Research proposal

Title

Multi-party quantum cryptographic primitives in realistic environments

Scientific context

In an increasingly connected and globalized world, the notions of security and privacy are an imperative, henceforth making cryptography a very important research field. When one is concerned with the notion of security, it is wise to build systems that are secure not only against current adversaries, but also against future malicious parties with ever more sophisticated computational abilities. In the not so far future, such adversaries are likely to possess the ability to perform computations on quantum computers that would enable them to break most of the commonly used security systems.

It is, therefore, an urgency to strengthen the foundations of cryptography, in order to make them sufficient for a world where quantum computation and communication is an available resource. Hence, the aim of this doctoral project will be to produce novel and fundamental research in this field by focusing on unmet scientific goals that arise both from a theoretical and practical viewpoint.

Quantum computation has had a tremendous impact in the field of cryptography in the last decades. Peter Shor's algorithm for factoring large numbers [*Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computing, 1997] shows that quantum computers are probably more powerful than classical ones, since factoring is assumed to be hard for any classical computer. In fact, the hardness of factoring is used as proof of security for most currently used classical cryptographic systems, such as RSA, and hence Shor's result proves that classical cryptography is vulnerable against quantum computers.

Moreover, the ability to communicate over quantum channels has made it possible to revisit unconditionally secure cryptography. In one of the most celebrated results in quantum computation, Bennett and Brassard [*Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, 1984] showed that it is possible for two parties to distribute a secret key in a way which is unconditionally secure against all attacks. Hence, in theory it is possible to have quantum cryptography against any adversary.

Following this discovery, the resulting field of quantum key distribution has seen an unprecedented progress in the past two decades both from a theoretical and experimental perspective. Information-theoretic security proofs are now available for several protocols, and experimental systems have been tested in practical conditions [V. Scarani et al, *The security of practical quantum key distribution*, Reviews of Modern Physics, 2009]. These developments open the way to using the power of quantum mechanical systems to achieve a level of security in computer and communication infrastructures that is impossible by any classical means.

The proposed research project, described hereafter, is situated at the heart of this exciting field. It has the goal to build upon the wealth of knowledge available for quantum key distribution to explore advanced quantum cryptographic primitives in a realistic setting, which involves practical components and multiple communication parties.

Scientific content

Since the discovery of unconditionally secure key distribution, a series of works has investigated what other cryptographic primitives are possible or not in the quantum world. New cryptographic primitives without classical counterparts have been introduced and have required powerful tools from quantum information theory in order to prove their security. Such primitives include bit escrow, non-ideal coin flipping, cheat-sensitive bit commitment and oblivious transfer, data hiding and uncloneable encryption. Although these primitives might seem too abstract to be relevant to the real world, they are in fact at the core of any secure application that we might be interested in, including digital signatures, electronic voting, message authentication, or secure identification.

Among the aforementioned primitives, coin flipping has generated the most exciting recent developments. Coin flipping is the communication problem in which two distrustful parties wish to agree on a common random bit, by talking over the phone. This primitive is important for randomized distributed computations. When the two parties follow a protocol honestly, the bit they agree on is required to be 0 or 1 with equal probability. Ideally, they would also like that if any (dishonest) party deviates from the protocol, they will not agree on any particular outcome with probability more than 1/2. The deviation of this probability to 1/2 is called the bias. It is known that ideal coin flipping is impossible without any hardness assumptions, in both the classical and the quantum setting. In fact, in any classical protocol, the bias is 1/2. The best known quantum protocol is by Ambainis [*A new protocol and lower bounds for quantum coin flipping*, Proceedings of STOC, 2001], and achieves a bias 1/4. It is also known that quantum coin flipping protocols cannot achieve a bias smaller than 0.207, as was proven by Kitaev [results presented at QIP 2003]. Recently, the gap between these lower and upper bounds has been bridged by Chailloux and Kerenidis [*Optimal quantum strong coin flipping*, Proceedings of FOCS 2009].

The above results are all derived in an idealized setting, where there are no errors and losses in the communication channel. It is clear, however, that for quantum cryptography to reach a level of maturity that will allow its integration into practical communications systems offering a guaranteed level of security and performance that is superior to those of their classical counterparts, there is a need to address issues that appear when a realistic setting is considered.

In this perspective, it is important to note that the successful practical implementation of quantum key distribution systems has shown that quantum cryptography is not a scenario of the future, as might be the case for a quantum computer for example, but a much easier to reach technology. In the last decade, quantum key distribution systems have evolved from very basic laboratory experimental setups to fully automated end products that can be operated over long distances, are commercially available, and can be integrated into

classical optical fiber networks [M. Peev et al, *The SECOQC quantum key distribution network in Vienna*, New Journal of Physics, 2009]. To reach this state of the art many problems had to be overcome, ranging from purely theoretical issues, for example how security proofs for the various protocols can remain valid when realistic components are taken into account, to engineering problems that appear in large-scale practical implementations.

The first steps towards addressing realistic conditions in systems implementing quantum coin flipping have only recently been undertaken by Berlin et al [*Fair loss-tolerant quantum coin flipping*, Physical Review A, 2009; *Flipping quantum coins*, arXiv:quant-ph/0904.3946], who proposed a protocol that takes into account the losses that naturally occur in the communication channel and identified the corresponding optimal cheating strategies. In parallel, Wehner et al have studied the feasibility of protocols such as bit commitment and oblivious transfer when certain restrictions are placed on the capabilities of the cheating party, in particular with respect to her access to ideal quantum storage [*How to implement two-party protocols in the noisy-storage model*, arXiv:quant-ph/0911.2302]. Despite this progress, however, there is to date no complete study of feasibility or an actual development of a system implementing a quantum protocol other than key distribution. In particular, a general treatment of errors due to imperfections of practical components, and of the best strategy cheating attacks that can take advantage of them, is presently missing.

The main goal of this doctoral project is therefore to provide a general framework that will enable the implementation of loss and error-tolerant quantum cryptographic primitives such as coin flipping. The first step will be to extend the developed theoretical models in the realistic scenario and identify potential parameter regions where the implementation of such protocols is impossible or their premise significantly compromised, or, inversely, to regions where the desired security conditions are satisfied, i.e., the protocol with honest parties has negligible probability to abort and the maximum probability of successful cheating is limited to a reasonable value. We will also seek to define the optimal cheating strategies in these regions. This work will lead to a set of conditions that will render feasible an experimental implementation of the quantum coin flipping and similar protocols. The next step will then be to demonstrate such a system ideally using standard telecommunication and fiber optic components, and without the need for “expensive” resources, such as entangled-photon sources and quantum memories.

Another direction that the project will pursue is the extension of the aforementioned ideas to a multi-party structure. Indeed, as in any communication model, going beyond the basic two-party protocol implemented over a single communication channel to include multiple communicating parties distributed on a network structure has important advantages. Most importantly, this allows overcoming the main limitation imposed by the loss in the channel to the maximum possible communication distance between two parties and is better suited to a realistic scenario of communication systems for which point-to-point exchange links are not sufficient. This setting and the change of security conditions that it implies have only recently been studied in the context of quantum key distribution [L. Salvail et al, *Security of trusted repeater quantum key distribution networks*, Journal of Computer Security, 2010], while no related work has been conducted for advanced cryptographic primitives such as coin flipping and bit commitment.

As the deployment of quantum cryptography networks becomes an increasingly realistic perspective, it is therefore essential to conceive and implement adapted quantum protocols. Hence, this project will aim at studying the security of quantum cryptographic primitives taking into account practical implementation considerations related to the topology and resources of a network structure.

Management

The presented project is situated at the frontier between computer science and physics; we therefore propose the co-supervision of the candidate by two scientists, Eleni Diamanti and Iordanis Kerenidis, who belong in these two fields with common involvement and interest in quantum communication and quantum computation. Throughout her doctoral degree, the candidate will benefit from the extensive national and international collaborations the corresponding teams in Télécom ParisTech and Université Paris-Sud XI hold with prominent researchers in the field. Both researchers are members of the French National Research Agency (ANR) Jeunes Chercheurs research project CRYQ “Quantum cryptography in theory and in practice”, recently obtained by Iordanis Kerenidis. The proposed project will solidify and extend their ongoing collaboration in the field of quantum cryptography and will provide the synergy of experiment and theory required to successfully address the next-generation security. The ANR has awarded 40 k€ for equipment for this project as well as mobility opportunities for the doctoral candidate. Experimental work will be pursued in the laboratory space available in Télécom ParisTech.

We expect that the proposed research project will lead to several publications in internationally renowned journals, and to conference presentations. We also expect that the results will be of interest to a wide part of the scientific community, and will stimulate further research on these subjects that are of utmost importance for the establishment of quantum cryptography as an essential technology for the security assurance of future computer and communication systems.