様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 6 月 6 日現在

機関番号：１２６０１
研究種目：若手研究(B)
研究期間：2009～2011
課題番号：２１７６０２７５
研究課題名（和文）　選択暗号文攻撃に対して安全な公開鍵暗号の一般的構成法とその意義付け
研究課題名（英文）　Generic Constructions of CCA-Secure Public-Key Encryption Schemes and Their Significance Evaluation
研究代表者
松浦　幹太　（MATSUURA　KANTA）
東京大学・生産技術研究所・准教授
研究者番号：00292756

研究成果の概要（和文）：CPA 安全という弱い安全性しか持たない部品を用いて CCA 安全という強い安全性を持つ公開鍵暗号を一般的に構成できるか否かを論じるために、攻撃者モデルを拡張した。拡張したモデルに基づいて、CPA から CCA へ至る途上にある安全性を体系的に定義し、それらのいくつかを達成する一般的構成法を示した。また、これら一般的構成法の意義を経済学的に論じるモデルを応用し、暗号モジュール選択の指針となる枠組みを提示した。

研究成果の概要（英文）：In order to discuss the possibility of generic constructions of CCA-secure public-key encryption schemes from CPA-secure schemes, we extended adversary models. Based on the extended models, we defined intermediate securities between CPA and CCA, and presented some corresponding particular generic constructions. In addition, by using an economic model which can interpret the significance of such schemes, we proposed a framework of choosing cryptographic modules.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	800,000	240,000	1,040,000
２０１０年度	1,200,000	360,000	1,560,000
２０１１年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,000,000	900,000	3,900,000

研究分野：工学
科研費の分科・細目：電気電子工学、通信・ネットワーク工学
キーワード：暗号・セキュリティ

１．研究開始当初の背景

安全な情報通信環境を中長期的に維持発展させるためには、将来を見越しても現実的な仮定のもとで安全性の高い技術を、できるだけ自由に構築できることが望ましい。さらに、その成果が死の谷に埋もれぬよう、政策や経済の視点からも意義付けできれば、なお好ましい。

(1) まず、公開鍵暗号の技術分野では、選択暗号文攻撃に対して識別不可能性を確保する安全性(IND-CCA2、あるいは文脈から明らかな場合には短縮して単に CCA 安全性と呼ばれる)という強い安全性を、弱い安全性しかもたないが構成容易な方式(CPA 安全な方式)から構成できることが望ましい。とりわけ、ランダムオラクルに頼らないという意味で現実的な方式を効率的かつ一般的に構成できれば、インパクトが大きい。よって、そのような一般的構成法の可能性や不可能性を論じる問題が、当該分野において重要な未解

決問題と認識されていた。実際、本研究を開始した当初は、非対話型ゼロ知識証明という非効率的な要素技術を利用すれば一般的構成法を示すことができるけれども、効率的な要素技術の利用しか許さないという制限を付ければ素因数分解問題のように具体的な数論的問題に頼る必要がある（すなわち一般的構成法とはならない）という状況であった。
(2) 一方、政策や経済など社会科学的な視点から技術を意義付ける研究は、2002 年頃に形成されたセキュリティ経済学のコミュニティで行われてきた。本研究開始当初、強い安全性のもたらす防御力の意義を解釈するモデルに関しては理論研究と実証研究がともに存在するものの、攻撃抑止力や設計自由度の意義も解釈できるモデルに関しては基礎理論が提示されているだけであって、理論の成熟が見られず実証や応用などの実践的な研究に至っていない状況であった。

２．研究の目的
本研究では、ランダムオラクルに頼らず CCA 安全な公開鍵暗号の一般的構成法を示す（またはその不可能性や条件付き不可能性を示す）とともに、その経済学的意義を明らかにする実践的な成果をあげることを目的とした。
(1) 具体的には、技術研究では、安全性証明が容易で既に多く知られている CPA 安全な公開鍵暗号や同程度の安全性仮定といえる技術を構成要素とし CCA 安全な公開鍵暗号を構成する方法を目指すこととした。ただし、一つの可能性として、そもそも構成不可能な場合がある。したがって、本研究では、構成可能かどうかを含めて明らかにすることを目的とした。また、条件付きの構成可能性など、研究の柔軟な展開も考慮した計画としていた。
(2) 経済学的研究では、完全に新しいモデルに取り組むのではなく、研究代表者が既に考案していた基礎的なモデルを発展させて実践的に応用することを目的とした。

３．研究の方法
(1) 技術研究に関しては、①事前調査で有望と思われていたタグベース暗号という要素技術に着目して構成可能性を検討する理論研究から着手した。さらに、公開鍵暗号分野で近年盛んに研究されている様々な機能的暗号（秘匿以外の付加的な機能を実現する暗号）の一般的構成法を安全性モデルの体系化にまで踏み込んで研究することによって、本研究の主題である重要な未解決問題解決に役立つ知見等を一つ一つ蓄積させていった。そして、これら①の成果に基づいて、②主題における安全性モデルの体系化を行い、主題に一定の答えを与えるという、段階的な研究方法を採用した。
(2) 経済学的研究に関しては、基礎的なモデルにおいて、パラメータの変化に応じた特性変化を調べる感度分析を行い、研究目的に合う応用を試みるという方法を採用した。

４．研究成果
(1) ①技術研究の第一段階では、時間に基づいた開封制御機能を持つ暗号技術や、認証を伴う暗号技術の一般的構成法に関して、従来よりも高度な安全性モデルを構築した上で実際に構成法を示すという成果をあげた。それらの開発過程から得た知見に基づいて、本研究の主題へ取り組む上では、攻撃者に許される予備行為の順序や並行性を体系化した上で安全性モデル（図１）を構築することが有効であるという結論を得た。識別不可能性は、図１で「チャレンジャーが２つの平文 m_0 と m_1 からランダムに一方を選んで暗号化した暗号文を得た攻撃者が、どちらの平文が選ばれたかを推測し言い当てるという識別ゲームに、５０％よりも有意に高い確率で勝つことができない」という安全性である。図１において、最後の通信が、推測を伝える通信に相当する。
我々の提案したモデルでは、攻撃者が行う予備行為（図１における Phase1 と Phase2）を、単に CCA として捉えるのではなく、複数の問い合わせパターンの順序や並行性に着目して分類し、体系化した。モデルは、問い合わせの回数制限次第で、CPA から CCA に至る中間的な安全性に関して豊かな表現力を獲得することができる。したがって、たとえ CCA に到達できない場合でも、その途上のどこまで到達できるかを詳しく調べることが可能となる。

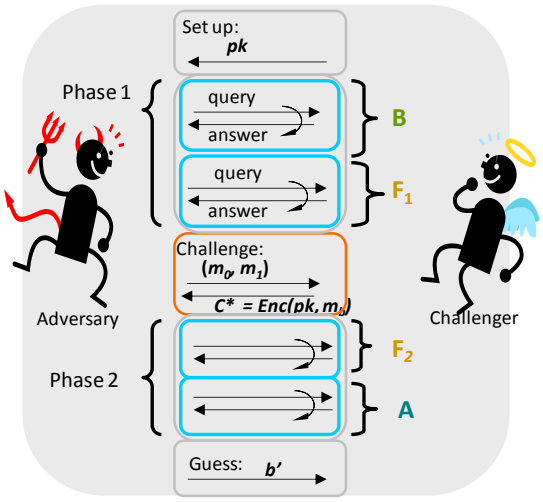

図１．体系化した CCA 安全性モデル

②技術研究の第二段階では、第一段階の結論に基づき、単一型と並行型の復号クエリを考慮した回数制限付き選択暗号文攻撃に対する安全性定義間の関係を明らかにした。さらに、構築した理論体系でもっとも CCA 安全性に近づいた一般的構成法を具体的に示すことに成功した。これらの成果は、暗号理論分野で一流と見なされている国際会議に採択された。国内学会においても、学生の発表が学生賞ではなく一般の賞を２件受賞するなどの高評価を得た。

(2) ①経済学的研究では、理論的な感度分析において、攻撃抑止力や設計自由度の意義も踏まえた適切な技術利用をした場合には利用者のセキュリティ投資行動を二種類に分類できることを詳細に示した。この知見に基づいて、暗号モジュールを選択する際に指針となる枠組みを構築した。具体的には、経験に基づいて選択した候補の妥当性を理論モデルで評価検証するという「Trust-Verify」サイクルを構築し、その利用ガイドラインを開発し公開した（図２）。

ガイドラインで定めた手順は以下の通りである。まず、事前に定めたコスト構造とリスク構造のもとで具体的なパラメータの値を経験的手法でアセスメントし、いったん結果を信用する(Trust)。その結果に基づいて暗号モジュールを取捨選択し、選ばれたモジュールに関する「コスト対リスクスコア」のプロット（図２の○印）とともに、選ばれたモジュールのリスクスコアに対して許容できるコストをプロットする（図２の×印)。システム設計を暫定的に終えた段階で、それまでの選択結果の集合がセキュリティ投資理論に矛盾するかしないかすなわち最適投資理論整合性を検証する(Verify)。検証結果が矛盾と出た場合には、構造定義またはアセスメントに立ち戻って再設計を行う。我々のケーススタディでは、アメリカ合衆国の国立標準技術研究所（NIST: National Institute of Standards and Technology)が運営している暗号モジュール評価認証制度（CMVP: Cryptographic Module Validation Program）における評価認証データを利用して、リスクスコアを評価した。

以上の手順は、製品認証制度が確立されているなどの理由でコスト構造とリスク構造を構築しやすい（あるいはパラメータのアセスメントを行いやすい）場合ほど、適用が容易である。

これらの成果は、情報セキュリティ経済学が比較的若い分野であることから注目度も高く、国内外で 3 件の招待講演につながった。また、図書や解説記事においても、本研究の基礎となったモデルを様々な形で取り上げ、若い分野の普及啓蒙に努めた。

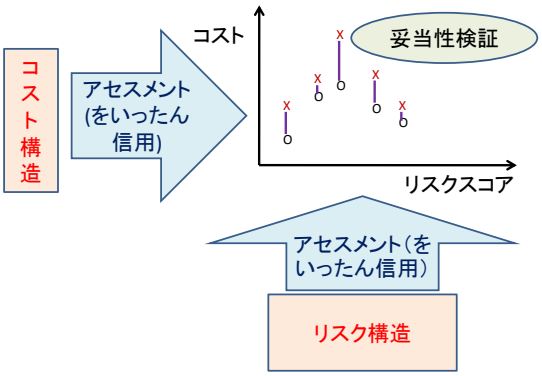

図２．暗号モジュール選択の枠組み

②さらに、研究を実施する中で実証的な感度分析の重要性が明らかとなったため、実際のセキュリティ投資データと産業連関表を用いた実証的な感度分析を行い、研究計画では予期していなかった知見も獲得した。

感度分析は、サプライチェーンにおける後方依存性の考え方に基づいた分析手法を独自にアレンジしたものである。経済学では、供給側のトラブルで産業連関表の特定の行が破壊された（取引額がゼロになった）場合に、着目している需要側のセクタ（産業分野）あるいは地域が受ける影響を総生産の減少で計量する理論がある。我々は、供給側の IT 事故などの影響が取引額減少となって現れるけれども取引額は必ずしもゼロにはならないと考え、減少の程度が製品認証された暗号モジュールなどの情報セキュリティ対策を高めれば高めるほど軽微になるというモデルを用いた。また、広域の自然災害のように供給側と需要側双方に大きな影響を与えるリスクの影響についても、東日本大震災を事例として取り上げ、同様の感度分析を行った。すなわち、高度なセキュリティ対策の意義を、セクタや地域の総生産への影響という観点で分析した。

具体的に得られた知見のうちで重要なものは、次のようにまとめられる。まず、東日本大震災のように予期せぬ大きなインパクトに直面した場合には、災害前に自己依存性（攻撃等を受けた影響が同じ地域や同じ産業分野の総生産に大きく現れる性質）を持つ地域や産業分野において、より緻密な事後投資計画が必要となることが示唆された。さらに、詳細な知見を求める場合、産業分野だけでなく地域にも同時に着目して詳細な分析を行うことが有効であることが分かった。これらは、今後、情報セキュリティ経済学分野における他の実証研究にも波及効果を与える知見である。例えば、研究開発投資の相互依存性を実証分析する際などに有効と期待される。

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 10 件）

①Takahiro Matsuda, Goichiro Hanaoka, and Kanta Matsuura: “Relations between Constrained and Bounded Chosen Ciphertext Security for Key Encapsulation Mechanisms,” Lecture Notes in Computer Science 7293, pp.576-594, Springer, 2012.（査読有り）
②Daiki Chiba, Takahiro Matsuda, Jacob C. N. Schuldt, and Kanta Matsuura: “Efficient Generic Constructions of Signcryption with Insider Security in the Multi-user Setting,” Lecture Notes in Computer Science 6715, pp.220-237, Springer, 2011.（査読有り）
③Takahiro Matsuda and Kanta Matsuura: “Parallel Decryption Queries in Bounded Chosen Ciphertext Attacks,” Lecture Notes in Computer Science 6571, pp.246-264, Springer, 2011.（査読有り）
④ Bongkot Jenjarrussakul and Kanta Matsuura: “A Survey on Information Security Economics,” 日本セキュリティ・マネジメント学会誌, Vol.24, No.3, pp.53-60, 2011.（解説記事）
⑤Takahiro Matsuda, Yasumasa Nakai, and Kanta Matsuura: “Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability,” Lecture Notes in Computer Science 6487, pp.225-245, Springer, 2010.（査読有り）
⑥Takahiro Matsuda, Kanta Matsuura, and Jacob C. N. Schuldt: “Efficient Construction of Signcryption Schemes and Signcryption Composability,” Lecture Notes in Computer Science 5922, pp.321-342, Springer, 2009.（査読有り）
⑦ Yasumasa Nakai, Takahiro Matsuda, Wataru Kitada, and Kanta Matsuura: “A Generic Construction of Timed-Release Encryption with Pre-open Capability,” Lecture Notes in Computer Science 5824, pp.53-70, Springer, 2009.（査読有り）

〔学会発表〕（計 19 件）
①Bongkot Jenjarrussakul, Hideyuki Tanaka, and Kanta Matsuura: “Sectoral and Regional Interdependency of Japanese Firms under the Influence of Information Security Risks,” The Eleventh Annual Workshop on the Economics of Information Security (WEIS2012), 2012 年 6 月 25 日発表予定（ベルリン、ドイツ）
②Bongkot Jenjarrussakul, Hideyuki Tanaka, and Kanta Matsuura: “Impact on Information Security from the Great East Japan Earthquake on March 11, 2011,” Eighth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective, College Park, MD, USA, January 18, 2012.
③松田隆宏, 松浦幹太: “単一型と並行型の復号クエリを考慮した回数制限付き選択暗号文攻撃に対する安全性定義間の関係,” 2011 年暗号と情報セキュリティシンポジウム(SCIS2011), 2011 年 1 月 26 日 （福岡県小倉市）.
④松田隆宏, 花岡悟一郎, 松浦幹太: “KEM の Constrained CCA 安全性と回数制限付き CCA 安全性の関係,” 2011 年暗号と情報セキュリティシンポジウム(SCIS2011), 2011 年 1 月 26 日 （福岡県小倉市）.
⑤Kanta Matsuura: “Security Economics and Cryptographic Industry,” 2010 Japan-Taiwan Joint Research Symposium on Cryptography and Information Technology toward Next IT-society, Kaohsiung, Taiwan, November 16, 2010. (invited speakers only)
⑥ Kanta Matsuura: “A Guideline for Product-Validation Systems Regarding Security Modules,” Computer Security Institute (CSI) Annual Conference 2010, Washington D.C., USA, October 28, 2010.
⑦松田隆宏, 松浦幹太: “開封時刻の秘匿性を持つ事前開封機能付きタイムリリース暗号の一般的な構成法,” 情報処理学会コンピュータセキュリティシンポジウム 2010(CSS2010), 2010 年 10 月 21 日 （岡山県岡山市）(優秀論文賞受賞)
⑧松浦幹太: “情報セキュリティ経済学の概要と最近の動向,” 日本セキュリティマネジメント学会 2010 年度第２回 IT リスク学研究会, 2010 年 9 月 18 日 （東京都千代田区）（招待講演）
⑨Kanta Matsuura: “Economic Implications of Light-Weight Security Mechanisms,” The 2010 Workshop on RFID Security, Singapore, February 22, 2010. (invited talk)
⑩松田隆宏, 松浦幹太: “公開鍵暗号の回数制限付き選択暗号文攻撃に対する安全性,” 2010 年暗号と情報セキュリティシンポジウム(SCIS2010), 2010 年 1 月 22 日 （香川県高松市）
⑪松田隆宏, 松浦幹太: “Mixed CCA 安全性: より強い安全性を持つ公開鍵暗号方式の CPA 安全な方式のみを用いた構成,” 2010 年暗号と情報セキュリティシンポジウム

(SCIS2010), 2010 年 1 月 22 日 （香川県高松市）
⑫松田隆宏, シュルツ ヤコブ, 松浦幹太: “多人数環境を考慮した Signcryption の簡潔な一般的構成法,” 情報処理学会コンピュータセキュリティシンポジウム 2009(CSS2009), 2009 年 10 月 27 日 （富山県富山市）（優秀論文賞受賞）
⑬Kanta Matsuura: “Economics of Provable Security and Probable Security,” 4th International Workshop on Mathematical Cryptology, Daejon, Korea, June 17, 2009. (invited talk)

〔図書〕（計 1 件）
①日本セキュリティ・マネジメント学会（監修）, 松浦幹太（編著）: “セキュリティマネジメント学 ～理論と事例～,” 共立出版, 2011. （総ページ数 262 ページのうち、まえがき、第１章（1～8 ページ）、および第５章（87～103 ページ）を担当）

６．研究組織
(1)研究代表者
松浦　幹太　（MATSUURA KANTA）
東京大学・生産技術研究所・准教授
研究者番号： 00292756

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：