Journal of Universal Computer Science, vol. 12, no. 6 (2006), 691-709
submitted: 31/5/06, accepted: 23/6/06, appeared: 28/6/06 © *J.UCS*

Progress in Quantum Computational Cryptography

Akinori Kawachi
(Tokyo Institute of Technology, Tokyo, Japan
kawachi@is.titech.ac.jp)

Takeshi Koshiba
(Saitama University, Saitama, Japan
koshiba@tcs.ics.saitama-u.ac.jp)

Abstract: Shor's algorithms for the integer factorization and the discrete logarithm problems can be regarded as a negative effect of the quantum mechanism on public-key cryptography. From the computational point of view, his algorithms illustrate that quantum computation could be more powerful. It is natural to consider that the power of quantum computation could be exploited to withstand even quantum adversaries. Over the last decade, quantum cryptography has been discussed and developed even from the computational complexity-theoretic point of view. In this paper, we will survey what has been studied in quantum computational cryptography.
Key Words: computational cryptography, quantum computing, quantum cryptography
Category: E.3, F.1.1

1 Introduction

Due to the rapid growth of electronic communication means, information security has become a crucial issue in the real world. Modern cryptography provides fundamental techniques for securing communication and information. While modern cryptography varies from encryption and digital signatures to cryptographic protocols, we can partition modern cryptography into public-key cryptography and secret-key cryptography. From the theoretical point of view, public-key cryptography has a computational complexity-theoretic flavor and secret-key cryptography has an information-theoretic flavor. Though the two disciplines of cryptography have different flavors, they do not separate from each other and rather complement each other.

The principal and classical task of cryptography is to provide confidentiality. Besides confidentiality, modern cryptography provides authentication, data integrity and so on. Since Diffie and Hellman devised the notion of public-key cryptosystem, complexity-theoretic approaches to cryptology have succeeded in theory and practice. The fundamental study of one-way functions and pseudorandom generators has developed computational complexity theory. Cryptographic protocols such as digital signatures, commitment schemes, oblivious transfer schemes and zero-knowledge proof systems have contributed to building various

information security systems. For each objective mentioned above, we should make models of adversaries so as to enable us to discuss whether some cryptographic protocols or methods fulfill the objective. For public-key cryptography, we typically suppose that the adversary should be a probabilistic polynomial-time Turing machine or a polynomial-size circuit family. For secret-key cryptography, the adversary might be the almighty or those who have some specific power.

It is when the adversary is physically realized that it could become a real threat. We know that the real world behaves quantum-mechanically. Thus, we may suppose that the adversary should run quantum-mechanically. Shor's algorithm on quantum computers for the integer factorization problem [56] illustrates that quantum adversaries would spoil the RSA cryptosystem, which is widely used for secure communications. Shor also proposed an efficient quantum algorithm for the discrete logarithm problem. Moreover, since the security of many cryptographic protocols relies on the computational hardness of these two problems, we might have to reconstruct cryptographic protocols to maintain information security technologies in future when the quantum adversary could have a physical implementation.

The quantum mechanism also has an impact on the other discipline of cryptography (i.e., secret-key cryptography). In 1984, Bennett and Brassard [4] proposed a quantum key distribution scheme which is a key distribution protocol using quantum communication. For two decades, so-called quantum cryptography has been developed dramatically. For example, its unconditional security proofs were provided, some alternatives were proposed and so on. We would like to specially mention that Mayers [41] and Lo and Chau [39] independently demonstrated that quantum mechanics cannot necessarily make all cryptographic schemes information-theoretically secure and proved that no quantum bit commitment scheme can achieve both concealing and binding unconditionally. Therefore, it is still important to take "complexity-theoretic" approaches to quantum cryptography.

As mentioned, secret-key cryptography enjoys the benefits of the quantum mechanism. On the other hand, Shor's algorithms can be regarded as a negative effect of the quantum mechanism on public-key cryptography. From the computational point of view, his algorithms illustrate that quantum computation could be more powerful than classical computation. It is natural to consider that the power of quantum computation could be exploited to withstand even quantum adversaries. Over the last decade since the negative impact on public-key cryptography due to Shor, quantum cryptography has been discussed and developed from the complexity-theoretic point of view in the literature. In this paper, we will survey what has been studied in quantum computational cryptography.

2 Foundations of Quantum Computational Cryptography

One-way functions are functions $f : \{0,1\}^* \to \{0,1\}^*$ such that, for each $x \in \{0,1\}^*$, $f(x)$ is efficiently computable but $f^{-1}(y)$ is computationally tractable only for a negligible fraction of all y's. The notion of one-way function is one of the most fundamental notions in cryptology. A construction of pseudorandom generators from any one-way functions [25] is one of the most important results in the foundations of cryptography, because pseudorandom generators are still primitive for other cryptographic protocols. Digital signature schemes are also constructible from one-way functions [47,53]. Besides one-way functions, bit commitment schemes are building blocks for cryptographic protocols and (non-uniform) computationally concealing statistically binding schemes are built in zero-knowledge proof systems, introduced in [20], for any NP language [17]. Furthermore, Naor, in [45], showed that computationally concealing statistically binding bit commitment schemes are constructible from pseudorandom generators (i.e., from one-way functions). Another type of bit commitment scheme, say statistically concealing computationally binding scheme, is constructible from 1-to-1 length-preserving one-way functions (i.e., one-way permutations) [36, 46] and from another special type of one-way functions [24].

Since modern cryptography depends heavily on one-way functions and utilized several candidates in practice, the existence of one-way functions is one of the most important open problems in theoretical computer science. On the other hand, Shor [56] showed that famous candidates of one-way functions such as the RSA function or the discrete logarithm function are no longer one-way in the quantum computation model. For quantum one-way permutations, we do not have any candidates.

2.1 Quantum One-Way Permutations

Kashefi, Nishimura and Vedral [30] gave a necessary and sufficient condition for the existence of *worst-case* quantum one-way permutations as follows. (In the classical case, different characterizations were obtained [28, 29, 54].)

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a permutation. Then f is worst-case quantum one-way if and only if there exists a unitary operator in $\mathcal{Q} = \{Q_j(f) \mid j = 0, 1, ..., n/2-1\}$ that is not efficiently computable. The reflection operators $Q_j(f)$ are defined as

$$Q_j(f) = \sum_{x \in \{0,1\}^n} |x\rangle\langle x| \otimes (2|\psi_{j,x}\rangle\langle\psi_{j,x}| - I),$$

where

$$|\psi_{j,x}\rangle = \frac{1}{\sqrt{2^{n-2j}}} \sum_{y:\mathrm{pref}(f(y),2j)=\mathrm{pref}(x,2j)} |y\rangle$$

and $\mathrm{pref}(s, i)$ denotes the i bits long prefix of a string s.

They also considered quantum weakly one-way permutations (i.e., weak in the cryptographic sense) and gave a sufficient condition on the existence. After that, Kawachi, Kobayashi, Koshiba and Putra [31] gave a necessary condition and completed an algorithmic characterization of quantum weakly one-way permutations. The characterization is similar to the case of worst-case quantum one-way permutation except that the unitary operators in $\mathcal{Q}$ permit of exponentially small errors. While, in [31], Kawachi et al. mentioned a characterization of quantum weakly one-way permutations only, a similar characterization holds for quantum *strongly* one-way permutations. These characterizations might be helpful either to search for candidates of quantum one-way permutations or to disprove their existence.

2.2 Quantum Hard-Core Predicates

Hard-core predicates for one-way functions are also important in computational cryptography. Goldreich and Levin [16] showed that a hard-core predicate is constructible from any one-way function f. Let $f'(x, r) = (f(x), r)$ be a function where $x, r \in \{0,1\}^n$. Here, it is easy to see that f' is also one-way. The predicate

$$GL(x, r) = \langle x, r \rangle = \sum_{i=1}^{n} x_i r_i \bmod 2$$

is a hard-core predicate for the one-way function f'. Moreover, they gave a way to construct a hard-core function of output length $O(\log n)$ for any one-way function. In [1], Adcock and Cleve considered quantum hard-core predicates (i.e., hard-core predicates against quantum adversaries) for quantum one-way functions. They showed that for any quantum one-way function f, $GL(x, r)$ is also a quantum hard-core predicate for the quantum one-way function $f'(x, r) = (f(x), r)$. Furthermore, they proved that the reduction between quantum hard-core predicates and quantum one-way functions is simpler and tighter than the classical reduction. Actually, they showed that a lower bound on the number of oracle calls in the classical reduction is properly larger than an upper bound in the quantum reduction.

It is widely known that list-decodable codes have many complexity-theoretic applications including hard-core functions [57]. Intuitively speaking, if we are given a corrupted codeword of a list-decodable code, we may output a short list containing messages close to the correct one rather than uniquely recover it. For example, the Goldreich-Levin Theorem [16] mentioned above can be regarded as an efficient list-decoding algorithm for the binary Hadamard code. Actually, for a message x, $GL(x, 0), ..., GL(x, 2^n - 1)$ correspond to a codeword of the binary Hadamard code. The prediction algorithm for the hard-core predicate GL also

corresponds to an access to a corrupted codeword. Suppose that we could obtain a polynomially long list that contains x with high probability by accessing the corrupted codeword. It implies that inverting the one-way function f is efficiently computable. Thus, we can say that there is no efficient algorithm to predict the hard-core value of GL.

From the quantum computational point of view, a general construction of quantum hard-core functions from quantum one-way functions has been obtained by Kawachi and Yamakami [33], who utilize a classical code that has a quantum list-decoding algorithm. Roughly speaking, they showed that any code that has an almost orthogonal structure in a sense has a quantum list-decoding algorithm. Consequently, it enables us to discover new (quantum) hard-core functions. Especially, the quantum list-decoding technique affirmatively but quantumly settled the open problem of whether Damgård's generator [12] is cryptographically secure or not.

Let us go into details about quantum hard-core predicates. Regard a mapping from a message space $\{0,1\}^n$ and an index set $\{0,...,M-1\}$ to a finite field $\mathbb{F}_q$ as a code C over $\mathbb{F}_q$. Let $C_x(r)$ be the value of the r-th block in the codeword C_x for a message x, with message length $|x| = n$ and block length (of codewords) $|C_x| = M$. For a codeword C_x, we define a codeword state $|C_x\rangle$ as follows:

$$|C_x\rangle = \frac{1}{\sqrt{M}} \sum_{r=0}^{M-1} \omega_q^{C_x(r)} |r\rangle,$$

where $\omega_q = e^{2\pi i/q}$. In [1], Adcock and Cleve implicitly considered codeword states for the case of binary codes, and the above is a natural extension.

One of the most important special cases is when two codeword states $|C_x\rangle$ and $|C_y\rangle$ are orthogonal, namely,

$$\langle C_x|C_y\rangle = \frac{1}{M} \sum_{r=0}^{M-1} \omega_q^{C_x(r)} \cdot \omega_q^{C_y(r)} = 0.$$

A code with the above orthogonality is said to be *phase-orthogonal*. The phase-orthogonal codes have good properties from the algorithmic point of view. If $M \leq 2^n$, there exist quantum states $|u_0\rangle, ..., |u_{2^n-M-1}\rangle$ such that

$$U = [|C_0\rangle \cdots |C_{q^n-1}\rangle \ |u_0\rangle \cdots |u_{2^n-M-1}\rangle]^\dagger$$

is unitary and $U|C_x\rangle = |x\rangle$. This implies that there exists a (possibly inefficient) decoding algorithm that, given a codeword (with no error added), recovers the original message.

Since it is easy to generate the codeword state from an "uncorrupted" codeword, we would like to obtain a quantum state close to the codeword state whose uncorrupted codeword is close to a given "corrupted" codeword.

Remember that our goal is to show the hard-core property by using list-decodable codes. Specifically speaking, by using an efficient quantum predictor for the hard-core function C, we only have to find a short list of pre-images for a given functional value of a quantum one-way function. The quantum predictor $\mathcal{A}$ can be written as the following unitary operator:

$$\mathcal{A}|r\rangle|0\rangle|0\rangle = \alpha_{r,C_x(r)}|r\rangle|C_x(r)\rangle|\phi_{r,C_x(r)}\rangle + \sum_{s\in\mathbb{F}_q-\{C_x(r)\}} \alpha_{r,s}|r\rangle|s\rangle|\phi_{r,s}\rangle,$$

where the last register is for the workspace $\mathcal{A}$ utilizes. Since $\mathcal{A}$ is a predictor, it is assumed that $C_x(r)$ be predictable with non-negligible probability. In other words, there exists a non-negligible fraction $S \subset \{0,1\}^n$, for every $x \in S$, for some non-negligible function ε such that

$$\sum_{r=0}^{M-1} |\alpha_{r,C_x(r)}|^2 > \frac{1}{q} + \varepsilon.$$

In case of binary codes, the predictor $\mathcal{A}$ can be written as

$$\mathcal{A}|r\rangle|0\rangle|0\rangle = \alpha_{r,C_x(r)}|r\rangle|C_x(r)\rangle|\phi_{r,C_x(r)}\rangle + \alpha_{r,\neg C_x(r)}|r\rangle|\neg C_x(r)\rangle|\phi_{r,\neg C_x(r)}\rangle.$$

Note that

$$\frac{1}{M}\sum_{r,x} |\alpha_{r,C_x(r)}|^2 > 1/2 + \varepsilon \text{ and } \frac{1}{M}\sum_{r,x} |\alpha_{r,\neg C_x(r)}|^2 \leq 1/2 - \varepsilon.$$

Here, let us consider the following procedure:

(1) Initialize the registers to $|0\rangle|0\rangle|0\rangle$.

(2) Make a uniform superposition in the first register and apply $\mathcal{A}$ to it:

$$\frac{1}{\sqrt{M}}\sum_{r=0}^{M-1} |r\rangle(\alpha_{r,C_x(r)}|C_x(r)\rangle|\phi_{r,C_x(r)}\rangle + \alpha_{r,\neg C_x(r)}|\neg C_x(r)\rangle|\phi_{r,\neg C_x(r)}\rangle).$$

(3) Shift the phase according to the second register:

$$\frac{1}{\sqrt{M}}\sum_{r=0}^{M-1} (-1)^{C_x(r)}|r\rangle(\alpha_{r,C_x(r)}|C_x(r)\rangle|\phi_{r,C_x(r)}\rangle - \alpha_{r,\neg C_x(r)}|\neg C_x(r)\rangle|\phi_{r,\neg C_x(r)}\rangle).$$

(4) Apply $\mathcal{A}^{-1}$ to all the registers:

$$\langle C_x|\langle 0|\langle 0|\mathcal{A}^{-1} = \frac{1}{\sqrt{M}}(-1)^{C_x(r)}\langle r|(\alpha^*_{r,C_x(r)}\langle C_x(r)|\langle\phi_{r,C_x(r)}| + \alpha^*_{r,\neg C_x(r)}\langle\neg C_x(r)|\langle\phi_{r,\neg C_x(r)}|).$$

Let

$$|\psi\rangle = \mathcal{A}^{-1}\frac{1}{\sqrt{M}}\sum_{r=0}^{M-1}(-1)^{C_x(r)}|r\rangle(\alpha_{r,C_x(r)}|C_x(r)\rangle|\phi_{r,C_x(r)}\rangle \\ -\alpha_{r,\neg C_x(r)}|\neg C_x(r)\rangle|\phi_{r,\neg C_x(r)}\rangle),$$

which is computable by the above procedure. Then

$$\langle C_x|\langle 0|\langle 0|\psi\rangle = \frac{1}{M}\sum_{r=0}^{M-1}|\alpha_{r,C_x(r)}|^2 - |\alpha_{r,\neg C_x(r)}|^2 \geq 2\varepsilon.$$

Thus, by applying the algorithm that, given an uncorrupted codeword state, computes the original message to a corrupted codeword state, we can obtain the original message with non-negligible probability. By repeating this process independently, we can get a polynomially long list including the original message x with high probability. Actually, in [1], Adcock and Cleve took the same approach.

In the case of q-ary codes, the matter is not simple. While the fidelity between $|\psi\rangle$ obtained in a naively generalized way and $|C_x\rangle|0\rangle|0\rangle$ is written as

$$\frac{1}{M}\left|\sum_{r=0}^{M-1}\sum_{s\in\mathbb{F}_q}\omega_q^{s-C_x(r)}|\alpha_{r,s}|^2\right|,$$

the fidelity cannot be bounded by a non-negligible function. To overcome the difficulty, Kawachi and Yamakami [33] introduced a new tool. They defined the k-shuffled codeword state as

$$|C_x^{(k)}\rangle = \frac{1}{\sqrt{M}}\sum_{r=0}^{M-1}\omega_q^{k\cdot C_x(r)}|r\rangle.$$

Intuitively speaking, the objective of the k-shuffled codeword state is the randomization over the phases in amplitude. After the randomization, we can say that there exists at least one value k such that a "good" k-shuffled codeword state can be computed by using the predictor $\mathcal{A}$. If $|\mathbb{F}_q| \in \mathrm{poly}(n)$, then we can similarly recover the original message with non-negligible probability.

3 Quantum Commitment and Oblivious Transfer

Since the BB84 protocol [4] was shown to be unconditionally secure, some other cryptographic protocols such as bit commitment and oblivious transfer schemes were expected to achieve the security without any computational assumption.

A bit commitment scheme is a two-party protocol. The protocol consists of two phases: the commit phase and the reveal phase. In the commit phase,

the sender Alice has a bit b in her private space and she wants to commit b to the receiver Bob. They exchange messages and at the end of the commit phase the receiver gets some information that represents b. In the reveal phase, Alice confides b to Bob by exchanging messages. At the end of the reveal phase, Bob judges whether the information gotten in the reveal phase really represents b or not. The security of bit commitment schemes consists of the concealing property and the binding property. The concealing property is satisfied if a cheating receiver cannot predict the committed value before the reveal phase. The binding property is satisfied if a cheating sender cannot reveal two different values in the reveal phase. In the classical setting, either the concealing or the binding property must be computational. By introducing quantum states into bit commitment scheme, unconditionally secure bit commitment schemes had been expected to be realized.

A 1-out-of-2 oblivious transfer (OT) is also a fundamental primitive in cryptography. Especially, it is well-known that 1-out-of-2 OT implies secure multiparty computation. Roughly speaking, a 1-out-of-2 OT is a two-party protocol, in which the sender Alice holds two secrets, s_0 and s_1, and the receiver Bob holds a secret bit b. If both parties follow the protocol, Bob learns s_b. Moreover, even a cheating receiver cannot learn more than a single value in $\{s_0, s_1\}$ and even a cheating sender cannot learn anything about b.

First, Crépeau and Kilian [10] showed a construction from unconditionally secure quantum commitment schemes to 1-out-of-2 quantum oblivious transfer schemes. Its information-theoretic security were proved in [8, 42, 61]. (Note that such a reduction in the classical setting is unknown.) Unfortunately, it was later shown that commitment schemes with unconditional concealing and binding properties are impossible even if quantum states are applicable [39, 41]. If we allow either the concealing or the binding condition of a bit commitment scheme to be computational, interesting commitment schemes utilizing quantum information are still possible. Dumais, Mayers and Salvail [14] proposed a perfectly concealing and computationally binding bit commitment scheme with constant-round interactions under the assumption that quantum one-way permutations exist. (In the classical case, schemes with $O(n/\log n)$ rounds are the best result known [36].) The use of quantum information enables us to transform from computationally concealing and computationally binding bit commitment scheme to statistically concealing and computationally binding scheme [11]. Since the former is constructible from any quantum one-way function, so is the latter. (In the classical case, a statistically concealing bit commitment scheme is constructible from one-way functions with special features [24].)

Here, let us consider some issues in defining quantum bit commitment. Though we can define the concealing condition of quantum bit commitments as in the classical case, some care must be taken to define the binding condition in the

quantum case. In the classical case, the binding property means that the probability that the bit value committed in the commit phase can be revealed as both 0 and 1 is negligibly small. However, this definition is too strong in the quantum case. Suppose that a sender in some quantum bit commitment scheme could generate the following state:

$$\frac{1}{\sqrt{2}}|0\rangle|\phi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle|\phi_1\rangle,$$

where $|\phi_0\rangle$ (resp., $|\phi_1\rangle$) is a quantum state to be sent when 0 (resp., 1) is honestly committed in the commit phase. Then the sender Alice sends the quantum state only in the second register to the receiver Bob and keeps the quantum state in the first register at her side. Alice can change the committed value with probability $1/2$ by measuring the quantum state left at her side just before the reveal phase. Since the above situation is essentially inevitable, the straightforward extension of the binding condition in the classical case is not satisfied in the quantum case. Thus, we have to weaken the definition of the binding condition in the quantum case. Actually, in [14], Dumais, Mayers and Salvail introduced a weaker definition of the binding property. Their weaker binding propety is satisfied if $p_0 + p_1 - 1$ is negligibly small, where p_0 (resp., p_1) is the probability that the committed value is revealed as 0 (resp., 1).

The following is the description of the quantum bit commitment scheme in [14]. Let $f : \{0,1\}^n \to \{0,1\}^n$ be any quantum one-way permutation

[Commit Phase]

1. Alice decides $w \in \{0,1\}$ as her committing bit. She also chooses $x \in \{0,1\}^n$ uniformly at random, and then computes $f(x)$.
2. Alice sends $|f(x)\rangle$ to Bob if $w = 0$ and $H^{\otimes n}|f(x)\rangle$ otherwise, where H is the Hadamard transformation.

[Reveal Phase]

1. Alice announces x and w to Bob.
2. If $w = 1$, Bob applies $H^{\otimes n}$ to the state sent from Alice. Otherwise, he does nothing to the state.
3. Bob measures the resulting state in the computational basis. Let y be the outcome. He accepts if and only if $y = f(x)$.

The above protocol satisfies the perfect concealing property. This is because for a bit w to be committed and for the corresponding quantum state ρ_w, Alice generates the following equalities:

$$\rho_0 = \frac{1}{2^n}\sum_{x\in\{0,1\}^n} |f(x)\rangle\langle f(x)| = I/2^n = \frac{1}{2^n}\sum_{x\in\{0,1\}^n} (H^{\otimes n}|f(x)\rangle)(\langle f(x)|H^{\otimes n\dagger}) = \rho_1.$$

This implies that both states generated by Alice are maximally mixed states and they are independent of w. On the other hand, the computationally binding property can be satisfied by constructing an inverter of the quantum one-way permutation f from a quantum adversary for the binding condition. In general, the space in which a quantum adversary can operate is partitioned into three subspaces: the register A for the working space, the register B that is sent to Bob in the reveal phase, and the register C that is sent to Bob in the commit phase. Suppose that the quantum adversary can change whatever the committed bit is and Bob accepts it. This essentially implies that the following transformation U_{AB} over registers A and B has a polynomial-size circuit for some vectors $|\gamma_x^0\rangle$ and $|\gamma_x^1\rangle$:

$$|\phi_0\rangle = \sum_{x\in\{0,1\}^n} |\gamma_x^0\rangle_A |x\rangle_B |f(x)\rangle_C \overset{U_{AB}}{\mapsto} |\phi_1\rangle = \sum_{x\in\{0,1\}^n} |\gamma_x^1\rangle_A |x\rangle_B H^{\otimes n} |f(x)\rangle_C.$$

(Note that the quantum adversary cannot access the register C after the commit phase because the values in C have already been sent to Bob.) Let $\sum_x \||\gamma_x^0\rangle\| = \sum_x \||\gamma_x^1\rangle\| = 1$.

Let us see that it is possible to construct an algorithm to compute $f^{-1}(y)$ from a given $y \in \{0,1\}^n$ by using the mapping U_{AB}. First, note that the state

$$|\phi_y\rangle = \sum_{x\in\{0,1\}^n} (-1)^{\langle y, f(x)\rangle} |\gamma_x^0\rangle_A |x\rangle_B H^{\otimes n} |y\rangle_C$$

can be computed from $|\phi_0\rangle$. Here, we consider to apply the projection $H^{\otimes n}|y\rangle\langle y|H^{\otimes n}$ to $|\phi_0\rangle$ in the register C and normalize the state. The resulting state indeed coincides with $|\phi_y\rangle$. This state $|\phi_y\rangle$ can be easily generated as follows. (1) We change the phase to $(-1)^{\langle y,f(x)\rangle}$ according to the value in the register C and y. (2) We set the register B to zero by computing f again. (3) We copy the input value y to the register B and apply $H^{\otimes n}$ to it. The above procedure implies that the mapping $T_C|\phi_0\rangle = |\phi_y\rangle$ has an efficient implementation. Moreover, U_{AB} and T_C commute, because U_{AB} acts on the registers A and B by the assumption and T_C is just the projection of the value in the register C to $H^{\otimes n}|y\rangle\langle y|H^{\otimes n}$ and thus does not act on the registers A and B. Hence,

$$U_{AB}T_C|\phi_0\rangle = T_C U_{AB}|\phi_0\rangle = T_C|\phi_1\rangle = |\gamma_{f^{-1}(x)}^1\rangle |f^{-1}(y)\rangle H^{\otimes n}|y\rangle.$$

Therefore, what we want to obtain appears in the register B. (Note that the inverter in the case where the adversary errs becomes more complicated.)

Last in this section, we mention a conversion from a quantum bit commitment scheme with computational assumption to quantum oblivious transfer with computational assumption. Crépeau and Kilian's conversion from quantum bit

commitment to 1-out-of-2 quantum oblivious transfer supposes that some classical information must be sent to a third party in the commit phase. Thus, since the statistically binding and "computationally" binding bit commitment scheme may use quantum information, their proof technique is not applicable. Crépeau et al. have shown a way to convert a statistically concealing and computationally binding bit commitment scheme to 1-out-of-2 quantum oblivious transfer [9].

4 Quantum Zero-Knowledge

The notion of zero-knowledge was introduced by Goldwasser, Micali and Rackoff [20]. Roughly speaking, an interactive proof system has the zero-knowledge property if any (possibly cheating) verifier that communicates with the honest prover learns nothing through the interaction except the validity of the claimed statement. Even in the classical case, there are several variants of zero-knowledge corresponding to how to formally define the notion that the verifier "learns nothing." Anyway, the verifier "learns nothing" if there exists a polynomial-time simulator whose output is indistinguishable in some sense from the information the verifier would have after the interaction with the honest prover.

At any round of interaction to simulate, a simulator typically generates a pair of a question from the verifier and a response from the honest prover. If this produces a pair that is inconsistent with each other (or with the other parts of the transcript of the interaction simulated so far), the simulator "rewinds" the process to simulate this round again. However, the "rewinding" technique is not generally applicable to quantum verifiers. First, quantum information cannot be copied; this fact is also known as the no-cloning theorem. Second, measurements are generally irreversible processes. This difficulty was explicitly pointed out by van de Graaf [21].

Since then the study of quantum zero-knowledge has developed from a computational point of view. For example, Watrous [58] defined the quantum counterpart of honest verifier statistical zero-knowledge and studied its properties. We denote by HVQSZK the class of languages that have honest verifier quantum statistical zero-knowledge proof systems. In [58], the following statements are shown: (i) There exists a complete promise problem, which is a natural generalization of a complete promise problem in statistical zero-knowledge (SZK) due to [55]. (ii) HVQSZK is contained in PSPACE. (iii) HVQSZK is closed under complement. (iv) Any HVQSZK protocol can be parallelized to a one-round HVQSZK protocol.

Kobayashi [35] defined non-interactive quantum perfect zero-knowledge (denoted by NIQPZK) and non-interactive quantum statistical zero-knowledge (denoted by NIQSZK) and studied their properties. Specifically speaking, (i) if the prover and the verifier do not beforehand have any shared randomness and

any shared entanglement, languages that have non-interactive quantum zero-knowledge proof systems are in BQP. (ii) Assuming that the verifier and the prover share polynomially many Einstein-Podolsky-Rosen (EPR) pairs a priori, NIQPZK with the one-sided error has a natural complete promise problem, which is a generalization of a complete promise problem in non-interactive statistical zero-knowledge (NISZK) due to Goldreich, Sahai and Vadhan [18]. (iii) The graph non-automorphism (GNA) problem has a NIQPZK proof system with prior EPR pairs. (Since it is unknown whether GNA is in BQP or not, NIQPZK with prior EPR pairs includes a nontrivial language.)

In order to circumvent problematic issues caused by the rewinding technique, Damgård, Fehr and Salvail [13] have shown a way to construct computational QZK proof and perfect QZK arguments against quantum adversaries in the *common reference string* model, wherein it is assumed that an honest third party samples a string from some specified distribution and provides both the prover and verifier with this string at the start of the interaction. They have also given a construction of unconditionally concealing and computationally binding string commitment protocols against quantum adversaries.

Very recently, Watrous [59] resolves in many cases the problematic issues caused by the rewinding technique in quantum zero-knowledge by introducing a success probability amplifying technique, which is successfully utilized to amplify the success probability in Quantum Merlin-Arthur protocols without increasing the witness sizes [40]. Specifically speaking, he showed (i) the graph isomorphism problem is in perfect zero-knowledge (PZK) even against an adversarial verifier who uses quantum computation to cheat, and (ii) if quantum one-way permutations exist, every problem in NP has ZK proof systems even against an adversarial verifier who uses quantum computation to cheat.

5 Quantum Public-Key Encryptions

As mentioned in the introduction, public-key cryptosystems are indispensable even in future where quantum computers might be physically realized. Unfortunately, almost all practical public-key cryptosystems are vulnerable to Shor's algorithm. On the other hand, there are public-key cryptosystems that have not shown to be vulnerable to quantum adversaries. Lattice-based cryptography [3, 15, 51, 52] is one example. In [3], Ajtai and Dwork proposed a semantically secure public-key cryptosystem based on the *worst-case* hardness of the n^8-unique shortest vector problem. The $s(n)$-unique shortest vector problem is the shortest vector problem with promise that the ratio of the shortest vector length to any other non-parallel vector length is at most $1/s(n)$. The security reducibility to the worst-case hardness of the underlying intractable problem is one of the remarkable features in lattice-based cryptography. Besides cryptography, problems with respect to the lattice structures have attracted much attention.

From now on, we focus on public-key cryptosystems associated with quantum computation. In 2000, Okamoto, Tanaka and Uchiyama [49] proposed a knapsack-based cryptosystem as a quantum public-key cryptosystem. The first knapsack-based cryptosystem was proposed by Merkle and Hellman [43]. They aimed to incorporate the hardness of an NP-hard knapsack problem into their cryptosystem. A knapsack problem is a search problem to compute a binary vector $(b_1, ..., b_n)$ such that $s = \sum_{i=1}^{n} a_i b_i$ from a positive integer s and a positive integer vector $a = (a_1, ..., a_n)$. The vector a corresponds to a public key. For an n-bit message $b = (b_1, ..., b_n)$, its encryption c is computed as $c = \sum_{i=1}^{n} a_i b_i$. So, the problem to find the message b from an encryption c and a public key a is just a knapsack problem. Merkle and Hellman utilized the fact that knapsack problems with the super-increasing property $a_i > \sum_{j=1}^{i-1} a_j$ are efficiently computable and let a public key be a vector obtained by applying a modular linear transformation to the super-increasing vector. Due to the linearity, their cryptosystem was cracked soon after the proposal. Since then, knapsack-based cryptography had been improved again and again. Eventually, Brickell [6] and Lagarias and Odlyzko [37] independently proposed a general attack (the so-called low-density attack) on knapsack-based cryptosystems. As a countermeasure, Chor and Rivest [7] introduced a non-linearity into the public key generation by using an easy special discrete logarithm problem and proposed yet another knapsack-based cryptosystem. The quantum public-key cryptosystem by Okamoto, Tanaka and Uchiyama [49] can be regarded as an extension of the Chor-Rivest cryptosystem. This is because they use the general discrete logarithm problem to generate public keys with the help of quantum computation.

In 2005, Kawachi, Koshiba, Nishimura and Yamakami [32] proposed a semantically secure (in a weak sense) quantum public-key cryptosystem based on the worst-case hardness of the graph automorphism problem. Actually, they introduced the computational problem of distinguishing between two specific quantum states as a new cryptographic problem to design their quantum public-key cryptosystem. The computational indistinguishability between quantum states is a generalization of the classical indistinguishability between two probability distributions, which plays an important role in computational cryptography (see, e.g., [19, 60]). Their problem QSCD_{ff} asks whether we can distinguish between two sequences of identical samples of $\rho_\pi^+(n)$ and of $\rho_\pi^-(n)$ for each fixed hidden permutation π for each length parameter n of a certain form. Let S_n be the *symmetric group* of degree n and let $\mathcal{K}_n = \{\pi \in S_n : \pi^2 = id \text{ and } \forall i \in \{1, ..., n\}[\pi(i) \neq i]\}$ for $n \in N$, where id stands for the identity permutation and $N = \{2(2n' + 1) : n' \in \mathbb{N}\}$. For each $\pi \in \mathcal{K}_n$, let $\rho_\pi^+(n)$ and $\rho_\pi^-(n)$ be two

quantum states defined by

$$\rho_\pi^+(n) = \frac{1}{2n!}\sum_{\sigma\in S_n}(|\sigma\rangle + |\sigma\pi\rangle)(\langle\sigma| + \langle\sigma\pi|) \text{ and}$$
$$\rho_\pi^-(n) = \frac{1}{2n!}\sum_{\sigma\in S_n}(|\sigma\rangle - |\sigma\pi\rangle)(\langle\sigma| - \langle\sigma\pi|).$$

The cryptographic properties of QSCD_{ff} follow mainly from the definition of the set $\mathcal{K}_n$ of the hidden permutations. Although the definition seems somewhat artificial, the following properties of $\mathcal{K}_n$ lead to useful cryptographic and complexity-theoretic properties of QSCD_{ff}: (i) $\pi \in \mathcal{K}_n$ is of order 2, which provides the trapdoor property of QSCD_{ff}. (ii) For any $\pi \in \mathcal{K}_n$, the conjugacy class of π is equal to $\mathcal{K}_n$, which makes it possible to prove the equivalence between the worst-case/average-case hardness of QSCD_{ff}. (iii) The graph automorphism problem is (polynomial-time Turing) equivalent to its subproblem with the promise that a given graph has a unique non-trivial automorphism in $\mathcal{K}_n$ or none at all. This equivalence is exploited to give a complexity-theoretic lower bound of QSCD_{ff}, that is, the worst-case hardness of the graph automorphism problem. For these proofs, they introduced new techniques: a new version of the so-called *coset sampling method*, which is broadly used in extensions of Shor's algorithm (see, e.g., [50]) and a quantum version of the hybrid argument, which is a strong tool for security reduction in modern cryptography.

Their problem QSCD_{ff} is closely related to a much harder problem: the hidden subgroup problem on the *symmetric groups* (SHSP). Note that no known subexponential-time quantum algorithm exists for SHSP. Hallgren et al. [27] introduced a distinction problem between certain two quantum states, similar to QSCD_{ff}, to discuss the computational intractability of SHSP by a "natural" extension of Shor's algorithm [56] with the quantum Fourier transformation. An efficient solution to this distinction problem gives an answer to a pending question on a certain special case of SHSP. To solve this distinction problem, as they showed, the so-called *weak Fourier sampling* on a single sample should require an exponential number of samples. This result was improved by Grigni et al. [22] and Kempe and Shalev [34]. In contrast, Hallgren et al. [26] proved that no time-unbounded quantum algorithm solves the distinction problem even from $o(n \log n)$ samples. Kawachi et al. [32] showed that the above distinction problem is polynomial-time reducible to QSCD_{ff}. This immediately implies that we have no time-unbounded quantum algorithm for QSCD_{ff} from $o(n \log n)$ samples. Even with sufficiently many samples for QSCD_{ff}, there is no known subexponential-time quantum algorithms for QSCD_{ff} and thus finding such an algorithm seems a daunting task.

Let us move to the description of the quantum public-key cryptosystem in [32]. Usually, public-key cryptosystems consist of three algorithms, for key

generation, encryption and decryption.

[Public Key Generation Algorithm]
Input: $\pi \in \mathcal{K}_n$
Procedure:

step 1. Choose a permutation σ from S_n uniformly at random and store it in the second register. Then, the entire system is in the state $|0\rangle|\sigma\rangle$.

step 2. Apply the Hadamard transformation to the first register.

step 3. Apply the Controlled-π to the both registers.

step 4. Apply the Hadamard transformation to the first register again.

step 5. Measure the first register in the computational basis. If 0 is observed, then the quantum state in the second register is ρ_π^+. Otherwise, the state of the second register is ρ_π^-. Now, apply the conversion algorithm to ρ_π^-.

Encryption algorithm consists of two parts: one is the conversion algorithm below and the other is so simple that we describe it in the description of the total system.

[Conversion Algorithm]
The following transformation inverts, given ρ_π^+, its phase according to the sign of the permutation with certainty.

$$|\sigma\rangle + |\sigma\pi\rangle \longmapsto (-1)^{\mathrm{sgn}(\sigma)}|\sigma\rangle + (-1)^{\mathrm{sgn}(\sigma\pi)}|\sigma\pi\rangle.$$

Since π is odd, the above algorithm converts ρ_π^+ into ρ_π^-.

Finally, we give a description of decryption algorithm.

[Decryption Algorithm]
Input: unknown state χ which is either ρ_π^+ or ρ_π^-.
Procedure:

step 1. Prepare two quantum registers: the first register holds a control bit and the second one holds χ. Apply the Hadamard transformation H to the first register. The state of the system now becomes

$$H|0\rangle\langle 0|H \otimes \chi.$$

step 2. Apply the Controlled-π operator C_π to the two registers, where $C_\pi|0\rangle|\sigma\rangle = |0\rangle|\sigma\rangle$ and $C_\pi|1\rangle|\sigma\rangle = |1\rangle|\sigma\pi\rangle$ for any $\sigma \in S_n$.

step 3. Apply the Hadamard transformation to the first register.

step 4. Measure the first register in the computational basis. Output the observed result.

The following is the description of the total cryptosystem consisting two phases: key transmission phase and message transmission phase.

[Key Transmission Phase]

1. Bob chooses a decryption key π uniformly at random from $\mathcal{K}_n$.
2. Bob generates sufficiently many copies of the encryption key ρ_π^+ by using the public key generation algorithm.
3. Alice obtains encryption keys from Bob.

[Message Transmission Phase]

1. Alice encrypts 0 or 1 into ρ_π^+ or ρ_π^-, respectively, by using the conversion algorithm, and sends it to Bob.
2. Bob decrypts Alice's message using the decryption algorithm.

Lastly, we mention a lattice-based cryptosystem due to Regev [52]. While his cryptosystem is a totally classical public-key cryptosystem based on the hardness of the approximation of the shortest vector problem, his reduction uses the power of quantum computation. Previous lattice-based cryptosystems have a provable security based on the hardness of the unique shortest vector problem or no security proof. While the unique shortest vector problem seems to be difficult, its computational complexity has not been investigated extensively. On the other hand, the approximation of the shortest vector problems has been well studied from the computational point of view. Actually, the computational complexity of the approximation depends on the approximation factor. For example, a polynomial-time algorithm (namely, the Lenstra-Lenstra-Lovász algorithm [38]) works for the approximation factor $2^{n/2}$, where n is the dimension of the lattice. On the other hand, the approximation with factor $\sqrt{2} - \epsilon$ is NP-hard under randomized reduction [44]. Though the underlying problem in [52] is neither NP-hard nor polynomial-time computable, his approach is right to the point.

6 Concluding Remarks

We have reviewed results in quantum computational cryptography for the last decade. Though Shor's factoring algorithm certainly had a great impact on computational cryptography, we can say that we have been developing alternatives and establishing new foundations. On the other hand, we have to say that quantum computational cryptography has much room for improvement and development. Especially, quantum counterparts of digital signatures have not been investigated so much yet.

Acknowledgments

We would like to thank Hirotada Kobayashi for his helpful comments on zero-knowledge systems.

References

1. M. Adcock, R. Cleve: A quantum Goldreich-Levin theorem with cryptographic applications. In *Proc. 19th Annual Symp. Theoretical Aspects of Computer Science*, Lect. Notes Comput. Sci. 2285, Springer, pp.323–334 (2002).
2. D. Aharonov, A. Ta-Shma: Adiabatic quantum state generation and statistical zero knowledge. In *Proc. 35th Annual ACM Symp. Theory of Computing*, pp.20–29 (2003).
3. M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. 29th ACM Symp. Theory of Computing*, pp.284–293 (1997).
4. C. H. Bennett, G. Brassard: Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conf. Computers, Systems, and Signal Processing*, pp.175–179 (1984).
5. G. Brassard, D. Chaum, C. Crépeau: Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189 (1988).
6. E. F. Brickell: Solving low density knapsacks. In *Proc. CRYPTO 1983*, Plenum Press, pp.25–37 (1984).
7. B. Chor, R. L. Rivest: A Knapsack type public key cryptosystem based on arithmetic in finite fields, *IEEE Trans. Inf. Theory*, 34(5):901–909 (1988).
8. C. Crépeau: Quantum oblivious transfer. *J. Mod. Opt.*, 41(12):2445–2454 (1994).
9. C. Crépeau, P. Dumais, D. Mayers, L. Salvail: Computational collapse of quantum state with application to oblivious transfer. In *Proc. 1st Theory of Cryptography Conf.*, Lect. Notes Comput. Sci. 2951, Springer, pp.374–393 (2004).
10. C. Crépeau, J. Kilian: Achieving oblivious transfer using weakened security assumptions. In *Proc. 29th Annual IEEE Symp. Foundations of Computer Science*, pp.42–52 (1988).
11. C. Crépeau, F. Legare, L. Salvail: How to convert the flavor of a quantum bit commitment. In *Advances in Cryptology — EUROCRYPT 2001*, Lect. Notes Comput. Sci. 2045, Springer, pp.60–77 (2001).
12. I. Damgård: On the randomness of Legendre and Jacobi sequences. In *Advances in Cryptology — CRYPTO '88*, Lect. Notes Comput. Sci. 403, Springer, pp.163–172 (1988).
13. I. Damgård, S. Fehr, L. Salvail: Zero-knowledge proofs and string commitments withstanding quantum attacks. In *Advances in Cryptology — CRYPTO 2004*, Lect. Notes Comput. Sci. 3152, Springer, pp.254–272 (2004).
14. P. Dumais, D. Mayers, L. Salvail: Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *Advances in Cryptology — EUROCRYPT 2000*, Lect. Notes Comput. Sci. 1807, Springer, pp.300–315 (2000).
15. O. Goldreich, S. Goldwasser, S. Halevi: Public-key cryptosystems from lattice reduction problems. In *Advances in Cryptology — CRYPTO 1997*, Lect. Notes Comput. Sci. 1294, Springer, pp.112–131 (1997).
16. O. Goldreich, L. A. Levin. A hard-core predicate for all one-way functions. In *Proc. 21st ACM Symp. Theory of Computing*, pp.25–32 (1989).
17. O. Goldreich, S. Micali, A. Wigderson: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. Assoc. Comput. Mach.*, 38(3):691–729 (1991).

18. O. Goldreich, A. Sahai, S. Vadhan: Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and NISZK. In *Advances in Cryptology — CRYPTO 1999*, Lect. Notes Comput. Sci. 1666, Springer, pp.467–484 (1999).
19. S. Goldwasser, S. Micali: Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299 (1984).
20. S. Goldwasser, S. Micali, C. Rackoff: The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208 (1989).
21. J. van de Graaf: Towards a formal definition of security for quantum protocols. PhD thesis, Université de Montréal (1997).
22. M. Grigni, L. J. Schulman, M. Vazirani, U. Vazirani: Quantum mechanical algorithms for the nonabelian hidden subgroup problem. *Combinatorica*, 24(1):137–154 (2004).
23. L. Grover: Quantum Mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328 (1997).
24. I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, R. Shaltiel: Reducing complexity assumptions for statistically-hiding commitment. In *Advances in Cryptology — EUROCRYPT 2005*, Lect. Notes Comput. Sci. 3494, Springer, pp.58–77 (2005).
25. J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby: A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396 (1999).
26. S. Hallgren, C. Moore, M. Rötteler, A. Russell, P. Sen: Limitations of quantum coset states for graph isomorphism. In *Proc. 38th ACM Symp. Theory of Computing*, (2006).
27. S. Hallgren, A. Russell, A. Ta-Shma: The hidden subgroup problem and quantum computation using group representations. *SIAM J. Comput.*, 32(4):916–934 (2003).
28. L. Hemaspaandra, J. Rothe: Characterizing the existence of one-way permutations. *Theor. Comput. Sci.*, 244(1-2):257–261 (2000).
29. C. M. Homan, M. Thakur: One-way permutations and self-witnessing languages. *J. Comput. Syst. Sci.*, 67(3):608–622 (2003).
30. E. Kashefi, H. Nishimura, V. Vedral: On quantum one-way permutations. *Quantum Inf. Comput.*, 2(5):379–398 (2002).
31. A. Kawachi, H. Kobayashi, T. Koshiba, R.R.H. Putra: Universal test for quantum one-way permutations. *Theor. Comput. Sci.*, 345(2-3):370–385 (2005).
32. A. Kawachi, T. Koshiba, H. Nishimura, T. Yamakami: Computational indistinguishability between quantum states and its cryptographic application. In *Advances in Cryptology — EUROCRYPT 2005*, Lect. Notes Comput. Sci. 3494, Springer, pp.268–284 (2005).
33. A. Kawachi, T. Yamakami: Quantum hardcore functions by complexity-theoretical quantum list decoding. In *Proc. 33rd International Colloquium on Automata, Languages and Programming*, Lect. Notes Comput. Sci. 4052, Springer, pp.216–227 (2006).
34. J. Kempe and A. Shalev: The hidden subgroup problem and permutation group theory. In *Proc. 16th ACM-SIAM Symp. Discrete Algorithms*, pp.1118–1125 (2005).
35. H. Kobayashi: Non-interactive quantum perfect and statistical zero-knowledge. In *Proc. 14th International Symp. Algorithms and Computation*, Lect. Notes Comput. Sci. 2906, Springer, pp.178–188 (2003).
36. T. Koshiba, Y. Seri: Round-efficient one-way permutation based perfectly concealing bit commitment schemes. Manuscript.
37. J. C. Lagarias, A. M. Odlyzko: Solving low-density subset sum problems. *J. Assoc. Comput. Mach.*, 32(1):229–246 (1985).
38. A. K. Lenstra, H. W. Lenstra Jr., L. Lovász: Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:513–534 (1982).
39. H.-K. Lo, H. F. Chau: Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17):3410–3413 (1997).

40. C. Marriott, J. Watrous: Quantum Arthur-Merlin games. In *Proc. 19th IEEE Conf. Computational Complexity*, pp.275–285 (2004).
41. D. Mayers: Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417 (1997).
42. D. Mayers, L. Salvail: Quantum oblivious transfer is secure against all individual measurements. In *Proc. Workshop on Physics and Computation*, pp.69–77 (1994).
43. R. C. Merkle, M. E. Hellman: Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inf. Theory*, 24:525–530 (1978).
44. D. Micciancio: The shortest vector problem is NP-hard to approximate within small constant. *SIAM J. Comput.*, 30(6):2008–2035 (2001).
45. M. Naor: Bit commitment using pseudorandomness. *J. Cryptol.*, 4(2):151–158 (1991).
46. M. Naor, R. Ostrovsky, R. Venkatesan, M. Yung: Perfect zero-knowledge arguments for NP using any one-way permutation, *J. Cryptol.*, 11(2):87–108 (1998).
47. M. Naor, M. Yung: Universal one-way hash functions and their cryptographic applications. In *Proc. 21st ACM Symp. Theory of Computing*, pp.33–43 (1989).
48. M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge Univ. Press (2000).
49. T. Okamoto, K. Tanaka, S. Uchiyama: Quantum public-key cryptosystems. In *Advances in Cryptology — CRYPTO 2000*, Lect. Notes Comput. Sci. 1880, Springer, pp.147–165 (2000).
50. O. Regev: Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760 (2004).
51. O. Regev: New lattice-based cryptographic constructions. *J. Assoc. Comput. Mach.*, 51(6):899–942 (2004).
52. O. Regev: On lattices, learning with errors, random linear codes, and cryptography. In *Proc. 37th Annual ACM Symp. Theory of Computing*, pp.84–93 (2005).
53. J. Rompel: One-way functions are necessary and sufficient for secure signatures. In *Proc. 22nd ACM Symp. Theory of Computing*, pp.387–394 (1990).
54. J. Rothe, L. Hemaspaandra: On characterizing the existence of partial one-way permutations. *Inf. Process. Lett.*, 82(3):165–171 (2002).
55. A. Sahai, S. Vadhan: A complete problem for statistical zero knowledge. *J. Assoc. Comput. Mach.*, 50(2):196–249 (2003).
56. P. Shor: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509 (1997).
57. M. Sudan: List decoding: Algorithms and applications. *SIGACT News*, 31(1):16–27 (2000).
58. J. Watrous: Limits on the power of quantum statistical zero-knowledge. In *Proc. 43rd IEEE Symp. Foundations of Computer Science*. pp.459–470 (2002).
59. J. Watrous: Zero-knowledge against quantum attacks. In *Proc. 38th Annual ACM Symp. Theory of Computing*, pp.296–305 (2006).
60. A. C.-C. Yao: Theory and applications of trapdoor functions. In *Proc. 23rd IEEE Symp. Foundations of Computer Science*, pp.80–91 (1982).
61. A. C.-C. Yao: Security of quantum protocols against coherent measurements. In *Proc. 27th Annual ACM Symp. Theory of Computing*, pp.67–75 (1995).