Each year, several international conferences are held in China on various topics related to cybersecurity. One major conference is the International Conference on Information Security and Cryptology (Inscrypt). Held annually for the past fifteen years, Inscrypt targets the top research results on topics of interest and advances in all areas of information security, Cryptology, and their applications. The most recent conference was held in Nanjing in December 2019 and had two tracks focused on cryptology and general cybersecurity. Presenters came from Japan, India, Australia, Vietnam, and Denmark, as well as China. Thirty-three papers were accepted and presented. This article will focus on papers from the cryptology track addressing post-quantum cryptography, artificial intelligence and machine learning, and cryptanalysis.

Inscrypt 2019 was organized by the State Key Laboratory of Information Security (SKLOIS) of the Institute of Information Engineering of Chinese Academy of Science and the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics. Other institutional participants included the Collaborative Innovation Center of Novel Software Technology and
Industrialization, the College of Computer, Nanjing University of Posts and Telecommunications and corporate support from Beijing Safe-code Technology Co. Ltd., Alibaba, Huawei, and Mitsubishi Electric.

Inscrypt is held in cooperation with the International Association for Cryptologic Research (IACR), the non-profit scientific organization whose purpose is to further research in cryptology and related fields. ICAR defines cryptology as "the science and practice of designing computation and communication systems which are secure in the presence of adversaries." Conference proceedings are published in English by Springer Verlag. Previous conference papers can also be reviewed on their site.

The session on Post-Quantum Cryptography included four presentations and was moderated by Dongdai Lin, State Key Laboratory of Information Security, Beijing. The first, "A Lattice-Based Certificateless Public Key Encryption with Equality Test in Standard Model," was presented by research collaborators from Australia and Vietnam. They propose a lattice-based certificateless public key encryption with equality test (CL-PKEET) standard model with security reduced to the hardness of the learning with errors problem. They argue their schemes are secure against two types of selective-identity adversaries first introduced by Qu et al. This work was supported by the Australian Research Council Discovery Project.

"Efficient Password-Authenticated Key Exchange from RLWE Based on Asymmetric Key Consensus" came from research at the Chinese Academy of Sciences' State Key Laboratory of Information Security. In this work, the authors propose an efficient password-authenticated key exchange protocol using a new error reconciliation mechanism based on the Ring Learning With Errors (RLWE) problem, which is considered to resist quantum attacks. Their protocol is proven secure, they assert, under the Bellare-Pointcheval-Rogaway (BPR) model. It is implemented using C language, which is both portable and optimized utilizing the Advanced Vector Extensions 2 (AVX2) instruction set. The National Natural Science Foundation of China, National Cryptographic Foundation of China, and the National S&T Major Project of China supported this work.

A lattice-based Key-Policy Attribute-Based Keyword Search (KP-ABKS) scheme supporting circuit policy of any predetermined polynomial depth was presented in "Attribute-Based Keyword Search from Lattices." "Our scheme," the authors assert, "is provably secure against chosen keyword attacks and keyword guessing attacks under the DLWE and ISIS assumptions in the random oracle model."

A multiparty key exchange protocol was proposed in "Group Key Exchange from CSIDH and Its Application to Trusted Setup in Supersingular Isogeny Cryptosystems." Two researchers from the Department of Mathematical Informatics at the University of Tokyo and a colleague from Mitsubishi Electric described a multi-party (group) key exchange protocol based on Commutative Supersingular Isogeny Diffie-Hellman (CSIDH), a post-quantum Diffie-Hellman type key exchange protocol from a commutative group action. Their proposed group key exchange protocol, called G-CSIDH, uses the same size prime
modulus $p$ as that in CSIDH for the same security level, and the security of G-CSIDH is reduced to the security of CSIDH. In addition, they propose the trusted protocol of generating public parameters of supersingular isogeny cryptosystems by using their proposed G-CSIDH.

The AI Security track was moderated by Weizhi Meng, Department of Applied Mathematics and Computer Science, at the Technical University of Denmark (DTU).

The presenters of "RoLMA: A Practical Adversarial Attack against Deep Learning-Based LPR Systems," describe RoLMA is an adversarial attack against deep learning-based License Plate Recognition systems. They physicalize perturbations on a real license plate by virtue of generated adversarial examples. Their experiments demonstrate that RoLMA can effectively deceive HyperLPR with an 89.15% success rate in targeted attacks and 97.3% in non-targeted attacks.

"A SeqGAN-Based Method for Mimicking Attack," the authors present a method for launching an advanced application-layer DDoS which masquerades as a Flash Crowd (FC). The attack strategy falls in two aspects: (1) extracting legitimate users' behaviors; and (2) instructing bots to behave as legitimate users. To achieve this, they propose a multi-step algorithm to extract user browsing behaviors and establish a Sequence Generative Adversarial Nets (SeqGAN) model to generate mimicking behaviors of bots. In addition, they experimentally study the effectiveness of this mimicking attack. The study shows that the mimicking attack can fool a detection system that is based on machine learning algorithms.

In "Suzzer: A Vulnerability-Guided Fuzzer Based on Deep Learning," researchers from the University of Science and Technology of China at Hefei, the National Engineering Laboratory for Public Safety Risk Perception and Control by Big Data (NEL-PSRPC), Beijing, and the Advanced Innovation Center for Human Brain Protection of Capital Medical University in Beijing describe a prediction model for finding software bugs. A software program oftentimes has only a fairly small portion that contains vulnerabilities, leading coverage-based fuzzers to work poorly.

They propose Suzzer, a vulnerability-guided fuzzer, to concentrate on testing code blocks that are more likely to contain bugs. Suzzer has a light-weight static analyzer to extract automated control flow graph (ACFG) vector from target programs and is equipped with prediction models which get the prior probability of each ACFG vector.

The Cryptanalysis session was moderated by Chunhua Su, Division of Computer Science, University of Aizu, Japan. In "Improved Integral Attack on Generalized Feistel Cipher," the authors consider improved integral attack on block ciphers with Generalized Feistel Structure (GFS cipher) by considering the linear transformation of the S-boxes. Taking the 16-branch GFS cipher with 4-bit S-boxes as an example, using this improved method, they can increase the round of
integral distinguishers by one round for many S-boxes. The result implies that ability to resist this improved integral attack should also be considered when designing corresponding GFS ciphers.

The second paper in this category, "Enhanced Differential Cache Attacks on SM4 with Algebraic Analysis and Error-Tolerance," the authors propose a method they call Algebraic Differential Cache Attack (ADCA) to enhance the attacks. By converting both cipher and cache leakages to algebraic equations, ADCA can, they report, reveal the cipher key automatically with the help of the SAT solver, which allows the analysis on much deeper rounds and makes a considerable reduction in attack complexity. When it is applied to the block cipher SM4, 10 plaintexts are enough to reveal the master key in 8-rounds analysis, half as many as the traditional differential cache attack needs. To eliminate the impact from noise, an error-tolerant method is proposed to deduce cache events from the leakage traces. This approach vastly enhances the robustness of attack, and makes the attack more practical. The experimental results show that the error-tolerant ADCA can correctly reveal the master key even when the uncertainty rate of cache events reaches to 60%. This work was supported in part by Alibaba-Zhejiang University Joint Institute of Frontier Technologies, State Key Laboratory of Cryptology, Natural Science Foundation of China and by Research Institute of Cyberspace Governance in Zhejiang University.

The remaining papers addressed authentication, mathematical foundations, systems security, side channel attacks, and signatures. All of them are available online through Springer Verlag.

As of this writing, no information has been published regarding the Inscrypt conference for 2020.