情報処理学会論文誌 Vol.59 No.9 1533–1544 (Sep. 2018)

招待論文

高度データ利活用促進のための高機能暗号とその研究動向

花岡 悟一郎[1,a)] 松田 隆宏[1] 山田 翔太[1] 坂井 祐介[1]

受付日 2018年4月4日, 採録日 2018年6月22日

概要：現在，従来の暗号技術に比べて高度な付加的機能を持つ高機能暗号技術の研究が活発に行われている．高機能暗号を用いることで，暗号化状態のままでデータ処理やアクセス制御などを行うことができるため，これまでプライバシ保護の観点から取扱いが難しかった個人情報などについても，安全性を保ったまま高度に活用することが可能になるものと期待される．本稿では，高機能暗号技術の最近の研究動向について紹介する．

キーワード：高機能暗号，秘匿化データ処理，準同型暗号，属性ベース暗号，関数暗号，代理再暗号化

Advanced Cryptosystems Envisioning Sophisticated Data Utilization and Their Research Trend

Goichiro Hanaoka[1,a)] Takahiro Matsuda[1] Shota Yamada[1] Yusuke Sakai[1]

Received: April 4, 2018, Accepted: June 22, 2018

Abstract: Recently, the research of cryptosystems with advanced functionalities envisioning complex utilizations and applications of data, has been a major trend in the community of cryptography. With such advanced cryptosystems, we can flexibly process data and/or perform access control on encrypted data. Thus, it is widely anticipated that they would enable us to use data such as personalized information, which were previously difficult to use from a privacy perspective, in a more secure and sophisticated manner. In this paper, we review recent research trends on some of the advanced cryptosystems.

Keywords: advanced cryptosystems, secure data processing, homomorphic encryption, attribute-based encryption, functional encryption, proxy re-encryption

1. はじめに

近年の人工知能技術などの目覚ましい発展により，個人情報など機密性の高い情報を用いて新たな価値ある情報を創出し，我々の生活に役立てられるものと考えられているが，プライバシ侵害の危険性などが大きな技術障壁となっている．既存の暗号技術により，これらの機密情報を暗号化することで，そのような機密情報の第三者への漏えいを防ぐことが可能であるが，これらの情報を用いてデータ解析を行う際は，結局暗号化を解く必要があるためデータ解析者への情報の暴露は免れない．また，既存の暗号技術を用いて暗号化を行う場合，暗号化された情報の閲覧は，対応する復号鍵を持つ利用者のみに限られてしまうため，情報の広範な利用は困難となる．そのため，暗号化状態のままでデータ解析やアクセス制御を行うことができる技術の実用化が強く求められている．

上記の問題の解決に向けて，現在，高機能暗号技術の研究が活発に行われている．高機能暗号とは，従来の暗号技術にはない高度な付加機能を持つ暗号技術の総称であり，特定の単一の暗号技術の呼称ではなく，これまでに多種多様な高機能暗号技術の提案がなされている．したがって，従来の暗号技術ではデータの利用と保護の両立が難しい諸状況に対して，個々の要求に応じた適切な高機能暗号技術をシステムごとに選択・設計していくことが求められる．

準同型暗号 [53] は，暗号化状態のままデータ処理を行うことが可能な高機能暗号であり，特に完全準同型暗号は理

[1] 国立研究開発法人産業技術総合研究所
National Institute of Advanced Industrial Science and Technology, Koto, Tokyo 135–0064, Japan
[a)] hanaoka-goichiro@aist.go.jp

論上では任意の計算処理を暗号化状態のまま実行することもできる方式となっている．たとえば，電子投票システムにおいては，各投票者の投票内容を秘匿にしたまま，各候補者の合計得票数を求める必要がある．このような場合，準同型暗号を用いることで，暗号化状態のまま票を集計し，個々の投票内容を明かすことなく合計得票数のみを出力することが可能となる．実際にそのような商用システムの開発もなされている [50]．また，準同型暗号を利用することで，入力情報を秘匿にしたまま，化合物どうしの類似度を計算するシステムなども知られている [64]．

関数暗号 [55] は，特定の 1 人の受信者ではなく，特定の条件を満たす受信者全員が復号可能な高機能暗号であり，また，当該条件を満たさない受信者は復号結果について知ることがいっさいできないという性質を持っている．たとえば，ファイル共有サーバにおいて，ファイルを単純に暗号化した場合，対応する復号鍵を持つ特定の利用者のみがファイルにアクセスすることが可能となる．一方，関数暗号を用いることで，ファイルごとにあらかじめ定められた条件を満たす利用者であれば誰でもファイルにアクセスできるため複数の利用者による広範なファイル共有が可能となる．関数暗号についても，そのような商用システムの開発がなされている [62]．

代理再暗号化 [40] も，特定の 1 人の受信者ではなく，複数の正当な受信者間でファイルの共有が可能な高機能暗号である．関数暗号においては，暗号化の際に指定された復号のための条件を後に変更することができないのに対し，代理再暗号化においては，通常は一般的な公開鍵暗号と同様の利用がなされつつ，必要に応じて本来の受信者が別の受信者を指定して，復号権限を委譲することが可能となっている．代理再暗号化も，以前に商用サービス化がなされている [63]．

本稿では，準同型暗号，関数暗号などを中心に，高機能暗号に関する最近の研究動向について紹介を行う．特に，2 章では準同型暗号およびその数学的基盤技術について，3 章では関数暗号について，4 章では代理再暗号化についてそれぞれ紹介し，5 章では高機能暗号の社会普及を促進させるための研究開発についても紹介を行う．

2. 準同型暗号の研究開発動向

2.1 準同型暗号の概要

公開鍵暗号や秘密鍵暗号においては，安全性要件として，平文情報が適切に秘匿されていることを要求する．一方で，機能性要件として暗号化したままの状態で平文に対して演算を行うことができるという性質を持つと便利な場合がある．このような，暗号化したままの状態で平文に対する演算が可能であるような暗号方式を準同型暗号と呼ぶ．暗号化鍵 EK から定まる暗号化関数を $Enc_{EK}(\cdot)$ で表すとする．直観的には，効率的な演算 $\tilde{\circ}$ が存在し，任意の暗号化鍵 EK およびメッセージ M_0，M_1 に対して $Enc_{EK}(M_1)\tilde{\circ}Enc_{EK}(M_2) = Enc_{EK}(M_1 \circ M_2)$ が成り立つとき，この暗号方式は演算 $\circ$ に対して準同型性を持つという[*1]．ここで，演算子 $\tilde{\circ}$ は（平文どうしに関する演算ではなく）暗号文どうしに対する演算を表しているため，$\circ$ と同じ演算とは限らないことに注意されたい．以下，暗号文の組に $\tilde{\circ}$ を作用させることを，「$\circ$ を暗号文に準同型的に作用させる」と表記する．乗法に関する準同型暗号は乗法準同型暗号，加法に関する準同型暗号は加法準同型暗号と呼ばれる．さらに，暗号化されたメッセージに対して，任意の演算が可能な暗号方式を，完全準同型暗号と呼ぶ．たとえば，完全準同型暗号は，以下のようなシナリオで有用である．企業 A が顧客に関するデータを大量に保持しており，そのデータに対して機械学習アルゴリズムを適用して有用な知見を取り出したいとする．しかし，当該企業は計算資源が乏しく，機械学習アルゴリズムを実行することはできないとする．大量の計算資源を供給できるサーバに計算を委託することで，企業 A は望んだ計算結果を得ることができるが，そのためには，顧客の生データをサーバに渡さなければならない．プライバシ保護の観点から，この方法は望ましくない．そこで，完全準同型暗号を用いた次のような解決策が考えられる．企業 A は，まず，暗号化鍵と復号鍵の組 (EK, DK) を作成する．その次に，自身の手元の顧客情報 D を暗号化鍵 EK で暗号化し，暗号文 $CT = Enc_{EK}(D)$ を作成する．そして，その暗号文 CT をサーバに送る．サーバは，関数 F を準同型的に暗号文に作用させ，$\widetilde{CT} = Enc_{EK}(F(D))$ を得る．ここで，F は機械学習アルゴリズムをデータに作用させる関数として表現したものである．そして，サーバは $\widetilde{CT}$ を企業 A に送る．企業 A は，復号鍵 DK で暗号文 $\widetilde{CT}$ を復号し，$F(D)$ を取り出す．この解決策の利点を確認してみよう．まず，サーバ側は，データ D は与えられず，暗号文 CT を企業 A から与えられただけである．暗号文 CT だけからはデータ D の情報は漏れず，サーバ側に対して顧客情報は守られているといえる．また，企業 A が上記プロトコルを実行するのに必要な計算資源は，データ D の暗号化と，暗号文 $\widetilde{CT}$ の復号のみである．すなわち企業 A は重い機械学習アルゴリズムを実行する必要はなく，比較的軽量な処理だけを行えばよいと考えられる．

[*1] 暗号化関数は一般にはランダム関数であるので，暗号化関数の入力に乱数 R も含め $Enc_{EK}(M, R)$ と記述するのがより正確である．また，演算後に生成される暗号文 $\widehat{CT}$ に対して，乱数 $\tilde{R}$ が存在して $\widehat{CT} = Enc_{EK}(M_1 \circ M_2, \tilde{R})$ と書けるとは限らないケースを考慮して，復号関数 Dec と復号鍵 DK に対して，$Dec_{DK}(Enc_{EK}(M_1)\tilde{\circ}Enc_{EK}(M_2)) = M_1 \circ M_2$ が成り立つ場合に暗号方式は準同型性を持つと定義する方が一般的である．加えて，自明な構成を排除するため，通常は上記の性質に加え，Compactness と呼ばれる条件が成立することを要求する．しかし本稿の目的は直観的アイデアを伝えることなので，細かいことが気になる読者または専門家以外はこの脚注は無視していただいてかまわない．

2.2 準同型暗号の動向

上記のほかにも，多数の理論的，実用的に重要な応用が，完全準同型暗号によって可能になることが知られている．完全準同型暗号の実現は，公開鍵暗号研究の最初期（1978年）にすでに未解決問題として提示されていたが [53]，実際に実現方法が提案されたのはほぼ30年後の2009年であった．ここでは，その歴史を簡単に紹介する．まず，最初の公開鍵暗号であるRSA暗号 [54] はすでに乗法に関する準同型性を有していた．RSA暗号においては，公開鍵が巨大な合成数 N と $\gcd(\phi(N), e) = 1$ であるような自然数 e で，暗号化処理は M を $M^e \bmod N$ に写像するというものである．すなわち，前節に記法を合わせると，

$$Enc_{EK}(M) = M^e \bmod N$$

と書ける．ここで，EK は $EK = (N, e)$ である[*2]．上記の定義に即して，RSA暗号が乗法準同型を満たしていることを確認してみよう．ここで，平文に関する乗法，暗号文に関する乗法をともに法 N での積と定義する．

$$\begin{aligned} & Enc_{EK}(M_1) \cdot Enc_{EK}(M_2) \bmod N \\ &= M_1^e \cdot M_2^e \bmod N \\ &= (M_1 \cdot M_2)^e \bmod N \\ &= Enc_{EK}(M_1 \cdot M_2). \end{aligned}$$

RSA暗号は上記のように乗法準同型性を有している一方で，加法準同型性は有していない（より正確には，暗号文に対して，加法を準同型的に作用させる方法が知られていない）．一方，同じく最初期の公開鍵暗号であるElGamal暗号 [20] や Goldwasser-Micali 暗号 [24] は，限られた意味での加法準同型性を有している．より詳しくは，平文空間がきわめて小さい場合にのみ，加法準同型暗号としてこれらの暗号方式を利用することができる．平文空間が大きい状況においては，Paillier 暗号 [49] や Okamoto-Uchiyama 暗号 [48] などが加法準同型性を持つことが知られている．上記の暗号方式は，暗号理論における古典的な道具である，整数剰余環の乗法群を使っている．2006年には，Boneh らが，暗号学的双線形写像という当時最先端の数学的な道具を利用することにより，さらに複雑な準同型演算が可能であることを示した [10]．具体的には，彼らの提案方式では，平文 $M_1, M_2, \ldots, M_n$ の暗号文から，$\sum M_i M_j$ の暗号文を得ることができる．しかし，彼らの方式では，平文どうしの積の回数が限定されており，任意の関数を暗号文に対して準同型的に適用することが可能なわけではない．たとえば，$M_1 M_2 M_3$ の暗号文を得ることは，彼らの方式ではできない．

[*2] ここで紹介しているのは，いわゆる「教科書RSA」であり，非常に弱い安全性しか有していないことが知られている．たとえば，実利用が可能な公開鍵暗号の安全性として必須とされる強秘匿性を達成していない．

初の完全準同型暗号は Gentry によって2009年に提案された [23]．Gentry の提案方式は多次元空間上の格子という上記で紹介してきた方式とは異なる数学的構造に依拠している．Gentry 方式は，研究コミュニティからは大きな注目を浴び，多くの後続研究によって効率性，安全性ともに提案当初の方式に比べ著しい改善がなされている．しかしながら，現時点ではいまだに十分な効率性を達成することはできておらず，前項で応用例としてあげた完全準同型暗号を利用した機械学習の実利用などは容易ではない．完全準同型暗号や，完全準同型暗号を用いた秘匿状態での機械学習の高速化はその有用性から，研究コミュニティから注目を浴びており，集中的に研究されている（最新の動向に関しては，たとえば文献 [36] や [13] などを参照）．次項では，完全準同型暗号の設計を可能にしている格子理論について解説する．

2.3 格子問題

まず，格子を定義する．線形独立なベクトル $\vec{v}_1, \ldots, \vec{v}_n \in \mathbb{R}^n$ に対して，これらのベクトルの張る格子 Λ は集合

$$\Lambda := \left\{ \sum_{i \in [n]} a_i \vec{v}_i \mid a_i \in \mathbb{Z} \right\}$$

として定義される．格子 Λ に対して，種々の計算問題を考えることができる．たとえば，Shortest Vector Problem（以下 SVP）では，入力としてベクトル $\vec{v}_1, \ldots, \vec{v}_n \in \mathbb{R}^n$ を与えられ，そのベクトルの張る格子の中で，ゼロベクトル以外の一番短いベクトルを求めることを要求される．SVP は NP 困難であることが示されており，きわめて難しい数学的問題だと考えられる．SVP では，（ゼロベクトル以外の）最短ベクトルを求めることを要求するが，この問題を緩和して，最短ベクトルの長さの γ 倍以内の長さを持つベクトルを求める近似問題を定義することもできる．この近似問題は，SVP_γ と呼ばれている．SVP_γ は，γ が次元 n に対して指数的に大きいときには，LLL アルゴリズムを用いて多項式時間で解くことができるが，γ が十分小さいときには NP 困難性が証明されている．SVP や SVP_γ のほかにも CVP や GapSVP といった格子上の問題が考えられている．これらの問題の定義や問題間の帰着に関しては，文献 [43] を参照されたい．格子問題の特徴は，適切にパラメータを選べば量子計算機が存在したとしても確率的多項式時間で解けないと信じられていることである．この特徴は，暗号設計の立場からは非常に重要な性質である．すなわち，格子問題の困難性をうまく利用して暗号技術の設計を行うことができれば，その暗号技術は量子計算機が存在しても破られないことが期待できる．一方で，多くの場所で実利用されている RSA 暗号や楕円曲線暗号などの公開鍵暗号は，量子計算機が登場すると簡単に破ることができることが知られている．より詳細には，RSA 暗号や楕円

曲線暗号は素因数分解問題や離散対数問題の困難性を安全性の根拠としているが，これらの問題は量子計算機の実用化後は高速に解けてしまう．このように，格子に基づく暗号には量子計算機に対する耐性という魅力的な性質があるが，それ以外にも複数の利点がある．まず，先ほども述べたように，完全準同型暗号を，格子構造を用いて設計することができる．また，完全準同型暗号だけではなく，他項に述べる関数型暗号やその他の高機能暗号の設計も可能であることが分かっている．次項では，格子暗号の歴史を簡単に説明する．

2.4 格子暗号の動向

初期の格子問題の困難性を利用した暗号技術の構成の試みとしては，96 年の Ajtai による暗号学的衝突困難ハッシュの構成 [1] があげられる．その後も格子理論を用いた暗号技術の研究は続いていたが，当該研究分野は，Regev の結果 [52] によって指数的に加速した．Regev は，LWE（learning with errors）問題という問題を導入し，当該問題の困難性をある種の格子問題に帰着した．この帰着は量子帰着であり，その格子問題が量子計算機を利用しても困難であるならば，LWE 問題も量子計算機を利用しても困難であることを証明した．LWE 問題は，大雑把にいえば，整数剰余環上のエラー付きの線形方程式の解を求める問題である．Regev は当該論文では，LWE 問題の困難性を仮定して公開鍵暗号を設計した．上記の量子帰着により，これは，その公開鍵暗号が量子計算機に対しても安全性を持つことが期待できる．Regev の論文の発表後，さらなる研究により，ID ベース暗号，属性ベース暗号，さらにはある種の関数型暗号のようなより高機能な暗号技術の設計が可能であることが分かった．属性ベース暗号や関数型暗号については 3 章を参照されたい．これらの拡張は，アクセス制御を高機能化する方向の拡張であるが，準同型性を高める方向の拡張の研究もさかんである．上記で述べたように，2009 年に Gentry によって初の完全準同型暗号が提案されたが，当該方式は，特殊な格子の上の特殊な問題の困難性を安全性の根拠としていた．安全性の根拠を改善し，LWE 問題の困難性に基づいた完全準同型暗号を構成できるかどうかは現時点でも大きな未解決問題である．一方，段階付き完全準同型暗号と呼ばれる完全準同型暗号の緩和版であれば，LWE 問題の困難性に基づいて構成可能であることが 2011 年に示された [14]．2011 年の提案方式では，方式の中で用いる整数剰余環の法のサイズが指数的に大きく非効率的であったが，これはのちに改善され，多項式程度まで引き下げられた [15]．しかしながら，先にも述べたように，実用的な効率性には達していないといえるので，これを改善することは今後の大きな課題であるといえる．

3. 関数暗号

3.1 関数暗号の概要

公開鍵暗号を用いて秘密通信を行おうとする場合，送信者は受信者の公開鍵を入手し，その公開鍵を用いて平文を暗号化する．このとき，平文を複数の受信者に向けて送信したいとすれば，各受信者ごとにその受信者の公開鍵を入手し，平文を個別に暗号化する必要があり効率的でない．また，平文を受信させたい宛先が暗号化の時点では確定しておらず，ある属性を持つ受信者に対して平文を送信したい場合も考えられる．たとえば，企業内の情報システムへの応用例では，ある課に属しているか，あるいは職位が部長以上といった属性を持つ受信者全員に宛てて暗号化を行いたいという場合がそのような状況の例である．このような要求にはそもそも従来の公開鍵暗号では対処できない．

このような要求にも応えられる暗号要素技術が関数暗号（および後述の属性ベース暗号）である．通常の公開鍵暗号においては暗号文は単一の受信者に宛てて暗号化され，その受信者のみが暗号文を復号することが可能である．関数暗号においては，単一の暗号文を複数の受信者に宛てて暗号化することができ，さらに，各受信者ごとに当該の平文の異なる部分情報のみを入手できるようにすることが可能である．具体的には，各受信者はそれぞれ異なる関数が割り当てられた復号鍵を保持する．送信者がある平文を暗号化したとき，各受信者は，平文そのものは入手できないが，平文に各人の関数を適用した値のみが入手できる．

関数暗号の利用シナリオをより具体的に説明する．関数暗号においては，システム全体の管理者である鍵発行センタが設けられる．この鍵発行センタは，システム全体の秘密であるマスタ鍵を秘密に保持し，このマスタ鍵を用いることで各受信者に受信者の関数に応じた復号鍵を発行する権限を持つ．送信者が平文を暗号化すると，受信者は自身の復号鍵を用いて，暗号化された平文に対して関数を適用した値を入手できる．

関数暗号の特殊な場合として，属性ベース暗号（ABE）と呼ばれる暗号要素技術が知られている．属性ベース暗号においては，関数暗号と同様システムの管理者である鍵発行センタが設けられる．各受信者は，鍵発行センタから自身の属性が紐づけられた復号鍵の発行を受ける．送信者は，どのような属性を持つ受信者に暗号文を復号させたいかを記述するポリシを指定して平文を暗号化する．受信者は，自身の属性がポリシを充足するときのみ暗号文を復号でき，平文を入手できる．

上記のような ABE は，暗号文にポリシが割り当てられていることから，暗号文ポリシ ABE（CP-ABE）と呼ばれる．一方で，復号鍵にポリシを割り当て暗号文に対して属性を割り当てる，鍵ポリシ ABE（KP-ABE）と呼ばれる要素技術も知られている．CP-ABE は，上述のとおり，企業

内における情報共有システムにおける利用が典型的な応用の 1 つである．一方 KP-ABE は，有料会員向けコンテンツ配信システムにおける利用が典型的である．すなわち，事業者は各コンテンツをそのコンテンツの属性（たとえば映画のジャンルなど）を用いて暗号化する．各加入者は，ABE 自身の購読条件（どのジャンルの映画を購入したかなど）が割り当てられた復号鍵の発行を受ける．これにより各加入者は各自の購読条件にあてはまるコンテンツのみを復号できるようになり，コンテンツを購読できる．

3.2 ABE の動向

3.2.1 Sahai-Waters ファジー IBE

ABE の概念は 2005 年に Sahai らによりファジー IBE として提案された [55]．

ID ベース暗号（IBE）とは，ABE の最も基本的な形式の 1 つである [56]．IBE は，通常の公開鍵暗号と同様に 1 対 1 の通信に用いるものであるが，暗号化の際に公開鍵証明書の検証が必要なくなるという利点がある．IBE においては，ABE と同様鍵発行センタが設けられ，この鍵発行センタは各受信者に対して受信者の ID が割り当てられた復号鍵を発行する．暗号化の際には，送信者は受信者の ID のみを用いて暗号化を行うことができ，受信者の公開鍵および公開鍵証明書を検証する必要はない．受信者は，鍵発行センタにより割り当てられた復号鍵を用いて暗号文を復号できる．この要素技術は，復号鍵，暗号文それぞれに ID が割り当てられ，両者が厳密に一致するときにのみ復号可能な ABE となっている．

ファジー IBE は IBE の拡張となっており，復号鍵と暗号文に割り当てられた ID どうしの距離がある閾値以内であるときに復号可能な ABE の一種である．具体的には，各復号鍵および各暗号文に集合が割り当てられ，その集合の共通部分が閾値個以上である場合にのみ復号が可能となる．

Sahai-Waters ファジー IBE 方式は，同時期に提案された IBE である Boneh-Boyen IBE [6], [8] の拡張として理解できる．そこでまず，Boneh-Boyen IBE 方式の概略を述べたあと，その拡張である Sahai-Waters ファジー IBE への拡張について述べる．IBE 方式の設計において中心的な課題は，すべての暗号文を復号する権限を持つマスタ鍵をいかにして特定の ID に宛てられた暗号文のみ復号できる復号鍵へと権限委譲するかにある．以下，Boneh-Boyen IBE 方式においてこの課題はどのようにして解決されたかを説明する．Boneh-Boyen IBE 方式において送信者は，ある ID を持つ受信者に対して平文を送信したいとき，鍵発行センタが公開する公開パラメータをある種の公開鍵として用いて一時鍵を生成し，それにより送信したい平文を暗号化する．これにより鍵発行センタは平文を復号する権限を持つが，この権限は以下のようにして各受信者に委譲される．まず，（鍵発行センタだけでなく）受信者が復号できるよう，送信者は暗号文に受信者の ID に応じた**補助情報**を添える．一方鍵発行センタは，受信者の ID（と乱数）を用いてマスタ鍵を**マスク**し，マスクされた鍵を復号鍵として受信者へ発行する．このマスクされた鍵は，上述の補助情報と組み合わせたときにのみ送信者のセッション鍵を復元することができる仕組みを備えており，それにより受信者は送信された暗号文を復号することが可能となる．

上記のような視点から Sahai-Waters ファジー IBE 方式を説明すると，以下のようになる．Sahai-Waters ファジー IBE 方式においては，上述の IBE と同様に鍵発行センタがマスタ鍵を保持する．鍵発行センタが各受信者に復号鍵を発行する際にはまず，各鍵ごとにマスタ鍵を閾値秘密分散法により分割する．このとき，秘密分散法のユーザとしては受信者の属性情報（属性集合）に含まれる各要素を用い，シェアを生成する．さらに，このユーザは上述の Boneh-Boyen IBE 方式における ID にも対応し，それぞれ Boneh-Boyen IBE 方式同様の**マスク**処理が施される．一方送信者は，自身の属性情報（属性集合）を Boneh-Boyen IBE 方式の ID に対応させて上述の**補助情報**を添えて暗号文を生成する．復号鍵に含まれる ID の集合と暗号文に含まれる ID の集合とが閾値個以上の共通部分を持てば，Boneh-Boyen IBE 方式における復号処理を実行することができることで閾値個以上のシェアが入手でき，最終的にセッション鍵が復元される．

3.2.2 Goyal-Pandey-Sahai-Waters ABE

Goyal らは，復号鍵に対してより広いクラスのポリシを割り当てられる，初めての KP-ABE を提案した [27]．この方式は，Sahai-Waters においては集合の共通部分の大小に限定されていたポリシのクラスについて，一般の単調論理式で記述されるポリシを取り扱える方式となっている．具体的には，セットアップ時に可能な属性値の集合が固定され，暗号文にはその可能な属性値から選ばれた属性値の集合が割り当てられる．一方復号鍵には，その可能な属性値をリテラルに持つ単調論理式が割り当てられる．復号の際には，単調論理式に現れる各リテラルについて，そのリテラルが暗号文に割り当てられた集合に属しているときに 1 を，属していないときに 0 を代入する．この操作によって単調論理式が充足されるときに，受信者は暗号文を復号できる．

このような構造は，一般のアクセス構造を利用できる秘密分散方式によって実現できる．そのような秘密分散方式においては，閾値秘密分散方式と同様，分散したい秘密をシェアに分解しそれらシェアをユーザに配布する．そのように分散された秘密情報を復元するためにどのユーザのシェアが必要であるかを記述するのがアクセス構造である．（我々の文脈では）アクセス構造はユーザの名前をリテラルに持つ単調論理式により記述される．ユーザのシェ

アが入手できているときは 1 を，そうでない場合には 0 をリテラルに割り当て，単調論理式が充足されるときかつそのときにのみ分散された秘密が復元されるのが，一般のアクセス構造を利用できる秘密分散方式である．

この技術を用いて，Goyal らは以下のようにして KP-ABE を構成した．まず鍵発行センタは，Sahai-Waters ファジー IBE 方式と同様に自身の秘密鍵を生成して秘密に保持し，その秘密鍵に対応する公開パラメータを公開する．鍵発行時には，鍵発行に用いるポリシを秘密分散方式のアクセス構造と見なし，秘密鍵をシェアに分解する．この秘密鍵を上述の Sahai-Waters ファジー IBE 方式，Boneh-Boyen IBE 方式と同様にマスクし，復号鍵として受信者に発行する．このとき，ポリシ中に現れるリテラル（すなわち属性値）が Boneh-Boyen IBE 方式における ID に対応する．送信者は，暗号文に属性として割り当てたい属性値の集合を鍵発行時と同様 ID と見なして平文を暗号化し，それに対応した補助情報を暗号文に含めておく．受信者は，受信した暗号文に含まれている補助情報を用いてシェアの復元処理を行い，セッション鍵を入手する．

3.2.3 Lewko-Okamoto-Sahai-Takashima-Waters ABE

Lewko らは，初めての適応的安全な ABE を提案した [38]．上述の 2 方式を含めそれ以前の方式はいずれも選択的安全性と呼ばれる弱い安全性しか証明されておらず，適応的安全な方式の構成は大きな未解決問題となっていた．ここで，適応的安全とは，攻撃の対象となる暗号文に割り当てられるポリシ（KP-ABE であれば属性）を攻撃対象となる暗号文を入手する直前に決定してよいモデルにおいて安全であることをいう．一方で，選択的安全とは，攻撃の対象となる暗号文に割り当てられるポリシを，攻撃対象のシステムの公開パラメータを見る前に決定しなければならないモデルにおいて安全であることをいう．

本方式の提案時点で知られていた適応的安全な IBE の構成法はいずれも，分割（partitioning）技法という技法に依存したものであった [6], [7], [9], [59]．この技法は，安全性証明を行う際の帰着アルゴリズムの構成に用いられる技法である．同方式は，可能な ID の集合を 2 つに分割し，一方に属する ID については帰着アルゴリズムが復号鍵を生成可能（よって鍵生成オラクルをシミュレート可能），もう一方に属する ID については安全性の根拠とする計算困難問題を埋め込みできる（よってその暗号文を解読する攻撃者の能力を使って計算困難問題を解くことができる），というように分割するというものである．

この技法は，IBE のようなポリシがきわめて限定された場合においては一定の成果をあげてきた．しかしながら，ABE のようなポリシの集合や属性の集合の要素が相互に関連を持つ場合においては，この技法を適用する方法は知られていなかった．

Lewko らは，Waters により開発された dual system encryption の技法 [58] を用いてこの困難を克服した．この dual system encryption 技法は，適応的安全な IBE を構成するための技法として提案されたものである．一方で，この技法は適応的安全な ABE を構成することにも有用であり，実際に，以下に述べるように，Lewko らはこの技法を用いて適応的安全な ABE を構成している．そこで，ここではまずこの dual system encryption 技法について説明する．この技法においては，IBE の復号鍵や暗号文に関して semi-functional と呼ばれる特殊な形式を導入する．この形式で生成される秘密鍵や暗号文は，方式の実利用の際にはいっさい用いられないが，安全性証明中でのみ用いられるものである．semi-functional な秘密鍵は，semi-functional でない秘密鍵とは計算量的に識別不可能であり，semi-functional な暗号文とそうでない通常の暗号文も同様である．このような暗号文，復号鍵について，semi-functional な暗号文は通常の復号鍵を用いて復号でき，また，semi-functional な復号鍵は通常の暗号文を復号できる．しかしながら，semi-functional な鍵を用いて semi-functional な暗号文は復号できず，復号アルゴリズムを実行してもランダムな値が出力されるだけである．

この技法を用いて，Waters は以下のようにして適応的安全な IBE の安全性証明を行った．証明はハイブリッド論法により行われる．第 1 のゲームは通常の平文の識別不可能性（IND-CPA 性）のゲームである．第 2 のゲームは，ゲーム中に現れるチャレンジ暗号文を semi-functional なものに変更する．このゲームは，semi-functional な暗号文が通常の暗号文と識別不可能であることから，第 1 のゲームと識別不可能である．以降のゲームでは，攻撃者が入手する復号鍵を，順次 semi-functional なものに変更していく．最終的に，ゲーム中に現れるすべての暗号文および復号鍵がすべて semi-functional となり，この状況下では比較的容易に平文の秘匿性を証明可能となる．

Lewko らは，上述の dual system encryption のテクニックを用いて CP-ABE 方式を構成している．構成には，上述の Goyal らの方法と同様，一般のアクセス構造を利用できる秘密分散方式を用いている．具体的には，送信者は，暗号化時にセッション鍵を生成するための乱数を秘密分散方式で分散し，それをマスクした値を暗号文に含めておく．受信者は，暗号文に含まれているシェアからセッション鍵を復元するための補助情報を復号鍵として鍵発行センタから受け取る．これを用いて受信者は暗号文からセッション鍵を復元する．

3.2.4 それ以降の進展

上述の属性ベース暗号方式はいずれも，楕円曲線上のペアリングと呼ばれる計算困難問題に基づく方式であった．その一方で，前節で述べたように，近年は格子問題にその安全性を依拠する方式が耐量子性，高機能性の双方の観点

から注目されている．そのような研究において特筆すべきは，Gorbunov らによる，任意の論理回路をポリシとして利用可能な方式があげられる [26]．また，本章の冒頭で述べたように，ABE は関数暗号の一種とも理解できるものであった．これに関して，より広いクラスの関数を利用可能な，一般の関数暗号を取り扱った研究も進められている．そのような関数暗号は，識別不可能性難読化と呼ばれるきわめて強力な暗号要素技術から構成されている [22]．識別不可能性難読化は，まだ社会実装までにはかなりの隔りがあるが，その具体的構成法（どのような計算困難問題から構成できるか）やそれを用いた他の暗号要素技術の構成法などに関して活発な研究の真っ只中にあり，今後の動向が注目される．

4. 代理再暗号化

4.1 代理再暗号化の概要

代理再暗号化（Proxy Re-encryption，以下 PRE）とは，事前に作成された “再暗号化鍵” $RK_{A,B}$ を用いて，ある受信者 A に向けて暗号化された暗号文 $CT_A = Enc_{PK_A}(M)$ を，復号することなく，別の受信者 B に向けた暗号文 $CT_B = Enc_{PK_B}(M)$ へと変換（再暗号化）することができる公開鍵暗号方式である（ここで，PK_A と PK_B は，それぞれ A と B の公開鍵を表す）．再暗号化手続きを行うエンティティ（代理人と呼ばれる）に対して平文の情報が漏れないことが PRE の安全性要件であり，この安全性のおかげで，再暗号化手続きを第三者に委託することができる．

PRE 方式は，再暗号化鍵を双方向の暗号文の再暗号化に使うことができるかどうか（すなわち，$RK_{A,B}$ をユーザ A 宛てからユーザ B 宛て，およびその逆方向の暗号文再暗号化に使用できるかどうか），そして，再暗号化された暗号文をさらに別のユーザ宛ての暗号文へとさらに再暗号化できるかどうか，により，4 種類に大別できる．$RK_{A,B}$ によってユーザ A 宛てからユーザ B 宛てへの暗号文の再暗号化，およびその逆方向の再暗号化も可能な “双方向型” PRE 方式の再暗号化方式では，再暗号化鍵の作成に，両ユーザの秘密鍵が必要となるが，ユーザ A 宛てからユーザ B 宛てへの暗号文の再暗号化のみが可能な “単方向型” PRE の場合は，通常は変換元のユーザの秘密鍵と変換後のユーザの公開鍵から再暗号化鍵を作成可能な方式を考える．

PRE の代表的な利用シナリオとして，「データ共有可能な暗号化クラウドストレージ」があげられる．各ユーザは，自分自身の公開鍵・秘密鍵を作成し，自分自身の公開鍵を用いて，クラウドサーバに暗号化したデータをアップロードする．もしあるユーザ A が，自身の所有する暗号化データ CT_A を別のユーザ B と共有したい場合は，再暗号化鍵 $RK_{A,B}$ を作成し，クラウドサーバに送る（ユーザ A はその後，オフラインになってもよい）．再暗号化鍵を受け取ったクラウドサーバは，$RK_{A,B}$ を用いて CT_A を再暗号化し，再暗号化された暗号文 CT_B を B へと送る．B は自身の秘密鍵 SK_B を用いて CT_B を復号することができる．PRE の安全性により，この操作において，クラウドサーバにはいっさい CT_A の中身の情報は漏れない[*3]．

このような代理再暗号化を利用したクラウドストレージサービスはすでに一部で商用化も開始されている（国内でも 2012 年に東芝によるサービスが開始したが [63]，現在は終了している）．

4.2 PRE の動向

ここでは，PRE に関する主要な研究成果を紹介する．なお，PRE は現在も活発に研究が進んでいるトピックの 1 つであり，重要な成果であっても紙面の都合上紹介できないものが数多くある．興味を持った読者は，ここであげた文献や近年のサーベイ [46] などを参照されたい．

4.2.1 代理人を用いた暗号技術，および初期の PRE の研究

PRE は，再暗号化および変換後の受信者による復号，という操作を一連の手続きと見なすと，元の暗号文の復号権限を第三者の “代理人” へと委譲することができる公開鍵暗号と考えることができる．このような，秘密鍵を利用する操作の一部を代理人へと委譲することができる機能を持つ公開鍵暗号技術の概念は，Mambo ら [40] により初めて提案され，Blaze ら [5] により拡張された．現在主流となっている PRE のシンタックスおよび安全性定義は，Ateniese ら [3] が提案したものが基礎となっている．

Blaze ら [5] は，ElGamal 暗号（の亜種）を基に，最初の双方向型 PRE 方式を提案した．この方式は非常に簡素であるため，ここで簡単に振り返る．以下では g を素数位数 p の巡回群の生成元とし，$a, b, r \in \mathbb{Z}_p$ を整数，M を平文とする．Blaze らの方式では，鍵対 $(PK_A, SK_A) = (g^a, a)$ を持つユーザ A 宛ての暗号文は $C_A = (c_1, c_2) = (g^{ar}, g^r \cdot M)$ という形である[*4]（r は暗号化用の乱数）．A は，$M = c_2/(c_1)^{1/a}$ と計算することで C_A を復号できる．この A 宛ての暗号文 C_A を，鍵対 $(PK_B, SK_B) = (g^b, b)$ を持つユーザ B 宛ての暗号文へと変換するには，変換鍵 $RK_{A,B} = b/a \bmod p$ を用いて，$c_1' = (c_1)^{RK_{A,B}} = g^{br}$ を計算し，$C_B = (c_1', c_2) = (g^{br}, g^r \cdot M)$ とすればよい．

Ivan ら [35] は，再暗号化鍵の生成に，代理人と再暗号化前の暗号文の受信者の相互通信を要する，現在主流のシンタックスとは異なる単方向型 PRE 方式を提案した．その後，Ateniese ら [3] が，代理人と受信者の相互通信を必要としない，現在主流のシンタックスでの単方向型 PRE を，双線形群（ペアリングと呼ばれる暗号学的な双線形写

[*3] この利用シナリオでは，ユーザ A が単独で（ユーザ B の秘密鍵を知らずに）再暗号化鍵を作成する必要があるため，単方向型の PRE 方式が必要である．

[*4] 暗号文の構成要素において A の秘密鍵 a が掛かる対象が，元来の ElGamal 暗号とは逆になっている．

像を持つ巡回群）を用いて初めて示した．また，彼らは，単方向型 PRE を用いた分散型暗号化ストレージにおけるデータのアクセスコントロール手法も提案している．このシステムの基本的なアイデアは，前述の暗号化クラウドストレージと同様である．

4.2.2 PRE の選択暗号文攻撃に対する安全性

上記の PRE 方式 [3], [5] は，受動的な攻撃者や代理人に対する安全性のみしか達成しておらず，暗号文を容易に改変可能である．一方，現在，（PRE でない，通常の）公開鍵暗号方式において，実システムで利用される際に事実上標準的な安全性要件とされるのは，選択暗号文攻撃に対する安全性（CCA 安全性）である．CCA 安全性は，攻撃者が攻撃対象とする暗号文以外のあらゆる暗号文の復号結果を観測できたとしても，攻撃対象の暗号文の秘密を得ることができない，ということを定式化したものであり，特に，暗号文を別の関連する内容の暗号文への改変しようとする攻撃に対する安全性（頑強性と呼ばれる）を保証することが知られている．実システムで利用される PRE でも，公開鍵暗号における CCA 安全性と同様の安全性を持つことが望ましいのはいうまでもない．ここで，PRE では，再暗号化鍵を持つ代理人に対しても秘匿性が保証されなければならないことを思い出されたい．すなわち，PRE の安全性を考える際は，攻撃対象のユーザ宛てから別のユーザ宛て暗号文への再暗号化を行うことができる再暗号化鍵を持つ攻撃者を想定しなければならない．しかし，再暗号化鍵を持つ代理人は，暗号文を他のユーザ宛ての暗号文へと変換できてしまう．このため，攻撃者にとっての，“攻撃対象の暗号文” を厳密に定義するのが難しい．現在主流となっている PRE の CCA 安全性は，Replayable CCA 安全性 [17] と呼ばれる，CCA 安全性を実用上問題ない程度に少し弱めた安全性を基にしたものである．現在主流の CCA 安全性を満たす初めての双方向型 PRE 方式は，Canetti ら [16] によって初めて示された．また，現在主流の CCA 安全性を満たす単方向型 PRE 方式は，Libert ら [39] によって初めて提案された．その後，上記 Replayable CCA 安全性を，通常の公開鍵暗号における CCA 安全性により近い（すなわち，より強い）安全性を満たす方式の提案がいくつかなされている [30], [34].

4.2.3 PRE の秘匿性以外の性質に関する研究

暗号文の秘匿性以外の安全性以外にも，PRE 方式が満たしていると有用な様々な性質や安全性が，これまでにいくつか提案されてきた．Ateniese ら [3] は，暗号文の受信者が，自身の受け取った暗号文が，送信者によって直接作成されたものか，それとも別のユーザ宛てに送られた暗号文が代理人によって再暗号化されたものかを識別できないこと（Proxy Invisibility），$RK_{A,B}$ を持つ代理人と，秘密鍵 SK_B を持つユーザ B が結託したとしても，A の秘密鍵 SK_A を構成できないこと（Collusion Safe），$RK_{A,B}$ を持つ代理人，SK_B を持つユーザ B，および別のユーザ C の公開鍵 PK_C を組み合わせたとしても，A 宛ての暗号文を C 宛ての暗号文へと変換できる再暗号化鍵 $RK_{A,C}$ を生成できないこと（Non-transferability），などを PRE 方式の望ましい性質としてあげた．単方向型 PRE の場合，その定義より，Collusion Safe を満たしていなければ，Non-transferability も満たすことができない．逆にいえば，後者の性質を満たしていれば，前者も満たすため，後者のほうがより望ましい（安全性として強い）性質である．しかし，Non-transferability は，そもそも厳密な定式化自体が難しく，著者らが知る限り，現在でもそれを達成した方式は知られていない．これに対し，Hayashi ら [31], [32] は，Non-transferability を弱めた安全性として，再暗号化鍵の偽造不可能性（Unforgeability）と呼ばれる性質を定式化し，それを満たす方式を提案した[*5]．Ateniese ら [2] は，再暗号化鍵から，元の暗号文の受信者と変換後の受信者の情報が漏れないという性質（Anonymity）を定式化し，その性質を満たす方式を示した．Hohenberger ら [33] は，代理再暗号化における再暗号化手続きのプログラムは，「元の受信者の秘密鍵で一度復号し，それを変換後の暗号文の受信者の公開鍵で暗号化する」という機能が（暗号学的な意味で）難読化されたプログラムである，と解釈し，暗号学的難読化の安全性を満たす方式を示した．

4.2.4 PRE の高機能化

ある一定の期間のみ再暗号化を可能にするなど，再暗号化鍵にある種の制限を加えることができる方式も考えられている．文献 [3] では，一定の期間のみ再暗号化鍵を利用可能となっている方式を “Temporary” な PRE 方式と呼び，自身らの方式を Temporary な方式へと拡張する方法が示された（しかし，Temporary な PRE 方式の厳密な定式化は与えられていない）．このような再暗号化機能を制限できる PRE 方式は，後に Type-based PRE [57] や Conditional PRE [60] として定式化されている．最近では，Derler ら [19] が，期間限定の再暗号化機能を持つ PRE の機能を拡張し，各受信者の秘密鍵や代理人の持つ再暗号化鍵を，一定時間ごとに，公開鍵の変更やユーザ同士またはユーザ・サーバ間の通信いっさいなしに更新できる機能，および，現在の秘密鍵や再暗号化鍵が漏洩しても，過去の暗号文の秘匿性が影響を受けない，という安全性（前進安全性，Forward Security）を PRE に導入し，それを満たす構成を提案した．また，別の方向性として，Ohata ら [47] は，代理人による再暗号化手続きが正しく行われたかを，再暗号化後の暗号文の受信者が検証できる PRE 方式を示した．

代理再暗号化機能を持つ高機能暗号の研究もいくつかなされてきている．たとえば，Green ら [28] の ID ベース

[*5] 文献 [32] で提案された方式には後に不備が見つかったが，文献 [31] で修正版の方式が示された．

PRE 方式や，Kawai ら [37] の属性ベース PRE 方式などがあげられる．また，暗号文を同一の暗号方式の中での暗号文へと変換するだけでなく，複数の暗号方式間にわたった再暗号化を可能とする方式も考案されている．たとえば，Matsuo [42] は，ある公開鍵暗号方式の暗号文から，ある IBE 方式の暗号文へと再暗号化が可能な方式を提案した．最近では，Yu ら [61] が，（1 つの方式だけでなく）ある要件を満たす ABE から，“任意の” 公開鍵暗号方式や ABE へと再暗号化可能な方式を提案した．この方式では，再暗号化後の暗号文は，実際の方式とは暗号文の形や復号方法が変わってしまうものの，その方式における復号鍵を用いて復号できる．

ただし，（再暗号化機能を持たない）通常の ABE と異なり，高機能な PRE では，まだ確立された安全性定義が存在しておらず，すべての方式が同じレベルの安全性を満たしているわけではない点に注意する必要がある．

4.2.5 更新可能（共通鍵）暗号

ここまで説明してきたものは，すべて “公開鍵” 版の PRE に関するものであったが，最後に，“共通鍵” 版の PRE ともいえる**更新可能暗号**についてふれる．更新可能暗号とは，その名のとおり鍵の更新が可能な共通鍵暗号方式であり，共通鍵で一度暗号化した暗号文を，全体を復号することなく別の新たな鍵で暗号化された暗号文へと変換することができる．このような鍵の更新機能は，Amazon の AWS Key Management Service [4] などでサポートされており，更新可能暗号は，実システムで利用されている機能が後で研究界で研究対象となった例の 1 つである．Boneh ら [11]（文献 [12] のフルバージョン）は，更新可能暗号方式の安全性定義を与え，鍵に関する準同型性を持つ疑似ランダム関数を用いた方式を示した．また，最近では，Everspaugh ら [21] が，Boneh らの定義では考えられていなかった認証暗号の安全性をとらえた定義を定式化し，Boneh らと同様の要素技術を用いてその新たな安全性を満たす方式を複数示すとともに，AWS などで実際に利用されている鍵更新手法や Boneh らの方式は，更新可能暗号としての十分な安全性を満たしていないことを示した．しかし，現在知られる鍵準同型性を持つ疑似ランダム関数は，巡回群や格子などの公開鍵系の技術を用いたものしか知られておらず，通常の認証暗号と比べて圧倒的に遅い．文献 [21] の安全性を満たしつつ，通常の認証暗号と同等の効率性を持つ更新可能暗号の構成は，重要な未解決問題として残されている．

5. 高機能暗号の社会普及促進に向けて

ここまでにおいて紹介を行ったとおり，現在までに様々な高機能暗号の提案がなされており，今後幅広い応用がなされるものと期待される．しかしその一方で，高機能暗号の機能は従来の暗号技術に対して複雑であるため，暗号理論分野の専門家以外には，詳細な理解が必ずしも容易ではなく社会普及の障壁ともなっている [29]（たとえば，準同型暗号によって入力情報を秘匿したままデータ処理を行い，その計算結果のみを導出したとしても，高機能暗号についての理解が十分でない利用者にとっては入力情報が本当に秘匿されているかは確信が持てず，導入には躊躇してしまうことも考えられる）．本章においては，そのような障壁を排除するための研究動向について紹介を行う．

暗号技術は機能や安全性を視覚的に把握することが難しい技術であるため，その理解を促す技術は古くから検討がなされている．たとえば，Quisquater らは，ゼロ知識証明 [25] の概念について，年少者でも理解ができるような平易な説明方法の検討を行っている [51]．また，Shamir らは，秘密分散を視覚化し，ノイズが印刷されたシートを重ね合わせると秘密情報が画像として復元される視覚的秘密分散の提案を行っている [45]．

これらの一連の研究において，近年では，物理的なカードを用いて秘密計算プロトコルを実現するカードプロトコル [18] の研究が活発に行われている．特に，近年では Mizuki ら [44] の成果を受けて，それを発展させる研究が数多く行われており，当該分野に関する研究発表数が急激に増加している．また，国内外のいくつかの教育機関においても，高度な暗号技術を紹介するためのツールとして導入がなされている [41]．

筆者らも準同型暗号の機能について社会全体における理解の促進を目的とし，準同型暗号の機能を物理的に再現した準同型暗号ボックスの開発を行っている．この詳細な紹介については稿を改めて紹介したい．

参考文献

[1] Ajtai, M.: Generating Hard Instances of Lattice Problems (Extended Abstract), *28th ACM STOC*, pp.99–108, ACM Press (1996).

[2] Ateniese, G., Benson, K. and Hohenberger, S.: Key-Private Proxy Re-encryption, *CT-RSA 2009*, Fischlin, M. (Ed.), LNCS, Vol.5473, pp.279–294, Springer, Heidelberg (2009).

[3] Ateniese, G., Fu, K., Green, M. and Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage, *ACM Trans. Inf. Syst. Secur.*, Vol.9, No.1, pp.1–30 (2006).

[4] AWS: Protecting Data Using Client-Side Encryption, available from ⟨https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html⟩.

[5] Blaze, M., Bleumer, G. and Strauss, M.: Divertible Protocols and Atomic Proxy Cryptography, *EUROCRYPT '98*, Nyberg, K. (Ed.), LNCS, Vol.1403, pp.127–144, Springer, Heidelberg (1998).

[6] Boneh, D. and Boyen, X.: Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles, *EUROCRYPT 2004*, Cachin, C. and Camenisch, J. (Eds.), LNCS, Vol.3027, pp.223–238, Springer, Heidelberg (2004).

[7] Boneh, D. and Boyen, X.: Secure Identity Based En-

cryption Without Random Oracles, *CRYPTO 2004*, Franklin, M. (Ed.), LNCS, Vol.3152, pp.443–459, Springer, Heidelberg (2004).
[8] Boneh, D. and Boyen, X.: Efficient Selective Identity-Based Encryption Without Random Oracles, *Journal of Cryptology*, Vol.24, No.4, pp.659–693 (2011).
[9] Boneh, D. and Franklin, M.K.: Identity-Based Encryption from the Weil Pairing, *CRYPTO 2001*, Kilian, J. (Ed.), LNCS, Vol.2139, pp.213–229, Springer, Heidelberg (2001).
[10] Boneh, D., Goh, E.-J. and Nissim, K.: Evaluating 2-DNF Formulas on Ciphertexts, *TCC 2005*, Kilian, J. (Ed.), LNCS, Vol.3378, pp.325–341, Springer, Heidelberg (2005).
[11] Boneh, D., Lewi, K., Montgomery, H. and Raghunathan, A.: Key Homomorphic PRFs and Their Applications, Cryptology ePrint Archive, Report 2015/220 (2015), available from ⟨http://eprint.iacr.org/2015/220⟩.
[12] Boneh, D., Lewi, K., Montgomery, H.W. and Raghunathan, A.: Key Homomorphic PRFs and Their Applications, *CRYPTO 2013, Part I*, Canetti, R. and Garay, J.A. (Eds.), LNCS, Vol.8042, pp.410–428, Springer, Heidelberg (2013).
[13] Bourse, F., Minelli, M., Minihold, M. and Paillier, P.: Fast Homomorphic Evaluation of Deep Discretized Neural Networks, *IACR Cryptology ePrint Archive*, Vol.2017, p.1114 (2017) (online), available from ⟨http://eprint.iacr.org/2017/1114⟩.
[14] Brakerski, Z. and Vaikuntanathan, V.: Efficient Fully Homomorphic Encryption from (Standard) LWE, *52nd FOCS*, Ostrovsky, R. (Ed.), pp.97–106, IEEE Computer Society Press (2011).
[15] Brakerski, Z. and Vaikuntanathan, V.: Lattice-based FHE as secure as PKE, *ITCS 2014*, Naor, M. (Ed.), pp.1–12, ACM (2014).
[16] Canetti, R. and Hohenberger, S.: Chosen-ciphertext secure proxy re-encryption, *ACM CCS 07*, Ning, P., di Vimercati, S.D.C. and Syverson, P.F. (Eds.), pp.185–194, ACM Press (2007).
[17] Canetti, R., Krawczyk, H. and Nielsen, J.B.: Relaxing Chosen-Ciphertext Security, *CRYPTO 2003*, Boneh, D. (Ed.), LNCS, Vol.2729, pp.565–582, Springer, Heidelberg (2003).
[18] den Boer, B.: More Efficient Match-Making and Satisfiability: The Five Card Trick, *EUROCRYPT '89*, Quisquater, J.-J. and Vandewalle, J. (Eds.), LNCS, Vol.434, pp.208–217, Springer, Heidelberg (1990).
[19] Derler, D., Krenn, S., Lorünser, T., Ramacher, S., Slamanig, D. and Striecks, C.: Revisiting Proxy Re-encryption: Forward Secrecy, Improved Security, and Applications, *PKC 2018, Part I*, Abdalla, M. and Dahab, R. (Eds.), LNCS, Vol.10769, pp.219–250, Springer, Heidelberg (2018).
[20] El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Information Theory*, Vol.31, No.4, pp.469–472 (1985).
[21] Everspaugh, A., Paterson, K.G., Ristenpart, T. and Scott, S.: Key Rotation for Authenticated Encryption, *CRYPTO 2017, Part III*, Katz, J. and Shacham, H. (Eds.), LNCS, Vol.10403, pp.98–129, Springer, Heidelberg (2017).
[22] Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A. and Waters, B.: Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits, *54th FOCS*, pp.40–49, IEEE Computer Society Press (2013).
[23] Gentry, C.: Fully homomorphic encryption using ideal lattices, *41st ACM STOC*, Mitzenmacher, M. (Ed.), pp.169–178, ACM Press (2009).
[24] Goldwasser, S. and Micali, S.: Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information, *14th ACM STOC*, pp.365–377, ACM Press (1982).
[25] Goldwasser, S., Micali, S. and Rackoff, C.: The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract), *17th ACM STOC*, pp.291–304, ACM Press (1985).
[26] Gorbunov, S., Vaikuntanathan, V. and Wee, H.: Attribute-based encryption for circuits, *45th ACM STOC*, Boneh, D., Roughgarden, T. and Feigenbaum, J. (Eds.), pp.545–554, ACM Press (2013).
[27] Goyal, V., Pandey, O., Sahai, A. and Waters, B.: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, *ACM CCS 06*, Juels, A., Wright, R.N. and Vimercati, S. (Eds.), pp.89–98, ACM Press (2006).
[28] Green, M. and Ateniese, G.: Identity-Based Proxy Re-encryption, *ACNS 07*, Katz, J. and Yung, M. (Eds.), LNCS, Vol.4521, pp.288–306, Springer, Heidelberg (2007).
[29] Hanaoka, G.: Towards User-Friendly Cryptography, *Mycrypt 16*, Phan, R.C.-W. and Yung, M. (Eds.), LNCS, Vol.10311, pp.481–484, Springer, Heidelberg (2016).
[30] Hanaoka, G., Kawai, Y., Kunihiro, N., Matsuda, T., Weng, J., Zhang, R. and Zhao, Y.: Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption, *CT-RSA 2012*, Dunkelman, O. (Ed.), LNCS, Vol.7178, pp.349–364, Springer, Heidelberg (2012).
[31] Hayashi, R. and Matsushita, T.: A Proxy Re-Encryption Scheme with the Unforgeability of Re-Encryption Keys against Collusion Attacks, Cryptology ePrint Archive, Report 2014/849 (2014), available from ⟨http://eprint.iacr.org/2014/849⟩.
[32] Hayashi, R., Matsushita, T., Yoshida, T., Fujii, Y. and Okada, K.: Unforgeability of Re-Encryption Keys against Collusion Attack in Proxy Re-Encryption, *IWSEC 11*, Iwata, T. and Nishigaki, M. (Eds.), LNCS, Vol.7038, pp.210–229, Springer, Heidelberg (2011).
[33] Hohenberger, S., Rothblum, G.N., Shelat, A. and Vaikuntanathan, V.: Securely Obfuscating Re-encryption, *TCC 2007*, Vadhan, S.P. (Ed.), LNCS, Vol.4392, pp.233–252, Springer, Heidelberg (2007).
[34] Isshiki, T., Nguyen, M.H. and Tanaka, K.: Proxy Re-Encryption in a Stronger Security Model Extended from CT-RSA2012, *CT-RSA 2013*, Dawson, E. (Ed.), LNCS, Vol.7779, pp.277–292, Springer, Heidelberg (2013).
[35] Ivan, A. and Dodis, Y.: Proxy Cryptography Revisited, *NDSS 2003*, The Internet Society (2003).
[36] Juvekar, C., Vaikuntanathan, V. and Chandrakasan, A.: GAZELLE: A Low Latency Framework for Secure Neural Network Inference, *IACR Cryptology ePrint Archive*, Vol.2018, p.73 (2018) (online), available from ⟨http://eprint.iacr.org/2018/073⟩.
[37] Kawai, Y. and Takashima, K.: Fully-Anonymous Functional Proxy-Re-Encryption, Cryptology ePrint Archive, Report 2013/318 (2013), available from ⟨http://eprint.iacr.org/2013/318⟩.
[38] Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K. and Waters, B.: Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, *EUROCRYPT 2010*, Gilbert, H.

(Ed.), LNCS, Vol.6110, pp.62–91, Springer, Heidelberg (2010).
[39] Libert, B. and Vergnaud, D.: Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption, *PKC 2008*, Cramer, R. (Ed.), LNCS, Vol.4939, pp.360–379, Springer, Heidelberg (2008).
[40] Mambo, M. and Okamoto, E.: Proxy cryptosystem: Delegation of the power to decrypt cipher-texts, *IEICE Transactions*, Vol.80, No.1, pp.54–63 (1997).
[41] Marcedone, A., Wen, Z. and Shi, E.: Secure Dating with Four or Fewer Cards, Cryptology ePrint Archive, Report 2015/1031 (2015), available from ⟨http://eprint.iacr.org/2015/1031⟩.
[42] Matsuo, T.: Proxy Re-encryption Systems for Identity-Based Encryption, *PAIRING 2007*, Takagi, T., Okamoto, T., Okamoto, E. and Okamoto, T. (Eds.), LNCS, Vol.4575, pp.247–267, Springer, Heidelberg (2007).
[43] Micciancio, D. and Goldwasser, S.: *Complexity of Lattice Problems – A Cryptographic Perspective*, Springer International Series in Engineering and Computer Science, Vol.671, Springer (2002).
[44] Mizuki, T., Kumamoto, M. and Sone, H.: The Five-Card Trick Can Be Done with Four Cards, *ASIACRYPT 2012*, Wang, X. and Sako, K. (Eds.), LNCS, Vol.7658, pp.598–606, Springer, Heidelberg (2012).
[45] Naor, M. and Shamir, A.: Visual Cryptography, *EUROCRYPT '94*, Santis, A.D. (Ed.), LNCS, Vol.950, pp.1–12, Springer, Heidelberg (1995).
[46] Nuñez, D., Agudo, I. and López, J.: Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation, *J. Network and Computer Applications*, Vol.87, pp.193–209 (2017).
[47] Ohata, S., Kawai, Y., Matsuda, T., Hanaoka, G. and Matsuura, K.: Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption, *CT-RSA 2015*, Nyberg, K. (Ed.), LNCS, Vol.9048, pp.410–428, Springer, Heidelberg (2015).
[48] Okamoto, T. and Uchiyama, S.: A New Public-Key Cryptosystem as Secure as Factoring, *EUROCRYPT '98*, Nyberg, K. (Ed.), LNCS, Vol.1403, pp.308–318, Springer, Heidelberg (1998).
[49] Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, *EUROCRYPT '99*, Stern, J. (Ed.), LNCS, Vol.1592, pp.223–238, Springer, Heidelberg (1999).
[50] PR Newswire Association LLC: BOSCoin Develops Electronic Voting System based on Homomorphic Encryption that Guarantees Anonymity and Singular Votes (2018), available from ⟨https://www.prnewswire.com/news-releases/boscoin-develops-electronic-voting-system-based-on-homomorphic-encryption-that-guarantees-anonymity-and-singular-votes-300641128.html⟩.
[51] Quisquater, J.-J., Quisquater, M., Quisquater, M., Quisquater, M., Guillou, L.C., Guillou, M.A., Guillou, G., Guillou, A., Guillou, G., Guillou, S. and Berson, T.A.: How to Explain Zero-Knowledge Protocols to Your Children (Rump Session), *CRYPTO '89*, Brassard, G. (Ed.), LNCS, Vol.435, pp.628–631, Springer, Heidelberg (1990).
[52] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, *37th ACM STOC*, Gabow, H.N. and Fagin, R. (Eds.), pp.84–93, ACM Press (2005).
[53] Rivest, R., Adleman, L. and Dertouzos, M.: *Foundations of Secure Computation*, chapter On data banks and privacy homomorphisms, pp.169–180, Academic Press (1978).
[54] Rivest, R.L., Shamir, A. and Adleman, L.M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (online), DOI: 10.1145/359340.359342 (1978).
[55] Sahai, A. and Waters, B.R.: Fuzzy Identity-Based Encryption, *EUROCRYPT 2005*, Cramer, R. (Ed.), LNCS, Vol.3494, pp.457–473, Springer, Heidelberg (2005).
[56] Shamir, A.: Identity-Based Cryptosystems and Signature Schemes, *CRYPTO '84*, Blakley, G.R. and Chaum, D. (Eds.), LNCS, Vol.196, pp.47–53, Springer, Heidelberg (1984).
[57] Tang, Q.: Type-Based Proxy Re-encryption and Its Construction, *INDOCRYPT 2008*, Chowdhury, D.R., Rijmen, V. and Das, A. (Eds.), LNCS, Vol.5365, pp.130–144, Springer, Heidelberg (2008).
[58] Waters, B.: Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions, *CRYPTO 2009*, Halevi, S. (Ed.), LNCS, Vol.5677, pp.619–636, Springer, Heidelberg (2009).
[59] Waters, B.R.: Efficient Identity-Based Encryption Without Random Oracles, *EUROCRYPT 2005*, Cramer, R. (Ed.), LNCS, Vol.3494, pp.114–127, Springer, Heidelberg (2005).
[60] Weng, J., Yang, Y., Tang, Q., Deng, R.H. and Bao, F.: Efficient Conditional Proxy Re-encryption with Chosen-Ciphertext Security, *ISC 2009*, Samarati, P., Yung, M., Martinelli, F. and Ardagna, C.A. (Eds.), LNCS, Vol.5735, pp.151–166, Springer, Heidelberg (2009).
[61] Yu, Z., Au, M.H., Yang, R., Lai, J. and Xu, Q.: Achieving Flexibility for ABE with Outsourcing via Proxy Re-Encryption, *ACM AsiaCCS 2018*, Kim, J., Ahn, G., Kim, S., Kim, Y., López, J. and Kim, T. (Eds.), pp.659–672, ACM Press (2018).
[62] 株式会社三菱電機ビジネスシステム：パッケージプラス(R) トランスポーター，入手先 ⟨https://www.melb.co.jp/products/general_affairs/transporter.html⟩.
[63] 株式会社東芝：デジタル貸金庫，入手先 ⟨https://tosafebox.com/⟩.
[64] 産業技術総合研究所：化合物データベースの秘匿検索技術【産総研公式】(2014)，入手先 ⟨https://www.youtube.com/watch?v=1J_wiykXArE⟩.

花岡 悟一郎

1997 年東京大学工学部卒業，2002 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 年産業技術総合研究所入所．現在，産総研情報技術研究部門高機能暗号研究グループ長．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．平成 30 年度科学技術分野の文部科学大臣表彰科学技術賞（2018 年），ドコモ・モバイル・サイエンス賞（2016 年），電子情報通信学会論文賞（2008 年），英国計算機学会 The Wilkes Award（2007 年）等受賞．

松田 隆宏

2006 年東京大学工学部卒業，2011 年同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）），以降日本学術振興会特別研究員（PD）を経て，2013 年産業技術総合研究所入所．現在，産業技術総合研究所主任研究員．暗号技術の設計・安全性証明をはじめとする暗号理論の研究に従事．ドコモ・モバイル・サイエンス賞（2016 年），SCIS イノベーション論文賞（2014 年，2012 年）等受賞．

山田 翔太

1987 年生．2009 年東京大学工学部計数工学科卒業．2011 年同大学院修士課程修了．2014 年同博士課程修了．博士（科学）．2014 年学術振興会特別研究員（PD）．2015 年産業技術総合研究所研究員．暗号理論の研究に従事．

坂井 祐介

2009 年電気通信大学電気通信学部卒業，2014 年同大学院情報理工学研究科総合情報学専攻博士後期課程修了（博士（工学）），2014 年より日本学術振興会特別研究員（PD）を経て，2017 年産業技術総合研究所入所．現在，産業技術総合研究所情報技術研究部門高機能暗号研究グループ研究員．公開鍵暗号技術に関する研究に従事．SCIS 論文賞（2011 年），IWSEC 2010 Best Student Paper Award（2010 年）受賞．