7-5　群構造維持暗号

大久保美也子

暗号技術は安全な情報システムに必要不可欠な技術であるが、暗号技術を用いたアプリケーション設計にはセキュリティに関する高度な専門知識が必要である。プライバシ問題が内在するIoTの普及につれて、様々な暗号アプリケーションのニーズが増大し、セキュリティを保つことは社会的に大きな課題となっている。

本研究は、高度な暗号アプリケーションを、統一されたデータ形式のインターフェースをもつ複数の暗号技術を相互接続して、簡単かつ安全に開発できるようにする新たな設計コンセプト「群構造維持暗号系（Structure-Preserving Cryptography: SP暗号系）」を提唱し、それを具体化するSPディジタル署名、SPコミットメント、その他の暗号技術を開発したものである。レゴブロック®のように簡単に相互接続可能で効率的な暗号技術の提供によって、アプリケーション開発における設計コストと脆弱性リスクを低減し、セキュリティな構成を容易に実現することにより"セキュア"なシステム設計に貢献する。

1　はじめに

暗号技術は安全な情報システムに必要不可欠な技術であるが、暗号技術を用いたアプリケーション設計にはセキュリティに関する高度な専門知識が必要である。プライバシ問題が内在するIoTの普及につれて様々な暗号アプリケーションのニーズが増大し、セキュリティを保つことは社会的に大きな課題となっている。

本研究は、高度な暗号アプリケーションを、統一されたデータ形式のインターフェースをもつ複数の暗号技術を相互接続して簡単かつ安全に開発できるようにする新たな設計コンセプト「群構造維持暗号系（Structure-Preserving Cryptography: SP暗号系）」[2] [11]を提唱し、それを具体化するSPディジタル署名[1] [2] [5] [8] – [12]、SPコミットメント[1] [4] [11]、その他の暗号技術[6] [7] [10]を開発し、またそれらの効率的構成の下限を理論的に示したものである[2] – [4]。レゴブロック®のように簡単に相互接続可能で効率的な暗号技術の提供によって、アプリケーション開発における設計コストと脆弱性リスクを低減し、セキュアなシステム構築に貢献する。

従来の構成原理は、データ形式が異なることを数学的構造として本質的に利用していた。本研究では、統一されたデータ形式で利用できる数学的構造を利用した新たな構成原理によって、具体的なSP暗号技術を構成することに成功している。

著名国際会議CRYPTO'10における世界初の効率的なSPディジタル署名の発表[1]によってSP暗号系の研究は急速に発展し、広範な応用に供している。多数の研究成果が著名国際会議・論文誌で発表されており、SP暗号系は暗号理論において活発な研究分野を形成している。

2　対象とする課題

情報がビジネス上の大きな価値を生み、社会システム上も重要な役割を果たす一方で、パスワードやマイナンバーなど重要情報の漏えいが後を絶たない。IoTにおけるプライバシ侵害の問題も懸念されるなど、安全・安心な情報システムを構築する暗号技術の重要性は一層増している。

クラウドのアクセス制御やビットコインに代表される暗号通貨といった高度なアプリケーションでは、ディジタル署名を付けて公開鍵暗号で暗号化し、その処理の正しさをゼロ知識証明で示す、というように様々な暗号技術を接続して利用することが多い。ところが、各々の暗号技術はそれ単体で安全であるように設計されており、安全性確保の都合によって入出力のデータ形式も異なる。このインターフェースの不一致が暗号技術の相互接続を困難にしており、設計コストの増大、現実的でない安全性仮定の導入、さらには脆弱性を生じる要因となっている。

この問題解決のため、各々の暗号技術のインターフェースを単一のデータ形式で統一し、簡単に直接接続できる暗号技術を探求した。本来、入出力のデータ形式が異なることは、暗号において本質的に重要な数

学的構造の実現に寄与するものである。例えば、従来のディジタル署名では、署名対象の文書とそれに対するディジタル署名を異なるデータ形式とすることで署名の偽造を困難にしている。これらを全てひとつの形式に統一してしまうことは、従来利用してきた数学的構造が利用できなくなることを意味し、単なる形式の変更ではない、本質的に新しい研究課題を生じることとなった。

3　構成要素

暗号に利用される効率的なペアリング群はデータ型としてスカラー値、ソース群要素、ターゲット群要素の 3 つの型を持つ。SP 暗号系は、

- 入出力がソース群要素のみからなっている
- 入出力関係の正しさが群演算とペアリング演算のみで検証できる

という特徴を有する暗号技術の総称であり、また、それらの暗号技術をシームレスに接続して安全なアプリケーションを構成する設計コンセプトである。前者の特徴は暗号技術の直接的な相互接続を可能とし、後者の特徴によって入出力関係の正しさを効率的に示すことが可能となる。

データ形式及び演算に関するこれらの規定は SP 暗号系の高い相互接続性と利便性を約束するが、一方で、具体的な SP 暗号技術の構成においては技術的なハードルとなる。特に、データ形式がソース群要素に限定されていることは、従来標準的に利用していたスカラー値からソース群要素、あるいはソース群要素からターゲット群要素への一方向性演算を直接的に利用できないという問題を生じる。

これに対して、本研究では、ソース群からターゲット群への一方向性を、ターゲット群の要素を用いずにソース群の要素のみで利用できるよう工夫することで効率的な SP 暗号技術を構成することに成功した。例えば、本研究による SP ディジタル署名では、2 対のソース群要素 (X1,Y1), (X2,Y2) のペアリングの積を 1 対のソース群要素 (X3,Y3) のペアリングで表すことが困難であることを利用して、ペアリングの結果であるターゲット群の要素を直接用いることなく、複数の正しい署名を合成して偽造署名を作ることができないように署名を構成した。

4　群構造維持暗号系のフレームワーク

SP 暗号系の入出力インターフェースはすべてペアリング群のソース群要素に統一されているため、複数の暗号技術を接続して用いる場合にも入出力の形式を合わせる変換は不要である。これによって、多様なアプリケーションの設計ごとに異なる暗号技術の組み合わせが存在する中で、個々の状況に沿った形式変換等を独自に考慮することによる設計コストや脆弱性発生のリスクを完全に取り除くことができる。

具体的な性能を以下に例示する。相互接続性のない一方の暗号技術がスカラー値を出力し、もう一方がソース群要素を入力として取る場合、スカラー値の各ビットをソース群要素 1 個による表現に形式変換するなどの処理が必要となる。スカラー値ひとつを知っていることをソース群要素に対する非対話証明で示すには、その形式変換の正しさの証明も含めて数千個のソース群要素が必要となることが知られている。ところが、SP 暗号技術で相互接続が可能になると、ソース群要素ひとつを知っていることを示す非対話証明によって十数個のソース群要素に抑えることができ、顕著な効率の改善が得られる。

ペアリング群上の暗号は、すでに様々な実装が実用に供しており、スマートフォンでも実行できる程度の演算で処理可能である。本研究で具体的構成を示した SP ディジタル署名、SP コミットメントも同様で、SP ディジタル署名は、署名・公開鍵とも高々数個のソース群要素からなり、署名生成、署名検証もそれぞれ群演算、ペアリング計算数回分程度の計算で実行でき、十分な実用性を備えている。SP ディジタル署名を応用したシステムのデモンストレーションも行われ、その性能が実証されている

(http://www.atmarkit.co.jp/ait/articles/1312 /05 / news103.html)。

5　従来技術に対する優位性

以下では、安全性を保証するために必要な仮定の妥当性、データサイズや計算の効率、相互接続性、脆弱性のリスクの観点から、従来技術と SP 暗号技術を比較する。

【従来技術 1: ランダムオラクルによる構成】

ハッシュ関数を理想化したランダムオラクル仮定に基づいて暗号技術を構成する研究が '90～ '00 年代を中心に行われ、多くの暗号技術がこのモデルで構成されている。このモデルでは暗号技術の相互接続は比較的容易で、個々の暗号技術も効率が良い。しかし、理想化されたハッシュ関数は現実には実装不可能であるため、このモデルによる安全性の保証は現実と乖離があると考えられている。

【従来技術 2: 一般的な計算量的過程に基づく構成】

一方向性関数の存在など一般的な仮定に基づく構成では、仮定の妥当性は高いものの、構成される個々の

暗号技術の効率が悪い上、直接的な相互接続ができない。例えば、ある処理手順が正しく実行されたことを保証するには、その手順を論理回路による表現に変換し、その回路の入出力関係をゼロ知識証明で示すことになる。複雑な形式変換による実装上の脆弱性リスクや著しい効率低下のため、理論的な実在証明の範ちゅうを出ないアプリケーションが多い。

【従来技術 3: ペアリング群を用いた構成】

ペアリング群を用いて構成した従来の暗号技術では、個々の暗号技術の効率は良いが、相互接続性がない。例えば、ディジタル署名においてスカラー値で表された秘密鍵を所有していることを非対話証明 [13] で示すことがあるが、**4** で述べたとおりデータ形式の変換に伴って数千から数万個のソース群要素が必要となり、実用的ではない。

【本研究の技術】

SP 暗号系によるアプリケーションの構成は、妥当性の高いペアリング群上の数学的困難性仮定に基づいて安全性が保証でき、実用的な演算量で容易に実現できる上、接続による脆弱性混入のリスクもない。以下に従来技術に対する優位点をまとめる。

従来技術 1 との比較：SP 暗号系はペアリング群上の数学的な困難性仮定に基づいており、一般的に利用される楕円離散対数問題と同様に高い妥当性を有する点で優れている。

従来技術 2 との比較：個々の暗号技術の効率及び相互接続性の点で SP 暗号系がはるかに優れている。

従来技術 3 との比較：相互接続性の点で SP 暗号系が優れている。例示した状況において本研究による完全 SP ディジタル署名を用いると、秘密鍵がソース群要素であるため直接接続による効率的な非対話証明によって数個から数十個のソース群要素で済む。

6 具体的な応用例

SP 暗号系は、モジュール的な構成を可能とする相互接続性を有する要素技術として、安全性とプライバーの両要件を必要とするシステムやアプリケーションの具現化に貢献する。

例えば、投票システムを電子的に実現する場合、投票者の本人認証を必要とする一方、投票内容に対する投票者の匿名性をも満たさねばならず、いずれが欠けても現在の物理的な投票プロセスに代わることはできない。このような一見相反する要求条件を満たさねばならないシステムやアプリケーションの構成に、SP 暗号系は特に有用であり、安全で効率的なシステムを構築することが可能となる。

本人認証と投票の匿名性を物理的に実現する場合、封筒と証明印が有効となる。それぞれの投票者は投票用紙を封筒に入れ、その封筒に選挙管理委員のような投票者の本人確認を行う第三者機関の証明印を押してもらう。投票者は、その証明印付きの封筒をポストに投函する。集計者は郵送されたその封筒を受け取り、その証明印が第三者機関のものであることを確認し、封筒を開け、中に入っている投票をカウントに含める。これを暗号技術を用いて、電子的に実現する場合、投票者は投票用紙を暗号化し、その暗号文に対する第三者機関が作成したディジタル署名を得る。次に、この暗号文を公開の通信路を経由して集計者に送る。この際、その暗号文は投票用紙を暗号化したものであり、第三者機関がディジタル署名を付与したものであるということを、暗号文やディジタル署名を直接見せずに証明する。このマジックのような仕組みは、理論的には暗号技術を用いることにより実現できる。群構造維持暗号系の技術は、実際にこの仕組み容易に実現することができる。群構造維持暗号系の暗号方式、ディジタル署名、証明方式を用いることで容易な相互接続を実現することができ現実的な電子投票システムの構成が可能となる。

また、SP 暗号系は、プライバシ保護を必要とするシステムやアプリケーション（例えば、クレデンシャルシステム [14] など）を構成するための実用性のある強力な構成部品である一方、形式検証を用いた安全性の解析やコンピュータによるシステムデザインなど分野でも研究対象として注目を集め始めている [15]–[17]。

7 今後の展望

初めての効率的な SP ディジタル署名の発表以来、様々な暗号技術が SP 暗号系のコンセプトに基づいて構成され、多数のアプリケーションが世界中の研究者によって開発された。公平な同時契約に役立つ検証可能暗号、アクセス制御に利用できる紛失通信、匿名の権限委譲を可能にするグループ署名などはその一例である。

また、一般的に効率の下界を示すことは困難な問題であるが、本研究で示した SP ディジタル署名と SP コミットメントは出力サイズに関する効率が理論的最適値と一致する初めての最適構成である [2]–[4]。

SP 暗号系の特性はまた、当初の意図を超えて利用され、新たな機能を実現した準同型ディジタル署名や同値類ディジタル署名と呼ばれる技術の出現をもたらし、応用の範囲が広がっている。さらに、限定された演算のみを用いて実現できる特徴を利用して、安全となる全ての構成を計算機によって全数探索して安全な SP ディジタル署名を設計するなど、自動設計・検証

の分野にも影響を及ぼしている。

ディジタル署名、コミットメント、公開鍵暗号はいずれも暗号の基盤技術であり、これらに対してSP暗号系のコンセプトに沿った具体的構成を与えたことで、多種多様なアプリケーションが実現されている。さらに、IDベース暗号など多様な暗号技術に対してSP特性を持つ構成を示すことで、SP暗号系の適用範囲拡大が期待できる。

また、SP暗号系のコンセプトは前述のとおり、既存の暗号技術に当てはまらない新しい機能や特徴を持つ暗号技術の出現を促しており、今後、別の発展の方向として、より多くの新しい暗号技術が生み出される土壌となることが期待される。

SP暗号系が基づくペアリング群は、暗号で利用される最も標準的な数学的基盤であり、様々なプラットフォームでの実装や高速化の研究が進展している。これらの技術の発展はSP暗号系の実用性をより高めるものである。さらに、将来的にはペアリングから多重線形写像への発展も考えられ、より高度な暗号技術がSP暗号系のコンセプトの下に開発されることも予想される。

【参考文献】

1 Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, “Structure-Preserving Signatures and Commitments to Group Elements,” CRYPTO 2010, pp.209–236, LNCS 6223, Springer, 2010.

2 Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, “Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups,” CRYPTO 2011, pp.649–666, LNCS 6841, Springer, 2011.

3 Masayuki Abe, Jens Groth, and Miyako Ohkubo, “Separating Short Structure-Preserving Signatures from Non-interactive Assumptions,” ASIACRYPT 2011, pp.628–646, LNCS 7073, Springer, 2011.

4 Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo, “Group to Group Commitments Do Not Shrink,” EUROCRYPT 2012, pp.301–317, LNCS 7237, Springer, 2012.

5 Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo, “Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions,” ASIACRYPT 2012, pp.4–24, LNCS 7658, Springer, 2012.

6 Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo, “Tagged One-Time Signatures: Tight Security and Optimal Tag Size,” Public Key Cryptography 2013, pp.312–331, LNCS 7778, Springer, 2013.

7 Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo, “Double-trapdoor anonymous tags for traceable signatures,” Int. J. Inf. Sec. 12(1), pp.19–31, 2013.

8 Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi, “Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures,” TCC 2014, pp.688–712, LNCS 8347, Springer, 2014.

9 Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi, “Structure-Preserving Signatures from Type II Pairings,” CRYPTO (1) 2014, pp.390–407, LNCS 8616, Springer, 2014.

10 Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi, “Fully Structure-Preserving Signatures and Shrinking Commitments,” EUROCRYPT 2015, pp.35–65, LNCS 9057, Springer, 2015.

11 Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, “Structure-Preserving Signatures and Commitments to Group Elements,” Journal of Cryptology 2015, pp.1–59, Springer, 2015.

12 Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo, “Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions,” Journal of Cryptology 2015, pp.1–46, Springer, 2015.

13 Jens Groth, Amit Sahai: Efficient Noninteractive Proof Systems for Bilinear Groups. SIAM J. Comput. 41(5), pp.1193-1232 (2012)

14 Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, Markulf Kohlweiss: Composable and Modular Anonymous Credentials: Definitions and Practical Constructions. ASIACRYPT (2) 2015, pp.262-288

15 Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, Mehdi Tibouchi: Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds. Public Key Cryptography 2015, pp.355-376

16 Gilles Barthe, Benjamin Grégoire, Benedikt Schmidt: Automated Proofs of Pairing-Based Cryptography. ACM Conference on Computer and Communications Security 2015, pp.1156-1168

17 Miguel Ambrona, Gilles Barthe, Benedikt Schmidt: Automated Unbounded Analysis of Cryptographic Constructions in the Generic Group Model. EUROCRYPT (2) 2016, pp.822-851

大久保美也子　（おおくぼ　みやこ）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、暗号プロトコル