セキュリティWG活動報告

KDDI総合研究所
三宅　優

2022年9月9日

What are security topics for future networks?

Changes	Examples	Issues
New Technologies	• Quantum Computer • AI technologies	• Future quantum computer can compromise current crypt algorithms. • AI will be used for cyber attacks. • AI itself will be target of attack.

New Services (New Use Cases)	• Holographic Communication
	• Tactile Internet
	• Unmanned mobility
		• New requirements should be considered.
		  • High speed/Large bandwidth communication
		  • Extremely low latency
		  • Time sensitive communication

New Functions	• Exposure of network and computing resource • In-time and on-time services • Security, Privacy, Trust	• API/Interconnecting should be secured. • What security/privacy/trust function will be required for B5G/6G network?
New Infrastructure	• Space-terrestrial Integrated Network • Intelligent Operation Network	• Networks will become even more complex, and security issues (vulnerabilities, configuration mistakes) cannot be found easily.

Security considerations for new features

Features	Security requirements
Ultra Fast & Large Capacity	• High speed encryption/decryption • New security monitoring and processing methods
Ultra Low Latency	• Seamless security architecture • Lightweight security
Ultra Numerous Connectivity	• Efficient authentication/authorization • Efficient security processing and monitoring mechanism
Ultra low power consumption	• Security mechanisms in hardware • Lightweight security architecture
Ultra security and resiliency	• New security monitoring and defensing mechanisms • Resilience mechanism for attacks/failures • Privacy preserving mechanisms • Trustworthiness of different nodes and domains • Accounting, accountability, validation of delivered services
Autonomy	• Trust mechanism without trusted parties
Scalability	• Interoperable security mechanism between different networks/domains • Optimization of security mechanism among

B5G/6Gに向けた
セキュリティ関連の取り組み

暗号関連

要件	対応方法
量子コンピュータ出現への対応	量子暗号通信（QKD：量子鍵配送）技術の展開
	耐量子計算機暗号アルゴリズム（PQC）の開発と応用
超高速、大容量、低遅延通信への対応	高速暗号アルゴリズムの開発

QKDに関する日本での活動

NICT

日本語 TOP | Access | Contact us | ENHANCED BY Google

NICT National Institute of Information and Communications Technology

About NICT | Research | Activities | Publicity | Employment Information

Home > Advanced ICT Research Institute > Quantum ICT Laboratory > Quantum Cryptography and Physical Layer Cryptography

Quantum ICT Laboratory

日本語 | PRINT

Quantum Cryptography and Physical Layer Cryptography

Article from NICT NEWS 2021 No. 2 (Vol. 486)

Researchers: Mikio FUJIWARA, Hiroyuki ENDO

The NICT has been conducting research and development of a technology for a cryptographic communication system that can not be broken even with the most advanced computers in the future, or a quantum cryptography network that ensures information-theoretically secure communication, as well as a technology for building a distributed storage on the network that is also theoretically secure. We have been operating a quantum cryptography network, Tokyo QKD Network, covering an area within 100 km from the center of Tokyo since 2010, and research on spaceborne implementation is also ongoing. This article introduces our efforts and the progress towards global deployment.

Background

RSA and DH are currently the most popular public key cryptography, and are used in cryptographic communication through TLS and digital signatures. However, they are known to be breakable in polynomial time using a quantum computer, and so there is an urgent need to make them stronger. In

Research Themes

- Overview
- Quantum Cryptography and Physical Layer Cryptography
- Photonic Quantum Technologies
- Trapped-ion Optical Clock and Quantum Network
- Quantum Control of Continuous Variable States
- Quantum Information Theory
- Quantum Communications
- Photon Detection
- Light-exciton Interaction
- Ion-photon Quantum Network

Return to the Main Menu

Toshiba

TOSHIBA | Quantum Key Distribution | Japanese | Contact us

Home | What is QKD | Why Toshiba QKD | Products | Use Cases | News/Topics

Quantum Key Distribution

The new age of secure communication, powered by quantum physics

Our vision is to secure the world's communications from the threats posed by advances in computing and mathematics. At a time when technological progress has created an almost constant state of data proliferation, the need for the secure transmission of sensitive information has never been more significant. It is essential to protect and future-proof data communication now through the advancement of reliable and ultra-secure quantum cryptography solutions.

At Toshiba, we are committed to delivering world's leading cyber-physical-system technology to protect the private information of citizens and companies. Our Quantum Key Distribution (QKD) offering applies the fundamental laws of

NEC

NEC Orchestrating a brighter world

Contact Us | Support & Downloads | Country & Region | Global Site

Products & Solutions | Case Studies | News | About NEC | Search NEC

Home > News Room > NEC, NICT and ZenmuTech use quantum cryptography to encrypt, transmit and backup electronic medical records

NEC, NICT and ZenmuTech use quantum cryptography to encrypt, transmit and backup electronic medical records

- Achieving secure and real-time cross-references between medical institutions -

News Room

Corporate/Financial

Sustainability

Tokyo, October 22, 2020 - NEC Corporation (NEC), National Institute of Information and Communications Technology (NICT) and ZenmuTech, Inc have succeeded in demonstrating a system that uses quantum cryptography to encrypt and securely transmit dummy electronic medical records compatible with SS-MIX standardized storage and to back the data up with a secret sharing technology (*1) over a wide area network. In addition, the cross-referencing of dummy data between this system and Kochi Health Sciences Center has also been demonstrated.

This demonstration experiment was conducted as a part of the Cross-ministerial Strategic Innovation

QKDに関する標準化状況（ITU-T）

ITU-Tで勧告化された文書

ITU-T SG13 (Future networks and emerging network technologies)

Y.3800: Overview on networks supporting quantum key distribution
Y.3801: Functional requirements for quantum key distribution networks
Y.3802: Quantum key distribution networks – Functional architecture
Y.3803: Quantum key distribution networks – Key management
Y.3804: Quantum key distribution networks – Control and management
Y.3805: Quantum key distribution networks – Software-defined networking control
Y.3806: Quantum key distribution networks – Requirements for quality of service assurance
Y.3807: Quantum key distribution networks – Quality of service parameters
Y.3808: Framework for integration of quantum key distribution network and secure storage network
Y.3809: A role-based model in quantum key distribution networks deployment
Y.3810 (draft): Quantum key distribution network interworking - framework
Y.3811 (draft): Quantum key distribution networks - Functional architecture for quality of service assurance
Y.3812 (draft): Quantum key distribution networks - Requirements for machine learning based quality of service assurance

ITU-T SG17 (Security)

X.1710: Security framework for quantum key distribution networks
X.1712: Security requirements and measures for quantum key distribution networks – key management
X.1714: Key combination and confidential key supply for quantum key distribution networks
X.1715: Security requirements and measures for integration of quantum key distribution network (QKDN) and secure storage network

ITU-Tにおける日本の貢献

日本からの寄書の提出状況（2022年のみ）

SG	番号	タイトル	提出元	会合
13	40	Supporting of consent on the draft Recommendation ITU-T Y.QKDN-iwfr “Quantum key distribution network interworking (QKDNi) - framework”	NICT、NEC、東芝	2022年7月
17	178	Revised baseline text for X.sec_QKDN_tn: Security requirements and designs for the protection of quantum key distribution node	NICT、NEC、東芝	2022年8～9月
	177	Revised baseline text for X.sec_QKDN_AA: Authentication and authorization in QKDN using quantum safe cryptography	NICT、NEC、東芝	2022年8～9月
	89	Revised baseline text for X.sec_QKDN_tn: Security requirements and designs for quantum key distribution networks - trusted node	NICT、NEC、東芝	2022年5月
	86	Revised baseline text for X.sec_QKDN_AA: Authentication and authorization in QKDN using quantum safe cryptography	NICT、NEC、東芝	2022年5月
	85	Revised baseline text for X_sec_QKDN_intrq: Security requirements and measures for integration of QKDN and secure storage network (for consent)	NICT、NEC、東芝	2022年5月

日本以外の寄書の提出状況（2022年のみ）

- 中国（CAS Quantum Network Co. Ltd., QuantumCTek Co., Ltd., Beijing University of Posts and Telecommunications, Ministry of Industry and Information Technology (MIIT) ）
- 韓国（SK Telecom）

耐量子計算機暗号（PQC）に関する取り組み

KDDI

MLWRSign for digital signature

2020 | OriginalPaper | Chapter

A Compact Digital Signature Scheme Based on the Module-LWR Problem

Authors: Hiroki Okada, Atsushi Takayasu, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi

Publisher: Springer International Publishing

Published in: Information and Communications Security

» Get access to the full-text

Abstract

We propose a new lattice-based digital signature scheme MLWRS
which is one of the second-round candidates of NIST's call for post-
standards. To the best of our knowledge, our scheme MLWRSign is t
security is based on the (module) learning with rounding (LWR) prob
LWR, the secret key size is reduced by approximately 30% in our sch
while achieving the same level of security. Moreover, we implement
the running time of our scheme is comparable to that of Dilithium.

Toshiba

Giophantus
for public-key cryptography

International Conference on Selected Areas in Cryptography
SAC 2017: Selected Areas in Cryptography – SAC 2017 pp 215-234 | Cite as

A Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations

Authors | Authors and affiliations

Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka

Conference paper
First Online: 23 December 2017

2 Citations 686 Downloads

Part of the Lecture Notes in Computer Science book series (LNCS, volume 10719)

Abstract

In this paper, we propose a post-quantum public-key encryption scheme whose security depends on a problem arising from a multivariate non-linear indeterminate equation. The security of lattice cryptosystems, which are considered to be the most promising candidate for a post-quantum cryptosystem, is based on the shortest vector problem or the closest vector problem in the discrete linear solution spaces of simultaneous equations. However, several improved attacks for the underlying problems have recently been developed by using approximation methods, which result in requiring longer key sizes. As a scheme to avoid such attacks, we propose a public-key encryption scheme based on the "smallest" solution problem in the *non-linear* solution spaces of multivariate *indeterminate equations* that was developed from the algebraic surface cryptosystem. Since no efficient algorithm to find such a smallest solution is currently known, we introduce a new computational assumption under which proposed scheme is proven to be secure in the sense of IND-CPA. Then, we perform computational experiments based on known attack methods and evaluate that the key size of our scheme is able to be much shorter than those of previous lattice cryptosystems.

NICT

LOTUS for public-key cryptography

Post-Quantum Cryptography

LOTUS

Home

Materials
Specifications
Implementation Code
Known Answer Tests

Related information

LOTUS

(Learning with errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era)

What's LOTUS?

LOTUS is a lattice-based cryptosystem developed by NICT. LOTUS consists of LOTUS-PKE for public key encryption and LOTUS-KEM for key encapsulation. LOTUS aims at providing post-quantum security, meaning it may remain secure against large-scale quantum computers. Some highlighted properties of LOTUS are as follows:

- Its security relies on the standard Learning With Errors (LWE) assumption.
- It targets IND-CCA2 security, even with 256-bit security level (the highest security level in NIST PQC project).
- It is based on a long line of research.

News

- December 27, 2017. Initial website is up.
- January 04, 2018. Update the implementation code t
failure. We thank Tancrède Lepoint for pointing out t
- October 15, 2018. LOTUS implementation codes are

Contacts

NTT

Improvement of
NTRU-HRSS
(Public-key Cryptography)

Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model ★

Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa

NTT Secure Platform Laboratories
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585 Japan
{saito.tsunekazu, xagawa.keita, yamakawa.takashi}@lab.ntt.co.jp

August 25, 2021

Abstract. Key-encapsulation mechanisms secure against chosen ciphertext attacks (IND-CCA-secure KEMs) in the quantum random oracle model have been proposed by Boneh, Dagdelen, Fischlin, Lehmann, Schafner, and Zhandry (CRYPTO 2012), Targhi and Unruh (TCC 2016-B), and Hofheinz, Hövelmanns, and Kiltz (TCC 2017). However, all are non-tight and, in particular, security levels of the schemes obtained by these constructions are less than half of original security levels of their building blocks.
In this paper, we give a conversion that tightly converts a weakly secure public-key encryption scheme into an IND-CCA-secure KEM in the quantum random oracle model. More precisely, we define a new security notion for deterministic public key encryption (DPKE) called the disjoint simulatability, and we propose a way to convert a disjoint simulatable DPKE scheme into an IND-CCA-secure key-encapsulation mechanism scheme without incurring a significant security degradation. In addition, we give DPKE schemes whose disjoint simulatability is tightly reduced to post-quantum assumptions. As a result, we obtain IND-CCA-secure KEMs tightly reduced to various post-quantum assumptions in the quantum random oracle model.

keywords: Tight security, chosen-ciphertext security, post-quantum cryptography, KEM.

耐量子計算機暗号（PQC）に関する取り組み

別紙

令和３年度から新たに実施する電波資源拡大のための研究開発

採択結果一覧表

研究開発課題	技術課題		研究機関 （下線は代表研究機関）
安全な無線通信サービスのための新世代暗号技術に関する研究開発	ア	５G等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）	株式会社 KDDI 総合研究所、 国立大学法人神戸大学、 公立大学法人兵庫県立大学、 株式会社国際電気通信基礎技術研究所
	イ	５G等のための耐量子計算機暗号の機能付加技術等（耐量子コンピュータセキュリティ技術）	国立大学法人横浜国立大学、 国立大学法人九州大学、株式会社東芝、 国立大学法人東京大学、 国立大学法人大阪大学、 国立研究開発法人情報通信研究機構、 株式会社国際電気通信基礎技術研究所

目的：５Ｇ等の様々なユースケースに合わせた耐量子公開鍵暗号の最適化技術等を確立し、無線リソースのひっ迫を抑止し、電波の有効利用を図る。

目標：オーバヘッドを最大８％以内に抑え、携帯端末等でも実装可能な技術を開発する。

高速暗号アルゴリズムに関する取り組み

別紙

令和３年度から新たに実施する電波資源拡大のための研究開発

採択結果一覧表

研究開発課題	技術課題		研究機関 （下線は代表研究機関）
安全な無線通信サービスのための新世代暗号技術に関する研究開発	ア	５G等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）	株式会社 KDDI 総合研究所、 国立大学法人神戸大学、 公立大学法人兵庫県立大学、 株式会社国際電気通信基礎技術研究所
	イ	５G等のための耐量子計算機暗号の機能付加技術等（耐量子コンピュータセキュリティ技術）	国立大学法人横浜国立大学、 国立大学法人九州大学、株式会社東芝、 国立大学法人東京大学、 国立大学法人大阪大学、 国立研究開発法人情報通信研究機構、 株式会社国際電気通信基礎技術研究所

目的：量子コンピュータに対しても、現在と同等の安全性を確保するために、鍵長を256ビットにしつつ、5G等の超高速・大容量に対応した共通鍵暗号方式を設計する。

目標：暗号処理速度80Gbpsを達成し、処理時間を従来方式と比較し、最大50％削減する。

超高速公開鍵暗号方式の検討

KDDI Research

世界最速 Beyond 5G/6Gに向けた超高速暗号アルゴリズム「Rocca」を開発

～256ビット暗号で初めて（注1）100Gbps超の処理性能を実現～

2021年11月9日
株式会社KDDI総合研究所
兵庫県公立大学法人兵庫県立大学

株式会社KDDI総合研究所と兵庫県立大学大学院 情報科学研究科の五十部孝典 准教授の研究グループは、Beyond 5G/6G時代に求められる処理性能と安全性を備えた新しい共通鍵暗号アルゴリズム「Rocca」を開発しました。「Rocca」は256ビットの鍵長に対応する認証付きストリーム暗号で、処理速度として世界最速（注1）となる138Gbpsを達成しました。

AESとの処理速度比較

暗号アルゴリズム	処理速度（注）
AES-256-GCM（AES-NIなし）	0.9Gbps
AES-256-GCM（AES-NIあり）	31Gps
Rocca（AES-NIあり）	138Gps

（注）Intel® Core™ i7-1068NG7での計測結果。AESはOpenSSLの実装を利用して計測。Roccaも同様にOpen SSLに組み込み計測を実施。

IETF（Internet-Draft）への展開（Rocca-S）

https://datatracker.ietf.org/doc/draft-nakano-rocca-s/

（報告）
ITU Workshop on "Security for 5G and beyond"

プログラム

ITU Workshop on "Security for 5G and beyond"	
Session 1: Understanding the current status of 5G security and identifying improvements towards 6G	
	5G security standardization roadmap (XSTP-5Gsec-RM), Yutaka Miyake (KDDI Research Inc.)
	Japan’s 5G security guidelines, Ayumu Kubota (KDDI Research Inc.)
	その他の発表者：　ロシア、韓国、中国
Session 2: Initial architecture and concept for 6G security	
	Brief introduction to the ITU-T FG NET-2030 and Japan’s Beyond 5G Promotion Consortium on their security-related activities, Yutaka Miyake (KDDI Research Inc.)
	Path to beyond 5G Security, Anand Prasad (Deloitte Tohmatsu Cyber LLC)
	その他の発表者：　フィンランド、中国、韓国、韓国
Session 3: Fundamental security requirements and functions for 6G	
	発表者：　韓国、中国、中国、フィンランド、中国
Session 4: Panel discussion – Collaboration and coordination on IMT-2020 and beyond security standardization activities	
	モデレータ：　中尾　康二（日本）
	パネリスト：　中国、中国、中国、日本（Prasad氏、前3GPP SA3議長）、フィンランド（3GPP SA3議長）

（日本からの発表タイトルを掲載）

Workshopで示された将来必要とされる技術

- Systematized built-in security to form an immune ability against internal attacks
- Enhanced security design e.g., wireless physical layer security
- Autonomous security frameworks (e.g. for patch management)
- Use of AI for bringing intelligence to security including establishment of cybersecurity AI datasets
- Use of DTN (Delay Tolerant Networking) for bringing certainty to security intelligence
- Technology transition from passive protection to active perception and protection
- Secure interoperability of heterogeneous network (air-space ground) convergence
- Coordination of computing and network security
- End, edge, network and cloud security capabilities collaboration
- Dynamic and flexible security capability deployed on demand for adapting evolution of 6G technologies
- Integrated response and recovery capabilities to improve network resilience
- B5G security technology to enhance sustainability
- Security enhancement for mobile communication system – authentication mechanisms, key management, identity management, etc.
- Enhancement of network management system – such as for access control
- Effective utilization of Zero trust and DLT
- Utilization of PQC for seeking effective crypto use

ITU-T SG17（セキュリティ）における今後の進め方

1. B5G/6Gセキュリティとして議論すべきセキュリティトピックの整理
   - セキュリティトピックの洗い出し
   - セキュリティトピックの分類
     - 一般的なセキュリティ技術
     - 他の標準化団体ですでに検討が始まっているセキュリティ技術
     - ITU-T SG17において特に検討が必要とされるセキュリティ技術

2. 特定のセキュリティトピックに対するSG17で議論するための分析
   - 検討の必要性
   - 他の標準化団体等が発行している文書との違い
   - その他

3. ITU-T内との他のSG、および、ITU-T以外の標準化団体等との連携強化
   - ワークショップの結果の共有（リエゾン文書をITU-T、ITU-R、3GPP、ETSI、CEN/CENELEC、等に送付）

B5GPC