LATTICE BASED COIN FLIPPING PROTOCOL

Literature Review

Arinta Primandini Auza
arintaprimandini.auza@student.uts.edu.au

Table of Contents

1. Introduction

Cryptography has been an important tool for thousands of years to hide secret messages and transmit them safely to a receiver. In today's digital world cryptography is essential to secure our data and transaction. The security of our cryptographic primitives relies on hardness assumption of some mathematical problems. The most used problems are factorization and discrete logarithm problem. However, in 1994 Shor (Shor 1994) shows that a quantum computer can break these problems efficiently which pose a threat to most of today's public key cryptosystems. For many years researchers have been studying post-quantum cryptography which refers to a cryptography that is safe against an attacker with a large quantum computer.

This project is dealing with an important cryptographic protocol which is a *coin flipping protocol* for an honest majority with some additional properties: Guaranteed Output Delivery (GOD), quantum resistant, and publicly verifiable. The protocol starts with N participants who pick a secret randomly that will be combined to obtain a randomness beacon. In order to achieve the guaranteed output delivery property, we will use a *publicly verifiable secret sharing scheme* that allows any set of participants with a certain threshold to reconstruct the secret. A quantum-safe *encryption* and *commitment* scheme will also be involved to ensure the security and to verify that the shares and the secret are valid. The schemes that will be used are *lattice-based* since they are believed to be quantum-safe. Another method that will be applied is *zero knowledge proof (ZKP)* protocol that will allow us to verify the consistency between the encrypted message and commitment. Since the computation is done on the encrypted messages, the schemes are required to be *fully homomorphic* so that the messages will not be destroyed after the computation.

2. Coin Flipping Protocol

Coin flipping protocol was first introduced by (Blum 1983) that involves two players, Alice and Bob, who want to flip a coin by telephone. Bob will guess the result and Alice will flip the coin. He wins if he guesses correctly and lose otherwise. The protocol guarantees that the result of coin flipping done by Alice is random and that Alice cannot cheat by declaring a different result than the side she obtained. A more general protocol where more players participate in this protocol require a public bulletin board to post the messages and verify the result. However, if half or more players are corrupted, adversary can bias the output or abort the protocol anytime.

A protocol by (Benny et al. 1985) guarantees the output through threshold verifiable secret sharing (VSS) if the majority of players are honest. However, this protocol requires interactions between the dealer and the players which challenges scalability. One solution is to use publicly verifiable secret sharing scheme (PVSS) which allows anybody to verify the validity of shares and reconstruct secrets without requiring any interaction between dealers and players. However, current PVSS construction has high computational overheard problem where verification of secrets requires $O(nt)$ exponentiations.

A recent work of (Cascudo & David 2017) introduced SCRAPE, a coin flipping protocol for an honest majority that improves the number of exponentiations to $O(n)$ which is obtained from the fact that sharing a secret by using Shamir secret sharing is equivalent to encoding the secret with

Reed-Solomon code. The protocol is using a publicly verifiable secret sharing scheme (PVSS) that can be instantiated by the Random Oracle Model (ROM) under Decisional Diffie Hellman (DDH) assumption or by the plain model under Decisional Bilinear Square (DBS) assumption. Basically, the protocol runs through these four phases below:

- **Setup:** Each participant generates their secret key, public key and post the public key to the bulletin board.
- **Distribution:** Each participant samples a random secret and create n shares of the secret through a secret sharing protocol where n is the number of participants. They then publish the encrypted version and commitment of each shares in the bulletin board.
- **Verification:** Each participant verifies that the shares they received are consistent with the commitment and that they are indeed part of the secret.
- **Reconstruction:** All participants reveal their secrets and if there are at most $n - t$ participants drop out of the protocol, the remaining participants reveal their shares and they reconstruct each of the quitters' secret by reconstruction algorithm according to the secret sharing protocol that the protocol uses.

Both the commitment and encryption schemes of this protocol are relied on DDH or DBS assumptions which we know to be unsecure against quantum attack. Therefore, we need to study a quantum secure scheme that can be implemented in this protocol.

3. Lattice Based Cryptography

Since quantum computer might be a reality in the near future, a number of studies have been conducted to construct quantum-safe cryptographic primitives such as encryption and commitment schemes. Currently, lattice-based cryptography is the most promising "post-quantum" replacement for factorization and discrete logarithm problem that we use as hardness assumption in so many cryptographic schemes today.

Definition 1. Given n linearly independent vectors $b_1, b_2, \cdots b_n \in \mathbb{R}^m$. A *lattice* Λ generated by them is defined as

$$\Lambda = \mathcal{L}(b_1, b_2, \cdots b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \middle| \; x_i \in \mathbb{Z} \right\}$$

where n is the rank of the lattice and m is the dimension of the lattice. The lattice is called *full-ranked* lattice if $n = m$.

Definition 2. Let Λ be a lattice of rank n. For $i \in \{1, \cdots, n\}$ we define the i^{th} successive minima as

$$\lambda_i = inf \left\{ r | dim \left(span\left(\Lambda \cap \bar{B}(0, r) \right) \right) \geq i \right\}$$

where $\bar{B}(0, r) = \{x \in \mathbb{R}^m | \; \|x\| < r\}$ is the closed ball of radius r around 0.

3.1. Several Lattice Problems

a. Closest Vector Problem (CVP)

Search CVP: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ and a target vector $t \in \mathbb{Z}^m$, find $x \in \mathbb{Z}^n$ that minimizes $\|\mathcal{B}x - t\|$.
Optimization CVP: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ and a target vector $t \in \mathbb{Z}^m$, find $dist(t, \mathcal{L}(\mathcal{B}))$.
Decisional CVP: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$, a target vector $t \in \mathbb{Z}^m$ and $r \in \mathbb{Q}$, determine whether $dist\big(t, \mathcal{L}(\mathcal{B})\big) \leq r$ or not.

The decisional variant of CVP is known to be in **NP.** Since there is a reduction from subset-sum problem which is known to be **NP-complete**, decisional CVP is also **NP-complete**. A solution to the search variant implies solution to the optimization variant and a solution to the optimization variant gives solution to the decisional variant, hence Decisional SVP $\leq$ Optimization SVP $\leq$ Search SVP.

Search CVP$_\gamma$: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ and a target vector $t \in \mathbb{Z}^m$, find a vector $v \in \mathcal{L}(\mathcal{B})$ such that $\|v - t\| \leq \gamma \cdot dist(t, \lambda_1(\mathcal{L}(\mathcal{B})))$.
Optimization CVP$_\gamma$: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ and a target vector $t \in \mathbb{Z}^m$, find d such that $d \leq dist(t, \lambda_1(\mathcal{L}(\mathcal{B}))) \leq \gamma \cdot d$.
GapCVP$_\gamma$: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$, a target vector $t \in \mathbb{Z}^m$ and $r \in \mathbb{Q}$,
YES = $dist(t, \lambda_1(\mathcal{L}(\mathcal{B}))) \leq r$.
NO = $dist(t, \lambda_1(\mathcal{L}(\mathcal{B}))) > \gamma \cdot r$.

b. Shortest Vector Problem (SVP)

Search SVP: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ find a vector $v \in \mathcal{L}(\mathcal{B})$ such that $\|v\| = \lambda_1(\mathcal{L}(\mathcal{B}))$.
Optimization SVP: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ find $\lambda_1(\mathcal{L}(\mathcal{B}))$.
Decisional SVP: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ and $r \in \mathbb{Q}$, determine whether $\lambda_1\big(\mathcal{L}(\mathcal{B})\big) \leq r$.

Search SVP$_\gamma$: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ find a vector $v \in \mathcal{L}(\mathcal{B})$ such that $v \neq 0$ and $\|v\| \leq \gamma \cdot \lambda_1(\mathcal{L}(\mathcal{B}))$.
Optimization SVP$_\gamma$: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ find d such that $d \leq \lambda_1(\mathcal{L}(\mathcal{B})) \leq \gamma \cdot d$.
GapSVP$_\gamma$: Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$ and $r \in \mathbb{Q}$,
YES = $\lambda_1(\mathcal{L}(\mathcal{B})) \leq r$.
NO = $\lambda_1\big(\mathcal{L}(\mathcal{B})\big) > \gamma \cdot r$.

It is easy to see that GapSVP$_\gamma \leq$ Optimization SVP$_\gamma \leq$ Search SVP$_\gamma$, however it is not known if Search SVP$_\gamma \leq$ Optimization SVP$_\gamma$. The exact version of SVP is proven to be **NP-hard** in the l_∞-norm (Emde Boas 1981), whereas in the other norms it is shown to be **NP-hard** for randomized reductions (Ajtai 1998; Khot 2005).

In (Goldreich et al. 1999) we can see that GapSVP$_\gamma \leq$ GapCVP$_\gamma$ by Cook reduction, however whether there exists a deterministic Karp reduction from GapSVP$_\gamma$ to GapCVP$_\gamma$ is still an open question.

c. Shortest Independent Vectors Problem (SIVP)

Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$, find n independent vectors $v_1, v_2, \cdots, v_n$ such that $\|v_1\| \leq \lambda_n(\mathcal{L}(\mathcal{B}))$ for all $i \in \{1,2,\cdots,n\}$.

d. Bounded Distance Decoding (BDD)

Given a lattice basis $\mathcal{B} \in \mathbb{Z}^{m \times n}$, $t \in \mathbb{R}^m$, and $d \in \mathbb{R}$ where $d < \lambda_1(\mathcal{L}(\mathcal{B}))/2$ such that $dist(t, \mathcal{L}(\mathcal{B})) \leq d$, find the unique $v \in \mathcal{L}(\mathcal{B})$ closest to t. This is equivalent to finding $e \in t + \mathcal{L}(\mathcal{B})$ such that $\|e\| \leq d$.

e. Short Integer Solution (SIS)

Given $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ consists of m uniformly random column vectors $a_i \in \mathbb{Z}_q^n$. Find a nonzero vector $x \in \mathbb{Z}^m$ such that:

a) $\|x\| \leq \beta$
b) $\boldsymbol{A}x = 0 \in \mathbb{Z}_q^n$

where $\sqrt{n \log q} \leq \beta < q$ and $m \geq n \log q$.

f. Learning With Errors (LWE)

Search LWE : Find a secret $\boldsymbol{s} \in \mathbb{Z}_q^n$ given a sequence of 'approximate' random inner products

$$b_1 = \langle \boldsymbol{s}, a_1 \rangle + e_1$$
$$b_2 = \langle \boldsymbol{s}, a_2 \rangle + e_2$$
$$\vdots$$
$$b_m = \langle \boldsymbol{s}, a_m \rangle + e_m$$

where $a_1, a_2, \cdots, a_m$ are random vectors in $\mathbb{Z}_q^n$ and $e_1, e_2, \cdots, e_m$ are randomly chosen from Gaussian distribution χ over $\mathbb{Z}$ with width $\alpha q > \sqrt{n}$.

Decision LWE : Distinguish $(\boldsymbol{A}, b^T = \boldsymbol{s}^T\boldsymbol{A} + e^T)$ from uniform $(\boldsymbol{A}, b^T)$.

There are several reasons for believing that LWE problem is hard: (1) The best known algorithms to solve this problem runs in exponential time, (2) It is a generalization of LPN problem which is believed to be hard, (3) LWE is hard if we assume the hardness of some other lattice problems such as quantum hardness of GapSVP_γ and SIVP_t (Regev 2009). Peikert (Peikert 2009) also proved similar results for classical hardness assumption of $\text{GapSVP}_{\zeta,\gamma}$. The search and decision variants of LWE are known to be equivalent as shown by (Regev 2009).

We know that LWE ≤ SIS from this observation: If we find a short vector z such that $\boldsymbol{A}z = 0$, then we can find $b^T z = \mathbf{s}^T\boldsymbol{A} + e^T z$ from $b^T z = \mathbf{s}^T\boldsymbol{A} + e^T z$. If $(\boldsymbol{A}, b^T)$ is from LWE distribution then $b^T z$ is short, otherwise $b^T z$ is rather well spread.

3.2. Public Key Cryptosystem using LWE

One example of public key cryptosystem using LWE introduced by (Regev 2009) is parametrized by integers n as the security parameter, m as the number of equations, q as modulus, and a real number $\alpha > 0$ as noise parameter. The cryptosystem is defined as follows:

Private key: A vector $\mathbf{s}$ chosen uniformly from $\mathbb{Z}_q^n$.
Public key: m samples $(\mathbf{a}_i, b_i)_{i=1}^m$ from the LWE distribution with secret s, modulus q, and error parameter α.
Encryption: Suppose the X is the message that we want to encrypt where $X = x_1 x_2 \cdots$, $x_i \in \mathbb{Z}_2$. Choose a random set S uniformly among 2^m subsets of $[m]$.

$$y_i = Enc(x_i) = \begin{cases} \left(\sum_{i \in S} \mathbf{a}_i, \sum_{i \in S} b_i\right) & \textbf{if } x_i = 0 \\ \left(\sum_{i \in S} \mathbf{a}_i, \left\lfloor \frac{q}{2} \right\rfloor \sum_{i \in S} b_i\right) & \textbf{if } x_i = 1 \end{cases}$$

Decryption: The decryption function is defined as

$$x_i = Dec(y_i) = \begin{cases} 0 \ \textbf{if } b - \langle \mathbf{a}, \mathbf{s} \rangle \text{ is closer to 0 than to } \left\lfloor \frac{q}{2} \right\rfloor \bmod q \\ 1 \quad \textbf{otherwise} \end{cases}$$

4. Commitment Schemes

Commitment schemes allow us to commit to a certain value and keep it hidden to other people with the intention to reveal the committed value at a later time. The schemes are designed such that we cannot alter the value after the commit phase, which is called the *binding* property of the protocol. In addition, the scheme must also have *hiding* property which means any adversaries will not be able figure out the message that is being committed.

In general, a commitment scheme consists of the following three algorithms :

Keygen : a PPT-algorithm that outputs public parameter PP.
Commit : a PPT-algorithm that on input PP and a message x, will output a random number r and $c = Com(x, r)$. The value c is called *the commitment*.
Open : a PPT-algorithm that on input PP, a message x, and values c, r will output a bit b.

As stated earlier, factorization-based cryptographic schemes are not considered secure by quantum attack and hence researchers are studying post-quantum cryptography especially lattice-based cryptography. Earlier work by (Kawachi, Tanaka & Xagawa 2008) constructs a string commitment scheme based on SIS assumption. This protocol requires the message space to be restricted to vectors of small norm, otherwise the binding property is lost. Another work by (Jain et al. 2012) based the hiding property on LPN and additionally they use zero knowledge proof (ZKP) to prove general relations on bit strings. In (Xie, Xue & Wang 2013), the scheme is based on Ring-LWE and they build Σ-protocol from it. The main drawback of these schemes is the ZKP has a non-negligible soundness error, hence they require many iterations to have full security.

In order to tackle this problem, (Benhamouda et al. 2015) propose a more efficient commitment scheme and ZKP which allows us to commit to a vector and the commitment is only a constant

factor larger than the message. In addition, the soundness error is negligible for a single iteration. This protocol is based on ring-LWE for the binding and hiding property. (Baum et al. 2018) Improves this protocol where the commitment can be done to vectors over polynomial rings. The binding property is based on module-LWE whereas the hiding property is based on module-SIS.

5. Zero Knowledge Proof

Zero knowledge proof protocols allow one party to convince another party that they know a certain secret x without revealing any information concerning this value. The party who knows the value x is called the *prover* while the other party is called *verifier*. The protocol must satisfy the following properties:

- **Completeness:** the honest verifier will be convinced by an honest prover if the statement is true.
- **Soundness:** if the statement is false, there is no dishonest prover who can convince the honest verifier except with some negligible probability.
- **Zero-knowledge:** if the statement is true, there is no honest verifier who knows anything about the secret except the fact that the statement is true.

6. Secret Sharing Schemes

Secret sharing is a method that allows a dealer to distribute shares of secret to a number of players where some subset of authorized players can reconstruct the secret together. It was first introduced by (Blakley 1979; Shamir 1979), motivated by the problem of secure information storage. Currently, there are many applications of secret sharing schemes including: secure multiparty computations, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer.

A secret sharing scheme should meet the following requirements:

- **Correctness:** Secret can be reconstructed by any authorized set of players.
- **Perfect Privacy:** Every unauthorized set of players cannot learn anything about the secret from the shares.

7. Homomorphic Encryption

Fully homomorphic encryption is considered as the 'holy grail' of cryptography because it allows any operations on encrypted information without destroying the original information. It opens the door to many new capabilities in the cloud-centric, data-driven world. Numerous practical applications have been proposed such as consumer privacy in advertising, medical applications, data mining, financial privacy, and forensic image recognition (Armknecht et al. 2015).

The idea of homomorphic encryption was first suggested by Rivest, Adleman and Dertouzos (Rivest, Adleman & Dertouzos 1978) in 1978. However, before Gentry's breakthrough in 2009

several candidates were partially homomorphic such as Paillier cryptosystem (Paillier 1999) which is homomorphic under addition where

$$Enc(m_1 + m_2, pk) = Enc(m_1, pk) + Enc(m_1, pk)$$

Another public key cryptosystem introduced by ElGamal (Elgamal 1985) is known to homomorphic under multiplication where

$$Enc(m_1 \cdot m_2, pk) = Enc(m_1, pk) \cdot Enc(m_1, pk)$$

Gentry (Gentry 2009a) showed that fully homomorphic encryption can be realised by modifying a somewhat homomorphic scheme to be bootstrappable and introducing squashing step to reduce the noise in the ciphertext. His cryptosystem used ideals over polynomial rings which security relies on the hardness of problems on ideal lattices.

Gentry's breakthrough has been used by many researchers as prototype to develop more efficient schemes. The first generation of FHE schemes such as (Gentry 2009b; Gentry & Halevi 2011; Smart & Vercauteren 2010) are based on ideal lattice and approximate GCD problem. The second generation such as (Brakerski, Gentry & Vaikuntanathan 2014; Brakerski & Vaikuntanathan 2014a) use LWE and ring-LWE assumption, and also develop new techniques such as modulus reduction, key-switching, and re-linearization. The third generation (Brakerski & Vaikuntanathan 2014b; Gentry, Sahai & Waters 2013) is based on ring-LWE and approximate eigenvalues with some new technique which is called flattening.

8. Conclusion

SCRAPE (Cascudo & David 2017) is a good source that gives framework for developing an honest majority coin flipping protocol. The next step is to modify several methods in the protocol especially the classical encryption and commitment schemes in order to obtain a quantum safe protocol. A good candidate for commitment scheme is the work of (Baum et al. 2018) whereas we need to study further about fully homomorphic encryption scheme.

References

Ajtai, M. 1998, 'Shortest vector problem in L2 is NP-hard for randomized reductions', *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 10-9.

Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C.A. & Strand, M. 2015, 'A guide to fully homomorphic encryption', *IACR Cryptography ePrint Archive*, p. 1192.

Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S. & Peikert, C. 2018, 'More efficient commitments from structured lattice assumptions', *Lecture Notes in Computer Science*, vol. 11035, pp. 368-85.

Benhamouda, F., Krenn, S., Lyubashevsky, V. & Pietrzak, K. 2015, 'Efficient zero-knowledge proofs for commtiments from learning with errors over rings', *Computer Security - ESORICS*, pp. 305-25.

Benny, C., Goldwasser, S., Silvio, M. & Baruch, A. 1985, 'Verifiable secret sharing and achieving simultaneity in the presence of faults', *Annual Symposium on Foundations of Computer Science*, pp. 383-95.

Blakley, G.R. 1979, 'Safeguarding cryptographic keys', *Proc. of the 1979 AFIPS National Computer Conference*, vol. 48, pp. 313-7.

Blum, M. 1983, 'Coin flipping by telephone a protocol for solving impossible problems', *ACM SIGACT News*, vol. 15, no. 1, pp. 23-7.

Brakerski, Z., Gentry, C. & Vaikuntanathan, V. 2014, '(Leveled) Fully homomorphic encryption wihtout bootstrapping', *ACM Transactions on Computation Theory (TOCT)*, vol. 6, no. 3, pp. 1-36.

Brakerski, Z. & Vaikuntanathan, V. 2014a, 'Efficient fully homomorphic encryption from (standard) lwe', *SIAM Journal of Computing*, vol. 43, no. 2, pp. 831-71.

Brakerski, Z. & Vaikuntanathan, V. 2014b, 'Lattice-based FHE as secure as PKE', *Proceedings of the 5th conference on innovations in theoretical computer science*, pp. 1-12.

Cascudo, I. & David, B. 2017, 'Scrape: Scalable randomness attested by public entities', *Applied Cryptography and Network Security*, pp. 537–56.

Elgamal, T. 1985, 'A public key cryptosystem and a signature based on discrete logarithms', *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-72.

Emde Boas, P.V. 1981, 'Another NP-complete problem and the complexity of computing short vectors', *Technical report, University of Amsterdam, Department of Mathematics*.

Gentry, C. 2009a, 'A fully homomorphic encryption scheme', Stanford University, ProQuest Dissertations and Theses.

Gentry, C. 2009b, 'Fully homomorphic encryption using ideal lattices', *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, pp. 169-78.

Gentry, C. & Halevi, S. 2011, 'Fully homomorphic encryption without squashing using depth-3 arithmetic circuits', *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pp. 107-9.

Gentry, C., Sahai, A. & Waters, B. 2013, 'Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based', *Lecture Notes in Computer Science*, vol. 8042, no. 1, pp. 75-92.

Goldreich, O., Micciancio, D., Safra, S. & Seifert, J.P. 1999, 'Approximating shortest lattice vectors is not harder than approximating closest lattice vectors', *Information Processing Letters*, vol. 71, no. 2, pp. 55-61.

Jain, A., Krenn, S., Pietrzak, K. & Tentes, A. 2012, 'Commitments and efficient zero-knowledge proofs from learning parity with noise', *Lecture Notes in Computer Science*, vol. 7658, pp. 663-80.

Kawachi, A., Tanaka, K. & Xagawa, K. 2008, 'Concurrently secure identification schemes based on the worst-case hardness of lattice problems', *Lecture Notes in Computer Science*, vol. 5350, pp. 372-89.

Khot, S. 2005, 'Hardness of approximating the shortest vector problem in lattices', *Journal of the ACM (JACM)*, vol. 52, no. 5, pp. 789-808.

Paillier, P. 1999, 'Public-key cryptosystems based on composite degree residuosity classes', *Lecture Notes in Computer Science*, vol. 1592, pp. 223-38.
Peikert, C. 2009, 'Public-key cryptosystems from the worst-case shortest vector problem', *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, pp. 333-42.
Regev, O. 2009, 'On lattices, learning with errors, random linear codes, and cryptography', *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1-40.
Rivest, R.L., Adleman, L. & Dertouzos, M.L. 1978, 'On data banks and privacy homomorphisms', *Foundations of Secure Computation*, pp. 169-77.
Shamir, A. 1979, 'How to share a secret', *Communications of the ACM*, vol. 22, pp. 612-3.
Shor, P.W. 1994, 'Algorithms for quantum computation: discret logarithms and factoring', *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124-34.
Smart, N.P. & Vercauteren, F. 2010, 'Fully homomorphic encryption with relatively small key and ciphertext sizes', *Lecture Notes in Computer Science*, vol. 6056, pp. 420-43.
Xie, X., Xue, R. & Wang, M. 2013, 'Zero knowledge proofs from ring-LWE', *Lecture Notes in Computer Science*, vol. 8257, pp. 57-73.