ISSN 2186-7437

NII Shonan Meeting Report

No. 195

Workshop on Encrypted Computation / Enhancing Functionality in Cryptography

Ryo Nishimaki
Hoeteck Wee

October 21–25, 2024

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

Workshop on Encrypted Computation / Enhancing Functionality in Cryptography

Organizers:
Ryo Nishimaki (NTT Social Informatics Laboratories, Japan)
Hoeteck Wee (NTT Research, USA)

October 21–25, 2024

Background and introduction

Recent computing and technological advances such as the ubiquity of high-speed network access and the proliferation of mobile devices have had a profound impact on our society, our lives and our behavior. In the past decade, we have seen a substantial shift towards a digital and paperless society, where individuals generate huge amounts of sensitive data: financial, medical records as well as personal information exchanged over email and social networks.

In this workshop, we will explore the latest advances in cryptography that allow individuals and organizations to share and collaboratively compute on these sensitive data while preserving the privacy of the data to the largest extent possible. The workshop covers two main topics:

- Computing on encrypted data and programs: from attribute-based and functional encryption to software obfuscation
- Secure multi-party computation: fully homomorphic encryption, function secret-sharing, pseudorandom correlation generators

Topic 1. Attribute-based and functional encryption is an emerging paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud. Together, they enable searches on encrypted travel records and surveillance video as well as medical studies on encrypted medical records in a privacy-preserving manner; we can give out restricted secret keys that reveal only the outcome of specific searches and tests. These mechanisms allow us to maintain public safety without compromising on civil liberties, and to facilitate medical breakthroughs without compromising on individual privacy. The workshop will cover 3 related notions: (i) attribute-based encryption (ABE), which enables fine-grained access control to encrypted data, so that only individuals satisfying a certain policy can decrypt and access the data, (ii) functional encryption, which enables selective computation on encrypted data, where a secret key enables a user to learn a specific function of the encrypted data and nothing else, and (iii) program obfuscation, where we make the leap from encrypting data to encryption software programs.

Topic 2. In secure multi-party computation, a group of mutually distrusting parties wants to compute a function defined jointly over their respective private inputs, while preserving privacy of the data to the largest extent possible. Research in this area started in the 1980s mostly as a question of theoretical interest. However, in the past decade, we have seen increased deployment of secure multi-party computation. One example is collaboration amongst different business entities performing joint computation on private data, e.g. between Google and payment processing companies to measure ad clicks-to-sales conversion rates. Another is cryptographic operations on cryptographic keys distributed across multiple devices to prevent a single point of failure. A third is manufacturers of hardware devices and software applications collecting aggregate statistics about how their products perform in practice.

Secure multi-party computation has grown into a very broad area of research within cryptography, and in the workshop, we will focus on three new

tools developed in the context of secure computation: (i) fully homomorphic encryption, which allows us to compute on encrypted data without knowing a key, (ii) function secret sharing, which allows two servers to carry out private computation with very small communication overhead, and (iii) pseudorandom correlation generators, a new technique for speeding up secure computation with a fast pre-processing phase.

Common Themes. In the past few years, we have seen tremendous research progress on both of these topics, as well as substantial interest in the industry (including Google, NTT as well as several start-ups) in deploying many of these new cryptographic technologies. There is also significant overlap and synergy between the two topics at the technical and conceptual level, including the use of lattice-based cryptography as well as homomorphic computation over matrices (most notably, a duality between attribute-based encryption and fully homomorphic encryption), garbling techniques as well as compressing computation to achieve sublinear communication.

Overview of the meeting

The NII Shonan Meeting "Workshop on Encrypted Computation / Enhancing Functionality in Cryptography" took place in Shonan, Japan from October 21 - 25, 2024. The workshop was organized by Ryo Nishimaki (NTT Social Informatics Laboratories, Japan) and Hoeteck Wee (NTT Research, USA). The focus of the workshop was: (i) Computing on encrypted data and programs, and (ii) Secure multi-party computation.

We hosted 26 participants from all over the world: 11 from North America, 5 from Europe and Israel, and 10 from Asia. There was a good mix of representation from both academia as well as industry research labs (e.g., NTT and PQShield). The participants comprised established researchers in cryptography, promising young researchers, as well as leading researchers for the two topics.

There were 16 talks altogether, including two invited talks, one by Henry Corrigan-Gibbs (MIT) on private information retrieval, and another by Shuichi Hirahara (NII) on meta-complexity and cryptography. We also allocated time for free discussions on each day of the workshop. We had the traditional seminar outing on the third day of the workshop, where we visited the Jomyoji and Hokokuji temples, and attended a traditional Japanese tea ceremony.

Overview of Talks

New Techniques for Preimage Sampling: Improved NIZKs and More from LWE

David Wu, UT Austin

Recent constructions of vector commitments and non-interactive zero-knowledge (NIZK) proofs from LWE implicitly solve a shifted multi-preimage sampling problem. We introduce the shifted multi-preimage sampling problem and then show how recent lattice-based constructions of vector commitments and hidden-bits model NIZKs can be viewed from the perspective of designing a solution to the shifted multi-preimage sampling problem. We then describe a new technique for solving the shifted multi-preimage sampling problem by deriving a structured matrix with a public trapdoor from a short random string.

These techniques immediately yield the following improvements to lattice-based vector commitments and hidden-bits model NIZKs:

- We provide a dual-mode instantiation of the hidden-bits model (and by correspondence, a dual-mode NIZK proof for NP) with (1) a linear-size common reference string (CRS); (2) a transparent setup in hiding mode (which yields statistical NIZK arguments); and (3) hardness from LWE with a polynomial modulus-to-noise ratio. This improves upon the work of Waters (STOC 2024) which required a quadratic-size structured reference string (in both modes) and LWE with a super-polynomial modulus-to-noise ratio.
- We give a statistically-hiding vector commitment with transparent setup and polylogarithmic-size CRS, commitments, and openings from SIS. This simultaneously improves upon the vector commitment schemes of de Castro and Peikert (EUROCRYPT 2023) as well as Wee and Wu (EUROCRYPT 2023).

What you can do for PIR and what PIR can do for you

Henry Corrigan-Gibbs, MIT

This talk surveys recent developments in private information retrieval (PIR). We sketch the fundamental PIR protocols along with recent work aimed at improving their concrete efficiency. In addition, we discuss a few exciting potential applications of PIR to real-world systems. We conclude with a discussion of open problems and directions for future work.

Multi-Authority Functional Encryption with Bounded Collusions from Standard Assumptions

Rishab Goyal, University of Wisconsin-Madison

Multi-Authority Functional Encryption [Chase, TCC'07; Lewko-Waters, Eurocrypt'11; Brakerski et al., ITCS'17] is a popular generalization of functional encryption with the central goal of decentralizing the trust assumption from

a single central trusted key authority to a group of multiple, *independent and non-interacting*, key authorities. Over the last several decades, we have seen tremendous advances in new designs and constructions for FE supporting different function classes, from a variety of assumptions and with varying levels of security. Unfortunately, the same has not been replicated in the multi-authority setting. The current scope of MMAFE designs is rather limited, with positive results only known for certain attribute-based functionalities or from general-purpose code obfuscation. This state-of-the-art in MAFE could be explained in part by the implication provided by Brakerski et al. (ITCS'17). It was shown that a general-purpose obfuscation scheme can be designed from any MAFE scheme for circuits, even if the MAFE scheme is secure only in a bounded-collusion model, where at most *two* keys per authority get corrupted.

In this work, we revisit the problem of MAFE, and show that existing implication from MAFE to obfuscation is not tight. We provide new methods to design MAFE for circuits from simple and minimal cryptographic assumptions.

Unclonable Puncturable Obfuscation: A Master Tool for Unclonable Cryptography

Prabhanjan Ananth, UC Santa Barbara

We explore a new pathway to designing unclonable cryptographic primitives. We propose a new notion called unclonable puncturable obfuscation (UPO) and study its implications for unclonable cryptography. Using UPO, we present modular (and in some cases, arguably, simple) constructions of many primitives in unclonable cryptography, including, public-key quantum money, quantum copy-protection for many classes of functionalities, unclonable encryption, and single-decryption encryption.

Notably, we obtain the following new results assuming the existence of UPO:

- We show that any cryptographic functionality can be copy-protected as long as this functionality satisfies a notion of security, which we term as puncturable security. Prior feasibility results focused on copy-protecting specific cryptographic functionalities.
- We show that copy-protection exists for any class of evasive functions as long as the associated distribution satisfies a preimage-sampleability condition. Prior works demonstrated copy-protection for point functions, which follows as a special case of our result.
- We show that unclonable encryption exists in the plain model. Prior works demonstrated feasibility results in the quantum random oracle model.

We put forward a candidate construction of UPO and prove two notions of security, each based on the existence of (post-quantum) sub-exponentially secure indistinguishability obfuscation and one-way functions, the quantum hardness of learning with errors, and a new conjecture called simultaneous inner product conjecture.

Simultaneous-Message and Succinct Secret Secure Computation

Akshayaram Srinivasan, University of Toronto

Consider the following scenario: Alice has a large private input X, Bob holds a small private input y, and Charlie wants to learn the output $f(X, y)$ of some public function f evaluated over the inputs of Alice and Bob. To achieve this with optimal communication cost, Bob can simply send his input to Alice, who then computes the output $f(X, y)$, and sends it to Charlie. This simple, but clearly insecure protocol achieves the following communication complexity:

1. The communication between Alice and Bob is simply $|y|$, and in particular, independent of the length of Alice's input as well as the function output.
2. The total communication received by Charlie is simply the length of the function output (and otherwise, independent of Alice and Bob's input lengths).

Furthermore, this protocol requires only a single message from Bob to Alice, and then from Alice to Charlie. Is it possible to design a secure computation protocol that preserves—to the extent possible—the communication complexity and the communication pattern of the above insecure protocol? We give positive answer to this question under standard cryptographic assumptions.

Circuit ABE with poly(depth, λ)-sized Ciphertexts and Keys from Lattices

Hoeteck Wee, NTT Research

We present new lattice-based attribute-based encryption (ABE) and laconic function evaluation (LFE) schemes for circuits with *sublinear* ciphertext overhead. For depth d circuits over ℓ-bit inputs, we obtain

- an ABE with ciphertext and secret key size $O(1)$;
- a LFE with ciphertext size $\ell + O(1)$ and digest size $O(1)$;
- an ABE with public key and ciphertext size $O(\ell^{2/3})$ and secret key size $O(1)$,

where $O(\cdot)$ hides $\mathrm{poly}(d, \lambda)$ factors. The first two results achieve almost optimal ciphertext and secret key / digest sizes, up to the $\mathrm{poly}(d)$ dependencies. The security of our schemes relies on ℓ-succinct LWE, a falsifiable assumption which is implied by evasive LWE. At the core of our results is a new technique for compressing LWE samples $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G})$ as well as the matrix $\mathbf{A}$.

Rate-1 Registration-Based Encryption & Laconic OT

Nico Döttling, CISPA

We study the communication complexity of registration-based encryption (RBE) and laconic oblivious transfer (OT) in the batch setting. We obtain the following results:

- A rate-1 batch-RBE in which a ciphertext encrypting k 1-bit messages to k different receivers has size $k + \mathrm{poly}(\lambda)$.
- A rate-1 laconic OT for which the total communication complexity is $2k + \mathrm{poly}(\lambda)$ for k executions of the protocol.

Both of our schemes are proven secure under standard assumptions on bilinear groups.

Fully Homomorphic Computation in Attribute-based Encryption, Reusable Garbling, and Laconic Function Evaluation

Rachel Lin, University of Washington

Although we have known about fully homomorphic encryption (FHE) from circular security assumptions for over a decade [Gentry, STOC '09; Brakerski–Vaikuntanathan, FOCS '11], there is still a significant gap in understanding related homomorphic primitives supporting all *unrestricted* polynomial-size computations. One prominent example is attribute-based encryption (ABE). The state-of-the-art constructions, relying on the hardness of learning with errors (LWE) [Gorbunov–Vaikuntanathan–Wee, STOC '13; Boneh et al., Eurocrypt '14], only accommodate circuits up to a *predetermined* depth, akin to leveled homomorphic encryption. In addition, their components (master public key, secret keys, and ciphertexts) have sizes polynomial in the maximum circuit depth. Even in the simpler setting where a single key is published (or a single circuit is involved), the depth dependency persists, showing up in constructions of 1-key ABE and related primitives, including laconic function evaluation (LFE), 1-key functional encryption (FE), and reusable garbling schemes. So far, the only approach of eliminating depth dependency relies on indistinguishability obfuscation. An interesting question that has remained open for over a decade is whether the circular security assumptions enabling FHE can similarly benefit ABE.

In this work, we introduce new lattice-based techniques to overcome the depth-dependency limitations:

- Relying on a circular security assumption, we construct LFE, 1-key FE, 1-key ABE, and reusable garbling schemes capable of evaluating circuits of unbounded depth and size.
- Based on the *evasive circular* LWE assumption, a stronger variant of the recently proposed *evasive* LWE assumption [Wee, Eurocrypt '22; Tsabary, Crypto '22], we construct a full-fledged ABE scheme for circuits of unbounded depth and size.

Our LFE, 1-key FE, and reusable garbling schemes achieve optimal succinctness (up to polynomial factors in the security parameter). Their ciphertexts and input encodings have sizes linear in the input length, while function digest, secret keys, and garbled circuits have constant sizes independent of circuit parameters (for Boolean outputs). In fact, this gives the first constant-size garbled circuits without relying on indistinguishability obfuscation. Our ABE schemes offer short components, with master public key and ciphertext sizes linear in the attribute length and secret key being constant-size.

Ciphertext-Simulatable HE: Theory and Construction

Yongsoo Song, Seoul National University

Homomorphic Encryption (HE) enables the evaluation of arbitrary circuits over encrypted data. One of its most prominent use cases is the construction of secure Two-Party Computation (2PC) protocols. However, one cannot directly build 2PC over HE, as the usual IND-CPA security of HE does not generally imply the simulation-based security of 2PC. Traditional solutions for ensuring the security of 2PC have relied on HE schemes with circuit privacy, which are either computationally intensive or require exponential parameter overhead.

In this work, we introduce a novel security notion called ciphertext simulatability, which precisely captures the security requirements of HE in the context of 2PC construction. We then present a randomized evaluation algorithm for BFV, transforming the standard BFV scheme to achieve ciphertext simulatability. Unlike existing solutions, our BFV variant has insignificant overhead in terms of parameter size and error growth.

Tutorial on Meta-Complexity and Cryptography

Shuichi Hirahara, NII

Meta-complexity refers to the computational complexity of problems that ask for complexity. A canonical example of meta-computational problems is the problem of computing the time-bounded Kolmogorov complexity of a given string. In the past few years, there have been a flurry of new characterizations of the existence of a one-way function using the notion of meta-complexity. These results give us hope that a deeper understanding of meta-complexity might help resolve long-standing open questions, such as excluding Pessiland from Impagliazzo's five worlds. This talk consists of three parts. In the first part of the talk, I present an overview of meta-complexity. I survey an approach towards eliminating Heuristica, i.e., basing the average-case hardness of NP on the worst-case hardness of NP, as well as Pessiland. In the second part of the talk, I present an exposition of the characterizations of the existence of one-way functions by the hardness of meta-computational problems, based on the paper of Hirahara and Nanashima (FOCS'23). I present a complete proof of the fundamental "Proposition 1" of Impagliazzo and Levin (FOCS'90), which contains many important ideas that underlie the recent characterizations of one-way functions. In the last part of the talk, I present the characterization of the existence of a one-way function by the worst-case complexities of zero knowledge, which is based on the joint work with Mikito Nanashima (STOC'24).

FSS for Branching Programs from PRGs with Encoded-Output Homomorphism

Lisa Kohl, CWI

Function secret sharing (FSS) for a class F allows to split a secret function $f \in F$ into (succinct) secret shares f_0, f_1, such that for all $x \in \{0,1\}^n$ it holds $f_0(x) - f_1(x) = f(x)$. FSS has numerous applications, including private database queries, nearest neighbour search, private heavy hitters and secure computation in the preprocessing model, where the supported class translates to richness in the application. Unfortunately, concretely efficient FSS constructions are only known for very limited function classes.

In this work we introduce the notion of pseudorandom generators with encoded-output homomorphism (EOH-PRGs), and give direct FSS constructions for bit-fixing predicates, branching programs and more based on this primitive. Further, we give constructions of FSS for deterministic finite automatas (DFAs) from a KDM secure variant of EOH-PRGs.

- New abstractions. Following the work of Alamati et al.(EUROCRYPT '19), who classify minicrypt primitives with algebraic structure and their applications, we capture the essence of our FSS constructions in the notion of EOH-PRG, paving the road towards future efficiency improvements via new instantiations of this primitive. The abstraction of EOH-PRG and its instantiations may be of independent interest, as it is an approximate substitution of an ideal homomorphic PRG.

- Better efficiency. We show that EOH-PRGs can be instantiated from LWE and a small-exponent variant of the DCR assumption. A theoretical analysis of our instantiations suggest efficiency improvements over the state of the art both in terms of key size and evaluation time: We show that our FSS instantiations lead to smaller key sizes, improving over previous constructions by a factor of and more. While for bit-fixing predicates our FSS constructions show comparable or mildly improved run time (depending on the instantiation), we achieve considerable improvements for branching programs by avoiding the expensive generic transformation via universal circuits, shaving off a factor of and more in the number of abstract operations, where corresponds to an upper bound on the width of the underlying class of branching programs.

- New constructions. We show that our instantiations of EOH-PRGs additionally support a form of KDM-security, without requiring an additional circular-security assumption. Based on this, we give the first FSS construction for DFAs which supports the evaluation of inputs of a-priori unbounded length without relying on FHE.

- Applications. We outline applications of our FSS constructions including pattern matching with wild cards, image matching, nearest neighbor search and regular expression matching.

Sparse LPN is as hard as LPN

Vinod Vaikuntanathan, MIT

We show that the sparse LPN (resp. sparse LWE) problem is as hard as the standard, dense, LPN (resp. LWE) probem. This talk is based on joint work with Kiril Bangachev, Guy Bresler and Stefan Tiegel.

Obfuscation of Quantum Computation

James Bartusek, New York University

This work presents a construction of quantum state obfuscation, a powerful notion formalized recently by Coladangelo and Gunn in their pursuit of better software copy-protection schemes. Quantum state obfuscation refers to the task of compiling a quantum program, consisting of a quantum circuit C with a classical description and an auxiliary quantum state ψ, into a functionally-equivalent obfuscated quantum program that hides as much as possible about C and ψ. Our obfuscator is proven secure when applied to any pseudo-deterministic quantum program, i.e. one that computes a (nearly) deterministic classical input / classical output functionality, and the proof is with respect to an efficient classical oracle, which may be heuristically instantiated using quantum-secure indistinguishability obfuscation for classical circuits. In particular, this yields the first candidate realization of a "best-possible" copy-protection scheme for all polynomial-time functionalities.

New Applications of Evasive LWE

Shweta Agrawal, IIT Madras

We provide the first construction of compact Functional Encryption (FE) for pseudorandom functionalities from the evasive LWE and LWE assumptions. Intuitively, a pseudorandom functionality means that the output of the circuit is indistinguishable from uniform for every input seen by the adversary. This yields the first compact FE for a nontrivial class of functions which does not rely on pairings. We demonstrate the power of our new tool by using it to achieve optimal parameters for both key-policy and ciphertext-policy Attribute Based Encryption (ABE) schemes for circuits of unbounded depth, from just the LWE and evasive LWE assumptions. This improves prior work along the twin axes of assumptions and performance. In more detail, this allows to: (i) replace the assumption of circular evasive LWE used in the work of Hseih, Lin and Luo (FOCS 2023) by plain evasive LWE, (ii) remove the need for the circular tensor LWE assumption in the work of Agrawal, Kumari and Yamada (CRYPTO, 2024), (iii) improve parameters obtained by both aforementioned works to achieve asymptotic optimality.

Attribute-Based Signatures for Circuits with Optimal Parameter Size from Standard Assumptions

Shota Yamada, AIST

Attribute-based signatures (ABS) allow users to simultaneously sign mes-

sages and prove their possession of some attributes while hiding the attributes and revealing only the fact that they satisfy a public policy. In this paper, we propose a generic construction of ABS for circuits of unbounded depth and size, with optimal parameter size—meaning the lengths of public parameters, keys, and signatures are all constant. Our construction can be instantiated from various standard assumptions, including LWE and DLIN. This substantially improves the state-of-the-art ABS scheme by Boyle, Goldwasser, and Ivan (PKC 2014), which, while achieving optimal parameter size, relies on succinct non-interactive arguments of knowledge that can only be constructed from non-standard assumptions. Our generic construction is based on RAM delegations. At a high level, we leverage the fact that the circuit associated with the signature can be made public and compress it using the power of RAM delegation. This allows us to achieve an overall optimal parameter size while simultaneously hiding the user's policy.

Lova: Lattice-Based Folding Scheme from Unstructured Lattices

Ngoc Khanh Nguyen, King's College London

Folding schemes (Kothapalli et al., CRYPTO 2022) are a conceptually simple, yet powerful cryptographic primitive that can be used as a building block to realise incrementally verifiable computation (IVC) with low recursive overhead without general-purpose non-interactive succinct arguments of knowledge (SNARK). Most folding schemes known rely on the hardness of the discrete logarithm problem, and thus are both not quantum-resistant and operate over large prime fields. Existing post-quantum folding schemes (Boneh, Chen, ePrint 2024/257) based on lattice assumptions instead are secure under structured lattice assumptions, such as the Module Short Integer Solution Assumption (MSIS), which also binds them to relatively complex arithmetic. In contrast, we construct Lova, the first folding scheme whose security relies on the (unstructured) SIS assumption. At the core of our results lies a new exact Euclidean norm proof which might be of independent interest.

List of Participants

- Shweta Agrawal, IIT Madras, India
- Prabhanjan Ananth, UCSB, USA
- James Bartusek, NYU, USA
- Kai-Min Chung, Academia Sinica, Taiwan
- Henry Corrigan-Gibbs, MIT, USA
- Nico Döttling, CISPA Helmholtz Center, Germany
- Rishab Goyal, University of Wisconsin-Madison, USA
- Shuichi Hirahara, NII, Japan
- Yuval Ishai, Techion, Israel
- Shuichi Katsumata, PQShield, AIST, Japan
- Dakshita Khurana, University of Illinois Urbana-Champaign, NTT Research, USA
- Fuyuki Kitagawa, NTT Social Informatics Laboratories, Japan
- Lisa Kohl, CWI Amsterdam, Netherlands
- Venkata Koppula, IIT Delhi, India
- Huijia (Rachel) Lin, University of Washington, USA
- Giulio Malavolta, Bocconi University, Italy
- Ngoc Khanh Nguyen, King's College London, UK
- Ryo Nishimaki, NTT Social Informatics Laboratories, Japan
- Amit Sahai, UCLA, USA
- Akshayaram Srinivasan, University of Toronto, Canada
- Yongsoo Song, Seoul National University, Korea
- Vinod Vaikuntanathan, MIT, USA
- Hoeteck Wee, NTT Research, USA
- David Wu, UT Austin, USA
- Shota Yamada, AIST, Japan
- Takashi Yamakawa, NTT Social Informatics Laboratories, Japan

Program of Shonan Meeting: Workshop on Encrypted Computation/Enhancing Functionality in Cryptography

	Sun, October 20	Mon, October 21	Tue, October 22	Wed, October 23	Thu, October 24	Fri, October 25
7:30 - 9:00		**Breakfast**	**Breakfast**	**Breakfast**	**Breakfast**	**Breakfast**
9:00 - 9:30						
9:30		**Welcome**	**Akshayaram Srinivasan:** *Simultaneous-Message and Succinct Secret Secure Computation*	**Shuichi Hirahara:** Tutorial on Meta-Complexity and Cryptography	**Lisa Kohl:** *FSS for Branching Programs from PRGs with Encoded-Output Homomorphism (45min)*	**Shota Yamada:** *Attribute-Based Signatures for Circuits with Optimal Parameter Size from Standard Assumptions*
		David Wu: *New Techniques for Preimage Sampling: Improved NIZKs and More from LWE*				
10:00			**Hoeteck Wee:** *Circuit ABE with poly(depth,λ)-sized ciphertexts and Keys from Lattices*			**Ngoc Khanh Nguyen:** *Lova: Lattice-Based Folding Scheme from Unstructured Lattices*
10:15					**Coffee Break**	
10:30		**Coffee Break**	**Coffee Break**	**Coffee Break**		**Coffee Break**
11:00		**Henry Corrigan-Gibbs:** *What you can do for PIR and what PIR can do for you*	**Nico Döttling:** *Rate-1 Registration-Based Encryption & Laconic OT*	**Shuichi Hirahara:** Tutorial on Meta-Complexity and Cryptography	**Vinod Vaikuntanathan:** *Sparse LPN is as hard as LPN (+ Applications) (45min)*	**Free Discussion**
11:30			**Group Photo**	**Free Discussion**		
					Free Discussion	
12:00 - 13:30		**Lunch**	**Lunch**	**Lunch**	**Lunch**	**Lunch**
13:30 - 14:15		**Rishab Goyal:** *Multi-Authority Functional Encryption with Bounded Collusions from Standard Assumptions*	**Rachel Lin:** *Fully Homomorphic Computation in Attribute-based Encryption, Reusable Garbling, and Laconic Function Evaluation*	**Excursion**	**James Bartusek:** *Obfuscation of Quantum Computation*	
14:15 - 14:45		**Coffee Break**	**Coffee Break**		**Coffee Break**	
14:45 - 15:30	Check-in (from 15:00)	**Prabhanjan Ananth:** *Unclonable Puncturable Obfuscation: A Master Tool for Unclonable Cryptography*	**Yongsoo Song:** *Ciphertext-Simulatable HE: Theory and Construction (30 min)*		**Shweta Agrawal:** *New Applications of Evasive LWE*	
15:30 - 18:00		**Free Discussion**	**Free Discussion**		**Free Discussion**	
18:00		**Dinner**	**Dinner**	**Main Banquet**	**Dinner**	
19:00	**Welcome Banquet**					
19:30			**Research Party @Research Wing Lounge**		**Research Party @Research Wing Lounge**	
21:00						

Summary of discussions, new findings, and future directions

Attribute-based and functional encryption. Rachel Lin, Shweta Agrawal, and Hoeteck Wee presented new constructions of attribute-based encryption (ABE) schemes for circuits from lattice assumptions; these schemes achieve a range of different trade-offs between parameter sizes and assumptions. Rishab Goyal presented new multi-authority functional encryption with bounded collusions from standard assumptions. These talks led to discussions on the following future research directions:

- Improve the assumptions for the state-of-the-art ABE for circuits, either to falsifiable lattice assumptions, or to public-coin evasive LWE.
- Construct multi-authority ABE for circuits from lattice asumptions.

Secure multi-party computation. Henry Corrigan-Gibbs surveyed recent developments in private information retrieval (PIR). Akshayaram Srinivasan presented new simultaneous-message protocols for secure computation with nearly optimal communication complexity. Yongsoo Song presented new security notions for (fully) homomorphic encryption along with new instantations based on the BFV scheme. Lisa Kohl presented new and improved constructions of functional secret sharing (FSS) schemes for branching programs based on a new abstraction: pseudorandom generators with encoded-output homomorphism. These talks led to discussions on the following future research directions:

- Construct practical doubly-efficient PIR. As an intermediate goal, simplify or improve the Kedlaya-Umans data structure for fast evaluation of multivariate polynomials.
- Construct simultaneous-message protocols for secure computation with additive instead of multiplicative overheads in the security parameter. Also, can we obtain protocols from assumptions different from LWE?
- Construct FSS beyond the two-party setting. The main challenge is to generalize the existing distributed rounding or distributed discrete logarithm to more than two parties.
- Construct FSS for branching programs or subclasses of AC0 (e.g. bit-fixing predicates or t-CNF) from different/weaker assumptions, notably LPN or one-way functions.

Cryptographic proof systems. David Wu presented new and improved constructions of non-interactive zero-knowledge proofs (NIZK) for NP based on LWE. Ngoc Khanh Nguyen presented new lattice-based folding schemes, which in turn yields new constructions of incrementally verifiable computation (IVC). These talks led to discussions on the following future research directions:

- Construct NIZK for NP from LWE with a transparent set-up and statistical soundness.
- Obtain a more direct and algebraic construction of NIZK for NP from LWE similar to the Groth-Ostrovsky-Sahai pairing-based schemes.

- Construct folding schemes and IVC from lattices with better concrete efficiency.
- Construct non-malleable cryptographic proof systems from lattices.

Obfuscating quantum computation. James Bartusek presented a new construction of quantum state obfuscation, which can be heuristically instantiated using quantum-secure indistinguishability obfuscation for classical circuits. Prabhanjan Ananth presented a new paradigm for designing unclonable cryptographic primitives based on a new notion called unclonable puncturable obfuscation (UPO), along with new candidates for UPO. These talks led to discussions on the following future research directions:

- Construct quantum state obfuscation without relying on ideal obfuscation for classical circuits.
- Obfuscate more general classes of circuits, such as sampling circuits.
- Do the techniques for quantum obfuscation yield new insights into a direct construction of attribute-based encryption for quantum circuits?
- Find new applications in quantum cryptography using obfuscation for quantum computation, and along the way, investigate and instantiate weaker or different security notions of quantum obfuscation.

Lattice assumptions. Vinod Vaikuntanathan presented new work showing that sparse LPN (resp. sparse LWE) is as hard as LPN (resp. LWE). Together with several earlier talks, this led to discussions on the following future research directions:

- Initiate a formal treatment of black-box use of lattices as well as a "generic adversary" for lattice assumptions, analogous to the existing notions for black-box use of cryptographic groups, as well as the generic group model of Maurer and Shoup.
- Explore the different notions of evasive LWE in the public-coin and private-coin setting, as well as various intermediate notions, such as circular-secure evasive LWE.

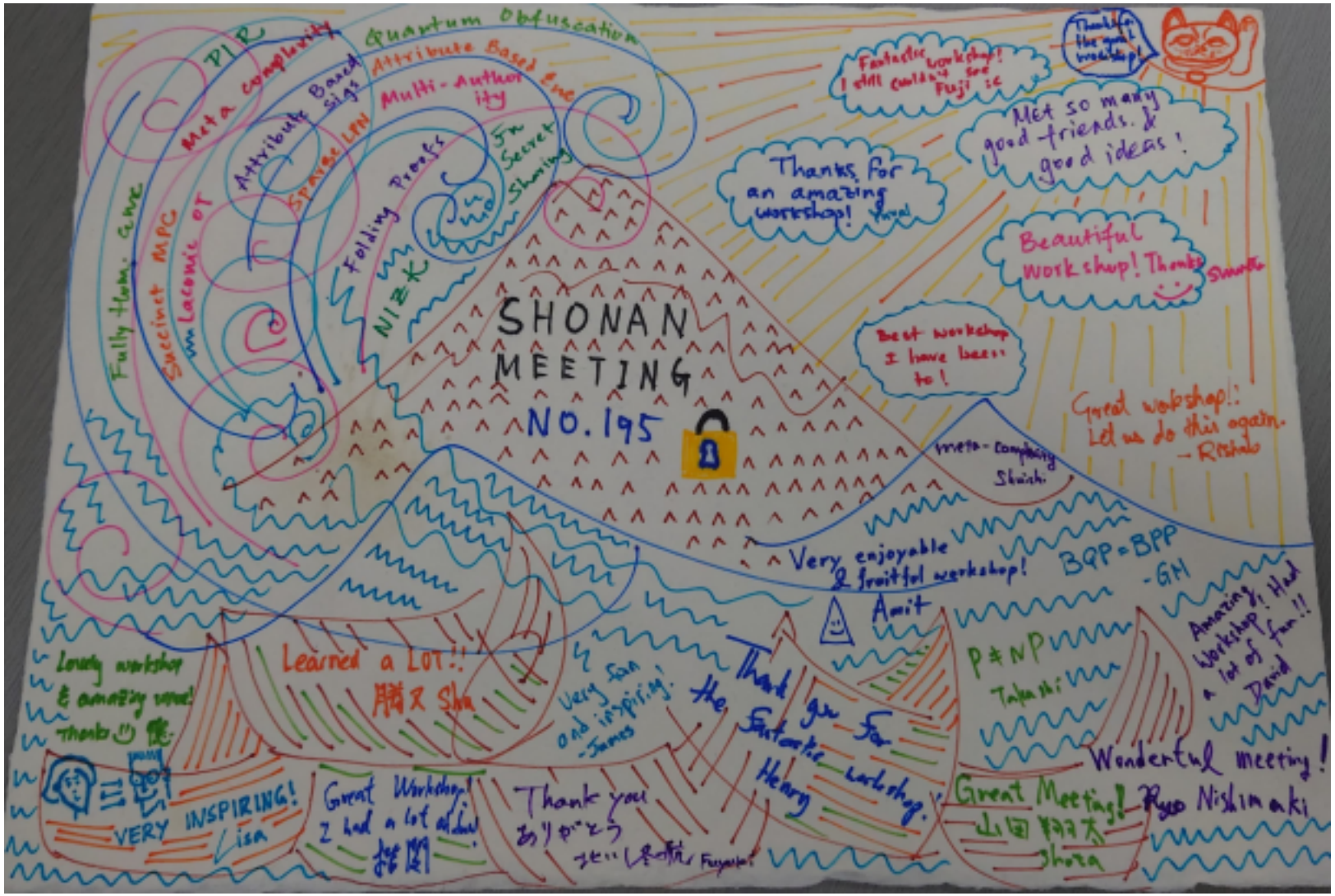
Additional presentations. Shuichi Hirahara gave an overview of meta-complexity, as well as connections between fundamental questions in cryptography (existence of one-way functions) and meta-complexity. Nico Döttling presented new pairing-based registration-based encryption (RBE) and laconic oblivious transfer (OT) in the batch setting. Shota Yamada presented optimal attribute-based signatures for circuits from standard assumptions.

Conclusion

This 4.5-day workshop brought together 26 researchers to explore the latest advances in cryptography pertaining to two main topics: (i) computing on encrypted data and programs, and (ii) secure multi-party computation. Along the way, we also touched on two exciting new themes in cryptography, namely quantum computation and meta-complexity.

In the past few years, we have seen a substantial growth in cryptographic research activities and community in Asia, as well as increased representation of Japanese and Asian cryptographers at the top cryptography publication venues; moreover, much of these activities pertain to the topics of this workshop. To the best of our knowledge, this is one of the first Oberwolfach/Dagsthul-style workshops in cryptography that has been held in Asia and pays special attention to researchers based in Asia. The overwhelming positive feedback we received from the participants indicates substantial interest and demand for more workshops of this kind.

We are extremely grateful to NII and Shonan Village Center for hosting this workshop, as well as all the attendees for their participation.


SHONAN
MEETING
NO.195
PIR
Meta complexity
Quantum Obfuscation
Attribute Based sigs
Attribute Based Enc
Multi-Authority
Succinct MPC
Laconic OT
Sparse LPN
Folding Proofs
NIZK
Fully Hom. Enc
Fantastic workshop! I still couldn't see Fuji :(
Thanks for the great workshop!
Met so many good friends & good ideas!
Thanks for an amazing workshop!
Beautiful Workshop! Thanks
Best workshop I have been to!
Great wokshop!! Let us do this again. -Rachel
Very enjoyable & fruitful workshop!
BQP=BPP
-GH
Amit
P≠NP
Takashi
Amazing! Workshop! Had a lot of fun!!
David
Wonderful meeting!
Ryo Nishimaki
Lovely workshop & amazing venue! Thanks!!
VERY INSPIRING!
Lisa
Learned a LOT!!
Very fun and inspiring!
-James
Thank you for the fantastic workshop!
Hoeteck
Great Workshop! I had a lot of fun!
Thank you
Great Meeting!
Shota