情報セキュリティ研究センター

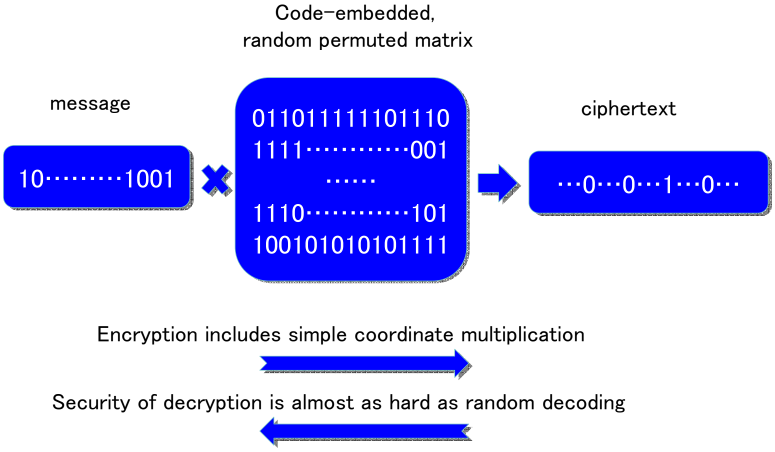
Research Center for Information Security
Yang CUI

Code-based Public Key Cryptosystem and its Applications
– 符号ベース公開鍵暗号とその応用

1. Code-based Public Key Cryptosystem (CPKC) is fast, secure and historical, which can be used to encrypt, sign, authenticate and hash, etc.
2. CPKC has varieties of interesting applications and is believed to be immune to Quantum Algorithm and have long-term security, unlike RSA or Discrete Log-based PKC.

Construction and Key Idea:

- Trapdoor: a secret decoding algorithm
- Public key: a correspondingly generated random matrix

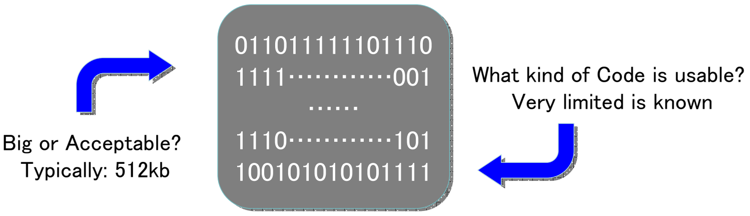


Fascinating Property:

- Speed: faster than multivariate PKC, such as Matsumoto-Imai, comparable to sym. key encryption, such as AES.
- Security: base on classic decoding problems

Disturbing Property:

- Public key storage: obviously larger than RSA or Discrete Log-based ones
- Security: heavily rely on certain error-correcting Code



Code-based PKC Research, in RCIS, AIST

Theoretical Approaches (Efficiency & Long-term Security)

1. Build the most compact Code-based encryption, while keeping the highest security level [SCIS'08, full version to be submitted]
2. In the first time, investigate the key-privacy issue of the Code-based encryption [AAECC'07]
3. Security enhancement of Code-based PKC, long-term secure and reliable [To be submitted]
4. Testify and select more error-correcting Codes than current ones (future work)

Practical Applications (Ubiquitous computing)

1. Apply Code-based PKC in lightweight cryptography, such as an authentication protocol for RFID environments [IEEE PerCom'07 Security Workshop, full version in IEICE Transaction]
2. A lightweight emergency broadcasting protocol, for ubiquitous computing [In submission]
3. Authentication protocol for RFID, with shortened public key (To be submitted)