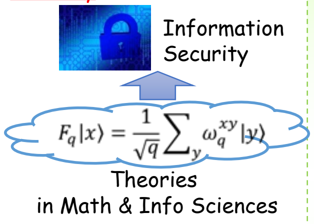
Crypto and Cyber SEC (CY^{2}SEC) - Miyaji Lab-

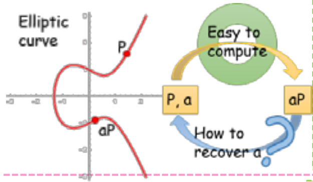
Cover all research areas necessary to achieve a safe and secure society, including key technologies of cryptology, Privacy, secure application, and cyber security.

Basic Researches

Foundations of Information Security


Information
Security
$F_q|x\rangle = \frac{1}{\sqrt{q}}\sum_y \omega_q^{xy}|y\rangle$
Theories
in Math & Info Sciences

Security of elliptic curve Cryptography



Achieve generic construction used for all cryptosystems and security analysis.

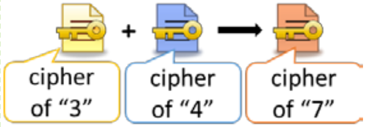
- Foundations of Information Security: are solidly supported by theories in mathematical and information sciences. We analyze (im)possibility of information security technologies from mathematics, computational complexity, coding theory, information theory, quantum computing, etc.
- Security of elliptic curve cryptography: depends on difficulty of ECDLP. We analyze using index calculus algorithm and study its core subroutine of multivariate polynomial system solving.
- Symmetric key encryption: is used to achieve the confidentiality and integrity. We analysis the security for symmetric key encryption and pseudo-random number generator.

Big Data

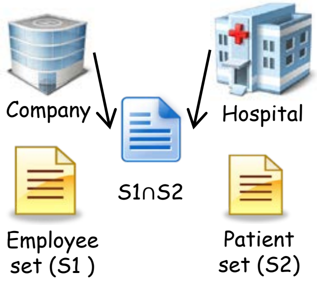
Achieve secure data utilization and privacy protection on big data.

- Homomorphic Encryption (HE): is a new crypto-technology that enables us to operate encrypted data without decryption, which is promising for privacy-preserving operations on big data. We study improvements of the performance and functionalities of HE. Further, we develop new applications of HE for big data.
- Private Set Intersection (PSI): is a way to utilize data while multiple organizations can collect big data but still protect their private data. PSI extracts intersections of data sets kept in organizations. In cooperation with research institutions to use the PSI, we are doing research on practical PSI. In addition, We research on the optimization of computation and communication complexities of PSI.

Homomorphic Encryption

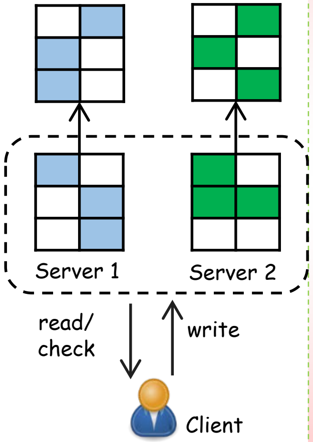


Private Set Intersection



Cloud

Oblivious RAM (ORAM)



Achieve a cloud system with access patter privacy, availability, integrity, & confidentiality.

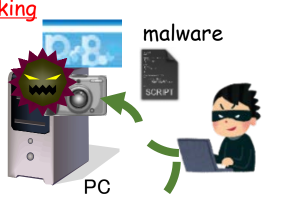
- Network coding: can improve network throughput. When (X,Y) sends (a,b) to (Z,T), central link can carry a+b (not only a or b). (Z,T) can receive (a,b) simultaneously. We research on the improvement of pollution attack detection and the designing new coding system with pollution resistance.
- Obvious RAM (ORAM): can protect client's access pattern. In every read/ write operation, data is mapped to a new position and is shuffled to let untrusted servers indistinguish which data being accessed.

IoT

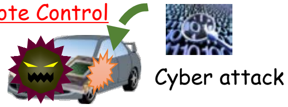
Achieve a new communication protocol & detect way for attack to IoT devices.

- Elliptic curve cryptography: is desired to utilize the embedded devices which is limited computational resources and memory capacity, since it can be realized with a short key length. We research the safety improvement and the efficiency of algorithm.
- Pseudo-random Number Generator: is one of the most important primitives for information security. We works on designing highly-random, low-cost and high-speed pseudo-random number generators which are resilient to various attacks.
- Tamper resistant: can protect the data for analysis. Our lab works the implementation cryptosystems with code obfuscation.

Hacking



Remote Control



Forged card