastructure. The certificate authority identifies an entity and signs a certificate that associates a public key with the entity description. The history of the Internet testifies to examples of the vulnerability of the trust associated with certificate authorities. For example, private keys that were used to sign certificates were stolen, and significant percentage of the Internet were not secure [7, 37]. Recently, Estonia, Canada, and other countries started to use distributed trust among several trusted and heterogeneous entities as a source for identification. Such distributed trust is enabled by blockchain technology [14]. Identity, verified by several trusted entities, possibly including governmental, financial, and notary entities, among others, is logged in a distributed fashion.

To communicate with an entity, a search of several participants in the distributed ledger returns contact information for the entity. Using the communication channels in the contact information and secret sharing enables the creation of a symmetric key. The newly created random symmetric key may, in turn, be used in

employing efficient advanced encryption standard (AES) over a single communication link. Unlike the functions used in asymmetric encryption, AES is crafted, rather than relying on number theory challenge, and believed to imply quantum-safe encryption. The key length should still be carefully selected to accommodate the quadratic speedup of search of Grover's algorithm [13]. Note that secure hash algorithms (SHA) are crafted, similarly to AES, and are also believed to be quantum safe, reducing the risk of finding an efficient number theory solution for a natural problem, such as discrete logarithm.

## 9. Quantum-safe signatures

The ability to perform a transaction in an undeniable fashion over the Internet is important, especially when financial transactions are executed. Lamport's one-time signature [21] is not tied to a particular one-way function. Thus, Lamport's signature can employ secure hash function, such as SHA. The use of Merkle trees with multiple private keys in the leaves (leaves that can also be produced by several nested hash functions) and the root of the tree serving as the public key yields an efficient, quantum-safe signature scheme.

In greater detail, the private key is an array of pairs of random numbers. The first random number pair is used to sign the first bit of the message; the second random number pair is used to sign the second bit of the message and so on. Note that, for reasons of efficiency, typically, the hash of the message is signed instead of signing the longer original message. Each random number in each pair is hashed (in fact, any other one-way functions can be used instead of hash), and the resulting array of hashed values serve as the public key. Once the public key is published in a way that links the signing entity to the public key, the construction can serve in signing any single binary string, a string that may be the hash of the original message to be signed. The actual signature is a sequence of random numbers from the private key, one from each pair, attached to the message to be signed. The first random number in the signature is the first (second) random number in the first pair if the first bit to be signed is zero (one, respectively). Similarly, the second random number in the signature is the first (second) random number in the second pair if the first bit to be signed is zero (one, respectively) and so on. Since the array of numbers in the public key are results of one-way hash function, no one but the producer of the public key is able (under standard computation assumptions) to know and expose the right portions of the private key. Hence, the signature is binding.

Still, the need to identify an entity and associate the entity to the public key is the most challenging stage in authentication. Lamport's signature essentially requires such an identification process for each signature. Fortunately, many of Lamport's signatures may share a single public key, which consists of the roots of Merkle tree, one tree for each position of a random number in each pair of the private keys. The first positions, representing the private keys used to sign a zero value of the strings, consist of random numbers, such that such numbers belonging to the first two private keys are concatenated and hashed to yield the value of their common parent in the first Merkle tree. Similarly, for the second positions, the two random numbers are concatenated and hashed to yield the value of their parent in a second Merkle tree and so on. The parent of any such two leaves is concatenated to the hash obtained from the next two random numbers that reside in the same positions in the next two private keys and hashed yielding the value of the grandparent of these four values and so on.

A signature will use one of the leaves, where each leaf is connected by a path to the roots of Merkle trees, one tree for each random number in the leaf. When using



a leaf to sign, the appropriate random number in each pair of the leaf is exposed together with the missing hash values that are concatenated in each level of the tree. Thus allowing the verifier to check that indeed any revealed random number leads to the corresponding value of the Merkle tree root public value.

The root value may be stored with the contact information that resides in the blockchain. The contact information with the public value of the root will be added to the distributed ledger after the blockchain participants verify and approve the identity of the contact information and root value owner.

## 10. Conclusion

Overlay security combined with distributed trust forms an immediate quantum-safe alternative to the public key infrastructure. The existing technologies enable (1) the use of multi-logical/multi-physical channels to create a random secret at will, (2) use of the blockchain distributed ledger as a replacement for single point of failure trusted authority, and to (3) produce quantum-safe signatures.

The suggested changes can gradually, seamlessly, and smoothly emerge over the existing infrastructure without the need to restructure any component of the Internet.


## Author details

Shlomi Dolev

Ben-Gurion University of the Negev & Secret Double Octopus Ltd, Israel

\*Address all correspondence to: [dolev@cs.bgu.ac.il](mailto:dolev@cs.bgu.ac.il)

## IntechOpen

© 2019 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Adrian D, Bhargavan K, Durumeric Z, Pierrick G, Green M, Halderman JA, et al. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In: CCS'15. 2015
- [2] Agrawal M, Kayal N, Saxena N. PRIMES is in P. *Annals of Mathematics*. 2004;**160**(2):781-793
- [3] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Vol. 175. New York; 1984. p. 8
- [4] Bernstein JB, Heninger N, Lou P, Valenta L. Post-quantum RSA. *International Workshop on Post-Quantum Cryptography*. 2017. pp. 311-329. A Preview of Bristlecone, Google's New Quantum Processor. Available from: <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>
- [5] Blakley GR. Safeguarding cryptographic key. In: *Managing Requirements Knowledge, International Workshop on (AFIPS)*. Vol. 48. 1979. pp. 313-317
- [6] Canada's New Partnership with Estonia is a Major Digital Government Milestone 28/5/18 Max Greenwood More can be found here at Techvibs: <https://techvibes.com/2018/05/29/canadas-new-partnership-with-estonia-is-a-major-digital-government-milestone>
- [7] News article, the real security issue behind the Comodo hack. CSO from IDG By Roger A. Grimes. Available from: <https://www.csoonline.com/article/2623707/hacking/the-real-security-issue-behind-the-comodo-hack.html>
- [8] Center for quantum computation & communication technology, Australian research council center of excellence. Available from: <http://www.cqc2t.org>
- [9] Diffie W, Hellman ME. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976;**22**(6):644-654
- [10] Dolev S, Panwar N, Segal M. Certifying vehicle public key with vehicle attributes. 2014. US US9769658B2
- [11] D-wave the quantum computing company. Available from: <https://www.dwavesys.com/d-wave-two-system>
- [12] Fedorov AK, Kiktenko E, Lvovsky AI. Quantum computers put blockchain security at risk. *Nature*. 2018;**7732**(465):563-663
- [13] Grover LK. A fast quantum mechanical algorithm for database search. In: *STOC*. 1996. pp. 212-219
- [14] Gheorghiu V, Gorbunov S, Mosca M, Munson M. Quantum Proofing the Blockchain. *Blockchain Research Institute: University of Waterloo*; 2017
- [15] Google Tests Post-Quantum Crypto Quantum Computing Will Shred Current Crypto Systems, Experts Warn Jeremy Kirk • July 11, 2016. Available from: <https://www.bankinfosecurity.com/google-adds-quantum-computing-armor-to-chrome-a-9253>
- [16] Available from: <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>
- [17] Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. *Reviews of Modern Physics*. 2017;**89**(1):015004
- [18] IBM Raises the Bar with a 50-Qubit Quantum Computer. MIT technology review. Available from: <https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer>

- [19] 2018 CES: Intel advances quantum and neuromorphic computing research. 2018. Available from: <https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/#gs.9ud403>
- [20] A true quantum leap. Introducing the first commercial trapped ion quantum computer. Available from: <https://ionq.co>
- [21] Lamport L. Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98. SRI International Computer Science Laboratory. 1979
- [22] Liao SK, Cai WQ, et al. Satellite-to-ground quantum key distribution. *Nature*. 2017;**549**:43-47
- [23] Merkle R. Secure communications over insecure channels. *Communications of the ACM*. 1978;**21**(4):294-299
- [24] Niederhagen R, Waidner M. Practical post-quantum cryptography. White Paper, Fraunhofer Institute for Secure Information Technology SIT. August 18, 2017
- [25] Perlner RA, Cooper DA. Quantum resistant public key cryptography: A survey. ID Trust. 2009. pp. 85-93
- [26] Post-quantum cryptography. Available from: [https://en.wikipedia.org/wiki/Post-quantum\\_cryptography](https://en.wikipedia.org/wiki/Post-quantum_cryptography)
- [27] Information about Post-quantum cryptography. Available from: <https://pqcrypto.org>
- [28] QPU Specifications. Rigetti Technical Publications. Available from: <https://www.rigetti.com/qpu>
- [29] Rivest RL, Shamir A, Adelman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978;**21**(2):120-126
- [30] Ren J-G et al. Ground-to-satellite quantum teleportation. *Nature*. 2017;**549**:70-73
- [31] Quantum Algorithm Zoo. Details about the Quantum algorithm Zoo, by Stephen Jordan. Available from: <https://math.nist.gov/quantum/zoo/>
- [32] Building quantum computers designed to scale published in QCI at: <https://www.quantumcircuits.com>
- [33] Shamir A. How to share a secret. *Communications of the ACM*. 1979;**22**(11):612-613
- [34] Shannon C. Communication theory of secrecy systems. *Bell System Technical Journal*. 1949;**28**(4):656-715
- [35] Shor WP. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*. 1999;**41**(2):303-332
- [36] Available from: <http://www.sussex.ac.uk/physics/iqt/index.html>
- [37] 23,000 HTTPS certs will be axed in next 24 hours after private keys leak Trustico, DigiCert come to blows as browsers prepare to snub Symantec-brand SSL by, By John Leyden 1 Mar 2018. Available from: [https://www.theregister.co.uk/2018/03/01/trusticodigicert\\_symantec\\_spat/](https://www.theregister.co.uk/2018/03/01/trusticodigicert_symantec_spat/)
- [38] Zomorodi-Moghadam M, Houshmand M, Houshmand M. Optimizing teleportation cost in distributed quantum circuits. *International Journal of Theoretical Physics*. 2018;**57**(3):848-861
- [39] Zych MD. Quantum safe cryptography based on hash functions: A survey [master's thesis]. Department of Informatics, University of Oslo. 2018