Institute of mathematics & its applications

18th IMA International Conference on Cryptography and Coding

ONLINE EVENT VIA ZOOM

14-16 December,

CONFERENCE ABSTRACT BOOK

Table of Contents

Security in the Quantum Age – Juliane Krämer

Abstract:

In this talk, I will give a brief introduction to post-quantum cryptography (PQC), explaining the need for PQC and presenting the current state of PQC research and PQC standardization. Further on, I will talk about a specific challenge in PQC research: provable security in the quantum random oracle model. I will explain the importance of the random oracle model and the challenges that the quantum random oracle model entails. Following this, I will present a framework to lift classical security proofs in the random oracle model to post-quantum security.

A Note on Quantum Collision Resistance of Double-Block-Length Compression Functions

Shoichi Hirose[1][0000–0001–6723–722X] and Hidenori Kuwakado[2]

[1] University of Fukui, Fukui, Japan hrs _shch@u-fukui.ac.jp

[2] Kansai University, Osaka, Japan kuwakado@kansai-u.ac.jp

Abstract. In 2005, Nandi presented a class of double-block-length compression functions specified as $h^{\pi}(x) := (h(x), h(\pi(x)))$, where h is assumed to be a random oracle producing an n-bit output and π is a non-cryptographic permutation. He showed that the collision resistance of h^{π} is optimal if π has no fixed point. This manuscript discusses the quantum collision resistance of $h^{\pi}(x)$. First, it shows that the quantum collision resistance of h^{π} is not always optimal even if π has no fixed point: One can find a colliding pair of inputs for h^{π} with only $O(2^{n/2})$ queries to h by using the Grover search if π is an involution. Second, this manuscript shows that there really exist cases that the quantum collision resistance of h^{π} is optimal. More precisely, a sufficient condition on π is presented for the optimal quantum collision resistance of h^{π}, that is, any collision attack needs $\Omega(2^{2n/3})$ queries to find a colliding pair of inputs. The proof uses the recent technique of Zhandry's compressed oracle. Finally, this manuscript makes some remarks on double-block-length compression functions using a block cipher.

Keywords: Hash function • Compression function • Double-block-length• Grover's search • Zhandry's compressed oracle

An extension of Kannan's embedding for solving ring-based LWE problems

Satoshi Nakamura[1] and Masaya Yasuda[2]
[1] NTT Social Informatics Laboratories, Tokyo, Japan satoshi.nakamura.xn@hco.ntt.co.jp
[2] Department of Mathematics, Rikkyo University, Tokyo, Japan myasuda@rikkyo.ac.jp

Abstract. The hardness of the learning with errors (LWE) problem supports the security of modern lattice-based cryptography. Ring-based LWE is the analog of LWE over univariate polynomial rings that includes the polynomial-LWE and the ring-LWE, and it is useful to construct efficient and compact LWE-based cryptosystems. Any ring-based LWE instance can be transformed to an LWE instance, which can also be reduced to a particular case of the shortest vector problem (SVP) on a certain lattice by Kannan's embedding. In this paper, we extend Kannan's embedding for solving the search version of the ring-based LWE problem. Specifically, we propose a new extended lattice to include multiple short errors that are amplified by rotation operations for the coefficient vector of an error polynomial. Since multiple short errors have the same length and are embedded in our extended lattice, our extension could increase the success probability of solving the ring-based LWE problem by using the Block Korkine-Zorotarev (BKZ) algorithm that is widely used in cryptanalysis. We demonstrate the efficacy of our extension by experiments for solving various ring-based LWE instances.

Keywords: Ring-based LWE • Embeddings • Rotations • Lattices • BKZ

An Isogeny-Based ID Protocol Using Structured Public Keys

Karim Baghery, Daniele Cozzo, and Robi Pedersen
imec-COSIC, KU Leuven, Leuven, Belgium. karim.baghery@kuleuven.be,
daniele.cozzo@kuleuven.be, robi.pedersen@kuleuven.be

Abstract. Isogeny-based cryptography is known as one of the promising approaches to the emerging post-quantum public key cryptography. In cryptography, an IDentification (ID) protocol is a primitive that allows someone's identity to be confirmed. We present an efficient variation of the isogeny-based interactive ID scheme used in the base form of the CSIFiSh signature, which was initially proposed by Couveignes-Rostovtsev and Stolbunov, to support a larger challenge space, and consequently achieve a better soundness error rate in each execution. To this end, we prolong the public key of the basic ID protocol with some *well-formed* elements that are generated by particular factors of the secret key. Due to the need for a well-formed (or structured) public key, the (secret and public) keys are generated by a trusted authority. Our analysis shows that, for a particular security parameter, by extending a public key of size 64 B to 2.1 MB, the prover and verifier of our ID protocol can be more than 14× faster than the basic ID protocol which has a binary challenge space, and moreover, the proof in our case will be about 13.5× shorter. Using standard techniques, we also turn the presented ID protocol into a signature scheme that is as efficient as the state-of-the-art CSI-FiSh signature, and is existentially unforgeable under chosen message attacks in the (quantum) random oracle model. However, in our signature scheme, a verifier should get the public key of a signer from a trusted authority, which is standard in a wide range of current uses of signatures. Finally, we show how to eliminate the need for a trusted authority in our proposed ID protocol.

Keywords: Isogeny-based Cryptography • Identification Protocols • Digital Signatures • Quantum Random Oracle Model

Tightness Subtleties for Multi-User PKE Notions

Hans Heum[1] and Martijn Stam[1]
Simula UiB, Norway. hansh,martijn@simula.no

Abstract. Public key encryption schemes are increasingly being studied concretely, with an emphasis on tight bounds even in a multi-user setting. Here, two types of formalization have emerged, one with a single challenge bit and one with multiple challenge bits. Another modelling choice is whether to allow key corruptions or not. How tightly the various notions relate to each other has hitherto not been studied in detail. We show that in the absence of corruptions, single-bit left-or-right indistinguishability is the preferred notion, as it tightly implies the other (corruption-less) notions. However, in the presence of corruptions, this implication no longer holds; we suggest the use of a more general notion that tightly implies both existing options. Furthermore, for completeness we study how the relationship between left-or-right versus real-or-random evolves in the multi-user PKE setting.

Keywords: Indistinguishability • Public Key Encryption • Multi-User Security • Adaptive Corruptions

Cryptanalysis of the Rank Preserving Signature

Nicolas Aragon[1], Maxime Bros[1], and Philippe Gaborit[1]
University of Limoges, CNRS, XLIM, UMR 7252, Limoges, France {nicolas.aragon, maxime.bros, philippe.gaborit}@unilim.fr

Abstract. In code-based cryptography, the rank metric usually allows one to have smaller keys and signatures than the traditional Hamming metric. Recently, a new rank-based signature was proposed: Durandal. It relies on the use of proofs of knowledge, namely the Schnorr Lyubashevsky approach. The authors of the Rank Preserving Signature (RPS) built upon this approach and proposed even smaller keys and signatures than Durandal.

In this paper, we describe attacks against the RPS scheme which break all proposed sets of parameters.

More precisely, our attacks enable us to forge valid signatures in 2^{68} and 2^{47} operations for sets of parameters whose claimed securities are, respectively, 128 and 192 bits. In addition to this, we give a quantum adaptation of our attack which yields an attack on the last two sets of parameters.

Overall, our attacks highlight weaknesses of the RPS scheme and give new constraints when designing new parameter sets.

In order to describe the complexities of our attacks, this paper contains theoretical arguments together with experimental results for which we give the source code of our programs.

Keywords: Rank-Metric based Cryptography • Post-Quantum Cryptography • Signature .

Black-Box Accumulation Based on Lattices

Sebastian H. Faller[1], Pascal Baumer[2], Michael Klooß[3], Alexander Koch[3], Astrid Ottenhues[3], and Markus Raiber[3]
Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany[1] sebastian.faller@mailbox.org

[3] ueeap@student.kit.edu, [3] firstname.lastname@kit.edu

[4]

Abstract. Black-box accumulation (BBA) is a cryptographic protocol that allows users to accumulate and redeem points, e.g. in payment systems, and offers provable security and privacy guarantees. Loosely speaking, the transactions of users remain unlinkable, while adversaries cannot claim a false amount of points or use points from other users. Attempts to spend the same points multiple times (double spending) reveal the identity of the misbehaving user and an undeniable proof of guilt. Known instantiations of BBA rely on classical number-theoretic assumptions, which are not post-quantum secure. In this work, we propose the first lattice-based instantiation of BBA, which is plausibly postquantum secure. It relies on the hardness of the Learning with Errors
(LWE) and Short Integer Solution (SIS) assumptions and is secure in the Random Oracle Model (ROM).
Our work shows that a lattice-based instantiation of BBA can be realized with a communication cost per transaction of about 199MB if built on the zero-knowledge protocol by Yang et al. (CRYPTO 2019) and the CL-type signature of Libert et al. (ASIACRYPT 2017). Without any zero-knowledge overhead, our protocol requires 1.8MB communication.

Keywords: Lattice-based Cryptography · Black-box Accumulation (BBA) · Electronic Funds Transfer · Security and Privacy · Learning with Errors (LWE) · Short Integer Solution (SIS)

Batch Codes from Affine Cartesian Codes and Quotient Spaces

Travis Alan Baumbaugh[1], Haley Colgate[2], Tim Jackman[3], and Felice Manganiello[4]
[1] ToposWare, Shibuya-ku, Tokyo 150-8010, Japan
[2] University of Wisconsin - Madison, Madison, WI 53706, USA
[3]Boston University, Boston, MA 02215, USA
[4] Clemson University, Clemson, SC 29634, USA manganm@clemson.edu

Abstract. Affine Cartesian codes are defined by evaluating multivariate polynomials at a cartesian product of finite subsets of a finite field. In this work we examine properties of these codes as batch codes. We consider the recovery sets to be defined by points aligned on a specific direction and the buckets to be derived from cosets of a subspace of the ambient space of the evaluation points. We are able to prove that under these conditions, an affine Cartesian code is able to satisfy a query of size up to one more than the dimension of the ambient space.

The Problem Landscape of SIDH

David Jao, coundergrad.officer@uwaterloo.ca University Of Waterloo

The Supersingular Isogeny Diffie-Hellman protocol (SIDH) has recently been the subject of increased attention in the cryptography community. Conjecturally quantum-resistant, SIDH has the feature that it shares the same data flow as ordinary Diffie-Hellman: two parties exchange a pair of public keys, each generated from a private key, and combine them to form a shared secret. To create a potentially quantum-resistant scheme, SIDH depends on a new family of computational assumptions involving isogenies between supersingular elliptic curves which replace both the discrete logarithm problem and the computational and decisional Diffie-Hellman problems. As in the case of ordinary Diffie-Hellman, one is interested in knowing if these problems are related. In fact, more is true: there is a rich network of reductions between the isogeny problems securing the private keys of the participants in the SIDH protocol, the computational and decisional SIDH problems, and the problem of validating SIDH public keys. In this talk we explain these relationships, in the hopes of providing a clearer picture of the SIDH problem landscape to the cryptography community at large.

Forward Secrecy without Diffie-Hellman

Colin Boyd, colin.boyd@ntnu.no, NTNU

Forward secrecy is today regarded as a basic security property for authenticated key exchange. Widely deployed protocols, particularly TLS, routinely provide forward secrecy using the Diffie-Hellman protocol. However, there are several situations in which Diffie-Hellman cannot be used, so what becomes of forward secrecy then? This talk will consider three such situations: when interaction is not possible; when computation is very limited; and when post-quantum adversaries are available. In each case we will examine alternatives to Diffie-Hellman and discuss to what extent such alternatives provide the same properties as Diffie-Hellman.

Asymptotically Tight Lower Bounds in Anonymous Broadcast Encryption and Authentication

Hirokazu Kobayashi[1], Yohei Watanabe[2], and Junji Shikata[1]
Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama,Kanagawa, 240-8501, Japan
The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan, kobayashi-hirokazu-dr@ynu.jp, watanabe@uec.ac.jp, shikata-junji-rb@ynu.ac.jp

Abstract. Broadcast Encryption (BE) is a cryptosystem that allows a sender to specify recipients so that only the specified recipients can perform decryption. Anonymity, which is one of additional but important security requirements of BE, guarantees that no information of the designated recipients is leaked from ciphertexts, and several BE schemes with anonymity (ANO-BE) have been proposed so far.

Kiayias and Samari (IH 2013) analyzed a lower bound on the ciphertext size required for ANO-BE. In their analysis, they derived the lower bound under the assumption that ANO-BE schemes meets a special property. However, it is unclear whether the special property holds for existing ANO-BE schemes. In other words, their analysis is insufficient to show that the existing ANO-BE schemes achieve the optimal ciphertext size. In this paper, we derive a lower bound on the ciphertext size in ANO-BE, assuming only properties that most existing ANO-BE schemes satisfy. In our analysis, we newly define several properties abstracted from existing (even non-anonymous) BE schemes and carefully analyze them to replace the Kiayias–Samari assumption with ours. As a result, we show that the existing ANO-BE schemes achieve the optimal ciphertext size. We further show that our analysis can be extended to the authentication setting. Specifically, we first derive a lower bound on the authenticator size required for anonymous broadcast authentication.

Keywords: Broadcast Encryption • Anonymity • Lower Bound

Attacks on a Privacy-Preserving Publish-Subscribe System and a Ride-Hailing Service

Srinivas Vivek
IIIT Bangalore, IN srinivas.vivek@iiitb.ac.in

Abstract. A privacy-preserving Context-Aware Publish-Subscribe System (CA-PSS) enables an intermediary (broker) to match the content from a publisher and the subscription by a subscriber based on the current context while preserving confidentiality of the subscriptions and notifications. While a privacy-preserving Ride-Hailing Service (RHS) enables an intermediary (service provider) to match a ride request with a taxi driver in a privacy-friendly manner. In this work, we attack a privacy-preserving CA-PSS proposed by Nabeel et al. (2013), where we show that any entity in the system including the broker can learn the confidential subscriptions of the subscribers. We also attack a privacy preserving RHS called lpRide proposed by Yu et al. (2019), where we show that any rider/driver can efficiently recover the secret keys of all other riders and drivers. Also, we show that any rider/driver will be able to learn the location of any rider. The attacks are based on our cryptanalysis of the modified Paillier cryptosystem proposed by Nabeel et al. that forms a building block for both the above protocols.

How to Find Ternary LWE Keys Using Locality Sensitive Hashing

Elena Kirshanova[1,2] ? and Alexander May[1] *

[1] Horst Go¨rtz Institute for IT-Security, Ruhr University Bochum

[2] Immanuel Kant Baltic Federal University, Kaliningrad, Russia elena.kirshanova, alex.may{@rub.de}

Abstract. Let $As = b+e \bmod q$ be an LWE-instance with ternary keys $s,e \in \{0,\pm 1\}^n$. Let s be taken from a search space of size S. A standard Meet-in-the-Middle attack recovers s in time $S^{0.5}$. Using the representation technique, a recent improvement of May shows that this can be lowered to approximately $S^{0.25}$ by guessing a sub-linear number of $\Theta(\frac{n}{\log n})$coordinates from e. While guessing such an amount of e can asymptotically be neglected, for concrete instantiations of e.g. NTRU, BLISS or GLP the additional cost of guessing leads to complexities around $S^{0.3}$.

We introduce a locality sensitive hashing (LSH) technique based on Odlyzko's work that avoids any guessing of e's coordinates. This LSH technique involves a comparably small cost such that we can significantly improve on previous results, pushing complexities towards the asymptotic bound $S^{0.25}$. Concretely, using LSH we lower the MitM complexity estimates for the currently suggested NTRU and NTRU Prime instantiations by a factor in the range $2^{20}-2^{49}$, and for BLISS and GLP parameters by a factor in the range $2^{18}-2^{41}$.

Keywords: Ternary LWE, Combinatorial attack, Representations, LSH. Supported by the Ministry of Science and Higher Education of the Russian Federation (agreement no. 075-02-2021-1748) and the ”Young Russian Mathematics” grant.

Structural properties of self-dual monomial codes with application to code-based cryptography

Vlad-Florin Drˇagoi1,2[0000−0002−8673−9097] and Andreea Szocs1[0000−0002−4308−8810]
[1] Aurel Vlaicu University of Arad, Romania, {vlad.dragoi,andreea.szocs}@uav.com
[3] LITIS, University of Rouen, Normandie, France
[4]

Abstract. This article focuses on the self-dual monomial codes that have an underlying structure of decreasing/weakly decreasing monomial codes. Having such a property permits an in-depth analysis of their structure: The permutation group of a subclass is (significantly) bigger than the affine group. Upon looking at higher powers of the code, we see that its third power is the entire space, but the dual of the square code gives information helpful for decoding. Using operations such as shortening, puncturing and taking the discrete derivative, we extract the subcode generated by the multiples of a certain variable. Recently, self-dual monomial codes have been proposed for a McEliece public key encryption scheme. They seem to possess strong security features - they have a large permutation group, they are self-dual, there are exponentially many of them by counting the possible monomial bases used in their construction. A more detailed analysis allows us to identify subclasses where the square code and shortening methods yield non-trivial results; in these cases, the security is dominated by the complexity of the Information Set Decoding, which is exponential in the square root of the length of the code. This is a solid argument for the security of the McEliece variant based on self-dual monomial codes.

Keywords: Monomial code • Self-dual code • Schur product • McEliece cryptosystem • Reed-Muller code.

Optimizing Registration Based Encryption

Kelong Cong[1], Karim Eldefrawy[2], and Nigel P. Smart[1,3]

[1]

imec-COSIC, KU Leuven, Leuven, Belgium.
SRI International, Menlo Park, California, USA.
Dept. Computer Science, University of Bristol, Bristol, UK.
kelong.cong@esat.kuleuven.be karim.eldefrawy@sri.com nigel.smart@kuleuven.be

Abstract. The recent work of Garg et al. from TCC'18 introduced the notion of registration based encryption (RBE). The principal motivation behind RBE is to address the key escrow issue of identity based encryption (IBE), where an IBE authority is trusted to generate private keys for all users in the system. Although RBE has excellent asymptotic properties, it is currently impractical; in our estimate, ciphertext size would be about 11 terabytes in an RBE deployment supporting 2 billion users. Motivated by this observation, our work attempts to reduce the concrete communication and computation cost of the current state-of-the-art construction. Our contribution is two-fold. First, we replace the usage of Merkle trees in RBE with crit-bit trees, a form of PATRICIA trie, without relaxing any of the original efficiency requirements introduced by Garg et al. This change reduces the ciphertext size by 15% and the computation cost of decryption by 30%. Second, we observe that increasing RBE's public parameters by a few hundred kilobytes could reduce the ciphertext size by an additional 50%. Overall, our work decreases the ciphertext size by 57.5%.

When HEAAN Meets FV: a New Somewhat Homomorphic Encryption with Reduced Memory Overhead

Hao Chen[1], Ilia Iliashenko[2], and Kim Laine[3]

[1] Facebook, Cambridge, USA sxxach@gmail.com

[2] imec-COSIC, Dept. Electrical Engineering, KU Leuven, Belgium ilia@esat.kuleuven.be

[3] Microsoft Research, Redmond, USA kim.laine@microsoft.com

Abstract. We demonstrate how to reduce the memory overhead of somewhat homomorphic encryption (SHE) while computing on numerical data. We design a hybrid SHE scheme that exploits the packing algorithm of the HEAAN scheme and the variant of the FV scheme by Bootland et al. The ciphertext size of the resulting scheme is 3-18 times smaller than in HEAAN to compute polynomial functions of depth 4 while packing a small number of data values. Furthermore, our scheme has smaller ciphertexts even with larger packing capacities (256-2048 values).

Secure Multiparty Computation in the Bounded Storage Model

Jiahui Liu* and Satyanarayana Vusirikala*

* The University of Texas at Austin jiahui@cs.utexas.edu, satya.vus@gmail.com

Abstract. Most cryptography is based on assumptions such as factoring and discrete log, which assume an adversary has bounded computational power. With the recent development in quantum computing as well as concern with everlasting security, there is an interest in coming up with information-theoretic constructions in the bounded storage model.

In this model, an adversary is computationally unbounded but has limited space. Past works have constructed schemes such as key exchange and bit commitment in this model. In this work, we expand the functionalities further by building a semi-honest MPC protocol in the bounded storage model. We use the hardness of the parity learning problem (recently shown by Ran Raz (FOCS ’16) without any cryptographic assumptions) to prove the security of our construction, following the work by Guan and Zhandry (EUROCRYPT ’19).