FOCUS WEEK 3: QUANTUM CRYPTOGRAPHY

TITLES AND ABSTRACTS

———

MINICOURSE (3 hours)

Speaker: Florian Speelman

Title: Introduction to quantum cryptography

Abstract: The field of quantum cryptography aims to use quantum information to perform cryptographic tasks. This combination can take different forms: Quantum computation can be used to break cryptographic schemes, for example using Shor's algorithm, but quantum information can also achieve new goals that are impossible when using only classical information. In this lecture series, I will give a high-level overview of (parts of) this field, suitable for those without a background in cryptography.

Topics we will discuss include:
- Fully-quantum cryptography, such as the quantum one-time pad, quantum authentication, and secure quantum computation.
- How quantum information can help with cryptographic tasks, as seen in QKD and quantum money.
- Post-quantum cryptography, the influence of quantum attacks on classical cryptography.

See also https://arxiv.org/abs/1510.06120 for a recent survey on these topics.

———

TALKS

Speaker: Toni Acín

Title: Conditions for the implementation of device-independent cryptographic protocols.

———

Speaker: Anne Broadbent

Title: Quantum Encodings for Classical Messages

Abstract: We show that the encryption of classical data into quantum ciphertexts leads to cryptographic functionalities that are not achievable using classical information alone, and that furthermore these functionalities can be achieved by building on Wiesner's conjugate coding.

The first such property is *uncloneable encryption*. Here, classical data is encoded into a quantum ciphertext in a way that it is inherently protected against copying. That is, given a ciphertext, no adversary can produce two registers which, once isolated would *both* be useful in reconstructing the plaintext, given the decryption key. (1)

The second property is *certified deletion*. Here, classical data is encoded into a quantum ciphertext in a way that the recipient of the ciphertext can produce a *classical* string which proves to the originator that the recipient has relinquished any chance of recovering the plaintext, should the decryption key be revealed. (2)

The success of both of these schemes can be attributed informally to the quantum no-cloning principle; however the formal proofs use techniques from the analysis of monogamy-of-entanglement games (for the first scheme) and from the entropic uncertainty relations as developed in the security proofs of quantum key distribution (for the second scheme).

(1) Joint work with Sébastien Lord.
(2) Joint work with Rabib Islam.

———

Speaker: Harry Buhrman

Title: Quantum fine-grained complexity

———

Speaker: Eleni Diamanti

Title: Quantum cryptography: from security proofs to practical implementations

Abstract: In order to claim that a quantum cryptographic protocol is implemented properly and hence provides a well-defined security advantage in practice, it is necessary to address several theoretical and experimental challenges. We discuss methods and solutions that have been adopted in the last years in the effort to satisfy assumptions present in theoretical security proofs using practical, inevitably imperfect, photonic systems and to correctly benchmark the implementations with respect to classical resources. We illustrate these methods using as examples state-of-the-art demonstrations of quantum key distribution, coin flipping, quantum money, and entanglement verification.

———

Speaker: David Elkouss

Title: Design tools for long distance quantum cryptography

Abstract: Quantum communication enables a host of applications that cannot be achieved by classical communication means, with provably quantum key distribution (QKD) as one of the prime examples. The distance that quantum communication schemes can cover via direct communication is fundamentally limited by losses on the communication channel. By means of quantum repeaters, the reach of these schemes can be extended and chains of quantum repeaters could in principle cover arbitrarily long distances.

The experimental implementation of quantum repeaters has seen tremendous progress in the past year, with the first proof of principle setups achieving rates beyond the point to point channel capacity demonstrated. As the technology matures, it becomes relevant to develop tools capable of evaluating the feasibility of quantum network setups and quantifying the achievable rates. Here, I will present recent progress towards this goal. I will attack it from different angles.

First, I will present an abstract information theoretic approach, considering the channel description of each of the links in the network. This abstract approach allows for a simple solution in the form of efficiently computable lower and upper bounds for network capacities. For this we make use of the max-flow min-cut theorem and its generalization to multi-commodity flows to obtain linear programs (LPs).

Then I will move to a more practical situation, with limited processing power at the nodes and decoherence. In this setup, we provide two efficient algorithms for determining the generation time and fidelity of the first generated entangled pair between the end nodes of a quantum repeater chain. The runtime of the algorithms increases polynomially with the number of segments of the chain, which improves upon the exponential runtime of existing algorithms. Using our proof-of-principle

implementation, we are able to analyze repeater chains of thousands of segments for some parameter regimes.

Finally, I will present a discrete event simulator for quantum networks that allows to accurately model hardware and timing enabling accurate prediction of performance.

———————

Speaker: Omar Fawzi

Title: Generalizing the entropy accumulation theorem

Abstract: The entropy accumulation theorem states that the smooth min-entropy of an n-partite system A=(A1,…,An) is lower-bounded by the sum of the von Neumann entropies of suitably chosen conditional states up to corrections that are sublinear in n. This theorem is particularly suited to proving the security of quantum cryptographic protocols, and in particular so-called device-independent protocols for randomness expansion and key distribution. In this talk, I will review the statement of the theorem and how it is applied to analyze randomness expansion protocols and discuss ongoing work to generalize the theorem to allow a broader applicability.

———————

Speaker: Anthony Leverrier

Title: Theoretical challenges in continuous-variable quantum key distribution

Abstract: Continous-variable quantum key distribution (CVQKD) is quickly becoming a credible alternative to standard protocols like BB84, essentially because coherent detection is more practical than single-photon detection. The simplified experimental setup comes, however, at the price of significantly more complicated security proofs. In this talk, I will recall the basics of CVQKD and present the state-of-the-art concerning their security proofs, including some very recent developments for protocols with a discrete modulation of coherent states. I will then mention a few pressing open questions in the field and suggestions as how to attack them.

———————