Research Statement

YANG Guomin
School of Computing and Information Systems, Singapore Management University
Tel: (+65) 68284928; Email: gmyang@smu.edu.sg
23 December 2023

Background

My research area is applied cryptography and its applications in computer and network security. The first research topic I investigated during my PhD was privacy protection in authentication and key exchange protocols, which are among the most important and widely used security protocols for enabling secure communications. Since such protocols use different cryptographic primitives, investigating new cryptographic primitives that can provide novel security or privacy features also naturally became my research interest. Since then, my research focus has been following this paradigm, that is developing new cryptographic primitives that can provide security and privacy features demanded by emerging computing and communications models/platforms such as cloud computing, IoT, and blockchain.

Research Areas

A. Security Protocols

Authentication and key exchange (AKE) protocol, also known as secure handshake, allows two parties to establish a common secret key over an insecure network and forms the backbone of network security. My research has contributed to the development of secure and privacy-preserving AKE protocols for different network topologies and settings.

During my PhD study, motivated by the development of the 3GPP standard at that time, I focused on designing new privacy-preserving AKE protocols for wireless and roaming networks. To support anonymous authentication, I invented a new cryptographic primitive named “Anonymous Signature” [PKC’06] that can be used to build anonymous AKE secure against active network attacks. I also identified a new attack called “deposit-case attack” that could break many standardized AKE protocols for roaming networks. Subsequently, I proposed a secure roaming protocol that can resist the attack and ensure user anonymity and untraceability [TWC’07]. In a follow-up work [TWC’10], I proposed the notion of “Universal Authentication Protocol” for wireless and roaming networks, which does not require the home server to vouch for the validity of a roaming user in a foreign network and hence greatly reduces the protocol latency. Inspired by the reset attack against Virtual Machines, I initiated the research on “Authenticated Key Exchange under Bad Randomness” [FC’11] and proposed practical methods to convert standardized protocols to be secure under bad randomness attacks. In [TISS’14], I and my co-authors developed a practical password-based AKE for protecting cross-domain communications and our solution was recently standardized by ISO/IEC as a new international standard “ISO/IEC 11770-7 (2021)”. In recent years, side-channel and key leakage attacks become a concern for the security of cryptographic primitives and protocols. My PhD student

and I developed the first leakage-resilient AKE protocol [RSA'16] that can resist both secret key and randomness leakage.

B. Secure and Private Data Communications

Standard cryptographic primitives, such as encryption and digital signature, can ensure the confidentiality and integrity of data in storage and transmission. Nevertheless, some tricky attacks can bypass the protection provided by these standard security primitives. Meanwhile, in some applications, we want to protect the identity of the data sender and/or receiver to avoid traffic analysis or inference attack. My research has contributed to the design of new cryptographic primitives that can resist non-traditional attacks and enable anonymous data communication.

- Covert Channel Sanitization

Subversion attacks can undermine standard cryptographic algorithms by creating a covert channel for secret exfiltration. These attacks cannot be addressed by conventional cryptographic approaches. To resist subversion attacks, my PhD student and I developed a generic cryptographic tool called Malleable Smooth Project Hash Function [AC'16] and used it to construct Cryptographic Reverse Firewalls to remove the covert channel created by subverted security algorithms. We demonstrated that our approach could be used to protect different types of secure communication protocol, such as secure key transport, oblivious transfer and oblivious signature based envelop. In a subsequent work [ESORICS'18], I and my co-authors also extended the technique and proposed the first Cryptographic Reverse Firewall for attribute-based cryptosystems that support fine-grained access control.

- Anonymous Communication

To achieve anonymous communication, one widely used approach is to perform rerandomizable on the encrypted data by some network node, e.g., a router. However, constructing anonymous and rerandomizable encryption secure under adaptive chosen-ciphertext attacks, a *de facto* security requirement for encryption, is a non-trivial task. In fact, it has been an open problem for the cryptography research community since 2007. In [CRYPTO'21], I and my co-authors introduced a new primitive named Rerandomizable Smooth Project Hash Function and used it to construct the first practical anonymous and rerandomizable encryption secure under chosen-ciphertext attacks, hence provided an affirmative answer to the open problem.

C. Cloud Security

Cloud computing has brought new challenges to the cryptography and cybersecurity research community, such as enabling searching, deduplication, and computation over encrypted data in cloud storage. My research has contributed to the development of new cryptographic and security solutions to address the above problems.

Searchable encryption has become a prevalent research topic due to the popularity of cloud storage. Inspired by the concept of cloud computing, in [RSA'10], I and my co-authors proposed a new probabilistic public key encryption scheme that can support equality tests over encrypted data. This new primitive is useful in performing

searching and categorization for encrypted data. Later, this technique was also found useful in constructing secure Message Locked Encryption allowing deduplication over encrypted data, which is very important for saving cloud storage while preserving data privacy. The early constructions of Message Locked Encryption only supported file-level deduplication. To enable large file deduplication, my PhD student and I developed the first block-level message-locked encryption [TIFS'15] that can perform more efficient deduplication over encrypted data at the data block level. For public key searchable encryption, a challenge problem is to thwart keyword guessing attacks by the storage server. In the literature, this problem was addressed by sacrificing searching accuracy. My PhD student and I addressed this problem using a new approach. We proposed a new primitive named Linear and Homomorphic Smooth Projective Hash Function and used this tool to construct a novel dual-server searchable encryption scheme [TIFS'16] that can resist insider keyword guessing attacks. With the prevalence of outsourced computation, such as Machine Learning as a Service, protecting the privacy of sensitive data throughout the whole computation is a critical yet challenging task. The problem becomes even more tricky when multiple sources of input and/or multiple recipients of output are involved, who would encrypt/decrypt data using different keys. To address this challenge, my PhD student and I developed a general privacy-preserving multi-user outsourced computation framework for any computation that can be represented as Boolean circuits [TIFS'23].

D. Blockchain Security and Privacy

By allowing immutable record of transactions to be stored in a distributed ledger, blockchain has been shown to be very promising in many domains such as digital currency, digital identity, supply-chain, and many other industries. In my recent works, I and my co-authors developed several new cryptographic primitives to address and the security and privacy issues in blockchain.

In [EuroS&P'19], we identified a serious security issue in the one-time address/account management mechanisms used by several major cryptocurrencies, such as the Deterministic Wallet mechanism used by Bitcoin and the Stealth Address mechanism used by Monero. These schemes cannot provide the key-insulation property. In consequence, the compromising of a single one-time account would let the attacker break the master account and all the other one-time accounts linked to the master account. To address this serious security flaw, we proposed a new and efficient key-insulated digital wallet scheme that can in addition provide anonymity for confidential transactions. In a subsequent work [ESORICS'22], motivated by the virtues of a hierarchical digital wallet in practical scenarios, such as easy backup/recovery, convenient cold-address management, and supporting trust-less audits, we extended our key-insulated digital wallet scheme and developed the first hierarchical wallet supporting stealth address, which is the state-of-the-art digital wallet mechanism covering all the desirable features.

Equivocation is one of the fundamental problems that need to be solved for distributed protocols. In the literature, non-equivocation in blockchain mainly focused on preventing double-spending of a digital coin. In [ASIACCS'21], I and my co-authors developed a new policy-based non-equivocal signature scheme that can handle equivocation with regards to a complex policy. This tool is useful in a broader range of applications such as accountable delegation of signing right and policy-based insurance for a designated beneficiary. Protecting the privacy of data recorded in the blockchain transactions is an indispensable requirement to make the technology acceptable by both end users and regulatory bodies. On the other hand, accountability must not be sacrificed in critical businesses such as financial and medical sectors. Balancing privacy and accountability is an important but challenging research problem. In [TDSC'21], my PhD student and I proposed a solution for balancing privacy and accountability in the use case of anonymous digital currency Monero. The approach can ensure user privacy while allowing authority to identity illegal transactions, such as money laundering. In a subsequent work [CRYPTO'22], I and my co-authors developed a new digital signature primitive named "Multimodal Private Signature" that generalizes the concept of traceable anonymous signature and can enable various new and appealing privacy-preserving applications.

Future Directions

- TEE-assisted data security and privacy techniques

With the tremendous growth of data volume in the digital era, off-premises (e.g., cloud) data storage is becoming a prevalent storage model. Despite the great advancements and wide adoption of cloud systems in the last two decades, concerns regarding the security and privacy of off-premises data remain, which can be evidenced by the growing cloud data breach incidents in recent years. Access control is among the most important and effective approaches to deter data breaches. Existing access control systems such as Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) are crucial for ensuring data security and privacy in the traditional enterprise systems in which servers are fully trusted to keep users' data confidential and correctly enforce access control policy. However, deploying these access control systems in the zero-trust cloud environment has been very challenging due to the assumption that the cloud infrastructure and the service providers cannot be fully trusted to keep users' data and access control information confidential and to correctly enforce access control policy. The Trusted Execution Environment (TEE) is an emerging technology to offer security and privacy in a zero-trust environment. In a recent work [SP'24], we developed a TEE-assisted solution to address the long-standing problem of user revocation in attribute-based encryption. Designing secure and practical TEE-assisted access control solutions for zero-trust environments is one of my research priorities in the future.

- Trusted Decentralized Identities

A trusted digital identity is an essential component for securely and conveniently accessing services and authorizing transactions in cyberspace. It empowers users and organizations to safely communicate and transact in an open and borderless

digital society and is a key enabler of a vibrant digital economy. Driven by the rapid and enormous development of decentralized technologies and applications, such as distributed ledgers, Web3, and decentralized finance (DeFi), there is an urging demand for decentralized digital identities, also known as self-sovereign identities, which empower end users to create, own and govern their digital identities and assets in an autonomous, reliable, and privacy-preserving manner. Developing a trusted, versatile, reliable, and user-centric decentralized identity framework is another main research area in my agenda.

Selected Publications and Outputs

[PKC'06] Guomin Yang, Duncan S. Wong, Xiaotie Deng, Huaxiong Wang: Anonymous Signature Schemes. Public Key Cryptography 2006: 347-363

[TWC'07] Guomin Yang, Duncan S. Wong, Xiaotie Deng: Anonymous and Authenticated Key Exchange for Roaming Networks. IEEE Trans. Wirel. Commun. 6(9): 3461-3472 (2007)

[RSA'10] Guomin Yang, Chik How Tan, Qiong Huang, Duncan S. Wong: Probabilistic Public Key Encryption with Equality Test. CT-RSA 2010: 119-131

[TWC'10] Guomin Yang, Qiong Huang, Duncan S. Wong, Xiaotie Deng: Universal authentication protocols for anonymous wireless communications. IEEE Trans. Wirel. Commun. 9(1): 168-174 (2010)

[FC'11] Guomin Yang, Shanshan Duan, Duncan S. Wong, Chik How Tan, Huaxiong Wang: Authenticated Key Exchange under Bad Randomness. Financial Cryptography 2011: 113-126

[TISS'14] Liqun Chen, Hoon Wei Lim, Guomin Yang: Cross-Domain Password-Based Authenticated Key Exchange Revisited. ACM Trans. Inf. Syst. Secur. 16(4): 15:1-15:32 (2014)

[TIFS'15] Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo: BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication. IEEE Trans. Inf. Forensics Secur. 10(12): 2643-2652

[TIFS'16] Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo, Xiaofen Wang: Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage. IEEE Trans. Inf. Forensics Secur. 11(4): 789-798 (2016)

[RSA'16] Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, Fuchun Guo: Strongly Leakage-Resilient Authenticated Key Exchange. CT-RSA 2016: 19-36

[AC'16] Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, Fuchun Guo, Mingwu Zhang: Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions. ASIACRYPT (1) 2016: 844-876

[ESORICS'18] Hui Ma, Rui Zhang, Guomin Yang, Zishuai Song, Shuzhou Sun, Yuting Xiao: Concessive Online/Offline Attribute Based Encryption with Cryptographic Reverse Firewalls - Secure and Efficient Fine-Grained Access Control on Corrupted Machines. ESORICS (2) 2018: 507-526

[EuroS&P'19] Zhen Liu, Guomin Yang, Duncan S. Wong, Khoa Nguyen, Huaxiong Wang: Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key. EuroS&P 2019: 215-230

[TDSC'21] Yannan Li, Guomin Yang, Willy Susilo, Yong Yu, Man Ho Au, Dongxi Liu: Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. IEEE Trans. Dependable Secur. Comput. 18(2): 679-691 (2021)

[CRYPTO'21] Yi Wang, Rongmao Chen, Guomin Yang, Xinyi Huang, Baosheng Wang, Moti Yung: Receiver-Anonymity in Rerandomizable RCCA-Secure Cryptosystems Resolved. CRYPTO (4) 2021: 270-300

[ASIACCS'21] Yannan Li, Willy Susilo, Guomin Yang, Yong Yu, Tran Viet Xuan Phuong, Dongxi Liu: Non-Equivocation in Blockchain: Double-Authentication-Preventing Signatures Gone Contractual. AsiaCCS 2021: 859-871

[ESORCIS'22] Xin Yin, Zhen Liu, Guomin Yang, Guoxing Chen, Haojin Zhu: Secure Hierarchical Deterministic Wallet Supporting Stealth Address. ESORICS 2022: 89-109

[CRYPTO'22] Khoa Nguyen, Fuchun Guo, Willy Susilo, Guomin Yang: Multimodel Private Signatures. CRYPTO 2022: 792-822.

[TIFS'23] Xueqiao Liu, Guomin Yang, Willy Susilo, Kai He, Robert H. Deng, Jian Weng: Privacy-Preserving Multi-User Outsourced Computation for Boolean Circuits. IEEE Trans. Inf. Forensics Secur. 18: 4929-4943 (2023)

[SP'24] Xiaoguo Li, Guomin Yang, Tao Xiang, Shengmin Xu, Bowen Zhao, HweeHwa Pang, Robert H. Deng: Make Revocation Cheaper: Hardware-Based Revocable Attribute-Based Encryption. S&P 2024.