Research Statement

YANG Guomin
School of Computing and Information Systems, Singapore Management University
Tel: (+65) 68264928; Email: gmyang@smu.edu.sg
20 December 2024

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. Since such protocols use different cryptographic primitives, investigating new cryptographic primitives that can provide novel security, privacy and usability features also naturally became my research interest. Since then, my research focus has been following this paradigm, which is developing new cryptographic primitives that can provide special and unique features demanded by emerging computing and communications platforms such as cloud, IoT, and blockchain.

Research Areas

AKE 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 basis of network security. My research has contributed to the development of secure and privacy-preserving AKE protocols under different network settings.

During my PhD study, motivated by the development of the 3GPP security standard, 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 attacks. In addition, I identified a new type of attack called “deposit-case attack” against roaming protocols, and then proposed effective solutions to resist the attack while ensuring user anonymity and untraceability [TWC’07, WC’10]. Subsequently, 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 deal with the situations involving bad randomness. Following this work, to address the side-channel and key leakage attacks against cryptographic systems, I worked with my PhD student and developed the first leakage-resilient AKE protocol that can resist both secret key and randomness leakage [RSA’16]. In [TISS’14], I worked with my collaborators and developed a practical cross-domain password-based AKE, which was later standardized by ISO/IEC as an international standard “ISO/IEC 11770-7 (2021)”.

Data Communication Security

Standard cryptographic primitives, such as encryption and digital signature schemes, can ensure the confidentiality and integrity of data in transit. Nevertheless, some tricky attacks can bypass the protection provided by these standard security primitives. Meanwhile, in many applications, we want to protect the identity of the data sender and/or receiver to avoid traffic analysis and inference attacks. My research has contributed to the design of new cryptographic primitives that can resist non-traditional attacks and enable secure and 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 eliminate 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], the technique was extended to build Cryptographic Reverse Firewalls for attribute-based cryptosystems.

- Anonymous Communication

To achieve anonymous communication, one widely used approach is to perform rerandomizable on encrypted data by some network nodes known as mixers. However, constructing anonymous and rerandomizable encryption secure under adaptive chosen-ciphertext attacks, which is the *de facto* security requirement for encryption schemes, is a non-trivial task. In fact, it has been an open problem for the cryptography research community since 2007. In [CRYPTO'21], we introduced a new primitive named Rerandomizable Smooth Project Hash Function and used it to construct the first practical anonymous and rerandomizable public key encryption scheme secure under (replayable) chosen-ciphertext attacks, hence provided an affirmative answer to the open problem.

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 outsourced to a cloud server. My research has contributed to the development of new cryptographic and security solutions to address the above problems.

Searchable encryption is a prevalent research topic due to the popularity of cloud storage. In [RSA'10], I proposed a new probabilistic public key encryption scheme that can support equality tests over encrypted data. Later, this technique was also found useful in constructing secure Message Locked Encryption that allows

deduplication over encrypted data. 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. We 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 an important yet challenging task. The problem becomes even more tricky under the multi-user/key setting. To address this challenge, my PhD student and I developed a general privacy-preserving multi-user outsourced secure computation framework for Boolean circuits [TIFS'23].

Blockchain Security and Privacy

By allowing transaction records to be stored in a distributed and immutable ledger, blockchain has shown great potential in many application domains such as digital currency, digital identity, supply-chain, Web3, and so on. In my recent works, I developed new cryptographic primitives to address the security and privacy issues in blockchain.

In [EuroS&P'19], we identified a serious security issue in the one-time address management mechanisms used by several major cryptocurrencies, including 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 control all the other one-time accounts linked to it. To address this serious security flaw, we proposed a new 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 addressed in distributed protocols. In the literature, non-equivocation in blockchain mainly focused on preventing double-spending of a digital coin. In [ASIACCS'21], we 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 sensitive data recorded in blockchain transactions is a desirable feature to make the technology acceptable by both end users and different industries. On the other hand, accountability must not be sacrificed in critical business domains such as financial and medical sectors. Balancing privacy and accountability is an important but challenging research problem. In [TDSC'21], we proposed a solution for balancing privacy and accountability in a specific use case of anonymous digital currency. This approach can ensure user privacy while allowing an authority to identify illegal transactions, such as money laundering. In a subsequent work [CRYPTO'22], we developed a new digital signature primitive named "Multimodal Private Signature" that generalizes the concept of traceable anonymous signature and can be used in a wide range of applications demanding different levels of anonymity and accountability.

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 next few years.

- 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 task in my current research agenda.

- Post-Quantum Cryptography

The advent of a cryptographic relevant quantum computer will completely disrupt the global cybersecurity landscape due to its capability of breaking all the public key cryptographic algorithms, such as RSA, ECDSA, and Diffie-Hellman, which are widely deployed in various security standards (e.g., TLS, SSH, VPN, etc.) and software systems for safeguarding sensitive and valuable data. In August 2024, NIST published the first set of standardized PQC algorithms. However, deploying PQC technologies in existing computer and network infrastructures faces several challenges. First, due to the lack of cryptography agility of most information systems and the significant differences between classical and PQC algorithms, the migration process will be complex, error-prone, and requires substantial technical support. Also, due to the significant increase in computational resources (e.g., memory and bandwidth) demanded by PQC algorithms in comparison to their classical counterparts, deploying PQC algorithms on resource-limited devices poses a major challenge. Lastly, the current NIST standardization only focuses on the basic encryption and integrity protection schemes for protecting data in rest/transit, developing advanced and practical PQC algorithms for protecting data in use, such as in privacy-preserving machine learning and data analytics, remains as a research challenge. Developing novel and practical solutions to address the above challenges will be one of my focus areas in the next 5 years.

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.