Research of Cryptography & Information Security Laboratories

Tatsuaki Okamoto, Brent Waters, and Shin'ichiro Matsuo

Abstract

One of the three laboratories of NTT Research, Inc. launched in July 2019 in Silicon Valley, USA, is Cryptography & Information Security Laboratories (CIS Labs). CIS Labs (Director: Tatsuaki Okamoto) is engaged in basic research on cryptography and has two research groups, Cryptography, and Blockchain (Head: Shin'ichiro Matsuo). The Cryptography group also includes Waters Laboratory (Head: Brent Waters), which focuses on deep and foundational research of cryptography. In this article, we describe the research targets and themes of CIS Labs.

Keywords: cryptography, information security, basic research laboratories

1. Introduction

In this article, we introduce Cryptography & Information Security Laboratories (CIS Labs), which is one of the three laboratories of NTT Research, Inc. launched in July 2019 in Silicon Valley, USA. CIS Labs is engaged in basic research of cryptography with the potential for having a long-term impact and has two research groups, Cryptography and Blockchain. The Cryptography group also includes the Waters Laboratory headed by Brent Waters, which focuses on deep and foundational research of cryptography. We discuss the research targets and themes of CIS Labs, mainly those of Waters Lab and the Blockchain group.

2. Research of Cryptography group, specifically Waters Lab

Waters Lab focuses on many areas of cryptography ranging from achieving new functionality that goes beyond what cryptographic primitives were previously achievable to achieving a better and deeper understanding of the foundations of cryptography. One initial focus area is on encryption systems. Encryption is the process of encoding data into a ciphertext such that only the intended recipient can decode and learn the data. Encryption systems are a cornerstone of our security ecosystem. They are used to encrypt sensitive web traffic, protect information on devices (e.g., laptops, phones) that could be physically stolen, as well as hide sensitive data stored on third-party cloud servers. Encryption can often end up at the forefront of news or public debates, as in the case of the 2015 San Bernardino shooting and the debate over whether Apple should be compelled to decrypt the culprit's iPhone.

Traditionally, we have had an inert view of encryption where a user publishes a public key and keeps the corresponding secret key private. One can encrypt a data message using a public key to create a ciphertext. The data message can be decrypted by any holder of the secret key, but an attacker without this will learn nothing about the data.

Over time, we have discovered that this view of encryption may be too rigid for many applications. For example, suppose Alice's email server receives and stores emails encrypted under her public key. In addition to storing emails, she would like it to automatically discard spam (something current servers do on unencrypted emails) as well as send her a text alert if any email message with her child's name and the word "emergency" or "hospital" appears in it. To enable this functionality, she could hand over her secret key to the server, but this would allow a third party to read all her email messages; however, if Alice

holds it back then she cannot benefit from spam detection or emergency alerts. This is just one example of where we need to push beyond the confines of our traditional notions of encryption to obtain a desired result.

The research community has long recognized that doing this is important and there are various concepts of cryptosystems (some proposed by the PIs) that do this including: functional encryption, fully homomorphic encryption, identity-based encryption, attribute-based encryption, traitor tracing, and proxy re-encryption among others.

Our group's research will push the frontiers of what is achievable in this regime. We will focus on building encryption systems with advanced capabilities that have provable security under standard assumptions. We begin by focusing on three sub-areas.

2.1 Chosen ciphertext security

The chosen ciphertext security (indistinguishability under chosen-ciphertext attack: IND-CCA) is arguably the right notion of security both for traditional encryption systems as well as those with advanced functionality. However, most new results that push the envelope of functionality prove security in the indistinguishability against chosen plain-text attack (IND-CPA) model. We recently showed how to generically black-box convert any attribute-based encryption system that is IND-CPA secure into an IND-CCA one using a new tool called hinting pseudorandom generators (PRGs). We will build faster and smaller hinting PRGs from number theory and go beyond attribute-based encryption and discover CCA transformations for functional encryption and re-randomizable encryption. Finally, we will approach the classic problem of proving that IND-CPA implies IND-CCA with new ideas.

2.2 Tracing in encryption systems

Traitor tracing is the problem of determining the source of a decoder box in a broadcast system. We recently showed how to build *collusion-resistant* tracing systems with ciphertexts that scale in size with $lg(N)$ for N users from the learning with errors (LWE) assumption. The previous best results from standard assumptions achieved $N^{1/2}$-sized ciphertexts. We explore challenging new problems including: obtaining trace and broadcast systems with $N^{1/c}$-sized ciphertexts for any constant c, achieving public traceability for the same parameters, and using tracing techniques for proving adaptive security.

2.3 New frontiers in LWE-based encryption

The LWE assumption is a well-regarded tool in cryptography due to its apparent resistance to quantum attacks as well as connections to worst case lattice problems. It has also turned into an exciting avenue for producing new functionality in cryptography from a well-studied assumption. Recent examples of primitives include fully homomorphic encryption, attribute-based encryption for circuits, and lockable obfuscation. None are currently realizable from any other standard number theoretic assumptions. We propose ambitious goals for building LWE-based cryptography. We first discuss a new concept of obfuscating pseudorandom functions (PRFs) and its applications. We then describe a program for constructing witness encryption from LWE beginning with an intermediate goal of building constrained PRFs for the bit-fixing functionality.

Our research lab is off to a good start in this area. Waters and Wichs (with co-authors) have a paper in CRYPTO 2019, the top conference in cryptography, that shows how to combine bilinear map broadcast encryption techniques from traitor tracing ideas from LWE to achieve trace and broadcast functionality with $N^{1/c}$-sized ciphertexts. Currently, Waters, Wichs, and Zhandry are collaborating to explore new techniques and limitations on achieving adaptive security for LWE-based attribute-based encryption systems.

3. Research of Blockchain group

After Satoshi Nakamoto published a paper on Bitcoin in 2009, blockchain technology gained a great deal of attention as a new data trust model based on cryptography, peer-to-peer (P2P) networks, game theory, economics, and other academic areas. Bitcoin is a mechanism to periodically revise a common ledger that records payment history by users who are parts of a P2P network without the existence of a trusted third party (TTP). It applies this technology to payment among users by treating the history of a record as money. Thus, Bitcoin is a system specialized as a payment application. However, the idea of updating a common ledger by users connected by a P2P network without TTP applies to a broader area than payment. Therefore, extensive research and development are being globally conducted on blockchain, the core protocol of Bitcoin, as a fundamental technology.

The most crucial keyword to understand the real impact of blockchain is *permissionless innovation*. The Internet enables multi-lateral and global

communication without a central party, providing everyone a chance to be a creator of innovation. Similarly, blockchain enables multi-lateral and global maintenance of *programmable* ledger(s) by multi-stakeholders without any permission; therefore, anyone can freely create new applications and innovations based on a shared ledger. It is not easy to answer the frequently asked question, "What is an excellent application of blockchain?" as in the case of the similar question, "What is an excellent application of the Internet?" There is currently no right answer to this question, but the real value of blockchain is that it creates a place for experiments where anyone can try to create new applications based on a programmable ledger.

In this sense, the main goal of research and development on blockchain technology is creating a situation such that anyone can freely develop an application based on a shared and programmable ledger. We might think that blockchain is *ready* technology from news on such technology; however, achieving the above goal is a considerable challenge and requires long-term fundamental and theoretical research and development.

Building blocks of blockchain technology have been confirmed and are not new. ECDSA (Elliptic Curve Digital Signature Algorithm), a digital signature algorithm used in Bitcoin and SHA-2, a cryptographic hash function, are standard cryptographic techniques with a long history. Digital time-stamping, which certifies the order of the existence of digital data by linking hash values, was proposed at CRYPTO in 1990. Sharing digital data by a large number of people via a P2P network is not new technology. There is a long history in the research of distributed computing on achieving a consensus of data by multiple networked computers. In Bitcoin, a proof of work technique is used as a secure consensus protocol, but this was invented as an example of the cryptographic puzzle to reduce spam email then established as a part of HashCash, which is hash-function-based digital money.

The real breakthrough of Bitcoin and blockchain is the capability to combine such well-confirmed technologies to develop a method of updating a ledger with certain business logic (e.g., payment) without a trusted server. Such a mechanism did not exist before Bitcoin. To make such a P2P network sustainable, Bitcoin implements an incentive mechanism that gives rewards (e.g., Bitcoins) to network participants who contribute to maintaining the network.

The security of blockchain relies not only on cryptography and network theory but also on a good incentive design. There are many trade-offs between its security and scalability. If we try to scale the blockchain technology naturally, its security degrades. Such trade-offs have not yet been theoretically clarified. Thus, we need to develop theories and conduct experiments to clarify the relationships and make blockchain technology usable to general users with satisfactory performance. This is a fundamental and long-term research issue.

Another fundamental issue of blockchain is scalability. The current Bitcoin network can process seven transactions per second worldwide. It is quite difficult to increase the number of transactions without compromising security. Top-level researchers are conducting extensive research on this issue.

The Blockchain group at CIS Labs focuses on fundamental research to achieve the goal described above. Specifically, it focuses on secure and scalable distributed consensus algorithms, a secure programming environment for the programmable ledger, and privacy protection for data processing over blockchain.

As mentioned above, theoretical research on blockchain technology is composed of different areas. Therefore, we need to form a team of top-level researchers with diverse backgrounds. Experts on cryptographic protocols, software engineering, formal verification, game theory, and economics are encouraged to join this group. Because blockchain research is in its very early stage, it is essential to gather young researchers such as post-docs and assistant professors from whom we can expect top-level research results.

Moreover, as regulators are concerned about Facebook's Libra, harmonization with future regulations is essential for making blockchain a social foundation. This harmonization should be considered by design, and we are planning joint research with a leading university in the United States on this topic.

Trademark notes

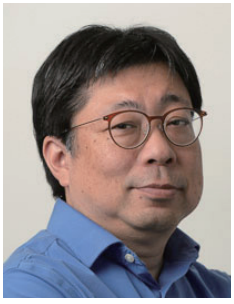
Tatsuaki Okamoto
Director, Cryptography & Information Security Laboratories, NTT Research, Inc.

He received a B.E., M.E., and Ph.D. from the University of Tokyo in 1976, 1978, and 1988. He has been working for NTT since 1978, and is an NTT Fellow. He is presently a Director of NTT Research in USA since 2019 and engaged in research on cryptography and information security. Dr. Okamoto served as President of the Japan Society for Industrial and Applied Mathematics (JSIAM), Director of International Association of Cryptology Research (IACR), and a program chair of many international conferences. Dr. Okamoto received the best and life-time achievement awards from the Institute of Electronics, Information and Communication Engineers (IEICE), the distinguished lecturer award from the IACR, the Purple Ribbon Award from the Japanese government, the RSA Conference Award, and the Asahi Prize.

Brent Waters
Distinguished Scientist, Cryptography & Information Security Laboratories, NTT Research, Inc.

Dr. Brent Waters received his Ph.D. in computer science from Princeton University, NJ, USA, in 2004. From 2004–2005, he was a postdoctoral researcher at Stanford University, CA, USA, then worked at SRI International as a computer scientist. In 2008 he joined the faculty at The University of Texas at Austin. In 2019 he joined NTT Research as a distinguished scientist. Dr. Waters' research interests are in the areas of cryptography computer security. His work has focused on identity-based cryptography, functional encryption, and code obfuscation. He is noted as a founder of functional encryption and attribute-based encryption.

Dr. Waters is a recipient of the National Science Foundation CAREER award, the Presidential Early Career Award for Scientists and Engineers (PECASE), and the 2015 ACM (Association for Computing Machinery) Grace Murray Hopper award. He has been a Microsoft Faculty Fellow, Sloan Research Fellow, a Packard Science and Engineering Fellow, and a Simons Investigator.



Shin'ichiro Matsuo
Head of Blockchain group, Cryptography & Information Security Laboratories, NTT Research, Inc.

He is the head of blockchain research at NTT Research. He is also a research professor at Georgetown University, Washington, D.C., USA, and works as a director and blockchain research lead of CyberSMART research center at Georgetown University. He has been engaged in research on cryptography and cryptographic protocols over 23 years. He was a program chair of Scaling Bitcoin workshop 2019 and program committee member of many blockchain related academic conferences such as IEEE S&B, CBT, Stanford Blockchain Conference and Crypto Economics and Security Conference. He is also a co-founder of BSafe.network, which is the global and neutral academic research testbed dedicated to blockchain research.