モジュール化に基づく高機能暗号の設計

―― 実社会への高機能暗号の導入における障壁の低減に向けて ――

花岡 悟一郎[1*]、大畑 幸矢[1,2]、松田 隆宏[1]、縫田 光司[1]、Nuttapong ATTRAPADUNG[1]

この論文では新たに設計される高機能暗号技術が提供する機能や安全性について第三者が理解することが容易でないことが同技術を実社会へ導入する際の大きな障壁となっていることを指摘し、それを軽減するための設計思想について議論を行う。そのような高機能暗号技術の例として代理再暗号化技術を取り上げ、提案する設計手法によってそのような障壁が軽減されていることを論ずる。

キーワード：公開鍵暗号、電子署名、代理再暗号化技術、証明可能安全性、標準化

Methodology for designing cryptographic systems with advanced functionality based on a modular approach

– Towards reducing the barrier to introducing newly-designed cryptographic schemes into real-world systems –

Goichiro HANAOKA[1*], Satsuya OHATA[1,2], Takahiro MATSUDA[1], Koji NUIDA[1] and Nuttapong ATTRAPADUNG[1]

In this article, we point out that in general, newly-designed highly functional cryptographic tools have significantly complicated structures that hinder user understanding. Furthermore, this fact may prevent these new technologies from being introduced into real world systems. We propose a new methodology for overcoming this barrier. We take proxy re-encryption as an example, and discuss how the barrier to user understanding is reduced by our proposed methodology.

Keywords：Public-key cryptosystems, digital signature, proxy re-encryption, provable security, standardization

1　はじめに

1.1　この研究の背景と目的

背景

ネットワーク社会の高度化に伴い、クラウドストレージに代表されるような複雑化する情報サービスをより安全に実現することを目的として、新たな高機能暗号技術の設計が盛んに行われている。そのような高機能暗号の代表例の一つとして、代理再暗号化技術[1]が挙げられる。

代理再暗号化技術とは、送信者はいったん受信者を指定したうえで暗号化を行い、その後必要に応じて“プロキシ（代理人）”と呼ばれるサーバが、復号を行うことなく別の受信者を指定し直すことを可能とする。この技術を用いることで不特定多数の正規利用者に対してデータアクセスを許しながら、その一方でそれ以外の利用者による閲覧を防ぐことができる。例えば、病院の電子カルテは機密情報であるがゆえに暗号化による保護を行いたいが、患者の転居や転院の際には病院間で共有する必要があり、このような場面で代理再暗号化技術は非常に有用となる。

しかし、代理再暗号化技術をはじめとするこれらの高機能暗号技術は極めて高度な安全性と利便性を提供可能であると期待されているものの、構成が非常に複雑となるためにその安全性や機能を直観的に理解することは容易でない。例えば、暗号理論分野に関して最も権威ある国際会議であるCRYPTO2012においては、4件の高機能暗号の論文が発表されているが、これらは平均して34ページあり、そのうち安全性定義および安全性証明の記述は平均して24ページ以上にのぼる。その内容も難解な数式の羅列からなっており、これらの数式と実用上の安全性の対応関係を把握することが困難になっている。このことはこれらの技術の実社会への導入の大きな阻害要因と考えられる。

1 産業技術総合研究所　セキュアシステム研究部門　〒305-8568 つくば市梅園1-1-1 中央第2、2 東京大学大学院　情報理工学系研究科　〒113-8656 文京区本郷7-3-1
1. Research Institute for Secure Systems, AIST　Tsukuba Central 2, 1-1-1 Umezono, Tsukuba 305-8568, Japan　* E-mail: hanaoka-goichiro@aist.go.jp, 2. Graduate School of Information Science and Technology, The University of Tokyo　7-3-1 Hongo, Bunkyo-ku 113-8656, Japan

Original manuscript received July 31, 2013, Revisions received November 9, 2013, Accepted November 15, 2013

特に、専門的な研究者ですら安全性に関する確信を得ることは非常に困難となるため、一般的な利用者がこれらの技術を安心して使用することは期待できない状況にある。事実、設計者によって安全であることを数学的に証明したとの主張がなされている方式に関しても、しばしば後になって証明の誤りが発見されるなどしている。以後、この問題を暗号の安全性検証問題と呼ぶことにする。

目的

この論文では上記の事態を鑑み、複雑な機能をもつ新たな高機能暗号技術の実社会への導入を促進するための方法論について議論を行う。特に、安全性の検証が非常に複雑で難解になりがちなそれらの暗号技術の安全性を、非専門的な研究者や技術者に対してもなるべく理解を容易とするための設計理念を提案する。より具体的には、複雑な機能をもつ高機能暗号の設計においていきなりスクラッチ開発[用語]を行うのではなく、設計を行う前にまずは求められる機能を分解し、なるべく簡潔な機能の組み合わせで記述することの重要性を示す。その際には、個別の各機能がすでに広く利用されている、より基本的な暗号技術の機能そのものであるように機能を分解することが望ましい。求められる機能の分解を行い、スクラッチ開発を行うことなく既存技術の組み合わせだけで複雑な機能を実現することで、安全性の根拠を要素技術となる既存暗号技術の信頼性に依拠することが可能となる。さらに、これらの既存技術はすでに実社会において広く利用がなされていることから、その信頼性は十分に高いものとみなすことができる。

複雑な問題をより小さく、理解しやすい要素に還元するモジュール化はプログラミング分野等の常套手段であるが、暗号技術研究においては導入が遅れていた。その理由の一つは、「適切なことを行う」通常の情報技術と比べて「不適切なことは行えない」ことを保証する暗号技術は特性が大きく異なり、モジュール化手法の正当性に新たな論拠が必要な点である。また、従来の高機能暗号技術分野では理論研究として専門家向けの方式設計が主であり、モジュール化のような「理解を容易にする」作業が軽視される傾向にあった。しかし、近年の高機能暗号技術の複雑化に伴い専門家ですら新提案方式の正しい理解が困難になりつつあり、実際に権威の高いとされる査読付き国際会議に採録された方式においても、後に安全性証明の誤りが指摘されている事例もある。また、高機能暗号の実用化が始まった現在では専門家以外への技術の説明がより重要であることから、暗号技術研究にもモジュール化手法を取り入れる必要性と重要性が高まっていると考えられる。

なお、提案する方法論は暗号技術の安全性を強化する目的ではなく、同等の安全性をより第三者（潜在的な利用者）が納得しやすい形で実現することを主目的としている点に注意されたい。この研究は、安全性に関する理論的な検証が（ある程度）なされているだけの暗号技術と安全性に関する検証結果の正当性が利用者にも納得されやすい暗号技術では、実社会への導入の容易さについて両者の間で有意な相違があることが新たな高機能暗号技術の実用化に向けた障壁となっていることを指摘し、この障壁を除去することでこれらの高機能暗号技術の実社会における広範な活用を促そうとするものである。

以下においては、特に代理再暗号化技術を具体的な例として取り上げ、これをケーススタディとして提案する設計方針の説明を行う。

1.2　代理再暗号化技術の概要と現状

代理再暗号化技術の概要

代理再暗号化技術は、ある受信者に宛てて暗号化がなされたデータを復号することなく、別の受信者に宛てた暗号化データへ変換することが可能な暗号技術であり（図1）、1998 年に Blaze ら [1] により最初の提案がなされた。代理再暗号化技術は通常時は一般的な公開鍵暗号と同様に機能するが、受信者は " プロキシ（代理人）" と呼ばれるサーバに対して自分以外の特定の利用者を指定し、それに対する " 再暗号化鍵 " を預託することができる。プロキシは各利用者に宛てられた暗号文に再暗号化鍵を作用させることで、指定された別の利用者宛ての暗号文に変換することが可能である。この技術を用いることで、特定の一人の利用者だけでなく複数の受信者を動的に指定可能となる。代理再暗号化技術においては再暗号化を複数回行えるものも存在するが、今回は再暗号化を一度だけ行えるものについて議論を行う。

代理再暗号化技術はクラウドストレージのような不特定多数が利用する環境における安全なアクセス制御を実現するうえで非常に有用であり、2006 年頃から世界的に活発な研究開発が進められている。1998 年当時は安全性に関する議論が十分になされていなかったのに対し、2006 年以降の一連の研究においては強力な安全性を数学的に証明

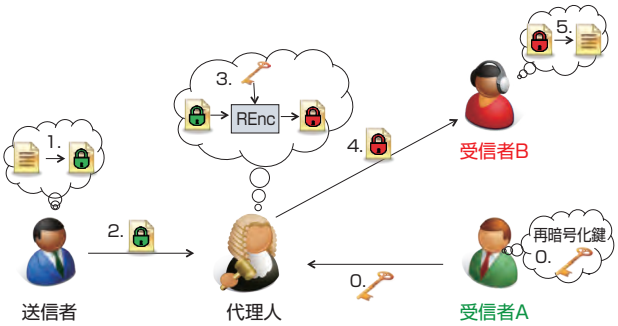

図1　代理再暗号化の概観

可能な方式の設計が主眼に置かれている。こうした強力な安全性の数学的証明は単なる理論的な興味の追求ではなく、実用上の必要に迫られてのものである。標準化の現場においても、例えば我が国の事実上の標準暗号とみなされているCRYPTREC電子政府推奨暗号[2]の選定において、数学的安全性証明の有無は重要な選考基準となっている。

代理再暗号化技術の必要性

広く普及しているDropbox[3]やGoogle Drive[4]などのクラウドストレージにおいては、正当な権限をもつ複数の利用者のみがファイルの読み書きが可能であり、またそのような権限の設定を柔軟に行うことが可能である。

しかし、これらのストレージ上に格納されているデータは複数ユーザーで共有することを想定しているため、暗号化がなされていないか、データを格納するサーバ自身で復号が可能な暗号化がなされており、サーバの管理者であればデータへのアクセスは容易である。したがって、利用者自身がデータ管理に細心の注意を払っていても、サーバ管理者の故意、もしくは不注意によりデータが漏洩する危険性をはらんでいる。最近でもアメリカの中央情報局（CIA）および国家安全保障局（NSA）の局員による内部告発が明らかとなり、国際的に大きな波紋を呼んでいる。またサーバ側の過失により、Facebookにおいて600万人のユーザーのメールアドレスや電話番号が他人と共有されてしまった可能性があるというケースも報告されている。こうした事件は、サーバを無条件に信頼したシステム設計の限界を表す一例であると言える。

上記のようなサーバによるデータの覗き見や漏洩を防ぐ手段として、利用者側で暗号化したデータをストレージに保管することが考えられる。復号鍵をもたないサーバはデータの解読を行うことはできず、またサーバから平文が漏洩することもない。しかし、データへのアクセスに必要な復号鍵は安全に正当な権限をもつ利用者だけに配布できると仮定すべきではない。なぜならば、もしも正当な利用者にのみ復号鍵を安全に配布可能な仕組みがあれば、そもそもその仕組みを用いて正当な権限者だけにデータを配布すればよいからである。

そのような状況において代理再暗号化技術を用いた場合、各利用者は暗号化された状態でデータをストレージ上に保管できるだけでなく、他の正当な権限者に対してはプロキシに再暗号化鍵を預託することで、柔軟にアクセス制御を行うことが可能となる。代理再暗号化を利用したクラウドストレージは、すでに一部で商用化も開始されている[5]。上記のFacebook等に生じた問題は複合的な要因で発生しているため、代理再暗号化技術の導入によってすべて解決されるとは限らないが、高度に信頼できるサーバの存在の仮定を排除することが可能となるため、極めて有効であると考えられる。

代理再暗号化技術の導入障壁

上述のとおり、サーバによるデータの覗き見や漏洩に対しても安全で、なおかつ柔軟なアクセス制御が可能なクラウドストレージの実現に関して代理再暗号化技術は極めて有用と考えられているが、実システムへの導入に関して障壁を残している。また、その障壁は代理再暗号化技術の機能に直接的に関係するものではなく、むしろ与えられた代理再暗号化技術が想定通りに機能することが確認できれば全く問題となるものではない。ここではそのような代理再暗号化技術の導入の障壁についてより詳しい説明を行う。

ほとんどの高機能暗号技術においては、本章の冒頭で述べた安全性検証問題を抱えており、代理再暗号化技術に関してはそれが特に顕著である。例えば、公開鍵暗号に関する権威ある国際会議PKC2009で提案された代理再暗号化方式[6]は優れた効率を誇っていたが、安全性証明が誤っており、攻撃可能であることが翌年のPKC2010において指摘されている[7]。同論文中においては新たな代理再暗号化方式を提案しているが、これもその翌年のPKC2011において安全性証明の誤りを指摘され、攻撃されている[8]。

そのためこれまで提案されたさまざまな代理再暗号化技術に関し、設計者の主張通りの機能と安全性が信認されている方式がほとんどないことが、実用化に向けた大きな障壁となっている。なお、上述の近年商用化された代理再暗号化技術[5]は設計者の所属する企業自体がサービスを行っているため、技術の正当性が十分に広く認められた末の実用化とはなっていないことに注意されたい。

その他の高機能暗号技術

すでに述べたとおり、この論文は近年提案がなされているさまざまな高機能暗号技術に関し、それらの実用化を進めるうえでの共通した問題点に対する解決の指針を提案するものであり、代理再暗号化技術はあくまで例示である。代理再暗号化技術以外の高機能暗号の例としては、属性ベース暗号、キーワード検索暗号、準同型暗号、グループ署名等がある。これらの高機能暗号技術においては、いずれも代理再暗号化技術と同様に構成や安全性定義が複雑になりがちであり、実用化に向けた大きな障害となっているものと考えられる。

2　代理再暗号化技術の機能と安全性定義

本章では代理再暗号化技術の機能と安全性を紹介し、それを満足する方式を従来の方法論により設計しようとし

た場合、方式の構成と安全性証明がいかに複雑となるのかについて議論を行う。

2.1　代理再暗号化技術の数学的モデル

ここではまず代理再暗号化技術の機能について整理を行う。代理再暗号化技術の機能は大雑把には以下のとおりである。

【機能 1】各利用者の鍵を生成する機能

代理再暗号化技術は、公開鍵暗号と同じく、各利用者は、公開される暗号化鍵と秘密にする復号鍵の生成を行う機能が必要となる。

【機能 2】再暗号化鍵を生成する機能

利用者A宛ての暗号文を利用者B宛ての暗号文に変換可能な再暗号化鍵の生成機能も必要となる。利用者Aは、利用者Aの復号鍵と利用者Bの暗号化鍵を用いて、上記の再暗号鍵を生成し、プロキシに預託することとなる。

【機能 3】暗号化を行う機能

従来の公開鍵暗号と同じく、特定の受信者のみが復号可能な暗号文を作成する機能が必要となる。その際、暗号化の対象となる平文と受信者の暗号化鍵を用いて暗号化がなされる。また、この暗号化によって作成された暗号文は、上述のとおり、再暗号化鍵によって、別の受信者が復号可能な暗号文に変換可能でなくてはならない。

【機能 4】再暗号化を行う機能

上記の機能 3. にある暗号化がなされた場合は、再暗号化鍵をもつプロキシが、元々指定された受信者とは異なる、別の利用者が復号可能となるよう暗号文の変換を行うことができる機能が必要となる。この機能では、変換前の暗号文と再暗号化鍵を用いて、変換後の暗号文の作成がなされる。

【機能 5】復号を行う機能

上記の機能 3. にある暗号化により作成された暗号文を復号するための機能も必要である。この機能では、公開鍵で暗号化された暗号文と正当な受信者の復号鍵を用いて、平文が復元される。

【機能 6】再暗号化された暗号文の復号を行う機能

同様に、上記の機能 4. にある再暗号化により作成された暗号文を復号するための機能も必要である。この機能では、復号の対象となる暗号文と正当な受信者の復号鍵を用いて、平文の復元がなされる。

以上の機能 1. ～ 6. を見てわかるとおり、代理再暗号化技術を構成するアルゴリズムは 6 つにのぼり、しかもその一つ一つが複雑なものとなっている。そのため、代理再暗号化技術の設計者が、提案方式がこの機能を満足していると主張をしたとしても、その正当性を検証することは必ずしも容易ではない。

2.2　代理再暗号化技術の安全性定義

2.1　節で述べたように、代理再暗号化技術の数学的モデル化はすでに非常に複雑であるが、安全性の定義はそれよりはるかに複雑で難解となる。本節では、代理再暗号化技術の安全性要件について整理を行う。詳細については、例えば文献 [9] を参照されたい。

代理再暗号化機能をもたない通常の暗号化・復号機能のみを有する公開鍵暗号方式に標準的に要求される安全性は、「選択暗号文攻撃に対する安全性」と呼ばれる。この安全性は、攻撃対象の暗号文以外の任意の暗号文の復号結果を得ることが許されている攻撃者をもってしても、攻撃対象の暗号文から平文の情報を 1 ビットも得ることができないということを保証する。

代理再暗号化技術にも、基本的には上記のような安全性が求められる。しかし、すでに 2.1 節で見てきたとおり、代理再暗号化技術には「再暗号化前の暗号文」、および「再暗号化後の暗号文」の 2 種類の暗号文があり、平文の情報を得たい攻撃者はどちらの暗号文を攻撃してもよい。さらに、代理再暗号化技術には再暗号化機能、および再暗号化鍵の鍵生成の機能も存在するため、攻撃者はこれらの機能を用いることで解読に関するヒントを抽出しようとすることも考えられる。したがって、代理再暗号化技術の安全性定義は、このような状況においても安全性を保証するものとなっていなければならない。特に重要なことの一つとして、再暗号化を行うプロキシに対しても暗号文からは情報が漏れないことをとらえた安全性定義でなければならない。さらに、現実での利用状況を考え、安全性は複数の利用者およびプロキシが結託をしたとしても、正規のユーザーの情報が守られるものになっていなければならない。以上を考慮して代理再暗号化技術に求められる安全性を整理すると、次のとおりとなる。（以下では便宜上、攻撃を受ける利用者を A と呼ぶことにする）：

「再暗号化前の暗号文の安全性」

本安全性は、「攻撃を防ぎようのない結託以外のありとあらゆる利用者・プロキシ間結託が起こったとしても、A 宛てに作成された再暗号化前の暗号文は平文の情報を 1 ビットも漏らさず、かつ A 宛ての再暗号化前暗号文は、「他の利用者宛て再暗号化暗号文」以外には意味のある別の暗号文へと改変ができないことを要求する。代理再暗号化技術の機能の定義から、「利用者 B」と「A 宛ての暗号文を B 宛ての暗号文へと再暗号化できるプロキシ」が結託すると、A 宛ての再暗号化前暗号文はすべて復号できてしまうことに注意されたい。本安全性は、この原理的に防ぎようがない結託以外のあらゆる攻撃状況を考慮している。

「再暗号化後の暗号文の安全性」

本安全性は、A 以外の利用者（B と呼ぶ）宛てに作成された再暗号化前の暗号文が A 宛てに再暗号化される状況において、A 以外のいかなる（B も含む）利用者・プロキシが結託したとしても、A 宛ての再暗号化暗号文は平文の情報を 1 ビットも漏らさず、かつ意味のある別の暗号文へと改変できないことを要求する。

以上が代理再暗号化に求められる安全性であるが、定義や証明が複雑難解という暗号の安全性検証問題が発生していることがわかる。

2.3　既存の代理再暗号化技術の例

図 2 に、Libert と Vergnaud[10] により提案された代理再暗号化技術の構成の一部を示す。この方式は、「ペアリング」と呼ばれる特殊な双線形写像（図中の関数 e）をもつ巡回群を使ってスクラッチから設計、実装されている。また、使用される巡回群上でのある計算問題を解くことの困難性を仮定することによって 2.2 節で挙げた安全性の証明もなされており、代理再暗号化技術の中でも安全性・効率性を両立した代表的な方式として知られている。

しかし、図からも明らかな様に方式の記述は複雑である。暗号文や各種鍵の各コンポーネントは、情報を隠すための部分、再暗号化を可能にするための部分、安全性に寄与する部分等に役割を明確に切り分けることができず、複雑に絡み合っている。方式の各パラメータの構成や計算順序は“職人芸的”に組み合わせられたものであり、暗号技術を専門としている我々でも個々の役割を明確に説明することは困難である。例えば、図 2 に示されるように、再暗号化暗号文中の構成要素 C_2', C_2'', C_2''' は互いに独立でなく、共通の内部乱数 t を介して相関をもっている。また、図中に明示的に記述されていないが、構成要素 C_2''', C_3, C_4 も同様に、共通の内部乱数 r を介して相関をもっており、さらに、構成要素 σ は、C_1, C_3, C_4 に依存して生成がなされている。これらから、暗号文中のすべての構成要素は、お互いに密接な相関をもっており、したがって、代理再暗号化技術の各機能に対して、なんらかの形で関与していることがわかる。また、上記の「ペアリング」をもつ巡回群は、現在のところ楕円曲線を用いた暗号技術の原理についての一定の知識をもつ技術者以外には扱うのが難しい特殊なライブラリを用いるしかなく、モジュラー性・移植性にも乏しい。

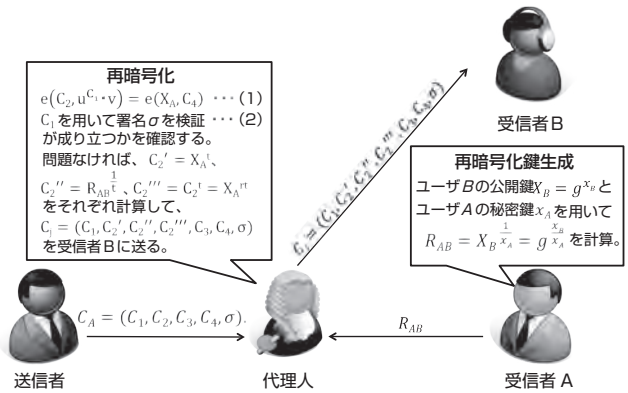

図2　代理再暗号化技術の一方式[10]の再暗号化機能

3　提案手法：方法論と代理再暗号化への適用例

本章では暗号の安全性検証問題を解決するため、代理再暗号化技術を始めとする複雑な機能および構造をもつ高機能暗号の機能や安全性が、潜在的な利用者となる第三者に対しても理解が容易となり、実社会に対して円滑に導入されるようになるための方法論について論じる。また、実際に同方法論に基づき設計された代理再暗号化技術を紹介し、その構成の背後にある設計思想について解説を行う。

3.1　提案する方法論の俯瞰

従来は複雑な機能をもつ高機能暗号技術において要求される機能と安全性をスクラッチ設計によって満足しようとするケースがほとんどであり、またスクラッチ設計により設計がなされた方式は求められる機能や安全性を膨大で複雑な数式により不可分な形で同時に達成しようとしているため、第三者による正当性の検証が極めて困難になっているものと考えられる。

ここでは高機能暗号技術の実社会への導入に関し、従来のスクラッチ設計が大きな阻害要因になっているものととらえ、この問題を解決するための方法論として、「実際に設計を開始する前段階において、要求される機能と安全性のモジュール化を可能な限り行うステップを挿入する」ことの重要性を示す（図 3）。特に、暗号の安全性検証問題に鑑みて、モジュール化された機能や安全性の概念が、すでに十分に解析のなされている既存技術の直接的な利用で充足されるようなモジュール化を追求する。既存技術に関する専門的知識が要求されることはやむを得ないが、それらはすでに十分な解析がなされており、代理再暗号化に比べれば正当性を検証できる研究者・技術者が格段に多い技術となっている。

このような機能と安全性に関する要件のモジュール化をしたうえで高機能暗号技術の設計を行うことにより、設計された方式が提供する機能や安全性について第三者に理解を促すことが可能となる。より詳しくは以下のような効果が期待できる。

- モジュール化された個々の機能や安全性が、方式の構成中においてどのような貢献をしているかの把握が容易となる。
- 構成要素となる各技術は機能や安全性についてすでに深

く理解されているため、方式の機能と安全性の正当性検証が容易となる。

・モジュール化された個々の機能や安全性について、アプリケーションに応じてより効果的に機能するものを選択することが可能となる。また、後に構成要素に問題が発見されても、他の構成要素へ置き換えることで容易に修正可能となる。

これらの効果により、新たに設計がなされた高機能暗号技術が実システムへ導入される際の障壁が著しく軽減されることとなる。

次節において、このような設計思想において設計がなされた具体的な代理再暗号化技術の例について紹介を行うが、それに先立ち、より簡潔な例として任意長の平文を許す公開鍵暗号のケースを取り上げ、提案手法により上述の効果が得られていることを確認する。

任意長の平文を許す公開鍵暗号の一般的構成

従来の公開鍵暗号技術、例えば[11][12]においてはそれらの方式が依拠する代数的構造により、暗号化の対象となる平文のサイズが厳しく制限されている。しかし、実用上はさまざまな長さのデータの暗号化を行う必要がある。一方、共通鍵暗号技術においては、従来より任意の長さの平文の暗号化が可能であった。それに対し、2000年初頭において任意長の平文を許す公開鍵暗号の構成方法が整理され、次のような一般的構成の提案がなされた：(1) まず固定長の共通鍵Kを選び、暗号化の対象となる平文を共通鍵Kを用いて共通鍵暗号により暗号化する。(2) 次に、共通鍵Kを（固定長の平文のみ許す）公開鍵暗号により暗号化する。最後に、上記、(1)、(2) によって得られた二つの暗号文の組を本構成における暗号文とする。

この構成は、この論文で提案する高機能暗号技術の設計手法の具体例とみなすことができる。すなわち、公開鍵暗号としての基本機能と任意長の平文を暗号化する機能をそれぞれ（従来の）公開鍵暗号と共通鍵暗号に分解している。この構成はその後一層洗練され、現在ではISOを始めとする公開鍵暗号技術の標準化の現場においても上記の(1)、(2) の機能に相当する部分について個別に標準化活動がなされている[13]。この事例からも、この論文で提案する設計手法の有効性が理解できる。

3.2 代理再暗号化技術への適用

ここでは、前節において提案を行った手法に基づいてHanaokaら[9]によって設計がなされた代理再暗号化技術について紹介する。この方式は、よく知られた暗号要素技術である公開鍵暗号[11][12]、電子署名[11][14]、閾値暗号[15]を組み合わせて構成されており、また、要求されている個別の機能や安全性がそれぞれどの要素技術によっていかに満足されているかについての対応関係が理解しやすい。

構成要素技術

以下ではまず、簡単に公開鍵暗号、電子署名、閾値暗号の説明を行う。これらを用いて代理再暗号化技術の6つの機能を構成する方法については4章で後述する。なお、これらの構成要素技術はそれぞれ複数の機能をもっており、これらの個別の機能を組み合わせることで代理再暗号化技術の6つの機能の実現が可能になる。

・公開鍵暗号

メッセージの受信者側で秘密鍵と公開鍵を生成し、公開鍵を公開する。メッセージの送信者は受信者の公開鍵を用いてメッセージの暗号化を行い、暗号文を受信者に送信する。受信者は秘密鍵を用いて暗号文を復号することができる。事前の共有情報無しに秘匿通信が可能であり、SSL、TLS[注)]等をはじめ、非常に幅広く利用されている最も基本的な暗号技術の一つである。

・電子署名

メッセージの署名者が署名鍵と検証鍵を生成し、検証鍵を公開する。メッセージの署名者は署名鍵を用いてメッセージに署名を行う。署名とメッセージを得た検証者は、検証鍵を用いて署名の検証を行うことができる。電子署名は現実世界における印鑑を電子社会において実現するものであり、ネットワーク社会における認証基盤を支える最も重

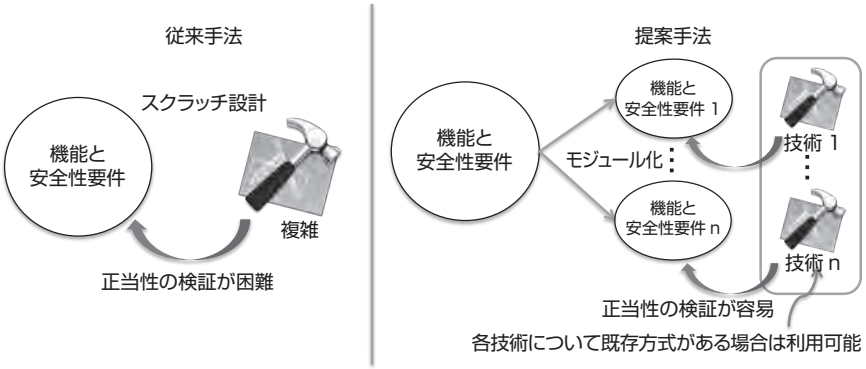

図3　従来手法と提案手法の構成指針の違い

要な要素技術となっている。PKI 等においてすでに広く利用がなされている。

・閾値暗号

公開鍵暗号の拡張であり、従来は単一となる秘密鍵が複数の部分秘密鍵に分割されていることが特徴となっている。閾値暗号においては従来の公開鍵暗号と同じく（単一の）公開鍵により平文の暗号化がなされ、そこで得られた暗号文に対して各部分秘密鍵を用いて復号を行うことで「復号シェア」と呼ばれる部分復号結果を導出することができる。そのような復号シェアを閾値以上集めることで復号が可能となる。なお、本節で紹介する代理再暗号化技術の構成においては秘密鍵を二つに分割し、復号シェアを二つとも集めることで復号可能になるような閾値暗号を用いる。

閾値暗号は電子投票システムの構成における重要な要素技術であり、1990 年代より活発に研究開発がなされている。すでに実用システム上にも導入がなされており、広く機能や安全性が理解されているものと考えられる。

構成方法

ここで紹介する代理人再暗号化方式の構成では、閾値暗号が中心的な役割を果たす。同構成においては図 4 に示されるように、メッセージの送信者は閾値暗号を用いて受信者 A 宛ての暗号化を行い、暗号文を送信する。この暗号文は閾値秘密鍵を所持している受信者 A は復号でき、これが通常の公開鍵暗号の機能に相当する。

図5に示されるように、再暗号化鍵を生成する際にはユーザー A は二つある部分秘密鍵の片方を再暗号化後の宛先ユーザー B の公開鍵で暗号化し、代理人に渡す。ここで、電子署名を用いることで再暗号化鍵の正当性を保証する。再暗号化の際には、代理人は暗号文を暗号化されていない方の部分秘密鍵を用いて部分復号して復号シェアを計算し、これと暗号化された部分秘密鍵を合わせてユーザー B に送信する。

図 6 に示されるように、再暗号化された暗号文を受信した B は、暗号化された部分秘密鍵を復号し、それを用いてもう一つの復号シェアを得ることで平文の復元を行う。

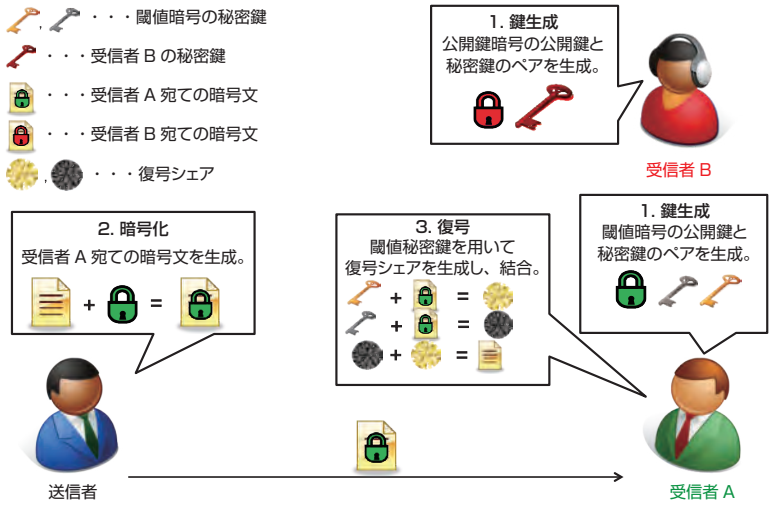

図4　提案手法の構成イメージ（鍵生成、暗号化、受信者Aの復号）

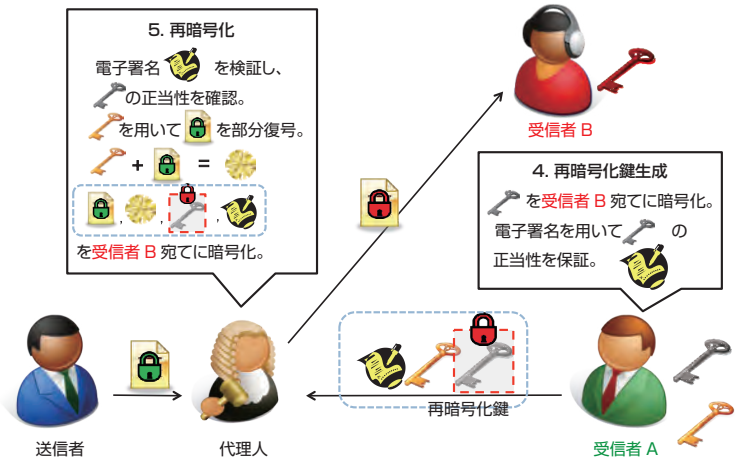

図5　提案手法の構成イメージ（再暗号化鍵生成、再暗号化）

4　提案手法の評価

高機能暗号技術の安全性を信頼できるようにするために、すでに広く用いられている基本的な技術に分解することが重要であることはこれまでに述べてきたとおりである。ここでは、まず、前章において紹介した代理再暗号化技術を例に、どのような基本的技術への分解が行われ、また、なぜそれらの基本的技術への分解を行ったのかについて、より詳しく説明を行う。

具体的には、前章の代理再暗号化技術は、公開鍵暗号、電子署名、閾値暗号といった基本的技術へ分解がなされているが、これらは、単に代理再暗号化技術に比べてより基本的なものであるだけでなく、いずれもすでに広く用いられている技術となっている。これは偶然にそのような分解がなされたのではなく、それらの技術について安全性を非常に高く信頼された実装がすでに存在することから、そのような分解がなされるよう意図されたうえでのものとなっている。すなわち、公開鍵暗号として RSA-OAEP 方式、電子署名として RSASSA-PKCS1-v1_5 方式等が SSL/TLS においてすでに広く利用されている。実際、米国シマンテック・コーポレーションが発行しインストールされた SSL サーバ証明書は 80 万枚以上 [16] に達しており、これほどまでに広く利用されていながらこれまでに安全性上の問題は見つかっていない。（ただし、RSASSA-PKCS1-v1_5 方式については、すべての実装が必ずしも安全でないため、利用実績が高い信頼できる実装を慎重に選ぶ必要がある。）閾値暗号に関しては上記二つの技術に比べて広く普及しているわけではないが、電子投票等において活用がなされており、十分に信頼できる技術と考えられる。以上のことから、前章の代理再暗号化技術において、どのような方針により機能の分解が行われているかが理解できる。

上記のような機能の分解を行うことによる利点として、以下の 5 点が挙げられる。

【利点 1】スクラッチな構成と比べて、代理再暗号化という高度な技術を達成できていることを把握しやすくなっている。2.1 節で述べた機能がどのように達成されているかを考えると、

- 機能1の鍵生成は、受信者Aが閾値公開鍵と閾値秘密鍵のペアを生成し、受信者Bが通常の公開鍵、秘密鍵のペアを生成することで実現される（図4）。
- 機能2の再暗号化鍵生成は、二つある閾値秘密鍵のうち片方を受信者Bの（通常の）公開鍵で暗号化し、残りの閾値秘密鍵と合わせたものを再暗号化鍵とすることで実現される（図5）。
- 機能3,5の暗号化と復号は、閾値暗号の暗号化と復号によって実現される（図4）。
- 機能4の再暗号化は、代理人が得た閾値秘密鍵を用いて暗号文を部分復号し、得られた復号シェアとA宛ての暗号文、暗号化された閾値秘密鍵をまとめて受信者B宛てに暗号化して送信することで実現される（図5）。
- 機能6の再暗号化暗号文復号は、受信者Bが送られてきた暗号文を自身の秘密鍵で復号し、さらにその中の暗号化された閾値秘密鍵を復号する。得られた閾値秘密鍵でA宛ての暗号文を部分復号すると二つ目の復号シェアが手に入り、メッセージを復号できるようになることで機能6が実現される（図6）。

ということが難しい数式を追わずとも直観的に理解できる。

【利点 2】利点 1 と関連して、代理再暗号化の各機能について構成要素技術間の役割分担を明確にしたことで、全体として達成できている安全性の把握も容易となっている。また、仮に安全性証明の誤りが発覚したとしても、誤り箇所がどの構成要素技術と対応しているか明確なため、証明の修正もしやすくなる。

【利点 3】構成要素である暗号方式の一部を同等の機能をもつ別の方式と交換することで、方式全体の性能向上やカスタマイズを容易に行える。スクラッチな構成の場合、例えば実行速度向上のために 1 か所の構造を組み替えるごとに、全体の構成まで立ち返ってその変更が機能や安全性を損なわないことを確認しなければならないため負担が大きい。一方、今回の方法論であれば、ある構成要素の構

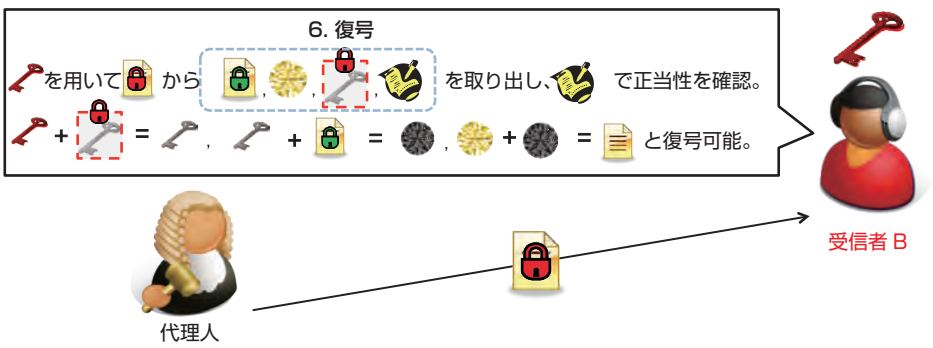

図6　提案手法の構成イメージ（受信者Bの復号）

造を変更する際には、その構成要素の機能が保たれているという局所的な性質のみ確認すればよいので作業が容易となる。

【利点 4】利点 3 と関連して、将来的な暗号攻撃技術の向上に伴い暗号方式のアップデートが必要となった際にも、今回の方法論であれば、安全性が危殆化した要素技術のみを安全なものに置き換えればよいので、アップデートにかかる運用コストを引き下げることができる。同様に、将来的な量子計算機の実現を見越して量子計算機でも破れない（耐量子）代理再暗号化技術を構成したい場合、上述の 3 つの構成要素をそれぞれ耐量子構成にすればよい。これは耐量子代理再暗号化技術を一から開発するのに比べてはるかに容易である。

【利点 5】利点 4 とも関連するが、今回の方法論の場合、例えば電子署名技術について従来よりも優れた方式を開発することで、電子署名技術それ自体の向上と、それを構成要素とする代理再暗号化技術の向上に同時に貢献できる。今回の方法論のこのような特徴は、暗号技術の研究開発という分野全体の研究資源配置の効率化にも資するものである。

5　他の高機能暗号技術への適用

本章ではこの論文にて提案を行った高機能暗号技術の設計方針について、代理再暗号化技術以外の暗号技術、特にグループ署名への適用可能性について議論を行う。また、提案手法を用いた場合に発生しうる構成要素同士の干渉、および回避方法についても併せて論じる。

5.1　グループ署名への適用について

グループ署名とは署名者のプライバシー保護機能が強化された電子署名技術であり、1991 年に Chaum ら [17] によりその概念が提唱されて以来、これまでに多くの具体的な構成方法が提案されている。グループ署名は従来の電子署名の機能の他に署名発行者の秘匿機能等を備えており、プライバシー保護機能が強化された電子署名であると言え、電子掲示板や電子オークション等において極めて有用な技術である。

しかし、従来の電子署名に比べ機能が非常に複雑となることから、代理再暗号化技術と同様に安全性が広く信頼されている方式はほとんど存在していなかった。それに対し、2003 年に Bellare ら [18] は電子署名、公開鍵暗号、ゼロ知識証明の機能を組み合わせることでグループ署名を実現できることを示した。この成果以降、グループ署名の設計者は上記のような機能の分解を念頭に、電子署名、公開鍵暗号、ゼロ知識証明の適切な選択を考慮した設計を行うようパラダイムシフトが起こっている。結果としてスクラッチ設計による従来の方式に比べ、新たに提案がなされた方式の機能や安全性が第三者によって深く理解されるようになり、商用化、標準化の進展にも大きく影響を与えるに至っている [19]。

なお、電子署名や公開鍵暗号については、前述のようにすでに広く利用されている信頼できる方式が存在する。ゼロ知識証明に関しても、利用者認証技術等において広く活用がなされており、十分に信頼できる技術と考えられる。

この論文において提唱しているような高機能暗号技術の設計に際しての機能分解の重要性は、ある意味 Bellare らによって暗に述べられていたともいえるが、それを陽に議論しグループ署名に留まらない汎用的な設計思想であることを提示したことがこの論文の主結果となる。また、この論文における提案手法が暗に利用されていたグループ署名に関し、同技術の標準化が進んでいることからも提案手法の有効性を理解することができる。

5.2　構成要素同士の安全性の干渉について

この論文は、設計対象となる高機能暗号技術の機能を基本的暗号技術の組み合わせによって実現することの有用性を主張するものである。しかしその際に利用される基本的暗号技術同士が干渉し、単体では安全性が保証されていても全体としては安全性が保証できなくなるケースが存在する。ここでは設計された方式において、そのような問題が生じていないかを検討する手法について述べる。

目的とする高機能暗号技術について基本的要素技術のみにより厳密な意味での一般的構成が行われた場合、同一般的構成の安全性証明さえ行えばその特殊なケースとなる個別の方式についての安全性証明は不要となる。つまり、同一般的構成を行ううえで求められる一定の条件を満足するものであれば、どのような基本的要素技術を構成要素として用いたとしてもそれらによって構成された具体的方式の安全性は自動的に保証される。この論文において紹介を行った代理再暗号化技術の構成方法は、そのような厳密な意味での一般的構成となっている。

また、要素技術同士が干渉しないことを保証する安全性の概念として汎用的結合可能性と呼ばれるものがあり、この安全性概念を満足する構成要素技術を用いることで要素技術間の干渉を防ぐことができる。

5.3　分解先とすべき基本的技術

高機能暗号技術の機能を分解するにあたり、分解先となる基本的技術がすでに安全性を高く信頼されているものとなることを念頭におく必要がある。その際、安全性を高く信頼されているものであるかを判断するための基準として、広い範囲での利用実績があり、なおかつ、長期間にわたり本質的な安全性上の問題点の指摘がなされていないこ

とが挙げられる。そのような観点からは、公開鍵暗号、電子署名、共通鍵暗号、メッセージ認証コード等は信頼できる技術として疑う余地がない。公開鍵暗号と電子署名については前述のとおり、高い利用実績をもつ実装が知られており、また、共通鍵暗号については AES（市販製品採用実績 95.4 %）、メッセージ認証コードについては HMAC（市販製品採用実績 82.1 %）等、すでに広く普及し、かつ安全性上の問題も見つかっていない技術が存在する[20]。これらに次ぐ基本的技術として、前述の閾値暗号やゼロ知識証明の他、放送暗号等もブルーレイディスクの著作権保護に広く実利用されており、十分に信頼できる技術であると考えられる。

6　まとめ

近年の高度化したネットワークにおいて高機能暗号技術は有用であるが、その社会への導入は進みづらい状況にある。この論文では、高機能暗号技術の活用を促すためには機能や安全性が高度であるだけでなく、それらが理解しやすいものであることの必要性を指摘し、またそれを実現するための設計思想について提案を行った。

今後の一層のネットワーク技術の進展に応じて、さらに高度な機能や安全性をもつ高機能暗号技術の実現が要求されるものと思われる。それらの実用化を考慮した場合、単に要求される機能や安全性を満足するのではなく、それらが第三者に理解できるようにする必要があるが、この論文における提案手法を用いることで実用化を促すことが可能と考えられる。なお、提案手法は、“理解のしやすさ”を改善するためのものであるため、同手法の有効性について社会に広く納得させるうえで、“理解のしやすさ”の定量的な評価手法の確立も重要な課題となる。そのような手法として、安全性の自動検証ツールへ入力する際のデータサイズ等を用いて評価を行うことなどが考えられるが、これについては今後の研究課題としたい。

注）セキュリティを要求される通信のためのプロトコルであり、認証・暗号化・改竄検出の機能を提供する。具体的なアルゴリズムとしてそれぞれ複数の選択肢が定義されており、通信の開始時に双方が許容するアルゴリズムの中から選択される。

用語の説明

用語：スクラッチ開発：すでに存在する技術を流用せず、ゼロから（暗号）方式を構成すること。

参考文献

[1] M. Blaze, G. Bleumer and M. Strauss: Divertible protocols and atomic proxy cryptography, *EUROCRYPT ’98*, 1403, 127-144 (1998).
[2] CRYPTREC暗号リスト, http://www.cryptrec.go.jp/list.html
[3] Dropbox https://www.dropbox.com/
[4] Google Drive https://drive.google.com/
[5] デジタル貸金庫 http://tosafebox.com/
[6] J. Shao and Z. Cao: CCA-secure proxy re-encryption without pairings, *PKC 2009*, 5443, 357-376 (2009).
[7] T. Matsuda, R. Nishimaki and K. Tanaka: CCA proxy re-encryption without bilinear maps in the standard model, *PKC 2010*, 6056, 261-278 (2010).
[8] J. Weng, Y. Zhao and G. Hanaoka: On the security of a bidirectional proxy re-encryption scheme from PKC 2010, *PKC 2011*, 6571, 284-295 (2011).
[9] G. Hanaoka, Y. Kawai, N. Kunihiro, T. Matsuda, J. Weng, R. Zhang and Y. Zhao: Generic construction of chosen ciphertext secure proxy re-encryption, *CT-RSA*, 7178, 349-364 (2012).
[10] B. Libert and D. Vergnaud: Unidirectional chosen-ciphertext secure proxy re-encryption, *PKC 2008*, 4939, 360-379 (2008).
[11] R. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 21 (2), 120-126 (1978).
[12] R. Cramer and V. Shoup: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, *CRYPTO ’98*, 1462, 13-25 (1998).
[13] V. Shoup: A proposal for an ISO standard for public key encryption (version 2.1), http://www.shoup.net/papers/iso-2_1.pdf (2001).
[14] Digital Signature Standard, http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
[15] Y. Desmedt and Y. Frankel: Threshold cryptosystems, *CRYPTO ’89*, 435, 307-315 (1989).
[16] 日本ベリサイン株式会社 「シマンテック、SSLサーバ証明書の発行が世界最多に」 https://www.verisign.co.jp/press/2012/pr_20120427.html (2012).
[17] D. Chaum and E. Heyst: Group signatures, *EUROCRYPT ’91*, 547, 257-265 (1991).
[18] M, Bellare, D. Micciancio and B. Warinschi: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions, *EUROCRYPT 2003*, 2656, 614-629 (2003).
[19] NECプレスリリース: NEC セキュリティとプライバシーを両立する匿名認証をクラウド環境で実現する技術を開発, http://www.nec.co.jp/press/ja/1106/0703.html (2011).
[20] CRYPTREC Report 2012 暗号運用委員会報告書(2013), http://www.cryptrec.go.jp/report/c12_opr_web.pdf

執筆者略歴

花岡 悟一郎（はなおか ごいちろう）

1997 年東京大学工学部卒業、2001 年同大学院工学系研究科電子情報工学専攻博士課程修了（博士（工学））、以降日本学術振興会特別研究員 PD を経て 2005 年産総研入所。現在、産総研セキュアシステム研究部門次世代セキュリティ研究グループ長。効率的な公開鍵暗号方式の設計・安全性証明をはじめとする暗号・情報セキュリティ技術の研究開発に従事。英国計算機学会 The Wilkes Award(2007 年)、電子情報通信学会論文賞(2008 年)、暗号と情報セキュリティシンポジウム（SCIS）イノベーション論文賞（2012 年）、電気通信普及財団賞（2005 年）、SCIS20 周年賞（2005 年）、SCIS 論文賞(2006 年)、情報理論とその応用シンポジウム(SITA）奨励賞（2000 年）等受賞。この論文の執筆全般を総括。

大畑 幸矢（おおはた さつや）

2011年3月千葉大学工学部情報画像工学科卒業、2013年3月東京大学大学院情報理工学系研究科修了（修士（情報理工学））。現在、東京大学大学院情報理工学系研究科博士課程在学中。2012年5月より、産総研セキュアシステム研究部門次世代セキュリティ研究グループテクニカルスタッフ。主な研究内容は公開鍵暗号技術、証明可能安全性とその応用。この論文では代理再暗号化技術の技術的研究動向の調査および系統化作業、図の作成を担当。

松田 隆宏（まつだ たかひろ）

2006年3月東京大学工学部電子情報工学科卒業、2011年3月東京大学大学院情報理工学系研究科電子情報学専攻博士課程修了（博士（情報理工学））。2011年4月より2年間、産総研情報セキュリティ研究センター（2012年4月よりセキュアシステム研究部門）での日本学術振興会特別研究員PDを経て、2013年4月より、同研究部門次世代セキュリティ研究グループ研究員。主な研究内容は、暗号技術の設計・安全性評価と暗号理論。この論文では代理再暗号化技術の安全性定義に関する整理を担当。

縫田 光司（ぬいだ こうじ）

2001年3月東京大学理学部数学科卒業、2006年3月東京大学数理科学研究科博士課程修了（博士（数理科学））。同年4月より、産総研情報セキュリティ研究センター産総研特別研究員、同物理解析研究チーム研究員、産総研セキュアシステム研究部門次世代セキュリティ研究グループ研究員を経て、現在は同グループ主任研究員。主な研究内容は、先端的数学を用いた暗号技術の構成と安全性評価、およびその基盤となる理論整備。この論文では提案手法と既存手法の比較に関する検討を担当。

Nuttapong ATTRAPADUNG（あったらぱどぅん なったぽん）

2001年タイChulalongkorn大学工学部卒業、2007年3月東京大学大学院情報理工学系研究科電子情報学専攻博士課程修了（博士（情報理工学））。同年4月より産総研情報セキュリティ研究センター・日本学術振興会外国人特別研究員、同セキュリティ基盤研究チーム研究員、産総研セキュアシステム研究部門次世代セキュリティ研究グループ研究員を経て、現在は同グループ主任研究員。主な研究内容は、高機能暗号・認証技術の設計および安全性評価。2010年Ericsson Young Scientist Awardを受賞。この論文では高機能暗号全般の研究動向調査、および図の作成を担当。

査読者との議論

議論1　対象とする問題の定義

質問・コメント（松井俊浩：産業技術総合研究所セキュアシステム研究部門）

高機能暗号の安全性の検証や証明が難しいことが繰り返し述べられています。この難しさを克服する方法がこの論文の主題ですので、この言明に適切な名前を付けて、参照してはどうか。

文中では、「職人芸的」という言葉で難しさを情緒的に表現していますが、安全性証明の難しさは、問題の定義にも当たるわけですから、より科学的に論述されるべきです。難しさの中身がわかれば、その解決法が導き出されるはずです。難しさは、複雑性と重なります。複雑性とは、要素の種類、リンク（関係性）の種類、またそれらの総数などの数の問題に帰着されます。それをいかに解きほぐすかが解決の糸口になりそうです。

回答（花岡 悟一郎）

高機能暗号技術の安全性を第三者に納得させることの困難性を、この論文では「暗号の安全性検証問題」と名付けることにしました。暗号の安全性検証が困難であることの根拠として、暗号のトップ会議における高機能暗号に関する論文を調べ、論文において安全性定義、方式の記述、安全性証明がかなりのページ数を占めていることを具体的な数値で示しました。また、暗号の安全性検証問題の解決手段として、機械による安全性証明の自動検証が考えられ、それを用いた場合における入力データサイズに基づいた複雑性の数値化を行うアプローチもあり得ると思われます。しかし、現在のところ、この論文で取り扱われているような高機能暗号技術に対して安全性証明の自動検証ツールの適用は依然困難であるため、これについては今後の研究課題としています。

議論2　モジュールによる解法

質問・コメント（松井 俊浩）

論文では、問題の解決を、問題の要素への分解によるモジュラー化に求めています。要素還元は、科学として正統的アプローチですが、正統的一般論の踏襲にもなってしまいます。モジュラー化と対比される他の問題解決法と比較することはできないでしょうか。あるいは、モジュラー化にも複数の方針があると推測されますが、高機能暗号の問題に即してより精密なガイドラインを与えることができないでしょうか。

質問・コメント（中島 秀之：公立はこだて未来大学）

難しい（あるいは一般の人に馴染みが薄い）話題なので、各所にもう少し説明が必要に思います。特に「どうしたか」だけではなく「何故そうしたか」という意図の記述がシンセシオロジーとしては重要に思います。

回答（花岡 悟一郎）

両編集委員よりいただきました上記の二つのコメントは、互いに深く関連しているものと解釈いたしましたので、まとめて返答させていただければと思います。

ご指摘の通り、提案手法は当然に検討されるべき正当的アプローチを踏襲したものと考えることもできると思います。しかし、これまでの暗号技術研究においてはモジュラー化というアプローチが取られてきませんでした。その理由は二つ考えられます。一つ目は暗号技術においては、達成したい機能が達成できているという「正当性」だけでなく、達成したいこと以外は何もできないという「安全性」を示さなければならないことです。そのため、セキュリティ技術のモジュラー化は他の技術に比べ一層複雑になります。二つ目の理由としては、これまで暗号技術研究者にとって、そのような複雑なモジュラー化を行う動機が不十分であったことが挙げられます。従来技術においては、あえてモジュラー化を行わなくても利用者側でなんとか技術的内容を理解できる範疇であったと考えられ、暗号技術研究者が多大な労力を割いてまでモジュラー化を行おうとするまでには及ばなかったのではないかと思います。それに対し、近年提案がなされている一連の高機能暗号については、その範疇を超えつつあるように思われます。そのような事態を迎え、要素還元という正当的一般論の重要性を明示的に指摘することは当該関連分野にとって極めて有益であると考えております。

また、モジュラー化の方針としては、より信頼できる安全性を追求する観点から、モジュラー化された個々の要素技術がすでに社会で

広く利用実績をもつようなものとなるようにすることを目指す方針を取ることにしています。

以上を含め、全体的に、この論文における著者らの意図が明確となるような記述を追加いたしました。

議論3　モジュールの干渉の問題

質問・コメント（松井 俊浩）

5.2 節に述べられる、構成要素間の干渉が、要素還元論に立ちはだかる壁です。要素技術の単純な加算によっては、全体最適化は達成されません。代理再暗号では、そのような干渉が起こっているのかいないのか、干渉があるとしたらいかに回避されたか、その経験をどの程度に一般化できるか（どういう場合は干渉が少ないと見なせるか）などの知見を追加できないでしょうか。

回答（花岡 悟一郎）

要素間の干渉の除去は、ご指摘の通り、本提案手法において慎重な検討を要する部分です。その対応方針としては、直感的で大雑把な要素還元ではなく、厳密な意味での一般的構成を数学的な安全性証明まで含めて行うことになります。この論文で取り上げた代理再暗号化方式については、そのような一般的構成となっており、個々の要素技術が安全であれば、方式全体の安全性も自動的に保証されるものとなっております。また、より一般的な議論として、暗号要素技術を組み合わせたときに相互に干渉を起こさないことを保証するための安全性概念として、汎用的結合可能性が知られており、これについてもこの論文にて簡単に触れております。

議論4　モジュラー化の効果

質問・コメント（松井 俊浩）

本問題に対比するアプローチである、全体最適化との比較があると説得力が増すでしょう。例えば、省エネシステムというのは、ボイラー、発電機、復水器等の要素機械を効率化するだけでなく、ボイラーで余った熱でお風呂をわかす、復水器の熱をボイラーに戻すなどの要素間の結合を増やして省エネ効果を増します。要素還元は強力ですが、究極の効率を求める場合は、全体で最適化を図る、スクラッチから作り込みをするという選択肢も魅力的なのです。そういう全体最適化と比べて、なぜ暗号技術の開発においては、モジュラー化の方が大切なのかを論じるのも一つの方法でしょう。

回答（花岡 悟一郎）

ご指摘の通り、効率の良さ（暗号文長の短さ、計算コスト等）の観点からはスクラッチから作り込むことによって全体最適を目指すほうが良いと言えます。その一方、暗号技術においては十分な安全性の確保が最優先であり、安全性検証問題を鑑みるにモジュラー化に分があると言えます。安全性証明がなされているかどうかは標準化の観点からも非常に重要であり、今後高機能暗号技術を普及させていくためにはこのような考え方が優先されるべきと思われます。また、モジュラー化によって構成・安全性証明を行った後、要素技術として具体的な構成を当てはめることができ、何を当てはめるかによって要求する性質を持つ、かつ安全性に問題のない高機能暗号技術を構成できることもモジュラー化の魅力と言えます。特に、各要素技術をより効率的なものに交換することで効率化も達成しやすくなることが考えられ、過去には実際にそのような研究例も存在します。