SESSION ON COMPUTATIONAL ALGEBRAIC GEOMETRY, AND POST-QUANTUM CRYPTOGRAPHY – MULTIVARIATE PUBLIC KEY CRYPTOGRAPHY

JINTAI DING, SHUHONG GAO, YOSSI PEREZ, LUDOVIC PERRET, DANIEL SMITH-TONE, TSUYOSHI TAKAGI

Organization Committee
Jintai Ding, University of Cininnati, jintai.ding@gmail.com
Shuhong Gao, Clemson university, sgao@clemson.edu
Yossi Perez, Jerusalem College of Technology, yosip@jct.ac.il
Ludvic Perret, Universit Pierre et Marie Curie ludovic.perret@lip6.fr
Daniel Smith-tone, University of Louiseville, daniel-c.smith@louisville.edu
Tsuyoshi Takagi, Kyushu University, takagi@imi.kyushu-u.ac.jp

Motivation: For the last three decades, public-key cryptosystems, a revolutionary breakthrough in cryptography, have completely changed the landscape of modern communication, becoming an indispensable part of the foundation of our communication network. With an array of applications integrated into our lifestyles— internet shopping, Facebook, software updates, VPN, etc.— the assurance of security in remote communication is of critical importance.

The Internet, as well as other communication systems, rely principally on the Diffie-Hellman key exchange, RSA, DSA, ECDSA and similar public key cryptosystems, the security of which depend on the difficulty of certain number theoretic problems such as Integer Factorization or the Discrete Log Problem over various groups. In 1994, however, Dr. Peter Shor of Bell Laboratories showed that quantum computers can solve each of these problems, thus rendering all public key cryptosystems based on such assumptions impotent. This means that if a reasonably powerful quantum computer can be built, it will put all modern communication— from key exchange to encryption to digital authentication— in peril.

In 2001, Dr. Chuang et al. at IBM implemented Shor's algorithm on a 7-qubit quantum computer. Some physicists predict that within the next 20 or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. A large international community has emerged to address this issue in the hope that our public key infrastructure may remain intact by utilizing new **quantum-resistant** primitives. In the academic world, this new science bears the moniker "**Post-Quantum Cryptography**."

Many resources around the world have been devoted to the search for alternative public key cryptosystems, both in academia and beyond. In May of 2006, the first of a continuing series of International Workshops on Post-Quantum Cryptography was organized by the European Network of Excellence for Cryptology (ECRYPT). The 7th

PQCRYPTO conference will be held in February of 2016 at the Institute of Mathematics for Industry at Kyushu University in Japan. There have been numerous high quality academic workshops devoted to quantum-resistant technologies, including workshops at DIMACS at Rutgers, the Lorentz Center in Leiden and Schloss Dagstuhl. Several academia-coordinated projects have been established to evaluate and develop the mathematics required for post-quantum security, including the EU's PQCRYPTO Project ICT-645622, SAFECRYPTO ICT-644729 and CREST Crypto-Math in Japan. This effort has also received attention within the standardization and policy spectrum. The National Institute of Standards and Technology (NIST) has held two workshops on post-quantum cryptography and the European Telecommunications Standards Institute (ETSI) has held three "Quantum-Safe Cryptography" workshops.

Even some of the more clandestine institutions have broken the silence on post-quantum cryptography. In the UK, the Government Communications Headquarters (GCHQ) has publicly acknowledged and published work on quantum-resistant cryptography. In the US, the National Security Agency (NSA) published a webpage including the quote:

> "Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to **quantum resistant** algorithms."

In February 2016 in the 7th PQCrypto workshop in Japan, NIST announced the call for proposals for quantum resistant algorithms with a deadline of the end of 2017. Considering all of these sources, it is clear that the effort to develop quantum-resistant technologies is intensifying. With historical perspective, it seems likely that the post-quantum standards derived from this process will be endorsed by other standards organizations around the world and set the stage for the maintenance of our e-society in the future generation.

Focus and Organization: Currently there are four main families of public key cryptosystems with the potential to resist attacks from quantum computers:

- Diffie-Lamport-Merkle Hash-based public key cryptosystems,
- lattice-based public key cryptosystems,
- McEliece code-based public key cryptosystems and
- multivariate public key cryptosystems (MPKCs).

An MPKC is a cryptosystem whose public key is given as a set of multivariate polynomials over a normally small finite field, namely, the public key is given as

$$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)),$$

where the $p_1, ..., p_m$ is a set of (usually quadratic) polynomials over a small finite field k. Here $P(x_1, ..., x_n)$ is a map from k^n to k^m. For an encryption scheme, the encryption process is the evaluation of the polynomials, namely of the plain text is $(x'_1, \ldots, x'_n)$, the ciphertext is given as:

$$(y'_1, \ldots, y'_m) = P(x'_1, \ldots, x'_n) = (p_1(x'_1, \ldots, x'_n), \ldots, p_m(x'_1, \ldots, x'_n).$$

The decryption process uses the hidden secret inside P, which is usually constructed as composition of three maps:

$$P = L_1 \circ \bar{P} \circ L_2,$$

where L_1 and L_2 are two invertible linear maps and $\bar{P}$ is a map easy to "Invert", that is to find its preimage computationally easily. Since the public key is known, to find the plaintext $(y'_1, \ldots, y'_m)$ is equivalent to solving the equation:

$$P(x_1, \ldots, x_n) = (y'_1, \ldots, y'_m).$$

The security of such systems is suggested by the fact that solving a system of multivariate polynomial equations over a finite field (PoSSo) is in general NP-complete. This implies that it is unlikely that a quantum-computer can solve PoSSo in polynomial-time. Furthermore, computations in a finite field are more efficient than the manipulation of large integers which is required by the systems based on hard number theory problems. Thus MPKC's can be less computationally intensive than these systems and consequently have the potential for application in small ubiquitous computing devices with limited resources.

MPKCs' theoretical foundation is algebraic; specifically, the science explores structure related to polynomials. Lying at the intersection of commutative algebra, algebraic geometry, discrete geometry and computational algebra, multivariate cryptography is a profoundly interdisciplinary and profoundly modern field in the mathematical sciences.

In the last two decades, tremendous progress has been made not only in the theoretical venue, but in the practical development of MPKCs, particularly in the area of signature schemes. One such MPKC is at the core of a digital signature scheme which is one of the fastest in existence and which has withstood more than 10 years of attacks.

The goal of this session is to bring together the leading researchers in the world in the area of quantum-resistant MPKCs and computational algebraic geometry, in particular, the area of polynomial solving, like Gröbner basis, so that we can, on one hand, combine our expertise, refine the theory and design the best possible MPKCs in the hope that we can establish confidence in a practical MPKC standard, on the other hand, we hope to bring new stimulus into computational algebraic geometry by introducing many interesting and exciting new problems to people in computational algebraic geometry. For instance, a fundamental issue is to bound precisely the complexity of computing a Gröbner basis for systems appearing in MPKC. This requires to understand the algebraic and geometric properties – such as the degree of regularity – of the ideal generated by the public polynomials. We already have techniques to derive upper bound on this degree of regularity. The question here is to derive tighter upper bounds. Another topic that requires at the intersection of MPKC and algebraic geometry is the so-called Fröberg conjecture about the existence of semi-regular sequences. This is important conjecture widely used to derive secure parameters for MPKC. Whilst many experimental evidences tends to validate the conjecture of Fröberg, very few theoretical results are known.

The current climate among standards organizations and policymakers as well as the rapid maturation of this field provide an environment that assures us that the products of this session will have profound practical as well as scientific impact.

The rationale behind the proposed session is to provide a framework to build a new research community of people from both cryptography and computational algebraic geometry to provide support for research in MPKC. This will help tremendously in building solid post-quantum multivariate candidates for international security standards and, in particular, a candidate for standardization by NIST. People in cryptography will present the state of art of research in cryptography and the critical mathematical problems and people in computational in algebraic geometry will present the current best methods and

tools in their area and then they will work together to find ways to solve those critical problems.

The basic philosophy on research in post-quantum cryptography is that our work should first be based on solid understanding of the hidden mathematical structures behind various applied problems, and we should also use the stimulus from the challenge in practical problems to help us to develop new concepts and new ideas in theory. In terms of practical applications, we believe there is clearly a gap in terms of what we can do and what is being used in information security, and we think it is time that we bridge this gap by combining the expertise of people in cryptography and computational algebraic geometry .

Currently, we are presented a great opportunity with the coming of age of post-quantum cryptography and we hope to use this session to make a difference at this exciting stage of development, in particular, in the area of MPKCs. With the science this workshop will help further evolve, we hope to make our society a better and more secure place.