Abstracts

Can code-based keys and cryptograms get smaller than their RSA counterparts?

Paulo Barreto

The most obvious task involved in making code-based cryptographic schemes practical is reducing the size of keys and cryptograms. A concrete metric for that task would be to take these sizes down to at least that of corresponding RSA keys and cryptograms at the same (pre-quantum) security level while keeping the resulting schemes efficient. This major challenge has seen a lot of progress in recent years, but so far code-based sizes have remained considerably larger than their RSA counterparts. In this talk we will review the main milestones involved in this process, indicate the underlying security assumptions, and present evidence that the goal of satisfying (and exceeding) the proposed metric is not only reachable, but apparently simple to attain.

Post-quantum cryptography – Multivariate public key cryptosystems

Jintai Ding

Multivariate public key cryptosystems (MPKCs), whose public key is mostly a set of quadratic polynomials over a finite field, are one of the four main families of public key cryptosystems that have the potential to resist future quantum computer attacks. This construction is based on the fact that solving a random multivariate polynomial system over a finite field is an NP-complete problem.

In this talk, we will present the main constructions of MPKCs and the main security analysis tools. We will also present a discussion on major challenges in the in the area of MPKCs.

Implementations of Code-based Cryptography

Stefan Heyse

In this talk we will review the description of code-based crypto systems and the underlying codes from an engineer’s point of view. After presenting the McEliece and Niederreiter scheme, we will discuss different algorithms for syndrome computation, decoding and root searching. We will also highlight some alternative code constructions (to reduce key size) and necessary

overhead to achieve practical security. The main focus will be on small embedded microcontrollers and high-end FPGAs.

Nadia Heninger

A lattice is a periodic arrangement of points in real space. Several computational problems on lattices are known to be NP-hard, including finding the shortest vector in a given lattice. These computational problems on lattices have several properties that make them an appealing foundation for cryptography: they permit reductions from average instances to the worst case hardness of certain problems, and are not known to be efficiently solvable using quantum techniques. In this tutorial, I will introduce the basics of lattices, computational problems on lattices, and cryptographic constructions.

Superpolynomial quantum speedups and their cryptographic implications

Stephen Jordan

It is now well-known that quantum computers, if built, could factor integers and perform discrete logarithms in polynomial time, thereby breaking the RSA and Diffie-Hellman cryptosystems. It is less well-known that quantum algorithms offering superpolynomial speedup have been discovered for several other problems, including solving Pell's equation, finding unit groups and class groups of number fields, approximating link invariants, and decomposing Abelian and solvable groups. In this tutorial, I will give a high-level overview of these algorithms and their cryptographic implications.

Polynomial Speed-Up Quantum Algorithms Overview

Frederic Magniez

A direction of research in quantum computation pioneered by Grover around search problems in unstructured, structured, or partially structured databases has constantly been infused with new ideas for algorithm design. In contrast to problems based on the Hidden Subgroup Problem (HSP), the speed-up for these search problems is often only polynomial. Nonetheless, those tools are conceptually rich and help us to improve our understanding on quantum computing.

Moreover, since the impact of quantum algorithms with exponential speed-up has been quite well-understood, research in post-quantum cryptography aims at finding and analyzing cryptosystems so that they are ready to be used once quantum computers become a reality. In this context, one has to understand the power of quantum computation in its full generality, since a significative polynomial speed-up could potentially be enough to break such a cryptosystem.

In this talk we will review most of popular tools for designing quantum algorithms for various search problems. We will start by Grover search algorithm and its extensions such as Amplitude Amplification. Then we will introduce the concept of quantum search via Quantum Walks. Last we will conclude by some new tools and results. All the concepts will be introduced without any need of background on quantum computing. They will be stated as black-box tools and we will show how they can be used through key examples. In particular, each quantum algorithmic concept will be presented with its randomized analogue. Then we will explain how one can derive its quantum complexity given its randomized one.

An MQ/Code Public-Key Cryptosystem

Leonard J. Schulman

I'll outline a new PKC proposal that relies on the hardness of tensor decomposition.

Code-based Cryptography

Nicolas Sendrier

Code-based cryptography is among the most attractive post-quantum cryptographic techniques. It allows the construction of the most important cryptographic primitives (encryption, signature, zero-knowledge, hashing...) often with efficient implementations and strong security reductions. Their practical security is very well understood and the the best known attacks can be precisely analysed, allowing a very accurate parameter selection. In this tutorial, we will first present the most important schemes in code-based crypto and examine their main features in terms of security and implementation.

Next, we will present the new trends, in particular concerning the the public-key size issues, but also about the interest of diversity in the choice of the code family. Hopefully this will allow us to make some guesses about the evolution of this area of research.

Cryptography based on ideal lattices

Damien Stehlé

Lattice-based cryptography is emerging as one of the strongest alternatives to contemporary public-key cryptography. Its two most attractive features are its unparalleled security assurances -- with well-studied worst-case hardness assumptions that seem to remain hard even in the context of quantum computing, and its great flexibility -- enabling the design of advanced cryptographic primitives such as fully homomorphic encryption.

On the other hand, lattice-based cryptography seems quite inefficient from a practical perspective, in comparison to contemporary cryptography. To circumvent this limitation, cryptographers consider restrictions of the underlying worst-case and average-case lattice problems to special families of lattices leading to faster cryptographic algorithms.
These special lattices correspond to ideals of the rings of integers of some number fields of large degrees, and to small-rank modules over these rings.
In this talk, I will describe these lattices, how cryptographic primitives are constructed from them, and the underlying hardness assumptions.

Multivariate PKC and the complexity of solving systems

Bo-Yin Yang

Solving a system of multivariate nonlinear equations is the most obvious attack for all Multivariate Public-Key Cryptosystems, and the complexity of many cryptographic attacks also depends on that of system-solving. We take a less travelled route in this talk by looking for situations where the standard approach using F4/F5 may not be best, and discussing assorted practical and theoretical issues associated with alternatives, particularly of XL variants based on sparse matrix solvers.