UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Quantum cryptography beyond quantum key distribution

Broadbent, A.; Schaffner, C.

DOI
10.1007/s10623-015-0157-4

Publication date
2016

Document Version
Final published version

Published in
Designs, Codes and Cryptography

License
CC BY

Link to publication

Citation for published version (APA):
Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, *78*(1), 351-382. https://doi.org/10.1007/s10623-015-0157-4

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:08 Nov 2026

Des. Codes Cryptogr. (2016) 78:351–382
DOI 10.1007/s10623-015-0157-4

Quantum cryptography beyond quantum key distribution

Anne Broadbent[1] · **Christian Schaffner**[2]

Accepted: 21 October 2015 / Published online: 21 December 2015
© The Author(s) 2015. This article is published with open access at Springerlink.com

Abstract Quantum cryptography is the art and science of exploiting quantum mechanical effects in order to perform cryptographic tasks. While the most well-known example of this discipline is quantum key distribution (QKD), there exist many other applications such as quantum money, randomness generation, secure two- and multi-party computation and delegated quantum computation. Quantum cryptography also studies the limitations and challenges resulting from quantum adversaries—including the impossibility of quantum bit commitment, the difficulty of quantum rewinding and the definition of quantum security models for classical primitives. In this review article, aimed primarily at cryptographers unfamiliar with the quantum world, we survey the area of theoretical quantum cryptography, with an emphasis on the constructions and limitations beyond the realm of QKD.

Keywords Conjugate coding · Delegated quantum computation · Limited-quantum-storage models · Quantum money · Quantum two-party computation · Survey

Mathematics Subject Classification 94A60 · 81P94

This is one of several papers published in *Designs, Codes and Cryptography* comprising the 25th Anniversary Issue.

✉ Anne Broadbent
abroadbe@uottawa.ca

✉ Christian Schaffner
c.schaffner@uva.nl

[1] Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada

[2] Institute for Logic, Language and Computation (ILLC), University of Amsterdam, and Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands

1 Introduction

The relationship between quantum information and cryptography is almost half-a-century old: a 1968 manuscript of Wiesner (published more than a decade later [233]), proposed *quantum money* as the first ever application of quantum physics to cryptography, and is also credited for the invention of oblivious transfer—a key concept in modern cryptography that was re-discovered years later by Rabin [195]. Still today, the two areas are closely intertwined: for instance, two of the most well-known results in quantum information stand out as being related to cryptography: quantum key distribution (QKD) [24] and Shor's factoring algorithm [206].

There is no doubt that QKD has taken the spotlight in terms of the use of quantum information for cryptography (in fact, so much that the term "quantum cryptography" is often *equated* with QKD—a misconception that we aim to rectify here!); yet there exist many other uses of quantum information in cryptography. What is more, quantum information opens up the cryptographic landscape to allow functionalities that do not exist using classical[1] information alone, for example uncloneable quantum money. We note, however, that the use of quantum information in cryptography has its limitations and challenges. For instance, we know that quantum information alone is insufficient to implement information-theoretically secure bit commitment; and that a proof technique called *rewinding* (which is commonly used in establishing a zero-knowledge property for a protocol) does not directly carry over to the quantum world and must re-visited in light of quantum information.

In this paper, prepared on the occasion of the 25th anniversary edition of *Designs, Codes and Cryptography*, we offer a survey of some of the most remarkable theoretical uses of quantum information for cryptography, as well as a number of limitations and challenges that cryptographers face in light of quantum information. We assume that the reader is familiar with cryptography, but we do not assume any prior knowledge of quantum information. Quantum cryptography is a flourishing area of research, and we have chosen to give an overview of only a limited number of topics. The reader is, of course, encouraged to follow up by consulting the references. To the best of our knowledge, prior survey work on the topic of "quantum cryptography beyond key exchange" is limited to a 2006 survey by Müller-Quade [186] and a 1996 survey by Brassard and Crépeau [45]; see also an interesting personal account by Brassard [43]. A number of surveys that focus on QKD exist and are listed in Sect. 3.2.

1.1 Overview

The predictions of quantum mechanics defy our everyday intuition: concepts such as *superposition* (a particle can be in multiple places or states at the same time), *entanglement* (particles are correlated beyond what is possible classically) and *quantum uncertainty* (observing one property of a particle intrinsically degrades the possibility of observing another) are partly responsible for the bewildering possibilities in the quantum world. Section 2 of this survey contains a brief introduction to the mathematical formalism of quantum information as it pertains to quantum cryptography (no prior knowledge of quantum mechanics is assumed). Topics covered in this section include the mathematical formalism for the representation and manipulation of *qubits* (the fundamental unit of quantum information). We also include a brief survey of concepts such as the quantum no-cloning theorem, entanglement and nonlocality—all of which play an important role in quantum cryptography.

[1] We use the word "classical" here and throughout to mean "non-quantum".

Section 3 of this survey is devoted to quantum cryptographic constructions. The principal appeal in using quantum information for cryptography is in establishing a *qualitative* advantage. More precisely, the goal is to develop quantum cryptographic protocols that achieve some functionality in a way that is fundamentally advantageous compared to using classical information alone. This quantum advantage can be of the following types:

- a quantum protocol achieves statistical (information-theoretic) security; any classical protocol achieves this task with computational security at best;
- a quantum protocol achieves computational security; no classical protocol can achieve this task, even with computational security.

Many of the quantum constructions that we cover in this survey (whether they are of the first or second type) are inspired by the original proposal of Wiesner called *conjugate coding*. This construction embodies many unique features of quantum information, as we explain in Sect. 3.1. In particular, conjugate coding is used in constructions for physically unforgeable quantum money (Sect. 3.1), as well as in QKD—a method that allows the information-theoretically secure expansion of shared keys (Sect. 3.2). Another application of conjugate coding in quantum cryptography is in showing that two basic cryptographic primitives, *bit commitment* and *oblivious transfer* are (information-theoretically) *equivalent* in the quantum world (Sect. 3.3)—an equivalence that is provably false in the classical world. Technologically speaking, perfect quantum communication and storage is a challenge; in building protocols in the *bounded- and limited-storage quantum models* (collectively known as *limited-storage models*), ingenious cryptographers have turned this challenge to their advantage (Sect. 3.4)—once again, the key ingredient in the construction being conjugate coding. Motivated by the perspective that quantum computations will, in the future, be outsourced to remote locations (again, because of technological challenges involved in building quantum computers), cryptographers have studied protocols for the *delegation of quantum computations*, which we cover in Sect. 3.5. In Sect. 3.6, we review the possibility of quantum primitives that accomplish a security against malicious participants that is typically too weak for cryptographic applications (since it does not provide *exponential* security), yet is still of interest due to the advantage that quantum information provides: this is embodied in quantum protocols for *weak coin flipping* and *imperfect bit commitment*. Finally, we survey *device-independent cryptography* (Sect. 3.7) which can be seen as a culmination of many of the constructions already mentioned: thanks to this sophisticated technique, it is possible to achieve cryptographic tasks such as QKD and randomness expansion/amplification, with *untrusted devices*, which are quantum devices that are assumed to have originated from an adversary. The very possibility of achieving this result stems from one of the most mysterious quantum phenomena, namely *nonlocality* (which is introduced in Sect. 2.5).

While quantum information provides a number of advantages for cryptography, it also has its unique limitations and challenges, which we survey in Sect. 4. The first limitations that we survey are in terms of *impossibility* results, namely the impossibility of information-theoretically secure quantum bit commitment (Sect. 4.1) and of information-theoretically secure two-party quantum computation (Sect. 4.2). Next, we cover two topics that are applicable to purely classical protocols, in which essentially the only concern is that the adversary is capable of quantum information processing: *quantum rewinding* (Sect. 4.3) and *superposition attacks* (Sect. 4.4). We emphasize that the cryptographic challenges encountered here are not related to the superior computational power of a quantum adversary, but rather stem from quantum phenomena such as the no-cloning theorem (which forces us to develop an alternative to the common *rewinding* method used in order to establish the zero-knowledge property of interactive protocols), and of quantum superposition (which requires a new frame-

work describing interactions with oracles—namely in the *quantum random oracle model*). Finally, in Sect. 4.5, we survey the research area of position-based quantum cryptography, where players use their geographical position as cryptographic credential; while the current main result in this area is a no-go theorem for quantum protocols for the task of position verification, the *possibility* of position-based quantum cryptography against *resource-bounded* adversaries remains a tantalizing open question.

One of the lessons learned from all these impossibility results is that quantum security is definitely a tricky business—quantum cryptographers should take this as a warning: the desire to find a "quantum advantage" (i.e. an application where quantum information outperforms all classical solutions) is extremely strong, and cryptographers must be vigilant since the quantum world comes with an abundance of subtleties.

We note that the bibliographic entries in this survey are available as an open-source BibTEX file at https://github.com/cschaffner/quantum-bib.

1.2 Further topics

Already, the literature on quantum cryptography is vast, and in this survey we have chosen to focus on only a few topics. We briefly mention here some topics that are *not* included in this survey:

- **Everlasting security** A protocol has everlasting security if it is secure against adversaries that are computationally unlimited *after* the protocol execution. This type of security is very difficult to obtain classically, even under strong setup assumptions such as a common reference string or signature cards [219]. Even though we do not treat the notion explicitly in this survey, many quantum-cryptographic protocols such as QKD (Sect. 3.2) and the limited-quantum-storage protocols (Sect. 3.4) come with the important benefit of everlasting security. In fact, everlasting security might be the most important reason to use QKD in the first place [211].
- **Quantum functionalities** In this survey, we focus mainly on classical functionalities, but *quantum* functionalities are of course also of interest: assuming full quantum computers for all parties, one can study the secure realization of a quantum ideal functionality. This includes topics such as the encryption of quantum messages in the information-theoretic [9,41,134,153], entropic [95,96] and computational [52] settings, quantum secret sharing [77], multi-party quantum computation [22], authentication of quantum messages [15], two-party secure function evaluation [98,99], quantum anonymous transmission [49,74], quantum one-time programs [54] and quantum homomorphic encryption [52,239].
- **Key recycling** Using quantum information, it is possible to detect eavesdropping such that key re-use is possible (if no eavesdropping is detected), while maintaining information-theoretic security [87].
- **Quantum uncloneability** Because quantum information cannot, in general, be duplicated, (see Sect. 2.4), we can achieve functionalities related to copy-protection that cannot be obtained in the classical world. These include uncloneable encryption [125], quantum copy-protection [1] and revocable time-release encryption [221].
- **Isolation assumptions** The *multi-prover* interactive proof scenario [21] enables the information-theoretic implementation of primitives that are unachievable in the single-prover setting. However, the study of quantum information has shed new light on the "isolation" assumptions that are required in order to establish security [84]. Related to this is the study of protocols which are secure against provers sharing correlations that are very strong, yet do not allow signalling: [110,139]. One particular way to enforce isolation is to spatially separate the players by a far enough distance: the relativistic no-signalling

principle ensuring that no information can travel faster than the speed of light between the two sites. A relativistic (classical) bit-commitment scheme was first proposed by Kent [142] and lately improved and experimentally implemented [160]. See also related work [159].

- **Leakage resilience using quantum techniques** In *leakage resilient computation*, we are interested in protecting computations from attacks according to various leakage models. In one of these models (the "split-state" model), it was shown [93] that quantum information allows a solution to the *orthogonal-vector problem*, while no classical solution exists. Also, related work [151] shows that techniques from fault-tolerant quantum computation can be used to construct novel leakage-resilient classical protocols.
- **Quantum cryptanalysis** Historically, the study of quantum algorithms is closely related to *quantum cryptanalysis*, which is the study of quantum algorithms for cryptanalysis. This is evidenced by some of the very early work on quantum algorithms, including Shor's algorithm for computing discrete logarithms and integer factoring in quantum polynomial-time [206], Grover's search algorithm [40,126] (which provides a square-root speedup in term of query complexity, for searching in an unstructured database). Recent work in the area of quantum cryptanalysis includes [33,71,127,128,150,196]. See also [13,184] for surveys on quantum algorithms, as well as the *Quantum Algorithm Zoo*.[2]
- **Merkle puzzles in a quantum world** The first unclassified proposal for *secure communication over insecure channels* was made by Merkle in 1974 (published years later [176]). The main idea is that honest parties can establish a secure communication channel by expending work proportional to N, yet any successful attack requires a computational effort proportional to N^2. In a nutshell, Grover's search algorithm [126] implies that quantum computers break the security of Merkle's scheme. However, [50] show how to restore security in the quantum context: either by using a new classical protocol (in which case an adversary can break the scheme by expending work proportional to $N^{5/3}$ (which is shown to be optimal), or by using a quantum protocol (in which case the quadratic security can essentially be restored).
- **From classical to quantum security** What can we say about the relationship between security in the classical setting versus the quantum setting? In this context, Unruh [216] shows that if a protocol is statistically secure in the universal composability (UC) framework [63,216], then the same protocol is quantum UC secure as well, and Fehr, Katz, Song, Zhou and Zikas [113] classified the feasibility of cryptographic functionalities in the universal composability (UC) framework,[3] and showed that feasibility in the quantum world is equivalent (for a large family of functionalities) to classical feasibility, both in the computational and statistical setting. See also [129,210].
- **Post-quantum cryptography** The area of *post-quantum cryptography* [32][4] finds alternatives to the RSA and discrete-log assumptions in (classical) cryptography, in order to circumvent quantum attacks stemming from Shor's algorithm. This area is traditionally considered a topic related to classical cryptography, but the issues arising from the problem of quantum rewinding (Sect. 4.3) and the superposition model for oracle access (Sect. 4.4) may be considered part of post-quantum cryptography as well.

[2] http://math.nist.gov/quantum/zoo/.

[3] A primitive is feasible if it can be implemented in the UC model from secure channels only.

[4] The term is quite well-established by now, but chosen somewhat unfortunately, because the research area is concerned with cryptography which is still secure *at the beginning* and not after the end of the era of large-scale quantum computers.

- **Experimental implementations** Experimental implementations of quantum cryptography are mostly focused on QKD (see [8]), but also include quantum coin flipping [31,182,189], quantum secret sharing [212], delegated quantum computation [17,114], limited-quantum-storage cryptography [105,188], and device-independent randomness generation [75,194].

2 Basics of quantum information

This section contains the rudiments of quantum information that are used in the main text; we assume of the reader only basic knowledge of linear algebra. The reader should be warned that quantum theory is actually much more rich, subtle and beautiful! Textbook references on quantum information include: [141,177,190,228,234].

2.1 State space

The *bit* is the fundamental unit of information for classical information processing. In quantum information processing, the corresponding unit is the *qubit*, which is described mathematically by a vector of length one in a two-dimensional complex vector space. We use notation from physics to denote vectors that represent quantum states, enclosing vectors in a *ket*, yielding, i.e. $|\psi\rangle$. We can write any state on one qubit as a $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where the states $|0\rangle$ and $|1\rangle$ form a basis for the underlying two-dimensional vector space, and where α, β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. If neither α nor β are zero, then we say that $|\psi\rangle$ is in a *superposition* (linear combination) of both $|0\rangle$ and $|1\rangle$. The quantum state of two or more qubits can be described by a tensor product. Hence, the four basis states for two qubits are $|0\rangle\otimes|0\rangle$, $|0\rangle\otimes|1\rangle$, $|1\rangle\otimes|0\rangle$, $|1\rangle\otimes|1\rangle$ which is usually abbreviated as $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Extending the concept of superposition to multiple qubits, we see that a system of n qubits can be in any superposition of the n-bit basis states $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$. Hence, an n-qubit state is described by 2^n complex coefficients. In case of *bipartite* quantum states shared among Alice and Bob, subscripts can be used to indicate which player holds which qubits. For instance, the 2-qubit state $|0\rangle_A \otimes |0\rangle_B = |00\rangle_{AB}$ means that Alice and Bob both hold a qubit in state $|0\rangle$.

2.2 Unitary evolution and circuits

Basic evolutions of a quantum system are described by linear operations that preserve the norm; formally, these operations can be expressed as *unitary* complex matrices (a complex matrix U is *unitary* if $UU^\dagger = \mathbb{I}$, where $U^\dagger$ is the complex-conjugate transpose of U). Quantum algorithms are commonly described as circuits (rather than by quantum Turing machines) consisting of basic quantum gates from a universal set. Commonly used single-qubit gates are the negation (X), phase (Z) and Hadamard (H) gates, expressed by the following unitary matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1}$$

An example of a two-qubit gate is the controlled-not operation ($CNOT$):

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2}$$

2.3 Measurement

In addition to unitary evolution, we specify an operation called *measurement*, which, in the simplest case, takes a qubit and outputs a classical bit. If we measure a qubit $|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$, we will get as outcome a single bit, which takes the value 0 with probability $|\alpha|^2$ and the value 1 with probability $|\beta|^2$. We further specify that, after the process of measurement, the quantum system *collapses* to the measured outcome. Thus, the quantum state is *disturbed* and it becomes *classical*: any further measurements have a deterministic outcome. We have described measurement with respect to the *standard basis*; of course, a measurement can be described according to an arbitrary basis; the probabilities of the outcomes can be computed by first applying the corresponding change-of-basis, followed by the standard basis measurement. Measurements can actually be described much more generally: e.g. we can describe outcomes of measurements of a strict subset of a quantum system—the mathematical formalism to describe the outcomes uses the *density matrix* formalism, which we do not describe here.

As a simple example of quantum measurements, consider the states $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \beta|1\rangle)$. Then measuring the state $|\psi_1\rangle$ yields the outcome 1 with unit probability and the state remains $|0\rangle$, while measuring $|\psi_2\rangle$ yields the outcome 0 or 1, each with probability $\frac{1}{2}$, and the post-measurement state is $|0\rangle$ if we observed outcome 0 and $|1\rangle$ if we observed 1.

2.4 Quantum no-cloning

One of the most fundamental properties of quantum information is that it is not physically possible, in general, to *clone* a quantum system [236] (i.e. there is no physical process that takes as input a single quantum system, and outputs two identical copies of its input). A simple proof follows from the linearity of quantum operations.[5] At the intuitive level, this principle is present in almost all of quantum cryptography, since it prevents the classical reconstruction of the description of a given qubit system. For instance, given a single copy of a general qubit $\alpha|0\rangle + \beta|1\rangle$, it is not possible to "extract" a full classical description of α and β, because measuring disturbs the state. At the formal level, however, we generally require more sophisticated tools to prove the security of quantum cryptography protocols (see Sect. 3.1).

2.5 Quantum entanglement and nonlocality

A crucial and rather counter-intuitive feature of quantum mechanics is *quantum entanglement*, a physical phenomenon that occurs when quantum particles behave in such a way that the quantum state of each particle cannot be described individually. A simple example of such an entangled state are two qubits in the state $(|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$. When Alice measures her qubit (in system A), she obtains a random bit $a \in \{0, 1\}$ as outcome and her qubit collapses to the state $|a\rangle_A$ she observed. At the same time, Bob's qubit (in system B) also collapses to $|a\rangle_B$ and hence, a subsequent measurement by Bob yields the same outcome $b = a$. It is important to realize that this collapse of state at Bob's side occurs simultaneously with Alice's measurement, but it does not allow the players to *send information* from Alice to Bob.

[5] Assume a quantum operation A which takes as input a qubit in state $|\psi\rangle$ (together with a "helping" qubit in state $|0\rangle$) and outputs $|\psi\rangle|\psi\rangle$. Hence, $A|0\rangle|0\rangle = |0\rangle|0\rangle$ and $A|1\rangle|0\rangle = |1\rangle|1\rangle$. By linearity of A, it must hold that $A\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle = \frac{A|0\rangle|0\rangle+A|1\rangle|0\rangle}{\sqrt{2}} = \frac{|0\rangle|0\rangle+|1\rangle|1\rangle}{\sqrt{2}}$ which is not equal to the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ which we would expect as output from a perfect copying operation A. Hence, such an A does not exist.

It simply provides Alice and Bob with a shared random bit. In general, quantum entanglement does not contradict the fundamental *non-signaling principle* of the theory of relativity stating that no information can travel faster than the speed of light.[6]

It turns out that by measuring entangled quantum states, Alice and Bob are able to produce correlations that are stronger than all correlations they could obtain when sharing only classical randomness. In this case, physicists say that the correlations *violate a Bell inequality* [20]. The most well-known example of such an inequality was proposed by Clauser, Horne, Shimony and Holt [76]. It can be described as a so-called *non-local game* among two players Alice and Bob. In this CHSH game, Alice and Bob can initially discuss in order to establish a joint strategy. Once the game starts, they are separated and cannot communicate. They receive as input uniformly random bits x and y and have to output bits a and b respectively. They win the game if and only if $a \oplus b = x \wedge y$ (imagine a third party, called a *referee* who chooses x and y, receives a and b and checks whether the relationship $a \oplus b = x \wedge y$ holds). A possible classical strategy for Alice and Bob is to ignore their inputs and always output $a = b = 0$. This strategy lets them win the game with probability $3/4$. It can be checked that there exist no better strategy for two classical players who are not allowed to communicate. In other words, we have the Bell inequality $\Pr[\text{classical players win CHSH}] \leq 3/4$. However, if Alice and Bob share a maximally entangled state (e.g. an EPR pair $(|00\rangle + |11\rangle)/\sqrt{2}$), they can perform a quantum measurement which allows them to win the CHSH game with probability $\cos^2(\pi/8) \approx 0.85$ which is strictly larger than $3/4$, hence violating the Bell inequality. Many experimental tests of this inequality have been performed and consistently found violations of this inequality, thereby proving that the world is actually more accurately described by quantum mechanics rather than by classical mechanics.

2.6 Physical representations

The mathematical model of quantum mechanics is currently the most accurate description of the physical world. This theory is without doubt the most successful and well-tested physical theory of all times; it describes a wide range of physical systems, and thus offers a large number of possible physical systems which can serve as quantum devices. These possibilities include photonic quantum computing, superconduction qubits, nuclear magnetic resonance, ion trap quantum computing and atomic quantum computing (see, e.g. [94]). For our purposes, at the abstract level, all of these systems are described by the same formalism; however there may be experimental reasons to prefer one implementation over the other (e.g. photons are well-suited for long-distance quantum communications, but other systems such as superconducting qubits are better suited for quantum interactions).

3 Quantum cryptographic constructions

In this section, we survey a number of quantum cryptographic protocols (see Sect. 1.1 for a brief overview of these topics). Many of these protocols share the remarkable feature of being based on a very simple pattern of quantum information called *conjugate coding*. Because of its paramount importance in quantum cryptography, we first present this notion in Sect. 3.1. We then show how conjugate coding is the crucial ingredient in the quantum-cryptographic constructions for quantum money (Sect. 3.1), QKD (Sect. 3.2), a quantum

[6] However, this "spooky action at a distance" puzzled Einstein a lot, and was the inspiration for his very influential paper co-authored with Podolsky and Rosen [103]. Nowadays, we often call two qubits in the maximally entangled state $(|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$ an *EPR pair*.

Table 1 Example of conjugate coding

Encoded bit:	0	0	1	0	1	1	0	0	0	0
Basis choice:	*R*	*D*	*D*	*D*	*R*	*R*	*D*	*R*	*R*	*D*
Quantum encoding	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$

Note that, we use the abbreviation *R* for the *rectilinear* basis and *D* for the *diagonal* basis

reduction from oblivious transfer to bit commitment (Sect. 3.3), the limited-quantum-storage model (Sect. 3.4) and delegated quantum computation (Sect. 3.5). Further topics covered in this section are quantum coin-flipping (Sect. 3.6) and device-independent cryptography (Sect. 3.7).

3.1 Conjugate coding

Conjugate coding [233] is based on the principle that we can encode *classical information* into *conjugate* quantum bases. This primitive is extremely important in quantum cryptography—in fact, the vast majority of quantum cryptographic protocols exploit conjugate coding in one way or another. Conjugate coding is also called *quantum coding* [30] and *quantum multiplexing* [26].

The principle of conjugate coding is simple: for clarity of presentation and consistency with commonly used terminology, we associate a qubit with a photon (a particle of light), and use photon polarization as a quantum degree of freedom. Among others, photons can be polarized horizontally ($|\leftrightarrow\rangle$), vertically ($|\updownarrow\rangle$), diagonally to the left ($|\nwarrow\rangle$), or diagonally to the right ($|\nearrow\rangle$). Photon polarization is a quantum property, and by associating $|\leftrightarrow\rangle = |0\rangle$,$|\updownarrow\rangle = |1\rangle$, $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, we can apply quantum operations to these states, as in Sect. 2.

Each set $R = \{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ and $D = \{|\nwarrow\rangle, |\nearrow\rangle\}$ forms a basis (called the *rectilinear* and *diagonal* bases, respectively), and can thus be used to encode a classical bit (see Table 1). *R* and *D* are *conjugate bases*.

The relevance of conjugate coding to cryptography is summarized by two key features that were, remarkably, already mentioned and exploited in Wiesner's work [233]:

1. Measuring in one basis irrevocably destroys any information about the encoding in its conjugate basis.
2. The originator of the quantum encoding can verify its authenticity; however, without knowledge of the encoding basis, and given access to a *single* encoded state, no third party can create two quantum states that pass this verification procedure with high probability.

In order to explain the first property, recall the well-known *Heisenberg uncertainty relation* [135], which forbids learning both the position and momentum of a quantum particle precisely and simultaneously. In terms of photon polarization, and for a single photon, let us denote by P_X the distribution of outcomes when measuring the photon in the rectilinear basis and by Q_X the distribution when measuring in the diagonal basis. Following Heisenberg, Maassen and Uffink [162] showed an *uncertainty relation*: $H(P_X) + H(Q_X) \geq 1$ (where H is the *Shannon entropy*, an information-theoretic measure of uncertainty given by $H(P_X) = -\sum_x p_x \log_2 p_x$). Intuitively, such a relation quantifies the fact that one can know the outcome exactly in one basis, but consequently has complete uncertainty in the other basis. Looking ahead, we will see that such uncertainty relations play a key role in proving security of quantum cryptographic protocols, e.g. in the limited-quantum-storage setting (Sect. 3.4).

The second property above is explained by noting that a quantum encoding can be verified by measuring each qubit in its encoding basis and checking that the measurement result corresponds to the correct encoded bit. Intuitively, the *no-cloning* theorem (Sect. 2.4) prevents a third party from *forging* a state that would pass this verification procedure; however, formalizing this concept requires more work (see Sect. 3.1).

What is more, the technological requirements of conjugate coding are very basic: the single-qubit "prepare-and-measure" paradigm of conjugate coding is feasible with today's technology—thus, many protocols derived from conjugate coding inherit this desirable property (which is, in fact considered the *gold standard* for "feasible" quantum protocols).

In the late 1960s, Wiesner [233] had the visionary idea that quantum information could be used to create unforgeable bank notes. His ideas were in fact so much ahead of their time that it took years to publish them! (According to [30], Wiesner's original manuscript was written in 1968.)

In a nutshell, Wiesner's proposal consists in *quantum banknotes* created by encoding quantum particles using conjugate coding (Sect. 3.1), with both the classical information and basis choice being chosen as random bitstrings. Thus, a banknote consists of a sequence of single qubits, chosen randomly from the states $\{|\updownarrow\rangle, |\leftrightarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle\}$. As discussed in Sect. 3.1, the originator of the quantum banknote (typically called "the bank") can verify that a quantum banknote is genuine, yet quantum mechanics prevents essentially any possibility of counterfeiting. Clearly such a functionality is beyond what classical physics can offer: since any digital record can be copied, classical information simply cannot be used for uncloneability (not even computational assumptions will help).

Wiesner's work was improved and extended in many ways: early work of Bennett, Brassard, Breidbart and Wiesner [26] showed how to combine computational assumptions with conjugate coding in order to achieve a type of *public verifiability* for the encoded states (they coined their invention *unforgeable subway tokens*). Further work on publicly-verifiable (also called *public-key* quantum money) includes schemes based on the computational difficulty of some knot-theory related problems [107] (see also [3]), verification "oracles" [1] and hidden subspaces [2].

Returning to Wiesner's scheme (which is often called *private-key* quantum money in order to distinguish it from the public-key quantum money schemes), we note that the first proof of security in the case of multiple qubits is based on semi-definite programming, and appeared only recently [181] (this result is tight, since it also gives an explicit *optimal* attack). We also note work on variants of Wiesner's scheme in which quantum encodings are returned after validation: in all cases (whether the post-verification state is always returned [108], or the post-verification state is returned *only for encodings that are deemed valid* [55]), the resulting protocol has been found to be insecure.

We also note that further work has studied the possibility of private-key quantum money that can be verified using only *classical* interaction with the bank [116,181], quantum *coins* [185] (which provide a perfect level of anonymity), as well as noise-tolerant versions of Wiesner's scheme [191].

3.2 Quantum key distribution

QKD is by far the most successful application of quantum information to cryptography. By now, QKD is the main topic of a large number of surveys (see, for instance, [23,45,56,109,120]). Due to abundance of very good references on this topic, we survey it only briefly here.

The "BB84" protocol [24,25] was the first to show how conjugate coding could be used for an information-theoretically secure key agreement protocol. In a nutshell, the protocol consists in Alice sending a sequence of single qubits, chosen randomly from the states $\{|\updownarrow\rangle, |\leftrightarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle\}$. Bob chooses to measure them according to his own random choice of measurement bases. They communicate their basis choice for each encoded qubit; *eavesdropper detection* is performed by comparing the measurement results on a fraction of the bases on which their choices coincide—if successful, this procedure gives a bound on the secrecy and similarity of the remaining shared string, which can be used to distill an almost-perfect shared secret between Alice and Bob. In order to prevent man-in-the-middle attacks, this procedure requires *authenticated* classical channels. Usually, authentication is achieved by an initial shared classical secret between Alice and Bob. Thus, QKD is more accurately described as a key-expansion primitive. We note that, as a theoretical or experimental tool, it is often useful to consider a protocol equivalent to BB84, where the random choice of encoding basis (rectilinear of diagonal) is *delayed*; thus a quantum source would produce a sequence of maximally entangled states $(|00\rangle + |11\rangle)/\sqrt{2}$, with both Alice and Bob then measuring in their random choice of bases. That an entangled system could be used in lieu of single qubits was suggested by Ekert [104], but note that Ekert's idea was to base security on the observation of a Bell-inequality violation—which implies a set of different measurements than in the rectilinear/diagonal bases. The entanglement-based ("purified") BB84 protocol was introduced by Bennett, Brassard and Mermin in [28].

We briefly mention that the formal security of QKD was originally left open, and that a long sequence of works (e.g. [158,171]) culminated in a relatively accessible proof by Shor and Preskill, based on the use of quantum error correction [207]. Further work by Renner [198] showed a very different approach for proving the security of QKD based on exploiting the symmetries of the protocol (and applying a *de Finetti* style representation theorem), and splitting the security analysis into the information-theoretic steps of error-correction and privacy amplification. Other proofs of QKD are more directly based on the complementarity of the measurements [148]. It is a sign for the complexity of QKD security proofs that most articles on this topic focus only on subparts of the security analysis and only very recently did a first comprehensive analysis of security appear [213].

The huge success of QKD is due in part to the fact that it is readily realizable in the laboratory (the first demonstration appeared in 1992 [27]). In light of practical implementations, security proofs for QKD need to be re-visited in order to obtain concrete security parameters—this is the realm of *finite-key security* [133,204,213,214]. Furthermore, we note that when it comes to real-world implementations, QKD is vulnerable to *side-channel* attacks, which are due to the fact that physical implementations deviate from the idealized models used for security proofs (this is often referred to as *quantum hacking* [161]).

We further note that the assumption of an initial short shared secret (for authenticating the classical channel) in the implementation of QKD can be replaced with a computational assumption or an assumption about the storage capabilities of the eavesdropper (see Sect. 3.4). The result is *everlasting* [219] or *long-term* [211] security: information-theoretic security is guaranteed *except* during the short period of time during which we assume a computational (or memory) assumption holds.

3.3 Bit commitment implies oblivious transfer

Oblivious transfer (OT) and bit commitment (BC) are two basic and important primitives for cryptography. In the classical case, it is easy to show that OT implies BC (in the information-

theoretic setting), but the implication in the other direction does not hold.[7] In stark contrast, OT and BC are known to be *equivalent* in the quantum world. In the following sections, we introduce these primitives (Sect. 3.3.1) and describe a quantum reduction from oblivious transfer to bit commitment (Sect. 3.3.2).

3.3.1 Oblivious transfer (OT) and bit commitment (BC)

Wiesner's paper about quantum cryptography [233] introduced "a means for transmitting two messages either but not both of which may be received". This classical cryptographic primitive was later rediscovered (under a slightly different form) by Rabin [195], and was given in the form of *1-out-of-2 Oblivious Transfer (OT)*) by Even, Goldreich and Lempel [106]. In OT, Alice sends two messages m_0, m_1 to Bob who receives only one of the messages m_c according to his choice bit c. Security for Alice (against dishonest Bob) guarantees that Bob receives only one of the two messages, whereas security for Bob (against dishonest Alice) ensures that Alice does not learn anything about Bob's choice bit.[8] In the version by Rabin [195], this primitive is essentially a secure erasure channel where Alice sends a single bit to Bob. This bit gets erased with probability 1/2 (in this case Bob receives $\perp$), but Alice does not learn whether the bit was erased. In fact, it is known that Rabin OT is *equivalent* to 1-out-of-2 OT [81].

The importance of OT is embodied by the fact that it is *universal* for secure two-party computation [145] (i.e. using several instances of 1-out-of-2 OT, any function can be securely evaluated among two parties such that no dishonest player can learn any information about the other player's input—beyond what can already be inferred from the output of the computed function).[9] Due to this universality, the innocent-looking OT primitive gives an excellent indicator for the cryptographic power of a model.

Bit Commitment (BC) is a cryptographic primitive that captures the following two-party functionality: Alice has a bit b that she wants to commit to Bob, but she wants to prevent Bob from reading b until she chooses to reveal it (*concealing* or *hiding*). Although Bob should not be able to determine b before Alice reveals it, Alice should be unable to change the bit after it is committed (*binding*). A physical-world implementation of bit commitment would be for Alice to write b on a piece of paper, lock it in a safe, and send the safe to Bob. Since Bob cannot open the safe, he cannot determine b (concealing), and since Alice has physically given the safe to Bob, she cannot change b after the commitment phase (binding). When Alice wishes to reveal the bit, she sends the key to Bob.

3.3.2 Quantum protocol for oblivious transfer

In [29], Bennett, Brassard, Crépeau, and Skubiszewska suggested a very natural quantum protocol for OT (assuming BC): suppose Alice would like to obliviously send m_0 and m_1 so that Bob receives the message m_c according to his choice bit c. She uses conjugate coding to send n quantum states each chosen randomly from the states $\{|\updownarrow\rangle, |\leftrightarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle\}$ to Bob. Let us denote by $x \in \{0,1\}^n$ the string of encoded bits and by $\theta \in \{R, D\}^n$ the string of basis

[7] See [219, Lemma 7] for a proof in the UC framework; the stand-alone impossibility is folklore and can be derived from the impossibility of OT in the plain model [156] (see also Sect. 4.2).

[8] In fact, formalizing these innocent-looking requirements correctly turns out to be rather tricky [83,111].

[9] A prime example of a secure two-party computation is Yao's millionaire's problem [237]: two millionaires want to compare their fortune without telling the other specifically how much money they own. This problem can be solved by the secure computation of the greater-than function.

choices. Bob measures the received qubits in a random basis $\theta' \in \{R, D\}^n$ of his choice, resulting in outcomes $x' \in \{0, 1\}^n$. After Alice tells Bob the bases $\theta \in \{R, D\}^n$ she was using, Bob can partition the set of indices into two disjoint sets $I_0 \cup I_1 = \{1, 2, \ldots, n\}$: depending on his OT choice bit c, he puts all the indices where he measured correctly in I_c and the rest in I_{1-c}. Bob then informs Alice about I_0, I_1 (in this fixed order, independent of c). Alice picks two independent hash functions f_0, f_1 (mapping from $n/2$ bits to 1 bit) and sends $s_i = f_i(x|_{I_i}) \oplus m_i$ for $i = 0, 1$ to Bob. Here, $x|_I$ denotes the substring of x with bit indices in I. Bob will be able to recover m_c by computing $f_c(x'|_{I_c}) \oplus s_c$.

While it is easy to show that the above protocol is correct and secure against dishonest Alice (i.e. Alice does not learn anything about Bob's choice bit c), it is clearly insecure against a dishonest Bob who is able to store all quantum states until Alice tells Bob the basis string θ. Such a Bob can then measure all positions in the correct basis and hence recover both m_0 and m_1. The idea of [29] was to *force* Bob to perform the measurement by requiring him to commit to the bases θ' and outcomes x'. Alice then checks a fraction of these commitments *before* Alice announces the basis string θ.

A long line of research [29,82,168,172,238] has worked towards proving the security of this protocol. However, the crucial tools for an actual proof were eventually developed by Damgård, Fehr, Lunemann, Salvail, and Schaffner [91] nearly two decades after the original protocol was proposed; Unruh subsequently used these techniques to formally establish the equivalence of BC and OT in the quantum UC model [216].

3.4 Limited-quantum-storage models

As we will see in Sect. 4.1, bit commitment is impossible to construct in the quantum world. More generally, it has been shown (see Sect. 4.2) that secure two-party computation is impossible in the plain quantum model, without any additional restrictions on the adversaries. One option in order to obtain security is to make computational assumptions. However, as we discuss below, it is also possible to obtain information-theoretic security, while making instead some reasonable assumptions about the storage capabilities of the adversary.

One of the challenges in building quantum devices is the difficulty of storing quantum information in a physical system (such as atomic or phototonic systems) under stable conditions over a long period of time—building a reliable quantum memory is a major research goal in experimental quantum physics (see e.g. [208] for a review produced by the European integrated project *Qubit Applications (QAP)*). Despite continuous progress over the last years, large-scale quantum memories that can reliably store quantum information are currently out of reach. As we discuss in this section, ingenious quantum cryptographers have turned this technological challenge into an advantage for quantum cryptography!

The *bounded-quantum-storage* model, introduced by Damgård, Fehr, Salvail and Schaffner in [86], is a model which assumes that an adversary can only store a limited number of qubits. Generally, protocols in this model require no quantum storage for the honest players, and are secure against adversaries that are unable to store a constant fraction of the qubits sent in the protocol.

This model is inspired by the classical bounded-storage model, as introduced by Maurer [62,167]. In this model, honest parties are required to store $\Theta(n)$ bits, but protocols (for OT and key agreement) are insecure against attackers with storage capabilities of $\Omega(n^2)$ bits. Unfortunately, this gap between storage requirements for honest and dishonest players can never be bigger than quadratic [101,102]. Combined with the fact that classical storage is constantly getting smaller and cheaper, this quadratic gap puts the classical-bounded-storage assumption on a rather weak footing. In sharp contrast, the *quantum* bounded-storage

model gives an unbounded gap between the quantum-storage requirements of the honest and dishonest players, making this model model robust to technological improvements.

In the bounded-quantum storage model, a protocol for OT was proposed [86]. Again, it is based on conjugate coding and is essentially identical to the protocol outlined in the previous Sect. 3.3.2, except that there is a waiting time Δt (say, 1 s) right after the quantum phase, before Alice sends her basis string θ to Bob. In this time, a dishonest receiver Bob is forced to use his (imperfect) quantum memory and therefore loses some information about Alice's string x which intuitively leads to the security of the oblivious transfer. In a subsequent series of works [88–90], protocols for BC, OT and password-based identification (i.e. the secure evaluation of the equality function) were presented. For an overview of these results, see [109,205].

The *noisy-quantum-storage* model, as introduced by Wehner, Schaffner and Terhal [231] captures the difficulty of storing quantum information more realistically. Whereas in the bounded-quantum-storage model, the *physical number of qubits* an attacker can store is limited, dishonest players are allowed arbitrary (but imperfect) quantum storage in the noisy-quantum-storage model.

Beyond limited quantum storage Continuing the idea of assuming realistic technological restrictions on the adversary, researchers have developed protocols that are secure under the assumption that certain classes of quantum operations are hard to perform. A natural class to study consists of adversaries who can store perfectly all qubits they receive, but who cannot perform any quantum operations, except for single-qubit measurements (adaptively in arbitrary bases) at the end of the protocol. Such a model was first studied by Salvail [201], and later by Bouman, Fehr, Gonzáles-Guillén and Schaffner [39] and Liu [138,154,155] under the name of "isolated-qubit model".

Cryptographic proof techniques In Sect. 3.1, we mentioned *uncertainty relations* (and in particular *entropic* uncertainty relations—which quantify uncertainty in information-theoretic terms). These relations play a key role in the security proofs for protocols in the limited-quantum-storage model. We refer to [229] for a survey by Wehner and Winter on this topic. In fact, one can argue that the areas of limited-quantum storage models and entropic uncertainty relations have benefited a lot from each other, as research questions in one area have led to results in the other and vice versa. This fruitful co-existence is witnessed by a series of publications: [34,35,39,100,187].

Composability It is natural to ask whether limited-quantum-storage protocols for basic tasks such as OT can be composed to yield more involved two- or multi-party secure computations. This question was answered in the positive in a number of works, including: Fehr and Schaffner [111], Wehner and Wullschleger [230] (for sequential composition) and Unruh [217] (for bounded concurrent composition).

Implementations The technological requirements to implement limited-quantum-storage protocols in practice are modest and rather similar to already available QKD technology (often, the actual quantum phase is the same as in QKD). A small but significant difference is that it makes sense to run secure computations among players which are located within a few meters of each other, whereas the task of distributing keys demands large separations between players. This difference allows experimenters to optimize some parameters (such as the rate) differently for secure-computation protocols. The experimental feasibility of these protocols was analyzed theoretically in [232] and demonstrated practically in [105,188].

3.5 Delegated quantum computation

Quantum computers are known to enable extraordinary computational feats unachievable by today's devices [126,184,206]. However, technologies to build quantum computers are currently in their infancy; the current state-of-the-art suggests that, when quantum computers become a reality, these devices are likely to be available at a few location only. In this context, we envisage the outsourcing of quantum computations from quantum computationally weak clients to universal quantum computers (a type of *quantum cloud* architecture). This scenario has appealing cryptographic applications, such as the delegated execution of Shor's algorithm [206] for factoring, and thus breaking RSA public keys [200]. From the cryptographic point of view, this scenario raises many questions in terms of the possibility of privacy in delegated quantum computation.

Pioneering work of Childs [70] and Arrighi and Salvail [12] studied this problem for the first time. The first practical and universal protocol for private delegated quantum computation, called "universal blind quantum computation" (uBQC) was given by Broadbent, Fitzsimons and Kashefi [53]. In uBQC, the client only needs to be able to prepare random single-qubit auxiliary states (the client requires no quantum memory or quantum processor). Via a classical interaction phase, the client remotely drives a quantum computation of her choice, such that the quantum server cannot learn any information about the computation that is performed—with only the client learning the output. The uBQC protocol has been demonstrated experimentally [17].

It is remarkable that uBQC is *also* based on conjugate coding! For the first time, it is an application where the states derived from conjugate coding are used to directly achieve *computational* cryptographic tasks (vs other applications of conjugate coding which essentially directly measure these states in order to extract classical information). This relationship with conjugate coding is more clearly apparent in a related protocol called "quantum computing on encrypted data" (QCED) [51,114]. Here, the computation (as given by a quantum circuit) is public, but is executed remotely on an *encrypted* version of the data (reminiscent of the work on classical *fully homomorphic encryption* [117,199]). In this situation, QCED shows that it is possible to achieve delegated quantum computation where the client only needs to send random states in $\{|\leftrightarrow\rangle, |\updownarrow\rangle, |\nwarrow\rangle, |\nearrow\rangle\}$ (hiding of the computation itself can be achieved via a universal circuit construction).

We mention further that the *verifiability* of delegated quantum computations has been addressed in [5,54], and has been the object of an experiment [18], and that security has been analyzed in terms of a strong notion of *composability* [97]. Furthermore, work of Reichardt, Unger and Vazirani shows that delegated quantum computation is achievable for a purely classical client, if we are willing to make the assumption of *two* universal quantum computers that cannot communicate [197] (see also Sect. 3.7).

3.6 Quantum protocols for coin flipping and cheat-sensitive primitives

In a classic cryptography paper [36], Blum describes how to "flip a coin over the telephone" with the help of bit commitment: Alice commits to a random bit a, Bob tells Alice another random bit b, and Alice opens the commitment to a. The outcome of the coin is $a \oplus b$ which cannot be biased by any of the two players (intuitively, because at least one random bit of an honest player was involved in determining the outcome). A coin flip with this property is called a *strong* coin flip. In contrast, for a weak coin flip, Alice and Bob have a desired outcome, i.e. Alice "wins" if the outcome is 0, and Bob "wins" if the outcome is 1. A weak-coin-flipping protocol with bias ε guarantees that no dishonest player can bias the coin towards his or her

desired outcome with probability greater than ε. In the classical world, coin-flipping can be achieved under computational assumptions. However, in the information-theoretic setting, it was shown [130,136] that one of the players can always achieve his desired outcome with probability 1.

In the quantum world, we note that the general impossibility results for quantum two-party computation (Sect. 4.2) are not applicable to coin flipping, since the participants in a coin flipping protocol have no inputs, and instead aim to implement a *randomized* functionality. Nevertheless, Kitaev showed [146] (see also [10]) that any quantum protocol for strong coin-flipping is insecure since it can be biased by a dishonest player. Formally, the bias of any strong coin-flipping protocol is bounded from below by $\frac{1}{\sqrt{2}} - \frac{1}{2}$. Interestingly, Mochon [180] managed to expand Kitaev's formalism of *point games* to prove the existence of a *weak* coin-flipping protocol with arbitrarily small bias $\varepsilon > 0$. Unfortunately, Mochon's 80-page proof has never been peer-reviewed and is rather difficult to follow. Aharonov, Chailloux, Ganz, Kerenidis and Magnin [6] have managed to simplify this proof considerably.

Based on this result, Chailloux and Kerenidis [66] derived an optimal strong-coin-flipping protocol with the best possible bias $\frac{1}{\sqrt{2}} - \frac{1}{2}$, matching Kitaev's lower bound. Also based on a weak-coin flip, Chailloux and Kerenidis [67] gave the best possible imperfect quantum bit commitment. For the optimality, they prove that in any quantum bit commitment protocol, one of the players can cheat with significant probability.[10] Such a result shows that an imperfect bit commitment cannot be amplified to a perfect one—which severely limits the applicability of the scheme to the cryptographic setting.

Cheat sensitivity Quantum mechanics offers the possibility to construct imperfect cryptographic primitives in the sense that they are correct (as long as the players are honest), but they are insecure, i.e. they do allow one of the players (say Alice) to cheat. However, the other player Bob has the possibility to check if Alice has been cheating (possibly by sacrificing the protocol outcome he would have obtained if he followed the protocol without checking). Hence, a cheating Alice has non-zero probability to be detected. These protocols are called *cheat sensitive* [4,57,118,119,132,137]. In this context, it is argued that one could set up a game-theoretic environment: a player caught cheating has to pay a huge fine (or undergo another punishment) and is therefore deterred from actually doing it.

We note, however, that the applications of cheat sensitive protocols to the cryptographic setting are limited: while quantum protocols for imperfect and cheat-sensitive primitives can provide nice examples of separations between the classical and quantum worlds, they fulfill their purpose as long as they are considered as "final products", for instance in case of private information retrieval. However, it is difficult to argue that a strong coin flip with a constant bias, an imperfect bit commitment, or imperfect OT are cryptographically useful primitives, because they do not inherit the cryptographic importance of their perfect counterparts which can be used as building blocks for more advanced cryptographic primitives. In the case of cheat sensitivity, it is often unclear how such primitives behave under composition. In fact, it is a challenging open question to come up with a composability framework for cheat-sensitive quantum primitives.

[10] Formally, $\max\{P_A^*, P_B^*\} \geq 0.739$ where P_A^* is the average over the probabilities that a dishonest committer Alice successfully reveals bit $b = 0$ and successfully reveals $b = 1$; and P_B^* is the probability that a dishonest verifier Bob guesses the committed bit b after the commitment phase. $P_A^* = P_B^* = \frac{1}{2}$ holds for a perfect bit-commitment protocol.

3.7 Device-independent cryptography

An exciting feature of quantum cryptography is that it allows the possibility of *device-independent cryptography* in the sense that protocols can be run on untrusted devices which have possibly been constructed by the adversary. The crucial insight is that the "quantumness" of two (or more) devices can be tested and guaranteed by using the devices to violate a Bell inequality, i.e. to produce correlations that are stronger than allowed by classical mechanics. As outlined in Sect. 2.5, the most well-known example of such an inequality is the CHSH game [76]. The key observation of device-independent cryptography is that in order to violate the CHSH inequality, a certain amount of intrinsic quantum randomness has to be present in the players' outputs. That we could exploit this relationship for cryptography was originally pointed out by Ekert [104], and further studied by Mayers and Yao [173] and Barrett, Hardy and Kent [16]. In fact, this latter work shows not only how to accomplish cryptography with untrusted devices, but also how to do away completely with assumptions on the validity of quantum mechanics: instead, it shows how to accomplish QKD solely based on the non-signaling principle [131,166]!

The relation between the CHSH violation and the amount of entropy in the outcomes of the measurements can be quantified exactly [194]. In fact, on the topic of *self-testing quantum devices* [163,174,175,178], Reichardt, Unger and Vazirani have shown a strong robustness result [197] in the sense that being close to winning the CHSH-game with optimal probability implies that the players must essentially be in possession of a state which is close to an EPR pair. This is an extremely powerful result which has various applications.

The two qubits of an EPR state are maximally entangled. Quantum mechanics forbids any third party to be entangled with such a state (a phenomenon called *monogamy of entanglement*). Hence, measurements on an EPR state result in shared randomness which is guaranteed to be unknown to any eavesdropper.[11] In a similar vein, one can argue that the measurement outcomes of Alice and Bob while successfully playing the CHSH game cannot be known to any adversary *even if this adversary has built the devices herself and is possibly still entangled with them*.

This effect leads to the interesting cryptographic applications of *device-independent randomness amplification and expansion* and *device-independent QKD*. In *randomness amplification*, the task at hand is to obtain near-perfect randomness from a weak random source using untrusted quantum devices (without using any additional randomness); this idea was originally proposed by Colbeck and Renner [80]. In *randomness expansion*, one wants to expand a few truly random bits into more random bits, again using untrusted quantum devices; this idea was originally proposed by Colbeck and Kent [67,78]. Providing formal security proofs has turned out to be rather challenging and was first established against classical adversaries [112,193,194], and later also against quantum adversaries [179,224]. A combination of the latest protocols allows to arbitrarily amplify very weak sources of randomness in a device-independent fashion. Experimental realizations of device-independent randomness include [75,194].

In device-independent QKD, we make the additional assumption that there is no communication between the adversary and the quantum devices. The first formal proof for a device-independent QKD scheme was given by Vazirani and Vidick [225]. Current research

[11] In fact, the first formal security proof of QKD by Shor and Preskill [207] exploited this monogamy of entanglement by showing that a QKD protocol can be transformed (in a series of steps) into a protocol that distills pure EPR states which Eve cannot be entangled with. These EPR states are then measured by Alice and Bob to obtain the secure shared key.

in this area aims to propose more practical device-independent QKD schemes that retain their functionality at realistic levels of noise.

4 Quantum cryptographic limitations and challenges

In this section, we survey a number of limitations and challenges of quantum cryptography (see Sect. 1.1 for a brief overview of these topics). We cover the impossibility of information-theoretically secure quantum bit commitment (Sect. 4.1) as well as the impossibility of information-theoretically secure two-party quantum computation (Sect. 4.2). Next, we survey the challenges imposed by quantum information in the context of *quantum rewinding* (Sect. 4.3) and superposition access to oracles in a quantum world (Sect. 4.4). Finally, we discuss impossibility results for position-based quantum cryptography (Sect. 4.5).

4.1 Impossibility of quantum bit commitment

The 10-year period following the publication of the first QKD protocol [24] saw only a handful of cryptographers working in quantum cryptography. This era was a period of vivid optimism. Indeed, the concept that quantum mechanics could allow unconditionally secure key expansion is mind-boggling, so why stop there? The next natural step to examine was *oblivious transfer*, which is an important building block for cryptography [145] (see Sect. 3.3.1 for definitions of *bit commitment* and *oblivious transfer*).

From this early period of quantum cryptography, we know of a quantum reduction from bit commitment to oblivious transfer [29] (see Sect. 3.3). Hence, the holy grail of oblivious transfer is achievable, *if only we have access to a bit commitment*! Thus, researchers explored the possibility of *quantum bit commitment* (i.e. of using quantum information in order to build bit commitment), with the hopes of founding all of cryptography on the unique assumption of quantum mechanics. This line of work started in [44], culminating in a claim of a unconditionally secure quantum bit commitment protocol [46]. However, the optimism for quantum cryptography lasted only a few years as Mayers [169] found a subtle flaw in the original argument of security. This result was generalized to rule out all quantum protocols for bit commitment by Mayers, and Lo and Chau [157,170]. Note that the *possibility* of bit commitment in the *limited-quantum-storage* model (Sect. 3.4) introduces an extra physical assumption, and does not contradict the impossibility as discussed here!

We now briefly review the main impossibility argument [47] (for ease of presentation, we focus on the exact case).[12] First, consider the following sketch of impossibility for perfectly secure *classical* bit commitment: suppose such a protocol exists. Then by the information-theoretic security requirement, at the end of the commitment phase, Bob's view of the protocol must be independent of b (since, otherwise, the protocol would not be perfectly hiding). But this independence implies that Alice can choose to reveal either $b = 0$ or $b = 1$ in the reveal phase, with both being accepted by Bob. Hence, the bit commitment cannot be binding. It is interesting that the same proof structure is applicable to the quantum case, albeit by invoking some slightly more technical tools. Namely, we first consider a *purified* version of the protocol, which consists in all parties acting at the quantum level (measurements are replaced by a unitary process via a standard technique). Next, by the information-theoretic hiding property, the reduced quantum state that Bob holds at the end of the commit phase

[12] See also a more recent proof exploiting "quantum combs" [72], as well as a more general result about the impossibility of "growing" quantum bit commitments [235].

must be identical, whether $b = 0$ or $b = 1$. This condition is enough to break the binding property, since it means [215] that Alice can locally perform a unitary quantum operation on her system in order to re-create a joint state consistent with either $b = 0$, or $b = 1$, at her choosing.[13] Hence, she can chose to open either $b = 0$ or $b = 1$ at a later time, and Bob will accept: the commitment scheme cannot be binding.

Going back to the original paper on quantum bit commitment [46], we note that a subtlety in the definition of the *binding* property is the origin of the false claim of security: while it is true that the protocol is such that Alice is unable to *simultaneously* hold messages that would unveil a commitment to $b = 0$ *and* as $b = 1$ (and thus, to be able to choose to open $b = 0$ *and* $b = 1$), this is insufficient to prove security, since in fact Alice is able to *delay* her choice of commitment until the very end of the protocol—at which point she can *choose* to open as either $b = 0$ or $b = 1$ (but not necessarily both at the same time!).

4.2 Impossibility of secure two-party computation using quantum communication

Given the impossibility of quantum bit commitment, the next question to ask is: are there any classical primitives that may be implemented securely using quantum communication? In fact, the possibility for OT was stated as a open problem in [45]. Unfortunately, this hope was shattered rather quickly, as impossibility results were given by Lo in [156] for one-sided computations (where only one party receives output). This result already shows the impossibility of 1-out-of-2 OT—the proof technique follows closely the technique developed for the impossibility of quantum bit commitment (see Sect. 4.1).

It took almost 10 years until Colbeck showed the first impossibility result for two-sided computations, namely that Alice can always obtain more information about Bob's input than what is implied by the value of the function [79]. In a similar vein, Salvail, Schaffner and Sotakova proved in [202] that any quantum protocol for a non-trivial primitive leaks information to a dishonest player. What is worse, even with the help of a trusted party, the cryptographic power of any primitive cannot be "amplified" by a quantum-communication protocol.

Buhrman, Christandl and Schaffner [58] have strengthened the above impossibility results by showing that the leakage in any quantum protocol is essentially as bad as one can imagine: even in the case of approximate correctness and security, if a protocol is "secure" against Bob, then it is *completely* insecure against Alice (in the sense that she can compute the output of the computation for *all* of her possible inputs). For impossibility results in the universal composability (UC) framework, see [113].

4.3 Zero-knowledge against quantum adversaries: "quantum rewinding"

Zero-knowledge interactive proofs, as introduced by Goldwasser, Micali, and Rackoff [124] are interactive proofs with the property that the verifier learns nothing from her interaction with the honest prover, beyond the validity of the statement being proved. These proof systems play an important role in the foundations of cryptography, and are also fundamental building blocks to achieve cryptographic functionalities (see [121] for a survey).

In zero-knowledge interactive proofs, the notion that the verifier "learns nothing" is formalized via the *simulation paradigm*: if, for every cheating verifier (interacting in the protocol on a positive instance), there exists a simulator (who does not interact with the prover) such that the output of the verifier is indistinguishable from the output of the simulator, then we say

[13] Technically, Uhlmann's theorem states that any two purifications of Bob's reduced quantum state are related by a unitary transform.

that the zero-knowledge property holds. In the classical world, a common proof technique used for establishing the zero-knowledge property is *rewinding*: a simulator is typically built by executing the given verifier—except that some computation paths are culled if the random choices of the verifier are not consistent with the desired effect. This selection is done by keeping a trace of the interaction, thus, if the interaction is deemed to have followed an incorrect path, the simulation can simply reset the computation ("rewind") to an earlier part of the computation (see [121] and references therein).

In the quantum setting, such a rewinding approach is impossible: the no-cloning theorem tells us that it is not possible, in general, to keep a secondary copy of the transcript in order to return to it later on. This problem is further aggravated by the fact that, in the most general case, the verifier starts with some *auxiliary* quantum information (which we do not, in general, know how to re-create)—thus even a "patch" that would emulate the rewinding approach in the simple case would appear to fail in the case of auxiliary quantum information. We emphasize that the above concerns about the zero-knowledge property are applicable to purely *classical* protocols: honest parties are completely classical, but we wish to establish the zero-knowledge property against a verifier that may receive, store and process quantum information (these concerns are independent of the *computational power* of the verifier—they simply relate to the computational model!).

The fundamental difficulty in proving the zero-knowledge property in the quantum world was first discussed by van de Graaf [223]; while some progress was made on this question [85], it is the breakthrough result of Watrous [227] that restored confidence that the zero-knowledge property of many standard classical zero-knowledge proofs is maintained in a quantum world.

In a nutshell, Watrous introduced the technique of *quantum rewinding*, which establishes that under some reasonable (and commonly satisfied) conditions, the success probabilities of certain processes with quantum inputs and outputs can be amplified. This technique therefore provides an alternative to the classical rewinding paradigm, and is used to show that the Goldreich-Micali-Wigderson graph 3-coloring protocol [122] is zero-knowledge against quantum attacks. We briefly mention that quantum rewinding is established using a technique resembling *amplitude amplification* [48] as is related to Grover's quantum search algorithm [126].

Further work on quantum rewinding has dealt with extending the domain of applicability to *proofs of knowledge* [218]. However, [11] show limitations to this technique (so that, in fact—relative to an oracle—there exists classical protocols that are insecure against quantum adversaries). See also [85].

4.4 Superposition access to oracles: quantum security notions

Post-quantum cryptography [32] (see Sect. 1.2) investigates classical cryptographic schemes which remain secure in the presence of quantum adversaries. In classical cryptography, security is often defined in terms of an interactive game between an adversary and a challenger: a scheme is deemed secure if the adversary can only win the game with negligible probability. When such notions are used to prove post-quantum security, one must consider quantum adversaries which are potentially able to communicate quantumly with the challenger. An example is the chosen-plaintext-attack (CPA) learning phase that is present in game-based security definitions, for instance for defining indistinguishability (IND) security of encryption schemes [123,140], where it is natural to consider attackers that can query superpositions of plaintexts to be encrypted and are returned superpositions of according ciphertexts from the challenger.

Another important example relates to the random-oracle (RO) model. A common technique used in classical cryptography is to assume that hash functions are perfect random oracles which adversaries can evaluate. It is well-known in classical cryptography that the RO-methodology comes with a plethora of techniques that can be employed in order to give formal proofs. Unfortunately, most of these tricks do not work in a quantum context for the following reason: a quantum adversary can always evaluate a classical hash function on an arbitrary superposition of inputs. Therefore, in the quantum random oracle (QRO) model, it is necessary to give the adversary superposition access to the oracle. As a consequence, standard techniques from the classical RO model (such as planting the challenge in a random one of the RO queries of the adversary) fail in the more realistic QRO model setting (the adversary might make a single quantum query with all input values in superposition).

Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry [38] first showed how to correctly define the random-oracle model in the quantum setting. They also showed a separation between the classical and quantum RO models. Zhandry [240] showed how to plant challenges in the QRO model at the beginning of the execution, and Unruh [222] showed how to reprogram the RO during runtime. Security definitions allowing superposition access have subsequently been studied by Boneh and Zhandry [37,240] in the context of encryption, digital signatures and the construction of pseudo-random functions. See also related work by Damgård, Funder, Nielsen and Salvail [92], who study superposition attacks on secret-sharing and multi-party protocols.

4.5 Position-based quantum cryptography

In cryptography, digital keys or biometric features are used to verify the identity of a person. The goal of position-based cryptography is to use the *geographical position* of an entity as a cryptographic credential. As a physical analogy, consider the scenario of a bank, where typically, the mere fact that a bank teller is behind the counter (her *position*) suffices as a credential in order to initiate the exchange of sensitive information.

A central building block of position-based cryptography is the task of *position verification*, a problem previously studied in the field of wireless security [42,61,64,65,203,209,226,241]. The goal is to prove to a set of verifiers that one is at a certain geographical location. Protocols typically exploit the relativistic no-signaling principle that messages cannot travel faster than the speed of light. By responding to a verifier in a timely manner, one can guarantee that one is within a certain distance of that verifier [42]. It was shown in [69] that classical position-verification protocols based only on this relativistic principle can be broken by multiple attackers who simulate being at the claimed position while physically residing elsewhere in space. Because of the no-cloning property of quantum information (see Sect. 2.4), it was believed that with the use of quantum messages one could devise protocols that were resistant to such collaborative attacks. Several schemes were proposed [68,144,152,164,165] that later turned out to be insecure. Finally, Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky and Schaffner showed that also in the quantum case, no unconditionally secure schemes are possible [60], as long as the colluding adversaries share a large enough amount of entanglement: attackers can break the protocol if the number of pre-shared EPR pairs is exponential in the size of the messages of the protocol [19]. This exponential overhead in resources (in terms of entanglement and quantum memory) leads to the main open problem in this research area, namely to find quantum protocols which remain secure under the assumption that adversarial resources are restricted to a polynomial amount, while at the same time, honest players can perform the schemes efficiently.

Historically, position-based schemes were first studied by Kent, Monroe and Spiller in 2002 under the name of "quantum tagging". A US-patent was granted in 2006 [143], but the results appeared in the scientific literature only in 2010 [144]. Some simple position-verification schemes are studied in [59,144]. The only quantum ingredient in these protocols is a single qubit sent to the prover who is required to route this qubit back to the correct verifier depending on the classical information he also receives from the verifiers. Note that the actions of the honest players are simple enough that they can be implemented using current quantum technology.

In order to analyze how much entanglement colluding adversaries need to break these simple schemes, a new model of (classical) communication complexity (called the *garden-hose model*) was introduced by Buhrman, Fehr, Schaffner and Speelman [59]. This model connects attacks on position-based quantum protocols to various interesting problems in classical complexity theory and communication complexity, as witnessed in related work [73,147]. In particular, the *garden-hose complexity* of a function gives an upper bound on the amount of entanglement required to break the security of the position-verification protocol based on that function. However, it is an open question whether more advanced techniques will allow to also prove lower bounds on the entanglement required to break these simple position-verification protocols.

In [220], Unruh introduces a helpful methodology for analyzing quantum circuits in space-time and gives a position-verification protocol in three dimensions which is secure in the quantum-random-oracle model. Furthermore, [60,220] give schemes for position-based authentication which allows the verifiers to be convinced that a message originated from a certain location. However, it remains an open problem to find efficient schemes which do not use random oracles.

5 Conclusion and open problems

Since its inception almost 50 years ago, quantum cryptography has developed into an active and exciting multidisciplinary area of research that combines state-of-the-art techniques from cryptography, quantum physics, complexity theory, information theory and beyond. While experimental implementations are still at the prototype level, our theoretical understanding of the power and limitations of quantum cryptography is continuously expanding.

Ongoing work on quantum cryptography consists in improving existing schemes as well as finding further applications and proof techniques. As final words, we mention here some open problems of interest.

- *What types of cryptosystems can quantum algorithms break?* The area of post-quantum cryptography bases classical cryptography on computational problems which are hard even for quantum computers. More research on quantum algorithms for quantum cryptanalysis is needed to fully understand how difficult these problems are. This understanding is also crucial when choosing the security parameters for post-quantum cryptographic schemes.
- *Can we make device-independent protocols that are feasible in practice?* It is a challenging open problem to develop device-independent protocols (for key distribution, but possibly also for other applications) which can tolerate a realistic amount of noise.
- *Can quantum protocols verify the position of a player?* As outlined in Sect. 4.5, one of the main open questions in the area of position-based cryptography is to find a protocol which can be executed efficiently (with current technology) by honest players, but requires an exponential amount of resources (such as entangled qubits) for attackers to break it.

- *How can we construct quantum-secure pseudorandom permutations (qPRP)?* Related to the topic of quantum security notions (Sect. 4.4), Zhandry [240] has shown how to construct quantum-security pseudo-random functions (qPRF). Classically, it is well-known that using the PRF in a three-round Feistel network yields a pseudo-random permutation. However, this construction is probably insecure in the quantum setting [149]. It is an open question how to construct quantum-secure pseudo-random permutations.
- *Which cryptographic functionalities can be achieved by quantum protocols?* The impossibility results from Sect. 4.2 are all concerned with *deterministic classical* functionalities. In Sect. 3.6, we have seen that quantum protocols for (weak or biased strong) coin flipping exist. Hence what exactly is the set of randomized classical functionalities that can be implemented by quantum protocols? More generally, can these impossibility results be extended to quantum functionalities?
- *Does quantum information allow for devices that hide the inner workings of a computer program?* Due to its diverse and far reaching applications, program obfuscation has been long considered as a holy grail of cryptography. However, hopes of attaining highly secure obfuscation were diminished in 2011 by an impossibility proof [14] (note, however that weaker security notions are attainable [115]). The situation is completely different in the quantum case, since the proof technique is not applicable (essentially due to the no-cloning theorem). As such, a positive result establishing that quantum information allows program obfuscation would unleash a number of powerful primitives, and would yield another qualitative advantage of quantum information over its classical counterpart.
- *What are the limits of the delegated quantum computation scenario?* In Sect. 3.5, we reviewed results on how a quantum computationally weak client can outsource a quantum computation. An open question that remains is to establish the ultimate limits in terms of the power of the client: can a fully classical client delegate a private quantum computation to a single quantum server, while ensuring privacy and/or verifiability? In the computational setting, this question is related to that of *quantum fully homomorphic encryption*: can we encrypt quantum data such that any quantum circuit can be applied to the encrypted data (without revealing the key, of course!)?
- *Can we build quantum public-key money from standard assumptions?* Current techniques for quantum public-key money rely on *ad hoc* assumptions (see Sect. 3.1). An open problem is to construct these primitives on standard cryptographic assumptions (such as the existence of quantum-secure one-way functions [7,183,192]).

Acknowledgments It is a pleasure to acknowledge conversations with Gilles Brassard, Gus Gutoski, Serge Fehr and Louis Salvail in the preparation of this document. We thank Romain Alléaume, Matthias Christandl, Claude Crépeau, Ivan Damgård, Tommaso Gagliardoni, Andreas Hülsing, Stacey Jeffery, Raza Ali Kazmi, Anthony Leverrier, Renato Renner, Fang Song, Douglas Stebila, Dominique Unruh, Thomas Vidick, Stefan Wolf, and Ronald de Wolf for very useful feedback on an initial draft of this document. We also thank Ronald Mullin for his invitation to submit this paper to the 25th anniversary edition of *Designs, Codes and Cryptography*, and an anonymous reviewer for helpful comments. We are deeply indebted to Barbara Caiçara Santos for help in managing our references database. A.B.'s work is supported by Canada's NSERC. C.S. is supported by an NWO VIDI grant, and the EU 7th framework project SIQS.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Aaronson S.: Quantum copy-protection and quantum money. In: CCC 2009, pp. 229–242 (2009). doi:10.1109/CCC.2009.42.
2. Aaronson S., Christiano P.: Quantum money from hidden subspaces. In: STOC 2012, pp. 41–60 (2012). doi:10.1145/2213977.2213983.
3. Aaronson S., Farhi E., Gosset D., Hassidim A., Kelner J., Lutomirski A.: Quantum money. Commun. ACM, **55**(8), 84–92 (2012). doi:10.1145/2240236.2240258.
4. Aharonov D., Ta-Shma A., Vazirani U., Yao A.: Quantum bit escrow. In: STOC 2000, pp. 705–714 (2000). doi:10.1145/335305.335404.
5. Aharonov D., Ben-Or M., Eban E.: Interactive proofs for quantumcomputations. In: ICS 2010, pp. 453–469 (2010). arXiv:0810.5375.
6. Aharonov D., Chailloux A., Ganz M., Kerenidis I., Magnin L.: A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias (2014). arXiv:1402.7166.
7. Ajtai M.: Generating hard instances of lattice problems. In: STOC 1996, pp. 99–108 (1996). doi:10.1145/237814.237838.
8. Alléaume R., Branciard C., Bouda J., Debuisschert T., Dianati M., Gisin N., Godfrey M., Grangier P., Länger T., Lütkenhaus N., Monyk P.P.C., Peev M., Poppe A., Pornin T., Rarity J., Renner R., Ribordy G., Riguidel M., Salvail L., Shields A., Weinfurter H., Zeilinger A.: Using quantum key distribution for cryptographic purposes: a survey. Theor. Comput. Sci. **560**, 62–81 (2014). doi:10.1016/j.tcs.2014.09.018.
9. Ambainis A., Mosca M., Tapp A., de Wolf R.: Private quantum channels. In: FOCS 2000, pp. 547–553 (2000). doi:10.1109/SFCS.2000.892142.
10. Ambainis A., Buhrman H., Dodis Y., Röhrig H.: Multiparty quantum coin flipping. In: CCC 2004, pp. 250–259 (2004). http://dl.acm.org/citation.cfm?id=1009561.
11. Ambainis A., Rosmanis A., Unruh D.: Quantum attacks on classical proof systems: the hardness of quantum rewinding. In: FOCS 2014, pp. 474–483 (2014). doi:10.1109/FOCS.2014.57.
12. Arrighi P., Salvail L.: Blind quantum computation. Int. J. Quantum Inf. **4**(5), 883–898 (2006). doi:10.1142/S0219749906002171.
13. Bacon D., van Dam W.: Recent progress in quantum algorithms. Commun. ACM **53**(2), 84–93 (2010). doi:10.1145/1646353.1646375.
14. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S., Yang K.: On the (im)possibility of obfuscating programs. J. ACM **59**(2), 6:1–6:48 (2012). doi:10.1145/2160158.2160159.
15. Barnum H., Crépeau C., Gottesman D., Smith A., Tapp A.: Authentication of quantum messages. In: FOCS 2002, pp. 449–458 (2002). doi:10.1109/SFCS.2002.1181969.
16. Barrett J., Hardy L., Kent A.: No signaling and quantum key distribution. Phys. Rev. Lett. **95**(1), 010503 (2005). doi:10.1103/physrevlett.95.010503.
17. Barz S., Kashefi E., Broadbent A., Fitzsimons J.F., Zeilinger A., Walther P.: Demonstration of blind quantum computing. Science **335**(6066), 303–308 (2012). doi:10.1126/science.1214707.
18. Barz S., Fitzsimons J.F., Kashefi E., Walther P.: Experimental verification of quantum computation. Nat. Phys. **9**(11), 727–731 (2013). doi:10.1038/nphys2763.
19. Beigi S., König R.: Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New J. Phys. **13**(9), 093036 (2011). doi:10.1088/1367-2630/13/9/093036.
20. Bell J.S.: On the Einstein-Podolsky-Rosen paradox. Physics **1**, 195–200 (1964). http://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf.
21. Ben-Or M., Goldwasser S., Kilian J., Widgerson A.: Multi-prover interactive proofs: how to remove intractability assumptions. In: STOC 1988, pp. 113–131 (1988). doi:10.1145/62212.62223.
22. Ben-Or M., Crépeau C., Gottesman D., Hassidim A., Smith A.: Secure multiparty quantum computation with (only) a strict honest majority. In: FOCS 2006, pp. 249–260 (2006). doi:10.1109/FOCS.2006.68.
23. Bennett C.H.: Quantum cryptography: uncertainty in the service of privacy. Science **257**(5071), 752–753 (1992). doi:10.1126/science.257.5071.752.
24. Bennett C.H., Brassard G.: Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984).
25. Bennett C.H., Brassard G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014). doi:10.1016/j.tcs.2014.05.025.
26. Bennett C.H., Brassard G., Breidbart S., Wiesner S.: Quantum cryptography, or unforgeable subway tokens. In: CRYPTO 1982, pp. 267–275 (1982). doi:10.1007/978-1-4757-0602-4_26.
27. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J.: Experimental quantum cryptography. J. Cryptol. **5**(1), 3–28 (1992). doi:10.1007/bf00191318.

28. Bennett C.H., Brassard G., Mermin N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**(5), 557–559 (1992). doi:10.1103/physrevlett.68.557.
29. Bennett C.H., Brassard G., Crépeau C., Skubiszewska M.-H.: Practical quantum oblivious transfer. In: CRYPTO 1991, pp. 351–366 (2001). doi:10.1007/3-540-46766-1_29.
30. Bennett C.H., Brassard G., Breidbart S.: Quantum cryptography ii: how to re-use a one-time pad safely even if P=NP. Nat. Comput. **13**(4), 453–458 (2014). doi:10.1007/s11047-014-9453-6.
31. Berlín G., Brassard G., Bussières F., Slater J.A., Tittel W.: Experimental loss-tolerant quantum coin flipping. Nat. Commun. **2**, 561 (2011). doi:10.1038/ncomms1572.
32. Bernstein D.J., Buchmann J., Dahmen E. (eds.): Post-quantum Cryptography. Springer, Berlin (2009). doi:10.1007/978-3-540-88702-7.
33. Bernstein D.J., Jeffery S., Lange T., Meurer A.: Quantum algorithms for the subset-sum problem. In: PQCrypto 2013, pp. 16–33 (2013). doi:10.1007/978-3-642-38616-9_2.
34. Berta M., Brandão F.G.S.L., Christandl M., Wehner S.: Entanglement cost of quantum channels. IEEE Trans. Inf. Theory **59**(10), 6779–6795 (2013). doi:10.1109/TIT.2013.2268533.
35. Berta M., Fawzi O., Wehner S.: Quantum to classical randomness extractors. IEEE Trans. Inf. Theory **60**(2), 1168–1192 (2014). doi:10.1109/TIT.2013.2291780.
36. Blum M.: Coin flipping by telephone a protocol for solving impossible problems. ACM SIGACT News **15**(1), 23–27 (1983). doi:10.1145/1008908.1008911.
37. Boneh D., Zhandry M.: Secure signatures and chosen ciphertext security in a quantum computing world. In: CRYPTO 2013, pp. 361–379 (2013). doi:10.1007/978-3-642-40084-1_21.
38. Boneh D., Dagdelen Ö., Fischlin M., Lehmann A., Schaffner C., Zhandry M.: Random oracles in a quantum world. In: ASIACRYPT 2011, pp. 41–69 (2011). doi:10.1007/978-3-642-25385-0_3.
39. Bouman N.J., Fehr S., González-Guillén C., Schaffner C.: An all-but-one entropic uncertainty relation, and application to password-based identification. In: TQC 2012, pp. 29–44 (2013).doi:10.1007/978-3-642-35656-8_3.
40. Boyer M., Brassard G., Høyer P., Tapp A.: Tight bounds on quantum searching. Fortsch. Phys. **46**(4–5), 493–505 (1998). doi:10.1002/(sici)1521-3978(199806)46:4/5<3.0.co;2-p.
41. Boykin P.O., Roychowdhury V.: Optimal encryption of quantum bits. Phys. Rev. A **67**(4), 042317 (2003). doi:10.1103/PhysRevA.67.042317.
42. Brands S., Chaum D.: Distance-bounding protocols. In: EUROCRYPT 1993, pp. 344–359 (1993). doi:10.1007/3-540-48285-7_30.
43. Brassard G.: Brief history of quantum cryptography: a personal perspective. In: IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, pp. 19–23 (2005). doi:10.1109/ITWTPI.2005.1543949.
44. Brassard G., Crépeau C.: Quantum bit commitment and coin tossing protocols. In: CRYPTO 1990, pp. 49–61 (1991). doi:10.1007/3-540-38424-3_4.
45. Brassard G., Crépeau C.: 25 years of quantum cryptography. ACM SIGACT News **27**(3), 13–24 (1996). doi:10.1145/235666.235669.
46. Brassard G., Crépeau C., Jozsa R., Langlois D.: A quantum bit commitment scheme provably unbreakable by both parties. In: FOCS 1993, pp. 362–371 (1993). doi:10.1109/SFCS.1993.366851.
47. Brassard G., Crépeau C., Mayers D., Salvail L.: A brief review on the impossibility of quantum bit commitment (1997). arXiv:quant-ph/9712023.
48. Brassard G., Høyer P., Mosca M., Tapp A.: Quantum amplitude amplification and estimation. Quantum Comput. Quantum Inf. **305**, 53–74 (2000). arXiv:quant-ph/0005055.
49. Brassard G., Broadbent A., Fitzsimons J., Gambs S., Tapp A.: Anonymous quantum communication. In: ASIACRYPT 2007, vol. 4833, pp. 460–473 (2007). doi:10.1007/978-3-540-76900-2_28.
50. Brassard G., Høyer P., Kalach K., Kaplan M., Laplante S., Salvail L.: Merkle puzzles in a quantum world. In: CRYPTO 2011, pp. 391–410 (2011). doi:10.1007/978-3-642-22792-9_22.
51. Broadbent A.: Delegating private quantum computations. Can. J. Phys. **93**(9), 941–946 (2015). doi:10.1139/cjp-2015-0030.
52. Broadbent A., Jeffery S.: Quantum homomorphic encryption for circuits of low T-gate complexity. In: CRYPTO 2015, pp. 609–629 (2015). doi:10.1007/978-3-662-48000-7_30.
53. Broadbent A., Fitzsimons J., Kashefi E.: Universal blind quantum computation. In: FOCS 2009, pp. 517–526 (2009). doi:10.1109/FOCS.2009.36.
54. Broadbent A., Gutoski G., Stebila D.: Quantum one-time programs. In: CRYPTO 2013, pp. 344–360 (2013). doi:10.1007/978-3-642-40084-1_20.
55. Brodutch A., Nagaj D., Sattath O., Unruh D.: An adaptive attack on Wiesner's quantum money (2014). arXiv:1404.1507.
56. Bruß D., Erdélyi G., Meyer T., Riege T., Rothe J.: Quantum cryptography: a survey. CSUR **39**(2), 6 (2007). doi:10.1145/1242471.1242474.

57. Buhrman H., Christandl M., Hayden P., Lo H.-K., Wehner S.: Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. Phys. Rev. A **78**(2), 022316 (2008). doi:10.1103/physreva.78.022316.
58. Buhrman H., Christandl M., Schaffner C.: Complete insecurity of quantum protocols for classical two-party computation. Phys. Rev. Lett. **109**(16), 160501 (2012). doi:10.1103/physrevlett.109.160501.
59. Buhrman H., Fehr S., Schaffner C., Speelman F.: The garden-hose model. In: ITCS 2013, pp. 145–158 (2013). doi:10.1145/2422436.2422455.
60. Buhrman H., Chandran N., Fehr S., Gelles R., Goyal V., Ostrovsky R., Schaffner C.: Position-based quantum cryptography: impossibility and constructions. SIAM J. Comput. **43**(1), 150–178 (2014). doi:10.1137/130913687.
61. Bussard L.: Trust establishment protocols for communicating devices. PhD Thesis, Eurecom-ENST. (2004). http://www.eurecom.fr/publication/1519.
62. Cachin C., Maurer U.: Unconditional security against memory-bounded adversaries. In: CRYPTO 1997, pp. 292–306 (1997). doi:10.1007/BFb0052243.
63. Canetti R.: Universally composable security: a new paradigm for cryptographic protocols. In: FOCS 2001, pp. 136–145 (2001). doi:10.1109/SFCS.2001.959888.
64. Capkun S., Hubaux J.-P.: Secure positioning of wireless devices with application to sensor networks. In: INFOCOM 2005, pp. 1917–1928 (2005). doi:10.1109/INFCOM.2005.1498470.
65. Čapkun S., Čagalj M., Srivastava M.: Secure localization with hidden and mobile base stations. In: INFOCOM 2006, pp. 1–10 (2006). doi:10.1109/INFOCOM.2006.302.
66. Chailloux A., Kerenidis I.: Optimal quantum strong coin flipping. In: FOCS 2009, pp. 527–533 (2009). doi:10.1109/FOCS.2009.71.
67. Chailloux A., Kerenidis I.: Optimal bounds for quantum bit commitment. In: FOCS 2011, pp. 354–362. (2011). doi:10.1109/FOCS.2011.42.
68. Chandran N., Fehr S., Gelles R., Goyal V., Ostrovsky R.: Position-based quantum cryptography (2010). arXiv:1005.1750.
69. Chandran N., Goyal V., Moriarty R., Ostrovsky R.: Position based cryptography. In: CRYPTO 2009, pp. 391–407 (2009). doi:10.1007/978-3-642-03356-8_23.
70. Childs A.M.: Secure assisted quantum computation. Quantum Inf. Comput. **5**(6), 456–466 (2005). arXiv:quant-ph/0111046.
71. Childs A., Jao D., Soukharev V.: Constructing elliptic curve isogenies in quantum subexponential time. J. Math. Cryptol. **8**(1), 1–29 (2013). doi:10.1515/jmc-2012-0016.
72. Chiribella G., D'Ariano G.M., Perinotti P., Schlingemann D., Werner R.: A short impossibility proof of quantum bit commitment. Phys. Rev. Lett. **377**(15), 1076–1087 (2013). doi:10.1016/j.physleta.2013.02.045.
73. Chiu W.Y., Szegedy M., Wang C., Xu Y.: The garden hose complexity for the equality function. In: Algorithmic Aspects of Information and Management, pp. 112–123 (2014). doi:10.1007/978-3-319-07956-1_11.
74. Christandl M., Wehner S.: Quantum anonymous transmissions. In: ASIACRYPT 2005, pp. 217–235 (2005). doi:10.1007/11593447_12.
75. Christensen B.G., McCusker K.T., Altepeter J.B., Calkins B., Gerrits T., Lita A.E., Miller A., Shalm L.K., Zhang Y., Nam S.W., Brunner N., Lim C.C.W., Gisin, N., Kwiat, P.G.: Detection-loophole-free test of quantum nonlocality, and applications. Phys. Rev. Lett. **111**(13), 130406 (2013). doi:10.1103/physrevlett.111.130406.
76. Clauser J.F., Horne M.A., Shimony A., Holt R.A.: Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. **23**(15), 880–884 (1969). doi:10.1103/PhysRevLett.23.880.
77. Cleve R., Gottesman D., Lo H.-K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648–651 (1999). doi:10.1103/PhysRevLett.83.648.
78. Colbeck R.: Quantum and relativistic protocols for secure multi-party computation. PhD Thesis, University of Cambridge, UK (2006). arXiv:0911.3814.
79. Colbeck R.: Impossibility of secure two-party classical computation. Phys. Rev. A **76**(6), 062308 (2007). doi:10.1103/physreva.76.062308.
80. Colbeck R., Renner R.: Free randomness can be amplified. Nat. Phys. **8**, 450–453 (2012). doi:10.1038/nphys2300.
81. Crépeau C.: Equivalence between two flavours of oblivious transfers. In: CRYPTO 1987, pp. 350–354 (1988). doi:10.1007/3-540-48184-2_30.
82. Crépeau C., Kilian J.: Achieving oblivious transfer using weakened security assumptions. In: FOCS 1988, pp. 42–52 (1988). doi:10.1109/SFCS.1988.21920.
83. Crépeau C., Savvides G., Schaffner C., Wullschleger J.: Information-theoretic conditions for two-party secure function evaluation. In: EUROCRYPT 2006, pp. 538–554 (2006). doi:10.1007/11761679_32.

84. Crépeau C., Salvail L., Simard J.-R., Tapp A.: Two provers in isolation. In: ASIACRYPT 2011, pp. 407–430 (2011). doi:10.1007/978-3-642-25385-0_22.
85. Damgård I., Fehr S., Salvail L.: Zero-knowledge proofs and string commitments withstanding quantum attacks. In: CRYPTO 2004, pp. 254–272 (2004).
86. Damgård I., Fehr S., Salvail L., Schaffner C.: Cryptography in the bounded quantum-storage model. In: FOCS 2005, pp. 449–458 (2005). doi:10.1109/SFCS.2005.30.
87. Damgård I., Pedersen T.B., Salvail L.: A quantum cipher with near optimal key-recycling. In: CRYPTO 2005, pp. 494–510 (2005). doi:10.1007/11535218_30.
88. Damgård I.B., Fehr S., Renner R., Salvail L., Schaffner C.: A tight high-order entropic quantum uncertainty relation with applications. In: CRYPTO 2007, pp. 360–378 (2007). doi:10.1007/978-3-540-74143-5_20.
89. Damgård I.B., Fehr S., Salvail L., Schaffner C.: Secure identification and QKD in the bounded-quantum-storage model. In: CRYPTO 2007, vol. 4622, pp. 342–359 (2007). doi:10.1007/978-3-540-74143-5_19.
90. Damgård I.B., Fehr S., Salvail L., Schaffner C.: Cryptography in the bounded-quantum-storage model. SIAM J. Comput. **37**(6), 1865–1890 (2008). doi:10.1137/060651343.
91. Damgård I., Fehr S., Lunemann C., Salvail L., Schaffner C.: Improving the security of quantum protocols via commit-and-open. In: CRYPTO 2009, pp. 408–427 (2009). doi:10.1007/978-3-642-03356-8_24.
92. Damgård I., Funder J., Nielsen J.B., Salvail L.: Superposition attacks on cryptographic protocols. In: Information Theoretic Security, pp. 142–161 (2014). doi:10.1007/978-3-319-04268-8_9.
93. Damgård I., Dupuis F., Nielsen J.B.: On the orthogonal vector problem and the feasibility of unconditionally secure leakage-resilient computation. In: Information Theoretic Security, pp. 87–104 (2015). doi:10.1007/978-3-319-17470-9_6.
94. de Martini F., Monroe C.: Experimental Quantum Computation and Information. International School of Physics Enrico Fermi. IOS Press, Amsterdam (2003). https://books.google.ca/books?id=7xrvAgAAQBAJ.
95. Desrosiers S.P.: Entropic security in quantum cryptography. Quantum Inf. Process. **8**(4), 331–345 (2009). doi:10.1007/s11128-009-0111-3.
96. Desrosiers S.P., Dupuis F.: Quantum entropic security and approximate quantum encryption. IEEE Trans. Inf. Theory **56**(7), 3455–3464 (2010). doi:10.1109/TIT.2010.2048488.
97. Dunjko V., Fitzsimons J.F., Portmann C., Renner R.: Composable security of delegated quantum computation. In: ASIACRYPT 2014, pp. 406–425 (2014). doi:10.1007/978-3-662-45608-8_22.
98. Dupuis F., Nielsen J.B., Salvail L.: Secure two-party quantum evaluation of unitaries against specious adversaries. In: CRYPTO 2010, pp. 685–706 (2010). doi:10.1007/978-3-642-14623-7_37.
99. Dupuis F., Nielsen J.B., Salvail L.: Actively secure two-party evaluation of any quantum operation. In: CRYPTO 2012, pp. 794–811 (2012). doi:10.1007/978-3-642-32009-5_46.
100. Dupuis F., Fawzi O., Wehner S.: Entanglement sampling and applications. IEEE Trans. Inf. Theory **61**(2), 1093–1112 (2015). doi:10.1109/TIT.2014.2371464.
101. Dziembowski S., Maurer U.: On generating the initial key in the bounded-storage model. In: CRYPTO 2004, pp. 126–137 (2004). doi:10.1007/978-3-540-24676-3_8.
102. Dziembowski S., Maurer U.: The bare bounded-storage model: the tight bound on the storage requirement for key agreement. IEEE Trans. Inf. Theory **54**(6), 2790–2792 (2008). doi:10.1109/TIT.2008.921864.
103. Einstein A., Podolsky B., Rosen N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. Lett. **47**(10), 777–780 (1935). doi:10.1103/physrev.47.777.
104. Ekert A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991). doi:10.1103/PhysRevLett.67.661.
105. Erven C., Ng N., Gigov N., Laflamme R., Wehner S., Weihs G.: An experimental implementation of oblivious transfer in the noisy storage model. Nat. Commun., **5**, 3418 (2014). doi:10.1038/ncomms4418.
106. Even S., Goldreich O., Lempel A.: A randomized protocol for signing contracts. Commun. ACM **28**(6), 637–647 (1985). doi:10.1145/3812.3818.
107. Farhi E., Gosset D., Hassidim A., Lutomirski A., Shor P.W.: Quantum money from knots. In: ITCS 2012, pp. 276–289 (2012). doi:10.1145/2090236.2090260.
108. Farhi E., Gosset D., Hassidimand A., Lutomirski A., Nagaj D., Shor P.: Quantum state restoration and single-copy tomography for ground states of hamiltonians. Phys. Rev. Lett. **105**(19), 190503 (2010). doi:10.1103/physrevlett.105.190503.
109. Fehr S.: Quantum cryptography. Found. Phys. **40**(5), 494–531 (2010). doi:10.1007/s10701-010-9408-4.
110. Fehr S., Fillinger M.: Multi-prover commitments against non-signaling attacks. In: CRYPTO 2015, pp. 403–421 (2015). doi:10.1007/978-3-662-48000-7_20.
111. Fehr S., Schaffner C.: Composing quantum protocols in a classical environment. In: Theory of Cryptography, pp. 350–367 (2009). doi:10.1007/978-3-642-00457-5_21.

112. Fehr S., Gelles R., Schaffner C.: Security and composability of randomness expansion from Bell inequalities. Phys. Rev. A **87**(1), 012335 (2013). doi:10.1103/physreva.87.012335.
113. Fehr S., Katz J., Song F., Zhou H., Zikas V.: Feasibility and completeness of cryptographic tasks in the quantum world. In: Theory of Cryptography, pp. 281–296 (2013). doi:10.1007/978-3-642-36594-2_16.
114. Fisher K.A.G., Broadbent A., Shalm L.K., Yan Z., Lavoie J., Prevedel R., Jennewein T., Resch K.J.: Quantum computing on encrypted data. Nat. Commun. **5**, 3074 (2014). doi:10.1038/ncomms4074.
115. Garg S., Gentry C., Halevi S., Raykova M., Sahai A., Waters B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: FOCS 2013, pp. 40–49 (2013). doi:10.1109/FOCS.2013.13.
116. Gavinsky D.: Quantum money with classical verification. In: CCC 2012, pp. 42–52 (2012). doi:10.1109/CCC.2012.10.
117. Gentry C.: Fully homomorphic encryption using ideal lattices. In: STOC 2009, pp. 169–178 (2009). doi:10.1145/1536414.1536440.
118. Giovannetti V., Lloyd S., Maccone L.: Quantum private queries. Phys. Rev. Lett. **100**(23), 230502 (2008). doi:10.1103/physrevlett.100.230502.
119. Giovannetti V., Lloyd S., Maccone L.: Quantum private queries: security analysis. IEEE Trans. Inf. Theory **56**(7), 3465–3477 (2010). doi:10.1109/tit.2010.2048446.
120. Gisin N., Ribordy G., Tittel W., Zbinden H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2002). doi:10.1103/revmodphys.74.145.
121. Goldreich O.: Zero-knowledge twenty years after its invention (2002). www.wisdom.weizmann.ac.il/~oded/PSX/zk-tut02v3.pdf.
122. Goldreich O., Micali S., Wigderson A.: Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. J. ACM **38**(3), 690–728 (1991). doi:10.1145/116825.116852.
123. Goldwasser S., Micali S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2), 270–299 (1984). doi:10.1016/0022-0000(84)90070-9.
124. Goldwasser S., Micali S., Rackoff C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**(1), 186–208 (1989). doi:10.1137/0218012.
125. Gottesman D.: Uncloneable encryption. Quantum Inf. Comput. **3**(6), 581–602 (2003). arXiv:quant-ph/0210062.
126. Grover L.K.: A fast quantum mechanical algorithm for database search. In: STOC 1996, pp. 212–219 (1996). doi:10.1145/237814.237866.
127. Hallgren S.: Fast quantum algorithms for computing the unit group and class group of a number field. In: STOC 2005, pp. 468–474 (2005). doi:10.1145/1060590.1060660.
128. Hallgren S.: Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. J. ACM **54**(1), 4:1–4:19 (2007).
129. Hallgren S., Smith A., Song F.: Classical cryptographic protocols in a quantum world. In: Advances in Cryptology—CRYPTO 2011, pp. 411–428 (2011). doi:10.1007/978-3-642-22792-9_23.
130. Hänggi E., Wullschleger J.: Tight bounds for classical and quantum coin flipping. In: Theory of Cryptography, pp. 468–485 (2011). doi:10.1007/978-3-642-19571-6_28.
131. Hänggi E., Renner R., Wolf S.: Efficient device-independent quantum key distribution. In: EUROCRYPT 2010, vol. 6110, pp. 216–234 (2010). doi:10.1007/978-3-642-13190-5_11.
132. Hardy L., Kent A.: Cheat sensitive quantum bit commitment. Phys. Rev. Lett. **92**(15), 157901 (2004). doi:10.1103/physrevlett.92.157901.
133. Hayashi M., Tsurumaru T.: Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. New J. Phys. **14**(9), 093014 (2012). doi:10.1088/1367-2630/14/9/093014.
134. Hayden P., Leung D., Shor P.W., Winter A.: Randomizing quantum states: constructions and applications. Commun. Math. Phys. **250**(2), 371–391 (2004). doi:10.1007/s00220-004-1087-6.
135. Heisenberg W.: Schwankungserscheinungen und quantenmechanik. Zeit. Phys. **40**(7), 501–506 (1927). doi:10.1007/BF01440827.
136. Hofheinz D., Müller-Quade J., Unruh D.: On the (im-)possibility of extending coin toss. In: EUROCRYPT 2006, pp. 504–521 (2006). doi:10.1007/11761679_30.
137. Jakobi M., Simon C., Gisin N., Bancal J.-D., Branciard C., Walenta N., Zbinden H.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**(2), 022301 (2011). doi:10.1103/physreva.83.022301.
138. Liu, Y.K.: Building one-time memories from isolated qubits. In: ITCS 2014, pp. 269–286 (2014). doi:10.1145/2554797.2554823.
139. Kalai Y.T., Raz R., Rothblum R.D.: How to delegate computations: the power of no-signaling proofs. In: STOC 2014, pp. 485–494 (2014). doi:10.1145/2591796.2591809.
140. Katz J., Lindell Y.: Introduction to Modern Cryptography. Chapman & Hall/CRC Cryptography and Network Security Series. Chapman & Hall/CRC, Boca Raton (2007).

141. Kaye P., Laflamme R., Mosca M.: An Introduction to Quantum Computing. Oxford University Press, New York (2007).
142. Kent A.: Unconditionally secure bit commitment. Phys. Rev. Lett. **83**(7), 1447–1450 (1999). doi:10.1103/PhysRevLett.83.1447.
143. Kent A., Munro W., Spiller T., Beausoleil R.: Tagging systems (2006) US patent US 10/903,220. https://www.google.com/patents/US20060022832.
144. Kent A., Munro W.J., Spiller T.P.: Quantum tagging: authenticating location via quantum information and relativistic signaling constraints. Phys. Rev. A **84**(1), 012326 (2011). doi:10.1103/PhysRevA.84.012326.
145. Kilian J.: Founding cryptography on oblivious transfer. In: STOC 1988, pp. 20–31 (1988). doi:10.1145/62212.62215.
146. Kitaev A.: Quantum coin flipping. In: Talk at the 6th Workshop on Quantum Information Processing—QIP (2003).
147. Klauck H., Podder S.: New bounds for the garden-hose model. In: FSTTCS 2014, pp. 481–492 (2014). doi:10.4230/LIPIcs.FSTTCS.2014.481.
148. Koashi M.: Simple security proof of quantum key distribution based on complementarity. New J. Phys. **11**(4), 045018 (2009). http://stacks.iop.org/1367-2630/11/i=4/a=045018.
149. Kuwakado H., Morii M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: ISIT 2010, pp. 2682–2685 (2010). doi:10.1109/isit.2010.5513654.
150. Laarhoven T., Mosca M., van de Pol J.: Solving the shortest vector problem in lattices faster using quantum search. In: PQCrypto 2013, pp. 83–101 (2013). doi:10.1007/978-3-642-38616-9_6.
151. Lacerda F.G., Renes J.M., Renner R.: Classical leakage resilience from fault-tolerant quantum computation (2014). arXiv:1404.7516.
152. Lau H.-K., Lo H.-K.: Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Phys. Rev. A **83**(1), 012322 (2011). doi:10.1103/PhysRevA.83.012322.
153. Leung D.W.: Quantum Vernam cipher. Quantum Inf. Comput. **2**(1), 14–34 (2002). arXiv:quant-ph/0012077.
154. Liu Y.-K.: Single-shot security for one-time memories in the isolated qubits model. In: CRYPTO 2014, pp. 19–36 (2014). doi:10.1007/978-3-662-44381-1_2.
155. Liu Y.-K.: Privacy amplification in the isolated qubits model. In: EUROCRYPT 2015, pp. 785–814 (2015). doi:10.1007/978-3-662-46803-6_26.
156. Lo H.-K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997). doi:10.1103/PhysRevA.56.1154.
157. Lo H.-K., Chau H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**(17), 3410–3413 (1997). doi:10.1103/PhysRevLett.78.3410.
158. Lo H.-K., Chau H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999). doi:10.1126/science.283.5410.2050.
159. Lunghi T., Kaniewski J., Bussières F., Houlmann R., Tomamichel M., Kent A., Gisin N., Wehner S., Zbinden H.: Experimental bit commitment based on quantum communication and special relativity. Phys. Rev. Lett. **111**(18), 180504 (2013). doi:10.1103/physrevlett.111.180504.
160. Lunghi T., Kaniewski J., Bussières F., Houlmann R., Tomamichel M., Wehner S., Zbinden H.: Practical relativistic bit commitment. Phys. Rev. Lett. **115**(03), 030502 (2015). doi:10.1103/PhysRevLett.115.030502.
161. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V.: Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photon. **4**, 696–689 (2010). doi:10.1038/nphoton.2010.214.
162. Maassen H., Uffink J.B.M.: Generalized entropic uncertainty relations. Phys. Rev. Lett. **60**(12), 1103–1106 (1988). doi:10.1103/PhysRevLett.60.1103.
163. Magniez F., Dominic M., Mosca M., Ollivier H.: Self-testing of quantum circuits. In: Automata, Languages and Progamming, pp. 72–83 (2006). doi:10.1007/11786986_8.
164. Malaney R.A.: Location-dependent communications using quantum entanglement. Phys. Rev. Lett. **81**(4), 042319 (2010). doi:10.1103/PhysRevA.81.042319.
165. Malaney R.A.: Quantum location verification in noisy channels. In: Proceedings of the Global Communications Conference—GLOBECOM 2010, pp. 1–6. IEEE, Miami (2010). doi:10.1109/GLOCOM.2010.5684009.
166. Masanes L., Pironio S., Acin A.: Secure device-independent quantum key distribution with causally independent measurement devices. Nat. Commun. **2**, 238 (2011). doi:10.1038/ncomms1244.
167. Maurer U.M.: Protocols for secret key agreement by public discussion based on common information. In: CRYPTO 1992, pp. 461–470 (1992). doi:10.1007/3-540-48071-4_32.

168. Mayers D.: Quantum key distribution and string oblivious transfer in noisy channels. In: CRYPTO 1996, pp. 343–357 (1996). doi:10.1007/3-540-68697-5_26.
169. Mayers D.: The trouble with quantum bit commitment (1996). arXiv:quant-ph/9603015.
170. Mayers D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414–3417 (1997). doi:10.1103/PhysRevLett.78.3414.
171. Mayers D.: Unconditional security in quantum cryptography. J. ACM **48**(3), 351–406 (2001). doi:10.1145/382780.382781.
172. Mayers D., Salvail L.: Quantum oblivious transfer is secure against all individual measurements. In: Workshop on Physics and Computation. PhysComp 1994, pp. 69–77 (1994). doi:10.1109/PHYCMP.1994.363696.
173. Mayers D., Yao A.: Quantum cryptography with imperfect apparatus. In: FOCS 1998, pp. 503–509. (1998). doi:10.1109/SFCS.1998.743501.
174. Mayers D., Yao A.: Self testing quantum apparatus. Quantum Inf. Comput. **4**(4):273–286. (2004). http://dl.acm.org/citation.cfm?id=2011827.2011830.
175. McKague M., Yang T.H., Scarani V.: Robust self-testing of the singlet. J. Phys. A **45**(45), 455304 (2012). doi:10.1088/1751-8113/45/45/455304.
176. Merkle R.C.: Secure communications over insecure channels. Commun. ACM **21**(4), 294–299 (1978). doi:10.1145/359460.359473.
177. Mermin N.D.: Quantum computer science: an introduction. Cambridge University Press, New York (2007).
178. Miller C.A., Shi Y.: Optimal robust self-testing by binary nonlocal XOR games. In: TQC 2013, pp. 254–262 (2013). doi:10.4230/LIPIcs.TQC.2013.254.
179. Miller C.A., Shi Y.: Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In: STOC 2014, pp. 417–426 (2014). doi:10.1145/2591796.2591843.
180. Mochon C.: Quantum weak coin flipping with arbitrarily small bias (2007). arXiv:0711.4114.
181. Molina A., Vidick T., Watrous J.: Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In: Theory of Quantum Computation, Communication, and Cryptography—TQC 2012, pp. 45–64 (2013). doi:10.1007/978-3-642-35656-8_4.
182. Molina-Terriza G., Vaziri A., Ursin R., Zeilinger A.: Experimental quantum coin tossing. Phys. Rev. Lett. **94**(4), 040501 (2005). doi:10.1103/PhysRevLett.94.040501.
183. Moore C., Russell A., Vazirani U.: A classical one-way function to confound quantum adversaries (2007). arXiv:quant-ph/0701115.
184. Mosca M.: Quantum algorithms. In: Encyclopedia of Complexity and Systems Science, pp. 7088–7118. (2009). doi:10.1007/978-0-387-30440-3_423.
185. Mosca M., Stebila D.: Quantum coins. Error Correct. Codes Finite Geom. Cryptogr. **523**, 35–47 (2010). arXiv:0911.1295.
186. Müller-Quade J.: Quantum cryptography beyond key exchange. Informatik Forsch. Entw. **21**(1), 39–54 (2006). doi:10.1007/s00450-006-0011-z.
187. Ng N.H.Y., Berta M., Wehner S.: Min-entropy uncertainty relation for finite-size cryptography. Phys. Rev. A **86**(4), 042315 (2012). doi:10.1103/physreva.86.042315.
188. Ng N.H.Y., Joshi S.K., Chen Ming C., Kurtsiefer C., Wehner S.: Experimental implementation of bit commitment in the noisy-storage model. Nat. Commun. **3**, 1326 (2012). doi:10.1038/ncomms2268.
189. Nguyen A.T., Frison J., Huy K.P., Massar S.: Experimental quantum tossing of a single coin. New J. Phys. **10**(8), 083037 (2008). doi:10.1088/1367-2630/10/8/083037.
190. Nielsen M.A., Chuang I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000).
191. Pastawski F., Yao N.Y., Jiang L., Lukin M.D., Cirac J.I.: Unforgeable noise-tolerant quantum tokens. Proc. Natl Acad. Sci. USA **109**(40), 16079–16082 (2012). doi:10.1073/pnas.1203552109.
192. Peikert C.: A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939 (2015). http://eprint.iacr.org/2015/939.
193. Pironio S., Massar S.: Security of practical private randomness generation. Phys. Rev. A **87**(1), 012336 (2013). doi:10.1103/physreva.87.012336.
194. Pironio S., Acín A., Massar S., de la Giroday A.B., Matsukevich D.N., Maunz P., Olmschenk S., Hayes D., Luo L., Manning T.A., Monroe C.: Random numbers certified by Bell's theorem. Nature **464**, 1021–1024 (2010). doi:10.1038/nature09008.
195. Rabin M.: How to exchange secrets by oblivious transfer. Technical Report TR-81. Harvard University, Cambridge (1981).
196. Regev O.: Quantum computation and lattice problems. SIAM J. Comput. **33**(3), 738–760 (2004). doi:10.1137/S0097539703440678.

197. Reichardt B.W., Unger F., Vazirani U.: Classical command of quantum systems. Nature **496**, 456–460 (2013). doi:10.1038/nature12035.
198. Renner R.: Security of quantum key distribution. Int. J. Quantum Inf. **06**(01), 1–127 (2005). doi:10.1142/S0219749908003256.
199. Rivest R.L., Adleman L., Dertouzos M.L.: On data banks and privacy homomorphisms. In: Foundations of Secure Computation, pp. 169–177 (1978). https://people.csail.mit.edu/rivest/pubs/RAD78.pdf.
200. Rivest R.L., Shamir A., Adleman L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978). doi:10.1145/359340.359342.
201. Salvail L.: Quantum bit commitment from a physical assumption. In: CRYPTO 1998, pp. 338–353 (1998). doi:10.1007/BFb0055740.
202. Salvail L., Schaffner C., Sotáková M.: Quantifying the leakage of quantum protocols for classical two-party cryptography. Int. J. Quantum Inf. **13**(04), 1450041 (2014). doi:10.1142/s0219749914500415.
203. Sastry N., Shankar U., Wagner D.: Secure verification of location claims. In: WiSe 2003, pp. 1–10. (2003). doi:10.1145/941311.941313.
204. Scarani V., Renner R.: Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys. Rev. Lett. **100**(20), 200501 (2008). doi:10.1103/physrevlett.100.200501.
205. Schaffner C.: Cryptography in the bounded-quantum-storage model. PhD Thesis, University of Aarhus (2007). arXiv:0709.0289.
206. Shor P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: FOCS 1994, pp. 124–134. IEEE, Los Alamitos (1994). doi:10.1109/SFCS.1994.365700.
207. Shor P.W., Preskill J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000). doi:10.1103/physrevlett.85.441.
208. Simon C., Afzelius M., Appel J., Boyer De La Giroday A., Dewhurst S.J., Gisin N., Hu C.Y., Jelezko F., Kröll S., Müller J.H., Nunn J., Polzik E.S., Rarity J.G., De Riedmatten H., Rosenfeld W., Shields A.J., Sköld N., Stevenson R.M., Thew R., Weber I.A.M.C., Weinfurter H., Wrachtrup J., Young R.J.: Quantum memories: a review based on the European integrated project "qubit applications (QAP)". Eur. Phys. J. D **58**(1), 1–22 (2010). doi:10.1140/epjd/e2010-00103-y.
209. Singelee D., Preneel B.: s using secure distance bounding protocols. In: MASS 2005, vol. 7, pp.–840 (2005). doi:10.1109/MAHSS.2005.1542879.
210. Song F.: A note on quantum security for post-quantum cryptography. In: PQCrypto 2014, pp. 246–265 (2014). doi:10.1007/978-3-319-11659-4_15.
211. Stebila D., Mosca M., Lütkenhaus N.: The case for quantum key distribution. In: Quantum Communication and Quantum Networking, vol. 36, pp. 283–296 (2010). doi:10.1007/978-3-642-11731-2_35.
212. Tittel W., Zbinden H., Gisin N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A **63**, 042301 (2001). doi:10.1103/PhysRevA.63.042301.
213. Tomamichel M., Leverrier A.: A rigorous and complete proof of finite key security of quantum key distribution (2015). arXiv:1506.08458.
214. Tomamichel M., Lim C.C.W., Gisin N., Renner R.: Tight finite-key analysis for quantum cryptography. Nat. Commun. **3**, 634 (2012). doi:10.1038/ncomms1631.
215. Uhlmann A.: The transition probability in the state space of a *-algebra. Rep. Math. Phys. **9**(2):273–279 (1976). doi:10.1016/0034-4877(76)90060-4.
216. Unruh D.: Universally composable quantum multi-party computation. In: EUROCRYPT 2010, pp. 486–505 (2010). doi:10.1007/978-3-642-13190-5_25.
217. Unruh D.: Concurrent composition in the bounded quantum storage model. In: EUROCRYPT 2011, pp. 467–486 (2011). doi:10.1007/978-3-642-20465-4_26.
218. Unruh D.: Quantum proofs of knowledge. In: EUROCRYPT 2012, pp. 135–152 (2012). doi:10.1007/978-3-642-29011-4_10.
219. Unruh D.: Everlasting multi-party computation. In: CRYPTO 2013, pp. 380–397 (2013). doi:10.1007/978-3-642-40084-1_22.
220. Unruh D.: Quantum position verification in the random oracle model. In: EUROCRYPT 2014, pp. 1–18 (2014). doi:10.1007/978-3-662-44381-1_1.
221. Unruh D.: Revocable quantum timed-release encryption. In: EUROCRYPT 2014, pp. 129–146 (2014). doi:10.1007/978-3-642-55220-5_8.
222. Unruh D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: EUROCRYPT 2015, pp. 755–784 (2015). doi:10.1007/978-3-662-46803-6_25.
223. van de Graaf J.: Towards a formal definition of security for quantum protocols. PhD Thesis, Université de Montréal (1997). http://www.collectionscanada.gc.ca/obj/s4/f2/dsk2/ftp03/NQ35648.pdf.
224. Vazirani U.V., Vidick T.: Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In: STOC 2012, pp. 61–76 (2012). doi:10.1145/2213977.2213984.

225. Vazirani U.V., Vidick T.: Robust device independent quantum key distribution. In: ITCS 2014, pp. 35–36 (2014). doi:10.1145/2554797.2554802.
226. Vora A., Nesterenko M.: Secure location verification using radio broadcast. Trans. Dependable Secur. Comput. **3**(4), 377–385 (2006). doi:10.1109/TDSC.2006.57.
227. Watrous J.: Zero-knowledge against quantum attacks. In: STOC 2006, pp. 296–305 (2006). doi:10.1145/1132516.1132560.
228. Watrous J.: Theory of quantum information (2015). https://cs.uwaterloo.ca/~watrous/TQI/.
229. Wehner S., Winter A.: Entropic uncertainty relations- a survey. New J. Phys. **12**(2), 025009 (2010). doi:10.1088/1367-2630/12/2/025009.
230. Wehner S., Wullschleger J.: Composable security in the bounded-quantum-storage model. In: Automata, Languages and Programming, pp. 604–615 (2008). doi:10.1007/978-3-540-70583-3_49.
231. Wehner S., Schaffner C., Terhal B.M.: Cryptography from noisy storage. Phys. Rev. Lett. **100**(22), 220502 (2008). doi:10.1103/PhysRevLett.100.220502.
232. Wehner S., Curty M., Schaffner C., Lo H.-K.: Implementation of two-party protocols in the noisy-storage model. Phys. Rev. A **81**(5), 052336 (2010). doi:10.1103/physreva.81.052336.
233. Wiesner S.: Conjugate coding. ACM SIGACT News **15**(1), 78–88 (1983). doi:10.1145/1008908.1008920.
234. Wilde M.M.: Quantum Information Theory. Cambridge University Press, New York (2013).
235. Winkler S., Tomamichel M., Hengl S., Renner R.: Impossibility of growing quantum bit commitments. Phys. Rev. Lett. **107**(9), 090502 (2011). doi:10.1103/PhysRevLett.107.090502.
236. Wootters W.K., Zurek W.H.: A single quantum cannot be cloned. Nature **299**, 802–803 (1982). doi:10.1038/299802a0.
237. Yao A.C.: Protocols for secure computations. In: FOCS 1982, pp. 160–164 (1982). doi:10.1109/SFCS.1982.38.
238. Yao A.C.-C.: Security of quantum protocols against coherent measurements. In: STOC 1995, pp. 67–75. (1995). doi:10.1145/225058.225085.
239. Yu L., Pérez-Delgado C.A., Fitzsimons J.F.: Limitations on information-theoretically-secure quantum homomorphic encryption. Phys. Rev. A **90**(5), 050303 (2014). doi:10.1103/physreva.90.050303.
240. Zhandry M.: How to construct quantum random functions. In: FOCS 2012, pp. 679–687 (2012). doi:10.1109/FOCS.2012.37.
241. Zhang Y., Liu W., Fang Y., Wu D.: Secure localization and authentication in ultra-wideband sensor networks. IEEE J. Sel. Areas Commun. **24**(4), 829–835 (2006). doi:10.1109/JSAC.2005.863855.