UNIVERSITY OF TARTU
Institute of Computer Science
Computer Science Curriculum

Kristiine Saarmann

Quantum-Secure Coin Toss Protocol Using Collapse-Binding Commitments

Bachelor's Thesis (9 ECTS)

Supervisor: Dominique Unruh, PhD

Tartu 2018

Quantum-Secure Coin Toss Protocol Using Collapse-Binding Commitments

Abstract:

Commitment schemes are a widely used cryptographic primitive that is used in a number of important applications, from zero-knowledge proofs to secure computation. In a classical setting, there are canonical security definitions that are proven to provide security against computationally bounded adversaries. Yet, there are no canonical security definitions that are provably secure and easy to use in the quantum case. One such definition for the quantum setting was proposed in [Dominique Unruh, *Computationally Binding Quantum Commitments*, EUROCRYPT 2016]. This paper presents the classical security definitions of commitment schemes, as well as the alternatives in the quantum setting. The advantages of the proposed security definition, called "collapse-binding" are presented, with an example use case in a quantum-secure coin toss protocol.

Keywords:

Quantum cryptography, commitment scheme, coin toss protocol

CERCS:

P175, Informatics, systems theory

Kvantturvaline mündiviske protokoll kasutades kollaps-siduvaid kinnistusskeeme

Lühikokkuvõte:

Kinnitusskeem on laialt kasutatav krüptograafiline primitiiv, mida kasutatakse ulatuslikult erinevates rakendustes, alates teabetust tõestustest turvalise arvutamiseni. Klassikalises krüptograafias on kasutusel definitsioonid, mis on tõestatult arvutuslikult turvalised. Seevastu kvantkrüptograafias ei leidu kanooniliselt kasutatavaid kinnitusskeemide turvadefinitsioone, mis oleksid tõestatavalt turvalised ning lihtsalt kasutatavad. [Dominique Unruh, *Computationally Binding Quantum Commitments*, EUROCRYPT 2016] esitles definitsiooni, mida kutsutakse „kollaps-siduvaks“, mida saaks kasutada turvadefinitsioonina kvantkinnistusskeemides. Selles töös tutvustatakse nii klassikalise krüptograafia kinnistusskeemides kasutatavaid turvadefinitsioone kui ka kvantkrüptograafia alternatiive. Kollaps-siduvate protokollide eelised eelnevate definitsioonide ees tuuakse välja, illustreerides kollaps-siduvate protokollide kasutusvõimalust kvant-turvalises mündiviske protokollis.

Võtmesõnad:

Kvantkrüptograafia, kinnistusskeem, mündiviske protokoll

CERCS:

P175, Informaatika, süsteemiteooria

Acknowledgements

I would like to thank my supervisor Professor Dominique Unruh, as without his help and guidance I could not have written a thesis on such a complex topic. I could always count on him to explain any concepts I was confused about and give valuable insight into the discussed topics.

Contents

Introduction

Commitment schemes are one of the most important primitives in cryptography. They are used in numerous applications such as zero-knowledge protocols, coin toss protocols and secure computation. A lot of the existing constructions are based on security against computationally bounded adversaries, while their security against quantum adversaries is unknown. Thus, finding a good protocol for quantum-secure commitment schemes is one of the open questions in quantum cryptography.

A commitment scheme is a protocol between two parties: the sender and the receiver. The protocol consists of two phases: the commit phase and the open phase. During the commit phase, the sender commits to a value. During the open phase, the sender sends the opening information to reveal, which value they committed to.

This thesis provides an overview of security definitions used in classical commitment schemes: binding property (the sender should not be able to change his mind about the sent message), hiding property (the recipient should not learn anything about the received message) and completeness (the recipient should always positively verify, given correct opening information). Then, the security properties for the quantum setting are introduced.

While hiding property and completeness have straightforward adaptations to the quantum setting, the definition of binding property cannot be easily adapted. This thesis gives an overview of the definitions proposed so far. A property called “collapse-binding”, as proposed in [1], is introduced as a good quantum analogue for binding property in the classical sense. The advantages of this definition include its parallel composability (the only definition with such property so far) and compatibility with short commitments.

The first chapter explains the mathematic and cryptographic preliminaries that are necessary for the comprehension of this paper. Presented are some definitions with illustrative examples. The first chapter is mainly meant for readers without a good working knowledge of quantum cryptography.

The second chapter gives some background on commitment schemes and explains in detail the security definitions needed in the classical case. It gives a formal definition of perfect completeness, hiding and biding property.

The third chapter presents some of the prior definitions that have been proposed for binding commitment schemes in the quantum case. Here, the definition of collapse-binding commitments is introduced. Additionally, formal definitions of perfect completeness and hiding property are given for the quantum setting.

The fourth chapter proposes a quantum-secure coin toss protocol using the definition of collapse-binding commitments to showcase a possible use case. The security definitions for the protocol are given along with two theorems.

The fifth chapter gives a conclusion as well as an overview of any further work planned for the future.

1. Quantum cryptography

This chapter gives an introduction to frequently used definitions and notations in quantum cryptography. The following concepts are necessary for understanding the protocols introduced further in the paper. A more thorough background on quantum computing can be found in [1] and in [2].

1.1 Notations

In this thesis only the finite-dimensional vector spaces over the complex numbers are considered. Such vector spaces are members of Hilbert spaces, hereon denoted by $\mathcal{H}$. To denote quantum states, the Dirac notation is used. That is, notation $|\cdot\rangle$ corresponds to a vector, and notation $\langle\cdot|$ to its complex conjugate transpose. Their inner products are written as $\langle \cdot | \cdot \rangle$. The length of a quantum system is denoted by $\|\cdot\|$. Notation $\oplus$ is used to indicate XORing and $\otimes$ to indicate tensoring.

1.2 Quantum states

In classical computation, every bit has a determined state – 0 or 1. In quantum computation, a quantum bit, or a qubit for short, can be in state $|0\rangle$ (corresponding to the classical state 0), in state $|1\rangle$ (corresponding to the classical state 1), or in superposition between the two:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Here, α and β are complex numbers with $|\alpha|^2$ representing the probability that $|\Psi\rangle$ yields the result 0 after measurement, and $|\beta|^2$ representing the probability that $|\Psi\rangle$ yields the result 1. A qubit is always of norm 1:

$$\||\Psi\rangle\| = \sqrt{|\alpha|^2 + |\beta|^2} = 1.$$

Quantum states can also be written in the vector form. The two qubits in the two-dimensional Hilbert space $\mathbb{C}^2$ corresponding to the classical states 0 and 1 are defined as

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Generalizing to higher-dimensional systems, any n-dimensional quantum state $|\Psi\rangle = \sum_{i=1,}^{n} \alpha_i |i\rangle$ can be written as a vector $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{C}^n$ of length $\||\Psi\rangle\| = \sqrt{|\alpha_1|^2 + \cdots + |\alpha_n|^2} = 1$.

1.3 Computational basis

Since Hilbert space is finite-dimensional, it is possible to assume a set of basis states and represent all the other states through them. In most cases, some orthonormal bases are assumed (representing the classical possibilities of the system) which are called the computational basis. Canonically, the vectors from the vector space $\{0,1\}^n$ form an orthonormal basis for quantum states.

Definition 1.1. Consider a Hilbert space $\mathcal{H}$ of dimension 2^n. A set of 2^n vectors $B = \{|b_m\rangle\} \subseteq \mathcal{H}$ is called an orthonormal basis for $\mathcal{H}$ if

$$\langle b_n | b_m \rangle = \delta_{n,m} \; \forall b_m, b_n \in B$$

and every $|\psi\rangle \in \mathcal{H}$ can be written as

$$|\psi\rangle = \sum_{b_n \in B} \psi_n \, |b_n\rangle, \text{for some } \psi_n \in \mathbb{C}.$$

The values of ψ_n satisfy $\psi_n = \langle b_n | \psi \rangle$, and are called the 'coefficients of $|\psi\rangle$ with respect to basis $\{|b_n\rangle\}$'.

A quantum system of length n has 2^n basis vectors, thus, a representation in the ket-form is often used instead of the vector-form. For example, a two-qubit system in $\mathbb{C}^4$ would be represented by four basis states:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$|01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix},$$

$$|11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

1.4 Density operators

To understand density operators, it is important to first define quantum ensembles.

Definition 1.2. Consider a quantum system that is a linear combination of pure states $|\Psi_i\rangle$ with respective probabilities p_i. $E = \{|\Psi_i\rangle, p_i\}$ shall be called a quantum ensemble with

1. $\forall i : |\Psi_i\rangle \in \mathcal{H}$,
2. $\forall |\Psi_i\rangle : \||\Psi_i\rangle\| = 1$,
3. $\forall i : p_i \geq 0$,
4. $\sum_i p_i = 1$.

The density operator, in turn, allows for a more convenient way of describing mixed states.

Definition 1.3. Consider a quantum ensemble $E = \{|\Psi_i\rangle, p_i\}$. The density operator of the quantum ensemble, also known as the density matrix, is defined as

$$\rho_E = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|.$$

Intuitively, a density operator is a matrix containing information about the probabilities of the outcomes of physical experiments. The simplest example of a density operator is the density operator of a pure state:

$$\rho = |\Psi\rangle\langle\Psi|.$$

In case of a two-dimensional quantum system $|\Psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, the corresponding density operator would be of form

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}I,$$

where I is the identity matrix.

1.5 Measurements

Measurement is a quantum operation that converts a quantum state into a probabilistic classical state. Provided that the chosen bases are orthonormal, it is possible to perform measurements with respect to any basis. Naturally, using different computational basis leads to different probabilities and different post-measurement states. In a classical system, a measurement would be merely an observation of state, whereas a measurement in the quantum setting disturbs the states.

An important case of measurements is called a projective measurement. Projective measurements are performed using orthogonal projectors.

Definition 1.4. An orthogonal projector is an operator Q that satisfies $Q^2 = Q$ and $Q^\dagger = Q$.

Definition 1.5. The trace of a matrix $M \in \mathbb{C}^{n\times n}$ is the sum of its diagonal elements:

$$tr(M) = \sum_i M_{ii}.$$

Definition 1.6. A projective measurement on a Hilbert space $\mathcal{H}$ is defined by a set of projectors $M = \{Q_1, \dots, Q_n\}$, where Q_i are orthogonal projectors that sum to the identity operator on $\mathcal{H}$:

$$\sum_i Q_i = I_{\mathcal{H}}.$$

Let $E = \{|\Psi_i\rangle, p_i\}$ be an ensemble over $\mathcal{H}$. When measuring the state described by E with M, the outcome j has probability

$$Pr(j) = \sum_i p_i \left\| Q_j |\Psi_i\rangle \right\|^2 = tr Q_j \rho_E.$$

If the measurement outcome is j, then after the measurement the system is in state

$$PMS(j) = \frac{p_i \left\| Q_j |\Psi_i \rangle \right\|^2}{\sum_i p_i \left\| Q_j |\Psi_i \rangle \right\|^2} = \frac{Q_j \rho_E {Q_j}^\dagger}{tr Q_j \rho_E {Q_j}^\dagger}.$$

2. Classical commitment schemes

This chapter introduces the concept of commitment schemes and gives formal definitions to the required properties in the classical setting.

2.1 Preliminaries

An algorithm is considered to be polynomial-time if its runtime is always bounded by a polynomial in its input length. The letter η denotes the security parameter and notation 1^{η} corresponds to a bit-string of 1-s of length η. The latter is used as an input in algorithms for making them run in polynomial-time. A function $\mu(n)$ is negligible if for any polynomial function $poly(\cdot)$ and for a large enough n:

$$\mu(n) \leq \frac{1}{poly(n)}.$$

Notation $a \leftarrow A(1^{\eta})$ is used to denote running some algorithm A with the security parameter in its input and assigning the value to a. $(c, u) \leftarrow commit(1^{\eta}, m)$ denotes running an algorithm $commit$ that returns a commitment-opening pair for some message m. Algorithm $verify(1^{\eta}, c, m, u)$ returns if m is a valid opening of c with u. Abbreviation MSP_{η} denotes a message space of valid messages for the algorithm $commit$, dependent on the security parameter η.

As a technicality, it is assumed to be possible to find triples (c, m, u) with $\Pr[verify(1^{\eta}, c, m, u) = 1] = 1$ in polynomial-time in η. Hereon, abbreviation "iff" corresponds to "if and only if".

2.2 Commitment schemes

A commitment scheme is a two-party protocol consisting of two phases: the commit phase and the open phase. The purpose of the protocol is to allow one party to commit to a value in such a way that the other party does not learn anything about the committed value before the open phase. At the same time, the commitment should be binding, meaning, the sender should not be able to change his mind about the message after making the commitment.

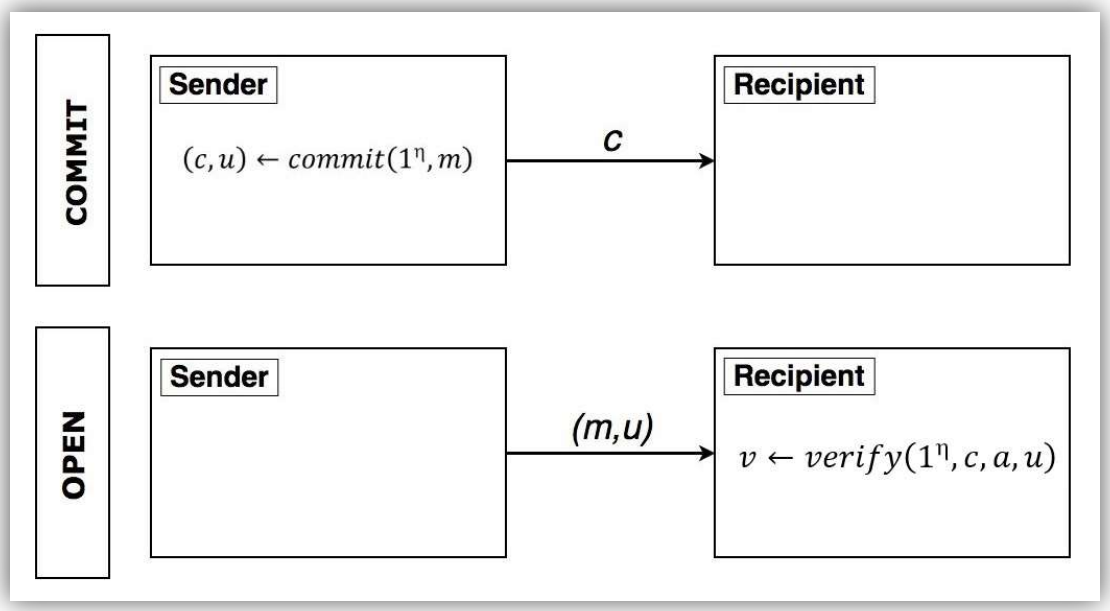

Figure 2.1: A commitment scheme.

In the commit phase, the first party, called the sender, runs a polynomial-time algorithm $commit$ to create a commitment-opening pair for some message m. Then, he sends the commitment value c to the second party, called the recipient. In the open phase, the sender sends the message m and the opening information u to the recipient. After that, the recipient runs a deterministic polynomial-time algorithm $verify$ to check if u is a valid opening of c for m. A graphical description is shown on Figure 2.1.

A commitment scheme has to satisfy the following requirements:

1. Binding property: After the commit phase, the sender should not be able to change, which value to open the commitment to.

2. Hiding property: After the commit phase, the recipient should not be able to gain any knowledge about the committed message.

3. Completeness: After the commit phase, given the correct opening information of the commitment, the recipient should always respond with positive verification.

2.3 Binding property

A formal definition of the binding property in the classical setting is given in [3]. Adapted to notations:

Definition 2.1. A commitment scheme $(commit,\ verify)$ is computationally binding iff for any polynomial-time algorithm A, any security parameter η, the following is negligible:

$$\Pr[verify(1^{\eta}, c, m, u) = 1 \wedge verify(1^{\eta}, c, m', u') = 1 \wedge m \neq m' : (c, m, u, m', u') \leftarrow A(1^{\eta})].$$

To put it differently, a commitment scheme is computationally binding if and only if for any polynomial-time algorithm A, there exist no triples (c, m, m') with $m \neq m'$ such that both m and m' are a valid opening for c with more than negligible probability.
Analogously:
Definition 2.2. A commitment scheme $(commit,\ verify)$ is statistically binding iff for any polynomial-time algorithm A, any security parameter η, the following is negligible:

$$\Pr[verify(1^{\eta}, c, m, u) = 1 \wedge verify(1^{\eta}, c, m', u') = 1 \wedge m \neq m' : (c, m, u, m', u') \leftarrow A(1^{\eta})].$$

In case of computational binding, the commitment scheme is only provably secure against polynomial-time adversaries. In case of statistical binding, the computational power of the adversary is unlimited.

2.4 Hiding property

Adapted from the definition of statistical hiding in [4]:

Definition 2.3. A commitment scheme $(commit, verify)$ is computationally hiding iff for any polynomial-time algorithm A, any security parameter η and any messages $m_0, m_1 \in MSP_{\eta}$, the probability $|p_0 - p_1|$ is negligible, where

$$p_i := Pr[b = 1 : (c, u) \leftarrow commit(1^{\eta}, m_i), b \leftarrow A(1^{\eta}, c)].$$

To put it another way, a commitment scheme is computationally hiding if and only if for any polynomial-time algorithm A and any messages m_0 and m_1 from the message space, the probability distribution of guessing the committed value is negligibly close to a uniformly random distribution.

Analogously:

Definition 2.4. A commitment scheme $(commit, verify)$ is statistically hiding iff for any algorithm A, any security parameter η and any messages $m_0, m_1 \in MSP_\eta$, the probability $|p_0 - p_1|$ is negligible, where

$$p_i := Pr[b = 1 : (c, u) \leftarrow commit(1^\eta, m_i), b \leftarrow A(1^\eta, c)].$$

Similarly to the binding property, the difference between computational hiding and statistical hiding is the computational bounds of the algorithm A in the former case.

2.5 Completeness

The definition of completeness in the quantum case from [3] can be directly applied to the classical case. Adapted to notations:

Definition 2.5. A commitment scheme $(commit, verify)$ has perfect completeness iff for all m ∈ MSP_η:

$$Pr[verify(1^\eta, c, m, u) = 1 : (c, u) \leftarrow commit(1^\eta, m)] = 1.$$

In other words, a commitment scheme has perfect completeness if and only if for all valid messages from the message space and all valid commitment-opening pairs generated by the algorithm $commit$, the algorithm $verify$ always returns 1.

3. Quantum commitment schemes

This chapter introduces the security properties used in quantum commitment schemes. An overview of previously proposed security definitions for the quantum setting is given, with a special focus on collapse-binding commitments.

3.1 Preliminaries

An algorithm is considered to be quantum-polynomial-time if it is a quantum algorithm and its runtime is always bounded by a polynomial in its input length. A commitment scheme composes sequentially if the security of the protocol is preserved when multiple commitments are executed one after another. A commitment scheme composes in parallel if the security of the protocol is preserved when multiple commitments are synchronously executed in parallel with all the rounds performed at the same time.

A trivial superposition is a superposition of states where one state occurs with probability 1 and others with probability 0. A non-trivial superposition is a mixed state where two or more states have probability greater than 0. A function f is called a trapdoor function if $f(x)$ is computable in polynomial time, but it is computationally infeasible to find the inverse of $f(x)$, unless some secret information, called the trapdoor, is given.

3.2 Prior approaches

When trying to adapt the definition of binding property to the quantum case, obvious approaches fail. In the classical setting, the binding property requires the adversary to be unable to open a commitment to more than one message, except with negligible probability. As shown in [5], in the quantum case, it is possible to construct a commitment scheme that is secure with respect to the definition of classical-style binding, yet, the adversary would be able to open a commitment to any message of his choosing. Namely, the commitment is a quantum state in a non-trivial superposition, therefore, measuring it makes it collapse, thereby destroying the state. Consequently, such a scheme would be considered classically binding, yet useless in real-life applications.

[6] first proposed an information-theoretically hiding and binding commitment scheme using quantum communication. However, [7] proved this construction to be faulty by showing the impossibility of information-theoretically hiding and binding commitments.

To ensure the security of the binding property, a number of protocols ([6], [7], [8], [9], [10]) have used the definition of sum-binding. Informally, sum-binding considers a bit-commitment scheme with $p_0 + p_1 \leq 1 + negligible$, where p_b is the probability that the adversary successfully opens the commitment to message b. However, such construction is specific to bit commitments and has no good generalization to the string commitment case (further discussion can be found in [9]). Furthermore, it is not clear whether the protocol composes in parallel or even sequentially. Consequently, sum-binding commitments are currently not used as a sub-protocol in any known protocol.

[9] introduced an oblivious transfer protocol that proposes a security property called CDMS-binding. This definition uses a family of functions, dependent on the particular use case, to specify in which way the commitment should be binding. Although CDMS-binding commitments have been used as a part of larger protocols, its composability by itself is not known.

Another possible construction of commitment schemes is using perfectly-binding commitments. Informally, perfectly-binding commitments require there to exist no such tuple (c, m, u, m', u'), that $verify(1^{\eta}, c, m, u) = 1$, $verify(1^{\eta}, c, m', u') = 1$ and $m \neq m'$. Notably, this definition requires the length of the commitment to be at least as long as the message, thus making the protocol less efficient. In addition, as shown in [7], perfectly-binding commitments cannot be statistically hiding. An example of a perfectly-binding commitment scheme can be found in [11].

[12] introduced the notion of UC-secure commitments. UC-secure commitments are constructed using some additional setup (e.g. a common reference strings) and a trapdoor function to allow the simulator to extract the committed message. As a result, UC commitments require stronger computational assumptions, tend to have a higher complexity and be less efficient. Additionally, depending on the setup used, UC commitments might not allow for short commitments (e.g. when using a common reference strings as a setup).

[13] proposed a computationally binding commitment scheme for string commitments. This protocol is based on the definition of Q-binding commitments. Namely, for an adversary A and a predicate Q, the adversary has at most $p_{ideal} + negligible$ probability of winning in a "betting game" over an adversary who uses the definition of perfect commitments. The protocol, however, comes with a number of drawbacks. Firstly, the only known way for

constructing statistically hiding Q-binding commitments requires using an equivocal trapdoor. Consequentially, this protocol would require stronger computational assumptions. In addition, it is not clear (or proven) if this construction could be used for parallel composition as it is mostly specialized for the commit-and-choose paradigm.

A property called DFRSS-binding was proposed in [14] to provide security in the bounded quantum storage model, meaning, in a setup where the adversary's quantum memory is limited to a fixed amount of qubits. The definition is specific to the bit commitment case with a possibility of extending the definition to bit-strings. Informally, in case of a DFRSS-binding commitment, given the classical part of the state of both the sender and the recipient, it is possible to extract what bit the sender will open to. Due to the fact that this definition was originally intended to be used in the bounded quantum storage model, some modifications are needed to allow usage in the unbounded storage model. As a result, DFRSS-binding commitments cannot be statistically hiding, nor do they allow for commitments that are shorter than the message (when used outside the bounded quantum storage model).

3.3 Binding property

In order to construct post-quantum secure commitment schemes, [3] proposed a property called "collapse-binding". This definition seems to provide the same properties in the quantum setting as computationally-binding property does in the classical setting. In particular, collapse-binding commitments are provably composable, can be used with statistical hiding, and allow for short commitments.

As proposed in [3]:

Definition 3.1. For algorithms A, B consider the following games:

$$Game_1\colon\ (S, M, U, c) \leftarrow A(1^{\eta}), \qquad m \leftarrow M_{comp}(\mathrm{M}), \qquad b \leftarrow B(1^{\eta}, S, M, U, c)$$

$$Game_2\colon\ (S, M, U, c) \leftarrow A(1^{\eta}), \qquad\qquad\qquad\qquad b \leftarrow B(1^{\eta}, S, M, U, c)$$

Here S, M, U are quantum registers. $M_{comp}(\mathrm{M})$ is a measurement of M in the computational basis.

We call an adversary (A, B) valid if $Pr[verify(1^{\eta}, c, m, u) = 1] = 1$ when running $(S, M, U, c) \leftarrow A(1^{\eta})$ and measuring M, U in the computational basis to obtain m, u.

A commitment scheme is collapse-binding iff for any quantum-polynomial-time valid adversary (A, B), the difference $|Pr[b = 1: Game_1] - Pr[b = 1: Game_2]|$ is negligible.

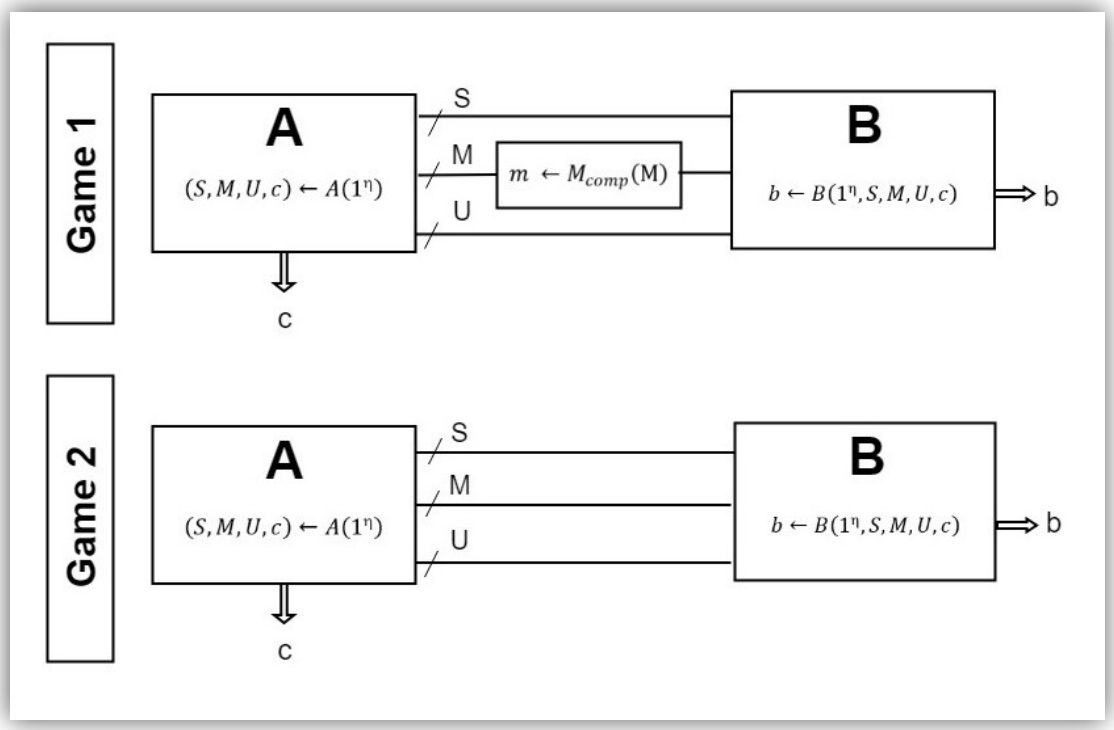

Figure 3.1: Collapse-binding commitments.

Collapse-binding commitments require the adversary A to only output states that look like a trivial superposition of messages. Since $M_{comp}(\mathrm{M})$ is a complete measurement in the computational basis, it disturbs the state if and only if it is not a computational basis state. Thus, the probability difference between $Game_1$ and $Game_2$ is more than negligible only if the commitment is a non-trivial superposition. Consequently, collapse-binding commitments can be easily used with rewinding-based proofs. In rewinding-based proofs, the adversary's state is saved and the adversary is executed multiple times, starting from that state. By definition, measuring the opened message should not disturb the state, hence allowing for easy rewinding.

As previously stated, collapse-binding commitments are composable. Namely, a proof was provided in [3] to show the possibility of parallel composition. More formally:

Lemma 3.1. Let $(commit, verify)$ be a collapse-binding commitment with message space M. Let $n = n(\eta)$ be a polynomially-bounded and quantum-polynomial-time computable integer.

Let $(commit^n, verify^n)$ be the n-fold parallel composition of $(commit, verify)$. That is, its message space is M^p. And $commit^n(m_1, \dots, m_n)$ computes $(c_i, u_i) \leftarrow commit(m_i)$ for $i = 1, \dots, n$, and returns (c, u) with $c \coloneqq (c_1, \dots, c_n)$ and u$\coloneqq (u_1, \dots, u_n)$. And $verify^n\big((c_1, \dots, c_n), (m_1, \dots, m_n), (u_1, \dots, u_n)\big) = 1$ iff $\forall i. verify(c_i, m_i, u_i) = 1$.

Then $(commit^n, verify^n)$ is collapse-binding.

3.4 Hiding property

In the quantum setting, computational hiding can be defined as proposed in [3], adapted to notations:

Definition 3.2. Let $(commit, verify)$ be a commitment scheme. $(commit, verify)$ is computationally hiding iff for any quantum-polynomial-time A and any polynomial ℓ, there is a negligible μ such that for any η, any $m_0, m_1 \in MSP_\eta$ with $|m_0|, |m_1| \leq \ell(\eta)$, and any $|\Psi\rangle$, $|p_0 - p_1| \leq \mu(\eta)$ where

$$p_i := Pr[b = 1 : (c, u) \leftarrow commit(1^\eta, m_i), b \leftarrow A(1^\eta, |\Psi\rangle, c)].$$

Informally, a commitment scheme is computationally hiding against quantum adversaries if and only if for any two messages that are bounded in length by a polynomial function, the probability difference of the adversary guessing the message is bounded by a negligible function.

Analogously:

Definition 3.3. Let $(commit, verify)$ be a commitment scheme. $(commit, verify)$ is statistically hiding iff for any quantum algorithm A and any polynomial ℓ, there is a negligible μ such that for any η, any $m_0, m_1 \in MSP_\eta$ with $|m_0|, |m_1| \leq \ell(\eta)$, and any $|\Psi\rangle$, $|p_0 - p_1| \leq \mu(\eta)$ where

$$p_i := Pr[b = 1 : (c, u) \leftarrow commit(1^\eta, m_i), b \leftarrow A(1^\eta, |\Psi\rangle, c)].$$

Just like in the classical case, statistical hiding does not require the adversary to be computationally bounded. Furthermore, the definition of collapse-binding in [3] allows for statistically hiding commitments in the quantum random oracle model. As shown in [4], it is possible to construct collapse-binding commitments that are also statistically hiding in the standard model.

3.5 Completeness

In the quantum setting, completeness can be defined as proposed in [3], adapted to notations:

Definition 2.4. A commitment scheme $(commit, verify)$ has perfect completeness iff for all m ∈ MSP_η:

$$Pr[verify(1^\eta, c, m, u) = 1 : (c, u) \leftarrow commit(1^\eta, m)] = 1.$$

Similarly to the classical case, a commitment scheme has perfect completeness in the quantum case if and only if for all valid messages from the message space and all valid commitment-opening pairs generated by the algorithm $commit$, the algorithm $verify$ always returns 1.

4. Quantum-secure coin toss

This chapter introduces the concept of coin toss protocols. Security definitions of a quantum-secure coin toss protocol are given for both bit commitments and string commitments. Additionally, two theorems are introduced.

4.1 Protocol using bit commitments

A coin toss protocol is a protocol between two parties that want to agree to a bit. At the same time, neither of them should be able to influence the final value of the bit to their advantage. The coin toss protocol presented in this paper uses classical communication, yet assumes an adversary that has the capacity of quantum computing. In the proposed protocol, the underlying commitment scheme is assumed to be collapse-binding and statistically hiding, as defined in Chapter 3.

A coin toss protocol proceeds as follows:

- A chooses a value $a \leftarrow \{0,1\}$.
- A runs an algorithm $commit$ to get a commitment-opening pair for a: $(c, u) \leftarrow commit(1^{\eta}, a)$.
- A sends the commitment c to B.
- B chooses a bit $b \leftarrow \{0,1\}$.
- B sends b to A.
- A computes $r := a \oplus b$.
- A sends (a, u) to B.
- B runs an algorithm $v \leftarrow verify(1^{\eta}, c, a, u)$.
- If $v = 1$, B computes $r := a \oplus b$. Otherwise, the protocol aborts.

A visual representation of the protocol is shown in Figure 4.1.

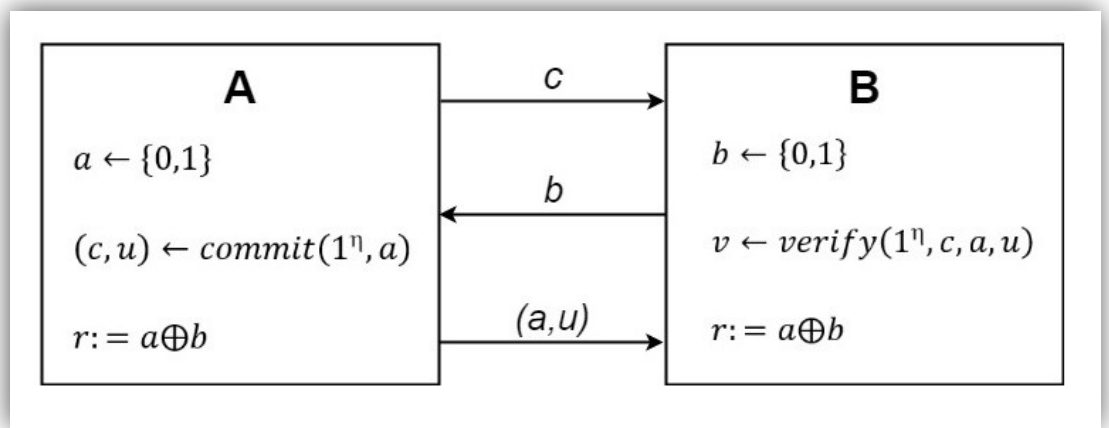

Figure 4.1: A successful coin toss.

4.2 Security definitions

Intuitively, a coin toss protocol is secure if the probability distribution of r is negligibly close to uniformly random, even if one of the parties is corrupted. To show the security of the resulting protocol, the advantage of a malicious adversary is defined as the advantage they have in a "betting game" over an ideal adversary. In the ideal setting, a uniformly random bit is 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$.

Formally:

Definition 4.1. Let r be B-s output in the coin toss protocol. For any quantum-polynomial-time malicious $\hat{A}$, let the advantage of $\hat{A}$ be defined as follows:

$$adv := max(Pr[r = 0], Pr[r = 1]) - \frac{1}{2}.$$

A coin toss protocol is secure iff for any quantum-polynomial-time $\hat{A}$, adv is negligible.

Definition 4.2. Let r be A-s output in the coin toss protocol. For any malicious $\hat{B}$, let the advantage of $\hat{B}$ be defined as follows:

$$adv := max(Pr[r = 0], Pr[r = 1]) - \frac{1}{2}.$$

A coin toss protocol is secure iff for any adversary $\hat{B}$, adv is negligible.

Theorem 4.1. If $(commit, verify)$ is collapse-binding, then the coin toss protocol is secure with respect to Definition 4.1. and Definition 4.2.

Proof sketch. Let (A_1, A_2) be an adversary against the coin toss protocol in the sense of Definition 4.1. Let $b \in \{0,1\}$ and let

$$win = \Pr[r = 1 \wedge verify(1^{\eta}, c, a, u) = 1 : (S, c) \leftarrow A_1, (S, a, u) \leftarrow A_2(S, b)].$$

Here, S denotes a quantum register and c, a, u, b classical values. The protocol is secure, if the advantage $\varepsilon = max(Pr[r = 0], Pr[r = 1]) - \frac{1}{2}$ is upper bounded by a negligible function μ.

Now, it is possible to apply a unitary circuit U_m to S in $A_2(S, b)$ (renaming the register S to S' to avoid confusion later):

$$(U, E) \leftarrow U_m(S').$$

Then, U is measured in the computational basis and a classical value u is returned.

Since $r = a \oplus b$, the probability win requires a malicious adversary $\hat{A}$ to output bit a such that $a := \bar{b}$, where $b \in \{0,1\}$. Thus, the probability win can be expressed in the new circuit as:

$$win := \Pr\big[r = 1 \wedge verify\big(1^{\eta}, c, \bar{b}, u\big) = 1 : (S', c) \leftarrow A_1, (E, U) \leftarrow A_2(S', b), u \leftarrow \mathcal{M}(U)\big].$$

Now, let U_M denote a unitary circuit and M a quantum register of length 1. Let U_M be defined as:

$$U_M : |\Psi\rangle_{S'} \otimes |b\rangle_M \mapsto U_m |\Psi\rangle_{S'} \otimes |b\rangle_M.$$

That is, the unitary circuit U_M takes as an input state $|\Psi\rangle_{S'}$ tensored with a one-bit quantum register, and applies the unitary circuit U_0 or U_1 to $|\Psi\rangle_{S'}$ according to the value of M.

Let $\mathcal{M}_+$ denote a measurement that takes as an input a one qubit register M and checks whether $M = |+\rangle$. Here, $|+\rangle$ is defined as a superposition of states $|0\rangle$ and $|1\rangle$:

$$|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

Now, let's define an adversary (A, B) against the coin toss protocol.

Algorithm A shall be defined as follows:

- $M := |+\rangle$.
- $(S', c) \leftarrow A_1$.
- $(E, U, M) \leftarrow U_M(S', M)$.
- $S := E$.
- Return (S, M, U, c).

Algorithm B shall be defined as follows:

- $E := S$.
- $(S', M) \leftarrow {U_M}^{\dagger}(E, U, M)$.
- $b \leftarrow \mathcal{M}_+(Y)$.
- Return b.

Now, two games $Game_1$ and $Game_2$ can be distinguished.

In $Game_1$, after running the adversary A, a measurement V is performed by a projector

$$P = \sum_{verify(1^\eta, c, \bar{b}, u)=1} |m\rangle\langle m| \otimes |u\rangle\langle u|.$$

Here, the probability of the measurement succeeding is equal to the probability of win. Then, M is measured in the computational basis. Consequently, the state collapses into one of two basis states: $|0\rangle$ or $|1\rangle$. In $Game_1$, the probability of $\mathcal{M}_+$ succeeding is $\frac{1}{2}$, according to the outcome probabilities of state M. Hence, the probability of V and $\mathcal{M}_+$ both succeeding is $win \times \frac{1}{2} = \frac{win}{2}$.

In $Game_2$, the qubit M is not measured. In this scenario, the probability of V and $\mathcal{M}_+$ both succeeding is equal to win^2.

By definition of collapse binding, the difference between measuring and not measuring M should be negligible. Yet, the difference between $Game_1$ and $Game_2$ is non-negligible, thus contradicting the definition.

The security of the protocol with respect to Definition 4.2. can be shown in a similar manner.

■

4.3 Protocol using string commitments

When using collapse-binding commitments, the coin toss protocol can be extended from using bit commitments to using string commitments.

A coin toss protocol with string commitments proceeds as follows:

- A chooses a value $a \leftarrow \{0,1\}^n$.
- A runs an algorithm $commit$ to get a commitment-opening pair for a: $(c, u) \leftarrow commit(1^\eta, a)$.
- A sends the commitment c to B.
- B chooses a bit-string $b \leftarrow \{0,1\}^n$.
- B sends b to A.
- A computes $r := a \oplus b$.
- A sends (a, u) to B.
- B runs an algorithm $v \leftarrow verify(1^\eta, c, a, u)$.
- If $v = 1$, B computes $r := a \oplus b$. Otherwise, the protocol aborts.

Understandably, a coin toss protocol using string commitments needs security definitions that are generalized to bit-strings. Namely, in case of string commitments, the statistical distance between r and r_{ideal} should be negligible:

$$adv := SD(r, r_{ideal}) = \max_{T=\{0,1,\perp\}} |Pr[r \in T] - Pr[r_{ideal} \in T]|.$$

The distribution of r_{ideal} is uniformly random. In other words, for a bit-string of length n and for all $r_{ideal} \in \{0,1\}^n$:

$$\Pr[r_{ideal}] = \frac{1}{2^n}.$$

However, statistical distance distinguishes the probabilities over all possible outputs, i.e. $0, 1, \perp$, with $\perp$ denoting negative verification by the algorithm $verify(1^\eta, c, a, u)$. Hence, for any r that outputs $\perp$ with more than negligible probability, the advantage would be considered to be non-negligible. By definition, non-negligible advantage would mean the adversary has broken the protocol. Henceforth, the definition of advantage is modified to only quantify over r, conditioned on $verify(1^\eta, c, a, u) = 1$.

Formally:

Definition 4.3. Let r be B-s output in the coin toss protocol. Let r_{ideal} be the ideal output of B. For any quantum-polynomial-time malicious $\hat{A}$, let the advantage of $\hat{A}$ be defined as follows:

$$adv := \max_{T=\{0,1\}} (Pr[r \in T] - Pr[r_{ideal} \in T]).$$

A coin toss protocol is secure iff for any quantum-polynomial-time $\hat{A}$, adv is negligible.

Definition 4.4. Let r be A-s output in the coin toss protocol. Let r_{ideal} be the ideal output of A in the coin toss protocol. For any malicious $\hat{B}$, let the advantage of $\hat{B}$ be defined as follows:

$$adv := \max_{T=\{0,1\}} (Pr[r \in T] - Pr[r_{ideal} \in T]).$$

A coin toss protocol is secure iff for any adversary $\hat{B}$, adv is negligible.

Theorem 4.2. If $(commit, verify)$ is collapse-binding, then the coin toss protocol is secure with respect to Definition 4.3. and Definition 4.4.

Proof idea. The proof of Theorem 4.2. could be constructed analogously to the proof of Theorem 4.1. Instead of initializing the qubit M with a bit $|+\rangle$, the register should be initialized with a bit-string of length n in superposition:

$$\sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2}} |x\rangle.$$

Obviously, the proof should be adapted to the bit-string case by using a different method for calculating the probabilities.

5. Summary

This paper presented the security definitions used in classical commitment schemes – hiding property, binding property and completeness. An overview was given of the definitions adapted to the quantum setting, with a special focus on binding property, as there is no canonical definition for the quantum case. A summary of previously proposed definitions was given, with some of their drawbacks and recommended use cases. A formal definition of collapse-binding commitments was provided with some insight into its advantages and useful properties.

Furthermore, the concept of coin toss protocols was introduced. To illustrate the usefulness of collapse-binding commitments, a quantum-secure protocol was constructed, using a statistically hiding and collapse-binding commitment scheme as the underlying protocol. The security definitions of the proposed protocol were defined, along with two theorems about the security of the protocol. The theorems were given with proof sketches, to show a possible way of formalizing the proofs.

First and foremost, as future work, the proposed theorems should be given formal proofs with respect to given definitions. In addition, the security definitions should be strengthened against some specific attacks for the protocol to be usable as a sub-protocol in larger systems. As such, the security of a coin toss protocol in case of string commitments should be modified, to prevent attack for any malicious adversary $\hat{A}$ that can find a function f such that $f(x) = c$.

6. References

[1] P. Kaye, R. Laflamme and M. Mosca, An Introduction to Quantum Computing, New York: Oxford University Press, Inc., 2007.

[2] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge: Cambridge University Press, 2010.

[3] D. Unruh, "Computationally Binding Quantum Commitments," in *Advances in Cryptology -- EUROCRYPT 2016*, New York, Springer , 2016, pp. 497-527.

[4] D. Unruh, "Collapse-Binding Quantum Commitments Without Random Oracles," in *Advances in Cryptology -- ASIACRYPT 2016*, Hanoi, Springer, 2016, pp. 166-195.

[5] A. Ambainis, A. Rosmanis and D. Unruh, "Quantum Attacks on Classical Proof Systems: The Hardness of Quantum Rewinding," in *Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, Washington, IEEE Computer Society, 2014, pp. 474-483.

[6] G. Brassard, C. Crepeau, R. Jozsa and D. Langlois, A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties, Bristol: University of Bristol, 1993.

[7] D. Mayers, "Unconditionally Secure Quantum Bit Commitment is Impossible," *Physical Review Letters,* vol. 78, no. 17, pp. 3414-3417, 1997.

[8] C. Crépeau, L. Salvail, J.-R. Simard and A. Tapp, "Two Provers in Isolation," *Asiacrypt 2011,* vol. 7073, pp. 407-430, 2011.

[9] C. Crépeau, P. Dumais, D. Mayers and L. Salvail, "Computational collapse of quantum state with application to oblivious transfer," *TCC 2004,* vol. 2951, pp. 374-393, 2004.

[10] P. Dumais, D. Mayers and L. Salvail, "Perfectly Concealing Quantum Bit Commitment From Any Quantum One-Way Permutation," *Eurocrypt 2000,* vol. 1807, pp. 300-315, 2000.

[11] B. Zeng, L. Chen and X. Tang, "A Perfectly Binding Commitment Scheme Against Quantum Attacks," in *IACR Cryptology ePrint Archive*, 2011, p. 223.

[12] D. Unruh, "Universally Composable Quantum Multi-Party Computation," in *Eurocrypt 2010*, Springer Berlin Heidelberg, 2010, pp. 486-505.

[13] I. Damgård, S. Fehr and L. Salvail, “Zero-Knowledge Proofs and String Commitments Withstanding Quantum Attacks,” in *CRYPTO 2004*, Berlin, Springer, 2004, pp. 254-272.

[14] I. Damgård, S. Fehr, R. Renner, L. Salvail and C. Schaffner, “A Tight High-Order Entropic Quantum Uncertainty Relation With Applications,” *Crypto 2007,* vol. 4622, pp. 360-378, 2007.

License

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Kristiine Saarmann**,
(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Quantum-Secure Coin Toss Protocol Using Collapse-Binding Commitments,
(*lõputöö pealkiri*)

mille juhendaja on Dominique Unruh,
(*juhendaja nimi*)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **15.05.2018**