様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ８ 日現在

機関番号：１７１０２
研究種目：若手研究(B)
研究期間：2012～2014
課題番号：２４７００００１３

研究課題名（和文）符号理論に基づくポスト量子暗号プロトコルとその安全性モデルの研究

研究課題名（英文）A Study on Code-Based Postquantum Cryptographic Protocols and Their Security Models

研究代表者
Ｍｏｒｏｚｏｖ　Ｋｉｒｉｌｌ（Morozov, Kirill）

九州大学・マス・フォア・インダストリ研究所・助教

研究者番号：８０４４３２３２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究課題では、符号理論を用いる暗号プロトコルについて以下2点の重要な研究成果が得られた:
1) 符号理論に基づく耐量子暗号プロトコルは量子コンピュータに対する攻撃に対しても安全性がある。そのプロトコルでは、世界初の平文知識証明プロトコルを発表した。それを応用して、世界初の検証可能な暗号化、および指名した確認者署名を発表した。
2)秘密分散法とは秘密情報データを分ける、“シェア”することでライバシーを保護できる情報セキュリティ技術である。この技術において、rushing不正者に対して安全な、同タイプの手法の中では現在最小シェアサイズを実現する新たな不正者を検知可能な秘密分散法を発表した。

研究成果の概要（英文）：Under this grant, we studied the following two important applications of coding in cryptography: 1) Code-based cryptographic protocols, which are secure even against attacks with quantum computers (such the protocols are called “post-quantum”). We presented the first proof of plaintext knowledge for the code-based public-key encryption, and applied it to obtain the first code-based verifiable encryption and the first designated confirmer signature. 2) Secret sharing (SS) - an information security technology allowing us to achieve privacy by splitting the secret data into “shares” that can be stored in a distributed manner. We presented new cheater-identifiable SS schemes and new robust SS schemes secure against rushing cheaters with share sizes which are minimal up-to-date, among the constructions of the same class. Finally, we presented a verifiable share redistribution scheme with perfect security when the number of corrupt parties $k<n/3$, where n is the number of participants.

研究分野：暗号理論

キーワード：耐量子暗号　符号理論に基づく暗号　暗号プロトコル　秘密分散法　不正者を検知可能な秘密分散法

１．研究開始当初の背景

(1) McEliece と Niederreiter による符号理論に基づく公開鍵暗号方式とその IND-CPA と IND-CCA のバリアントが知られている。２元符号に基づくゼロ知識・ユーザ認証プロトコルは Stern によって構成されているが、それに関して、Cayrel、Veron と Alaoui らはその q 元符号に基づくバリアントを構築できた。符号理論に基づく効率なデジタル署名は Courtois、Finiasz と Sendrier らで構成できた。

(2) 秘密分散法では、正直なディーラの場合は不正者を検知可能な秘密分散法によって不正直な参加者（不正者）に対する安全性を確保できる。このとき、不正者を検出し、秘密は復元することが必要ではない。Robust 秘密分散法では、秘密はいつも復元されるが、不正者を検知することは必要ではない。

２．研究の目的

本研究では主に下記の２つのトピックでの結果を達成することを目的とした：
(1) 符号理論に基づく暗号プロトコル。
(2) 正直なディーラである不正者に対して安全な秘密分散法。

３．研究の方法

(1) 最初は Stern ゼロ知識・ユーザ認証プロトコルを用いて、Niederreiter 公開鍵暗号方式の平文知識証明プロトコルができることを示した。この観察を一般化して、McEliece 公開鍵暗号方式の平文知識証明プロトコルと暗号化されたデータについてさらに進んだ知識証明プロトコルを構築した。安全性証明はスタンダードモデルにおいて行った。

(2) 情報理論的安全なメッセージ認証符号を応用して、正直なディーラである不正者に対して安全な秘密分散法のシェアサイズと安全性を改善できた。特にマルチレシーバー・マルチメッセージ認証符号を用いて新たな不正者を検知可能な秘密分散法を構築し、新たなリード・ソロモン符号のバリアントを用いた新たなシェア再配布（share redistribution）プロトコルを発明した。

４．研究成果

(1) McEliece と Niederreiter 公開鍵暗号方式とそのセマンティック安全な改良といった符号理論に基づく暗号方式について、それぞれに Jain その他らと Stern のゼロ知識証明プロトコルを応用して、平文知識証明プロトコルを構築した。その平文知識証明プロトコルを用いて、McEliece 公開鍵暗号方式に基づく検証可能な暗号化 (verifiable encryption)を提案した。

Equivalent security (bits)	80	128
Public key size (Kbytes)	452	1838
Ciphertext size (bits)	2048	4096
Communication (Kbytes)	16.0	30.0
Prover's computation (operations over $\mathbb{F}_2$)	$2^{26.63}$	$2^{28.65}$

図１．McEliece 暗号化の平文知識証明プロトコルの性能評価

Equivalent security (bits)	80	128
Public key size (Kbytes)	61	210
Ciphertext size (bits)	242	420
Communication (Kbytes)	9.1	16.1
Prover's computation (operations over $\mathbb{F}_2$)	$2^{23.73}$	$2^{25.52}$

図２．Niederreiter 暗号化の平文知識証明プロトコルの性能評価

(2) 世界初の符号理論に基づく指名した確認者デジタル署名(designated confirmer signature)を構築した。El Aimani の枠組を使用したが、本枠組では準同型暗号化か一般的な知識証明が必要なので、符号理論の手法を使用して、次のような単純化に当てはめた。確認のプロトコルは上で述べた符号理論に基づく検知可能な暗号化を応用し構築した。また、与えられた平文は McEliece 暗号文の中に含まれていない新たなゼロ知識証明プロトコルを提案し、拒否のプロトコルを構築した。

(3) q 元符号に基づくユーザ認証プロトコルを調査した。小さい q（3、4）である時、q 元 Stern ユーザ認証プロトコルは Cayrel その他ら（CVA）のプロトコルより効率的であることを示した。

$q=3, n=396, k=198, \omega=62$	CVA [7]	Our Proposal
Number of Rounds	39	28
Matrix size (kilobytes)	9.57	9.57
Public key (bits)	396	396
Secret key (bits)	792	792
Communication (kilobytes)	7.50	4.79
Prover's Computation over $\mathbb{F}_3$	$2^{20.58}$ multiplications, $2^{20.54}$ additions	$2^{20.08}$ multiplications, $2^{20.07}$ additions

図３．符号理論に基づくユーザ認証プロトコルの性能比較

(4) マルチレシーバー・マルチメッセージ認証符号に基づいた rushing 不正者を検知可能な秘密分散法を構築した。本構築は同タイプの手法の中で現在最小シェアサイズを実現できるものとなる。我々の研究チームの本論文は International Workshop on Information Security (IWSEC) 2014 で発表し、最優秀学生論文賞を受賞した。

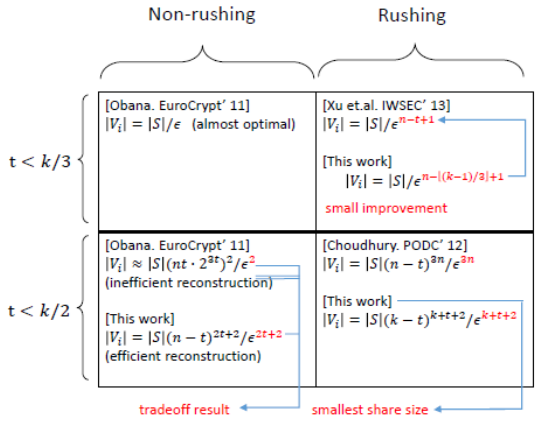

図４．不正者を検知可能な秘密分散法のシェアサイズ比較

(5) 新たな robust 秘密分散法を構築した。Carpentieri の手法を用いて、Cevallos その他の Eurocrypt 2012 からの robust 秘密分散法のシェアサイズは定数因子により改善した。

(6) 新たなシェア再配（share redistribution）プロトコルを発明した。本プロトコルは n 参加者の中に t 能動的な攻撃者あり、n>3t の際、情報理論的な（perfect）安全性がある。Shamir 秘密分散法の特定の場合では、新たなリード・ソロモン符号の復号問題を定式化したと（非効率的な）復号アルゴリズムを提案した。

(7) Harn と Lin らと（Design Codes and Cryptography, 2009）、Harn で（IET Information Security, 2014）提案された不正者を検知可能な秘密分散法の解析を行った。2009 のプロトコルの安全性証明に対して色々な反例を示して、2014 のプロトコル安全性証明は不正確であることを示した。

(8) McEliece 公開鍵暗号方式を用いて、符号理論に基づく決定的暗号化（deterministic encryption）と効率的探索可能な暗号化（efficiently searchable encryption）を構築した。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 10 件）

① Rui Xu, Kirill Morozov, Tsuyoshi Takagi, Cryptanalysis of Some Recent Cheater Identifiable Secret Sharing Schemes, 査読有, Vol. E98-A, No. 8, 2015, 印刷中.

② Yvo Desmedt, Kirill Morozov, Parity Check Based Redistribution of Secret Shares, 2015 IEEE International Symposium on Information Theory (ISIT), 査読有, 2015, 印刷中.

③ Yang Cui, Kirill Morozov, Kazukuni Kobara, Hideki Imai, Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE, International Journal of Network Security, 査読有, Vol. 16, No. 1, 2014, pp. 19-28.
http://ijns.femto.com.tw/contents/ijns-v16-n1/ijns-2014-v16-n1-p19-28.pdf

④ Partha Sarathi Roy, Avishek Adhikari, Rui Xu, Kirill Morozov, Kouichi Sakurai, An Efficient Robust Secret Sharing Scheme with Optimal Cheater Resiliency, 4th International Conference on Security, Privacy and Applied Cryptographic Engineering, SPACE 2014, 査読有, LNCS 8804, 2014, pp. 47-58.
DOI: 10.1007/978-3-319-12060-7_4

⑤ Rui Xu, Kirill Morozov, Tsuyoshi Takagi, Cheater Identifiable Secret Sharing Schemes Via Multi-Receiver Authentication, 9th International Workshop on Security, IWSEC 2014, 査読有, LNCS 8639, 2014, pp. 72-87.
最優秀学生論文賞
DOI: 10.1007/978-3-319-09843-2_6

⑥ Rong Hu, Kirill Morozov, Rui Zhang, Tsuyoshi Takagi, Confirmer Signatures from McEliece Assumptions (Extended Abstract), 31st Symposium on Cryptography and Information Security, SCIS 2014, 査読なし, 2014, 5 pages.

⑦ Rui Xu, Kirill Morozov, Tsuyoshi Takagi, On Cheater Identifiable Secret Sharing Schemes Secure Against Rushing Adversary, 8th International Workshop on Security, IWSEC 2013, 査読有, LNCS 8231, 2013, pp. 258-271.
DOI: 10.1007/978-3-319-09843-2_6

⑧ Rong Hu, Kirill Morozov, Tsuyoshi Takagi, On Zero-Knowledge Identification Based on q-ary Syndrome Decoding", 8th Asia Joint Conference on Information Security, AsiaJCIS 2013, 査読有, 2013, pp. 12-18.
DOI: 10.1109/ASIAJCIS.2013.10

⑨ Rong Hu, Kirill Morozov, Tsuyoshi Takagi, Proof of Plaintext Knowledge for Code-Based Public-Key Encryption Revisited (Short paper), 8th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2013, 査読有, 2013, pp. 535-540.
DOI: 10.1145/2484313.2484385

⑩ Kirill Morozov and Tsuyoshi Takagi, Zero-Knowledge Protocols for the McEliece Encryption, 17th Australasian Conference on Information Security and Privacy, ACISP 2012, 査読有, LNCS 7372, 2012, pp. 180-193.
DOI: 10.1007/978-3-642-31448-3_14

〔学会発表〕(計5件)

① Kirill Morozov, Zero-Knowledge Protocols for Code-Based Public-Key Encryption, Seminar of Department of Mathematics, 講演, 2015年1月12日, Seoul National University, Seoul, Korea.

② Kirill Morozov, Verifiable Code-Based Encryption, Dagstuhl Seminar 13371 "Quantum Cryptanalysis" (招待者のみ), 講演, 2013年9月10日, Leibniz Center for Informatics, Saarland, Germany.

③ Kirill Morozov, Secret Sharing, Proof of Plaintext Knowledge, and Their Applications to Secure Cloud Storage, 2013 International Symposium on Data Security and Identity Privacy in Cloud Computing (DSIP2013), 招待講演, 2013年5月6日, Hubei University of Technology, Wuhan, China.

④ Kirill Morozov, Zero-Knowledge Protocols for Code-Based Encryption, State Key Laboratory Of Information Security (SKLOIS) Seminar, 招待講演, 2012年9月20日, Chinese Academy of Sciences, Beijing, China.

⑤ Kirill Morozov, Zero-Knowledge Identification Protocols from Coding, State Key Laboratory Of Information Security (SKLOIS) Seminar, 招待講演, 2012年9月20日, Chinese Academy of Sciences, Beijing, China.

〔図書〕(計1件)

① Kirill Morozov, Code-Based Public-Key Encryption, Section of the book Ryuei Nishii et al. (eds.), "A Mathematical Approach to Research Problems of Science and Technology - Theoretical Basis and Developments in Mathematical Modeling", Mathematics for Industry, vol. 5, Springer, 2014, pp. 47-56.

〔その他〕

ホームページ：
http://imi.kyushu-u.ac.jp/~morozov/

Google Scholarのプロフィール：
https://scholar.google.co.jp/citations?user=NcYfeG4AAAAJ

DBLPページ：
http://dblp.uni-trier.de/pers/hd/m/Morozov:Kirill

６．研究組織
(1)研究代表者

モロゾフ　キリル　(MOROZOV　KIRILL)
九州大学マス・フォア・インダストリ研究所
助教
研究者番号：80443232