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　 ９ 日現在

機関番号：１２６０８
研究種目：基盤研究(C)
研究期間：2011～2014
課題番号：２３５０００１０

研究課題名（和文）ゲーム理論にもとづく暗号プロトコル

研究課題名（英文）Game Theoretic Studies on Cryptographic Protocols

研究代表者
田中　圭介（Tanaka, Keisuke）

東京工業大学・情報理工学（系）研究科・准教授

研究者番号：２０３３４５１８

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：大きく分けて二つの成果が得られた。まず、2メッセージを用いた紛失通信についての考察である。 具体的には、攻撃者のモデルをプロトコルの実行を途中で中止させるだけのfail-stopモデルからプロトコル中のアルゴリズムを任意に変更する攻撃を許すmaliciousモデルへの拡張を行い、既存のある種の暗号理論的な安全性と等価なゲーム理論的安全性を与えることに成功している。
さらに、ビットコミットメントについての考察である。具体的には、malicious モデルの攻撃者を対象とし、既存のある種の暗号理論的な安全性と密接に関連するゲーム理論的安全性を与えることに成功している。

研究成果の概要（英文）：We characterize the properties of two-message oblivious transfer protocols by using a game-theoretic concept. Specifically, we present a single two-player game for two-message oblivious transfer in the game-theoretic framework, where it captures the cryptographic properties of correctness and privacy in the presence of malicious adversaries.
In addition we also focus on bit commitment, and study it from a perspective of game theory. In a similar manner to the work on oblivious transfer, we consider bit commitment in the malicious model. In order to naturally capture the security properties of bit commitment, we characterize them with a single game where both parties are rational. In particular, we define a security notion from a game theoretic viewpoint, and prove the equivalence between it and the standard security notion.

研究分野：暗号理論

キーワード：暗号理論　プロトコル　ゲーム理論　安全性

１．研究開始当初の背景

(1) ゲーム理論と暗号プロトコル

従来の暗号理論において、プロトコルの参加者は基本的に、正直者か攻撃者かのどちらかであると考えられてきた。

例えば、紛失通信などの、双方が秘密情報をもつ二者間の暗号プロトコルを考える。まず、一方の参加者 A が正直者で暗号プロトコルの記述に完全に従うと仮定したとき、もう一方の参加者 B が攻撃者となり可能な限りの手段によって攻撃可能であるかについての安全性を考察する。次に、逆の状況を考える。すなわち、参加者 B が正直者で暗号プロトコルの記述に完全に従うと仮定したとき、参加者 A が攻撃者となり可能な限りの手段によって攻撃可能であるかについての安全性を考察する。どちらの安全性も満たされるときに、この暗号プロトコルは安全性を満たすという。

しかしながら、このような設定は現実的とは必ずしもいえない。現実世界を考えたとき、攻撃者も暗号プロトコルの安全性を破るためには計算コストがかかったり不正が発覚したりなどのリスクがある。そのため、攻撃によって得られる情報がリスクに見合わない場合、攻撃するとは考えにくい。また、正直者も、与えられた暗号プロトコルの記述に常に完全に従うとは考えにくく、自分にとって不利にならなければ、プロトコルの記述の一部に(複雑な乱数生成処理を省くなどして)従わないかもしれない。つまり、正直者と攻撃者という分け方は、参加者を極端に分類していると考えられる。

そこで、2004 年に Halpern と Teague により、参加者がある種の合理性に従って行動するもとでの暗号プロトコルの安全性はどのように変化するかについての考察、すなわち、ゲーム理論と暗号プロトコルの研究がはじめられた。

(2) 国内・国外の研究動向

2004 年に Halpern と Teague によって考察対象となった暗号プロトコルは秘密分散だった。この研究の後、毎年論文は 2-3 本程度発表されている状況であるが、ほぼすべての論文は、はじめに考察された秘密分散を対象としており、他の暗号プロトコルには余り発展していない状況である。ただし、まったくないわけではなく、リーダー選出問題を対象とした Gradwohl の研究や、真鍋と岡本によるケーキ・カット問題の研究など成功している例もある。

この分野の国外の研究者は、アメリカやヨーロッパに少なからずいる。この分野は今後大きく発展する可能性があるにもかかわらず、国内の研究者は極端に少ない状況である。国際会議や研究会等を通して我々が知る限り、我々を含む研究グループ以外には、NTT/京都大学の真鍋、岡本のグループしかいない。

(3) 参考文献

-J. Halpern, V. Teague, Rational Secret Sharing and Multiparty Computation, STOC 2004.
-R. Gradwohl, Rationality in the Full-Information Model, TCC 2010.
-真鍋 義文, 岡本 龍明, Cryptographic Cake-Cutting Protocols, SCIS2010.

２．研究の目的

研究代表者の田中は、それまで主に行っていた通常の公開鍵暗号システムの研究に加え、2008 年頃から、本研究に関連するゲーム理論にもとづく秘密分散の研究を始めた。

これまでの研究対象は秘密分散であったが、既存の研究とは異なる特徴をもつ研究を行ってきた。秘密分散の機能の拡張や、数論問題に関する複雑さの仮定の導入、ランダムオラクルの導入である。このなかでも、秘密分散の機能の拡張に関する研究は、対象として秘密分散以外を扱うという、本研究の大きなきっかけとなるものだった。

研究分担者の安永も、田中と同じ時期から、それまで主に行っていた符号理論の研究に加え、ゲーム理論にもとづく暗号プロトコルの研究を始めた。

そこで、同じ研究興味をもった田中と安永は、本研究の内容に関して頻繁に議論をもつようになりそのなかで、秘密分散以外の暗号プロトコルがほとんど対象となっていない状況に疑問をもつようになった。特に、基本的な暗号プロトコルである、公開鍵暗号や、電子署名、相手認証などが対象でないことに疑問をもつようになった。

このように、秘密分散以外、特に、基本的な暗号プロトコルである、公開鍵暗号や、電子署名、相手認証などを対象にゲーム理論的考察を行うことが本研究の目的である。

３．研究の方法

本研究では研究期間 4 年を三つのフェーズに分ける。

第 1 フェーズ (H23): 秘密分散に適したモデルとプロトコルの調査および設計
第 2 フェーズ (H24,25): 公開鍵暗号および電子署名に適したモデルとプロトコルの設計
第 3 フェーズ (H26): 他の基本的なプロトコルを対象としたモデルとプロトコルの設計

各々のフェーズにおいては、各々のプロトコルに対して、1)モデル設計　2) アルゴリズム設計　3) 行動解析　4) 安全性・効率解析 といった、フィードバックを適宜含むよ

うなおおまかな流れで研究をすすめる。また、本研究が計画どおりに進まない場合は、海外研究者、企業研究者を含む研究協力者を活用して情報収集および議論を行うことにより問題解決を行う。

４．研究成果

本研究の目的は、秘密分散以外、特に、基本的な暗号プロトコルである、公開鍵暗号や、電子署名、相手認証などを対象にゲーム理論的考察を行うことが本研究の目的である。

本研究では、紛失通信およびビットコミットメントと呼ばれる基本的な暗号プロトコルに対してゲーム理論的考察を行うことに成功した。

(1) Asharov, Canetti, Hazay は Eurocrypt 2011 において、暗号プロトコルの正しさ、秘匿性、公平性を fail-stop モデルという枠組みで考察していた。本研究では、彼らの研究で考察された枠組みを拡張する形で、2 メッセージを用いた紛失通信についての考察を行った。具体的には、攻撃者のモデルをプロトコルの実行を途中で中止させるだけの fail-stop モデルからプロトコル中のアルゴリズムを任意に変更することのできる攻撃を許すような malicious モデルへの拡張を行い、既存の暗号理論的な安全性と等価なゲーム理論的安全性を与えることに成功している。この成果は、Higo, Tanaka, Yamada, Yasunaga: A Game-Theoretic Perspective on Oblivious Transfer, The 17th Australasian Conference on Information Security and Privacy として、国際会議に採択され、発表を行っている。

(2) (1)の研究成果をさらに拡張する形で、ビットコミットメントと呼ばれる重要な基本暗号プロトコルを対象に考察を行うことに成功した。具体的には、ビットコミットメントに対して malicious モデルの攻撃者を対象とし、既存の暗号理論的な安全性と密接に関連するゲーム理論的安全性を与えることに成功している。この成果は、Higo, Tanaka, Yasunaga: Game-Theoretic Security for Bit Commitment, The 8th International Workshop on Security として、国際会議に採択され発表を行っている。

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 8 件）

① Eiichiro Fujisaki, Akinori Kawachi, Ryo Nishimaki, Keisuke Tanaka, Kenji Yasunaga: Post-Challenge Leakage Resilient Public-Key Cryptosystem in Split State Model, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 98-A(3). 853-862 (2015), 査読有, http://search.ieice.org/bin/summary.php?id=e98-a_3_853

② Hitoshi Namiki, Keisuke Tanaka, Kenji Yasunaga: Randomness Leakage in the KEM/DEM Framework, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 97-A(1). 191-199 (2014), 査読有, http://search.ieice.org/bin/summary.php?id=e97-a_1_191

③ Manh Ha Nguyen, Kenji Yasunaga, Keisuke Tanaka: Leakage-Resilience of Stateless/Stateful Public-Key Encryption from Hash Proofs, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E96-A. 1100-1111 (2013), 査読有, http://search.ieice.org/bin/summary.php?id=e96-a_6_1100

④ Tatsuya Akutsu, Daiji Fukagawa, Magnus M. Halldorsson, Atsuhiro Takasu, Keisuke Tanaka: Approximation and parameterized algorithms for common subtrees and edit distance between unordered trees, Theoretical Computer Science 470. 10-22 (2013), 査読有, doi:10.1016/j.tcs.2012.11.017

⑤ Ryo Nishimaki, Eiichiro Fujisaki, Keisuke Tanaka: A Multi-Trapdoor Commitment Scheme from the RSA Assumption, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 95-A (1). 176-184 (2012), 査読有, http://search.ieice.org/bin/summary.php?id=e95-a_1_176

⑥ Ryo Nishimaki, Eiichiro Fujisaki, Keisuke Tanaka: An Efficient Non-interactive Universally Composable String-Commitment Scheme, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 95-A (1). 167-175 (2012), 査読有, http://search.ieice.org/bin/summary.php?id=e95-a_1_167

⑦ Mario Larangeira, Keisuke Tanaka: Programmability in the Generic Ring and Group Models, Journal of Internet Services and Information Security 1 (2/3). 57-73

(2011), 査読有,
http://www.jisis.org/vol1no23.php

⑧ Christopher Portmann, Keisuke Tanaka: Information-theoretic secrecy with access to decryption oracles, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 94-A (7). 1585-1590 (2011), 査読有,
http://search.ieice.org/bin/summary.php?id=e94-a_7_1585

〔学会発表〕(計 20 件)

① Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka: Completeness of single-bit projection-KDM security for public key encryption, RSA Conference Cryptographer's Track 2015 (CT-RSA 2015), 2015 年 4 月 20 日, San Francisco (USA)

② Ai Ishida, Keita Emura, Goichiro Hanaoka, Yusuke Sakai, Keisuke Tanaka: Disavowable Public Key Encryption with Non-interactive Opening, 10th ACM Symposium Information Computer and Communications Security 2015 (ASIACCS 2015), 2015 年 4 月 14 日, Singapore

③ Ta Minh Thanh, Keisuke Tanaka: Blind watermarking using QIM and the quantized SVD domain based on the q-logarithm function, Proceeding of the 10th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISAPP), ISI Conference, 2015 年 3 月 11 日, Berlin (Germany)

④ Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka: Efficient key dependent message security amplification against chosen ciphertext attacks, Information Security and Cryptology 2014 (ICISC 2014), 2014 年 12 月 3 日, Seoul (Korea)

⑤ Yuyu Wang, Keisuke Tanaka: Generic Transformation to Strongly Existentially Unforgeable Signature Schemes with Leakage Resiliency, Provable Security (ProvSec 2014), 2014 年 10 月 9 日, Hong Kong

⑥ Ta Minh Thanh, Keisuke Tanaka: A proposal of novel q-DWT for blind and robust image watermarking, Proceeding of IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2014), 2014 年 8 月 30 日, Washington DC (USA)

⑦ Yuyu Wang, Keisuke Tanaka: Strongly Simulation-Extractable Leakage-Resilient NIZK, Information Security and Privacy 19th Australasian Conference (ACISP 2014), 2014 年 7 月 7 日, Wollongong (Australia)

⑧ Toshiyuki Isshiki, Manh Ha Nguyen, Keisuke Tanaka: Attacks to the Proxy Re-Encryption Schemes from IWSEC2011, 8th International Workshop on Security (IWSEC2013), 2013 年 11 月 18 日, Okinawaken Shichouson Jichikaikan, Okinawa (Japan)

⑨ Haruna Higo, Keisuke Tanaka, Kenji Yasunaga: Game-Theoretic Security for Bit Commitment, 8th International Workshop on Security (IWSEC2013), 2013 年 11 月 18 日, Okinawaken Shichouson Jichikaikan, Okinawa (Japan)

⑩ Toshiyuki Isshiki, Manh Ha Nguyen, Keisuke Tanaka: Factoring-Based Proxy Re-Encryption Schemes, 7th International Conference on Provable Security (Provsec2013), 2013 年 10 月 23 日, Casa del Rio Hotel, Melaka (Malaysia)

⑪ Hirotoshi Takebe, Keisuke Tanaka: Grey-Box Public-Key Steganography, 10th Annual Conference on Theory and Applications of Models of Computation (TAMC2013), 2013 年 5 月 20 日, The University of Hong Kong (Hong Kong)

⑫ Toshiyuki Isshiki, Manh Ha Nguyen, Keisuke Tanaka: Proxy Re-Encryption in a Stronger Security Model Extended from CT-RSA2012, Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, 2013 年 2 月 25 日, San Francisco (USA)

⑬ Akinori Kawachi, Hirotoshi Takebe, Keisuke Tanaka: Symmetric-Key Encryption Scheme with Multi-ciphertext Non-malleability, 7th International Workshop on Security, IWSEC2012, 2012 年 11 月 7 日, Fukuoka (Japan)

⑭ Mario Larangeira, Keisuke Tanaka: Reduction-Centric Non-programmable Security Proof for the Full Domain Hash in the Random Oracle Model, 13th International Workshop on Information Security Applications, WISA2012, 2012 年 8 月 16 日, Jeju Island (Korea)

⑮ Haruna Higo, Keisuke Tanaka, Akihiro Yamada, Kenji Yasunaga: "A Game-Theoretic Perspective on Oblivious Transfer" 17th Australasian Conference on Information Security and Privacy (ACISP 2012) , 2012年7月9日, Wollongong (Australia)

⑯ Manh Ha Nguyen, Keisuke Tanaka, Kenji Yasunaga: Leakage-Resilience of Stateless/Stateful Public-Key Encryption from Hash Proofs, 17th Australasian Conference on Information Security and Privacy (ACISP 2012), 2012年7月9日, Wollongong (Australia)

⑰ Hitoshi Namiki, Keisuke Tanaka, Kenji Yasunaga: Randomness Leakage in the KEM/DEM Framework, 5th International Conference on Provable Security - ProvSec 2011, 2011年8月17日, Xi'an Tang Cheng Hotel, 西安 (中国)

⑱ Keisuke Tanaka, Akihiro Yamada, Kenji Yasunaga: Weak Oblivious Transfer from Strong One-Way Functions, 5th International Conference on Provable Security - ProvSec 2011, 2011年8月16日, Xi'an Tang Cheng Hotel, 西安 (中国)

⑲ Manh Ha Nguyen, Keisuke Tanaka, Kenji Yasunaga: Leakage-Resilient CCA2 Public-Key Encryption from 4-wise independent hash functions, 2011 International Conference on Advanced Technologies for Communications - ATC 2011, 2011年8月2日, Da Nang University of Technology, Da Nang (ベトナム)

⑳ Akinori Kawachi, Christopher Portmann, Keisuke Tanaka: Characterization of the Relations between Information-Theoretic Non-malleability, Secrecy, and Authenticity, 5th International Conference on Information Theoretic Security- ICITS 2011, 2011年5月22日, CWI, アムステルダム (オランダ)

〔図書〕(計0件)

〔産業財産権〕
○出願状況(計0件)

○取得状況(計0件)

〔その他〕
特になし

６．研究組織
(1)研究代表者
田中 圭介 (TANAKA, Keisuke)
東京工業大学・大学院情報理工学研究科・准教授
研究者番号：20334518

(2)研究分担者
安永 憲司 (YASUNAGA, Kenji)
金沢大学・電子情報学系・助教
研究者番号：50510004