所属：鶴岡工業高等専門学校　創造工学科　情報コース

研究タイトル：

量子コンピュータでも破れない暗号技術

氏名：	手塚　真徹　／　TEZUKA Masayuki	E-mail：	tezuka.m@tsuruoka-nct.ac.jp
職名：	助教	学位：	博士（理学）
所属学会・協会：	電子情報通信学会		

キーワード：	暗号理論，証明可能安全性
技術相談 提供可能技術：	・暗号技術における安全性モデルのアドバイス ・帰着の手法を用いた暗号技術の安全性証明と解析 ・高機能暗号の応用相談

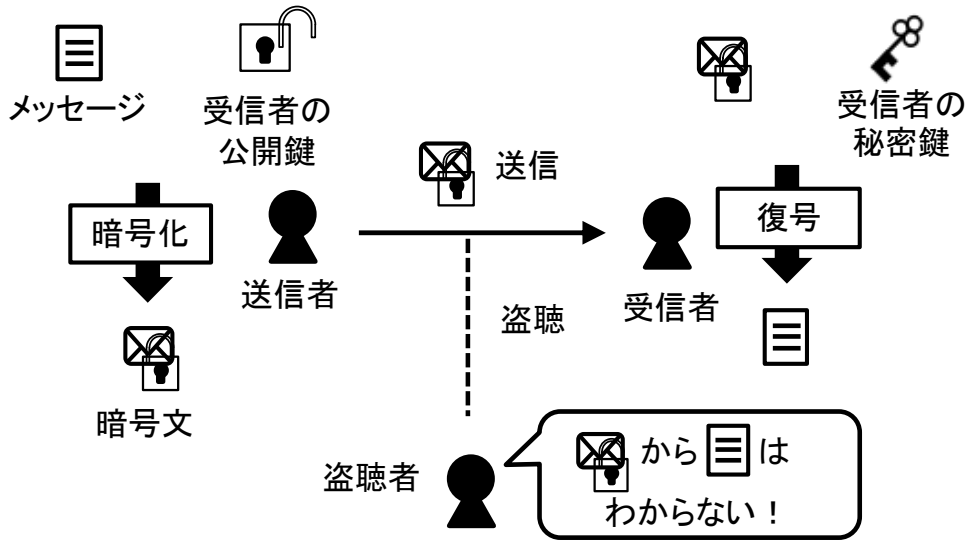
研究内容：耐量子暗号の構成研究

社会の情報化が進み、個人情報や金融情報などのインターネットを用いた通信でやりとりされます。
安全な情報社会を実現するためには、これらの情報を他者に漏らさず通信する技術が必要です。
暗号は通信の内容を送信者と受信者以外にわからないようにすることを可能にする技術です。

現在、幅広用いられている公開鍵暗号に RSA 暗号があります。ところが、量子コンピュータを用いると RSA 暗号が短時間で破られます。大規模な量子コンピュータが実現した未来の社会では RSA 暗号の安全性を保証することができません。

そこで、量子コンピュータが完成した未来に備えるために量子コンピュータでも解くことが難しい耐量子暗号の研究に取り組んでいます。

公開鍵暗号



提供可能な設備・機器：

名称・型番（メーカー）	

National Institute of Technology, Tsuruoka College
Department of Creative Engineering, Course of Information Systems

Post-quantum cryptography

Name	TEZUKA Masayuki	E-mail	tezuka.m@tsuruoka-nct.ac.jp
Status	Assistant professor		
Affiliations	The Institute of Electronics, Information and Communication Engineers (IEICE).		

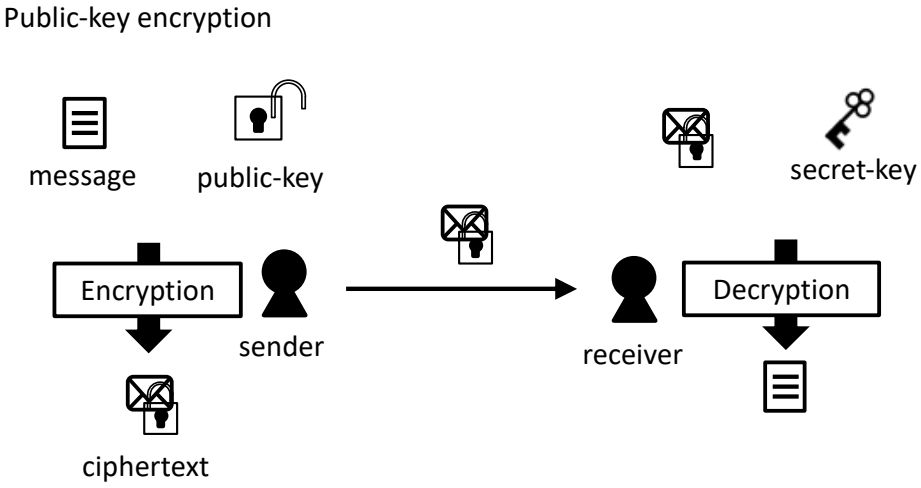
Keywords	Cryptography, Provable Security
Technical Support Skills	・Security model for cryptographic schemes ・Security analysis for cryptographic schemes via reduction technique ・Application of cryptography with advanced functionality

Research Contents

Currently, sensitive information such as personal private information and financial information is sent via the Internet. In order to realize a secure information society, we need a technique for sending private information from a sender to a receiver without leaking any information about communication. Public key encryption serves as a mechanism to ensure confidentiality.

The RSA cryptosystem proposed by Rivest, Shamir, and Adleman is widely used. However, by using a quantum computer, the security of the RSA cryptosystem can be broken. In recent years, the realization of quantum computers is an active study field in computer science.

To prepare for a time when a quantum computer is realized, we study post-quantum cryptosystems whose security cannot be broken by using a quantum computer.



Available Facilities and Equipment
