様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　５　月　２５　日現在

機関番号：　１１３０１
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１６００１

研究課題名（和文）属性ベース署名の集約化による機能向上と効率化

研究課題名（英文）A proposal of attibute-based aggregate signatures

研究代表者
長谷川　真吾（Hasegawa, Shingo）

東北大学・教育情報基盤センター・助教

研究者番号：８０５６７２１４

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：本研究では、デジタル署名方式の発展方式である属性ベース署名方式について、複数の文書と署名を同時に扱い、その検証コストを削減する集約機能を持つ方式を考案した。具体的には、集約機能つき属性ベース署名方式のフレームワークを考案し、その構成方法を与えた。
また、研究の遂行にあたり、基礎研究として、署名方式の安全性として求められる安全性証明の構築条件について考察を行い、種々の条件、およびそれを回避し高い安全性を持つデジタル署名方式の構成方法を与えた。

研究成果の概要（英文）：We propose attibute-based aggregate signatures. We introduce a formal definition and framework of attibute-based aggregate signatures and its security models, and also construct a concrete scheme which satisfies the definition and the security of attibute-based aggregate signatures.
Additionally, we consider several conditions so that signature schemes achieve the provable security which is the standard security notion in the modern cryptography. We give some impossibilities on proving the security of signature scheme, and also give several constructions of signature scheme to avoid such impossibility results and have high security.

研究分野：　暗号理論

キーワード：　デジタル署名　安全性証明　IDベース署名　属性ベース署名

１．研究開始当初の背景

通常のデジタル署名方式では、個人に対して秘密鍵が発行され、その秘密鍵を用いて作成された署名は対応する文書が秘密鍵の所有者により作成されたことを保証する。一方、実際の運用においては、文書を作成した個人よりもその個人の所属や肩書きといった属性が重視されることが多い。このような状況に対応したデジタル署名の発展系として、属性ベース署名方式が考案された。属性ベース署名方式は、その名前の通り各個人が持つ属性を元に署名を作成する方式であり、秘密鍵は個人ではなく属性に対して発行される。また、署名者は自身が持つ属性に対応する秘密鍵を自由に組み合わせて署名を作成することができる。さらに、作成された署名から実際に署名を作成した者の情報を入手することが不可能であることも合わせて保証される。この特性は、政府が募集するパブリックコメントなど、文書内容の正当性確保のため作成者の属性を保証したいが、回答は匿名で行いたいといった要請がある場合に非常に有効に働く。

しかしながら、現代の日常生活においては、各種機関の発行する証明書などはそれを単一で使用するのではなく、複数の機関が発行する複数の証明書を組み合わせて使用する場合が多い。例えば、大学の卒業証明書、住民票、病院の発行する健康診断書などである。この場合、証明書それぞれに機関が発行する署名が添付されるため、それら全てを合わせたもののサイズは非常に大きなものとなってしまうという問題がある。

２．研究の目的

上記のような、複数の文書と署名を同時に扱う際に、その合計サイズを縮小するための方式として、集約署名方式が知られている。集約署名方式とは、複数の文書とその署名があった場合に、それらの署名を１つの署名に圧縮することのできる署名方式である。すなわち、集約署名方式を使用することで、どれだけ多くの文書があろうとも、単一の署名でそれら全ての正当性を検証することができることになる。しかしながら、現在のところ属性ベース署名方式の中で集約機能を持つものは存在していない。そこで、本研究では集約機能を持つ属性ベース署名方式の開発を行い、その現実世界に即した利便性を高めることを目的とする。

３．研究の方法

(１)デジタル署名における安全性証明構築のための基礎研究

デジタル署名をはじめとする現代の暗号プロトコルには、その安全性を保証するために、安全性証明と呼ばれる数学的証明を構成することが実質的に標準の安全性保証手段となっている。

つまり、デジタル署名の設計の際には、それに付随する安全性証明の構成も考慮しなければならない。しかしながら、どのような方式にも安全性証明が構成できるという訳ではなく、一部の条件の下では安全性証明を構成することがそもそも不可能であるという研究も行われてきている。すなわち、やみくもに方式の設計を行い、安全性証明を構成できるか試行する、というアプローチは非効率であるといえる。

よって、本研究を進める上では、まず安全性証明が構成できる、またできないための条件を明らかにすることを基礎研究として行う。

研究を進めるにあたっては、２大安全性モデルであるランダムオラクルモデルと、標準モデルの２つについて、署名方式が安全性証明を持つための条件解明を行う。ランダムオラクルモデルとは、理想的なハッシュ関数を仮定するモデルであり、方式の構成が効率的になる、安全性証明が簡素になるなどの利点がある。標準モデルとは、現実に運用されているハッシュ関数をモデル化したものであるため、より現実世界での安全性に直結した安全性解析が可能になる。

(２)集約機能を持つ属性ベース署名の設計

研究の最終目標である集約機能を持つ属性ベース署名方式を開発する。

まず、上記(１)で得られた結果を参考に、通常の属性ベース署名を開発し、その安全性証明を行う。安全性証明において採用するモデルは、現実世界への影響を考慮し、標準モデルでの構成を基本とするが、開発方式の処理効率が悪くなる場合には、ランダムオラクルモデルでの開発も検討することとする。

４．研究成果

(１)デジタル署名の安全性証明構築の可能・不可能性

デジタル署名の安全性証明において、証明が成立するための条件を考察した。一般に安全性証明を構成する際には、様々な暗号学的仮定を使用するのが通常であるが、そのような仮定の使用はより実現性が高い仮定であるほど、また使用する仮定の個数が少ないほど望ましいとされている。

まず、研究の土台として、代表的なデジタル署名方式の１つである、Schnorr 署名方式の安全性を考察した。Schnorr 署名は既にその安全性がランダムオラクルモデルにおいて証明されているが、研究の結果、従来用いられている数学的仮定をより強力なものに置き換えたとしても、標準モデルにおける安全性は証明できないことを示した。これは、Schnorr 署名方式の安全性は理想的な実装技術の元では保証されるが、現在の暗号技術でそのまま実装した場合、その安全性が保証さ

れないことを意味する。
続いて、Schnorr 署名方式が属する、Fiat-Shamir 型デジタル署名と呼ばれる署名方式のカテゴリについても研究を行った。
Fiat-Shamir 型デジタル署名は、処理速度が効率的なデジタル署名を構築できるフレームワークであるが、研究の結果、Schnorr 署名の場合と同様に、ランダムオラクルモデルでは安全性を証明できるが、ノンプログラマブルランダムオラクルモデルでは安全性を証明できないことを示した。ノンプログラマブルランダムオラクルモデルとは標準モデルに近い証明モデルであり、このモデルで安全性が証明できなことは、標準モデル、すなわち現実世界における安全性が保証されないことを意味する。これは、Fiat-Shamir 型デジタル署名の安全性は理想的な実装モデルの元では保証されるが、現実の暗号技術でそのまま実装した場合、その安全性が保証されないことを意味し、暗号技術における安全性と処理速度におけるトレードオフについて、１つの境界を与えたといえる。

(２)高い安全性を持つデジタル署名方式の開発
上記の結果で示された安全性証明の限界を回避するため、Fiat-Shamir 型デジタル署名を改良した一般的構成法を考案し、その安全性を証明した。提案構成法は、既存の Fiat-Shamir 型デジタル署名の全てに適用可能な変換方法でもあり、その安全性はノンプログラマブルランダムオラクルモデルで証明されているため、現実世界においても同等の安全性を持つことが期待される。また、処理効率においては従来の Fiat-Shamir 型デジタル署名よりも若干落ちるものの、同程度の処理効率を保つことに成功した。すなわち、既存の Fiat-Shamir 型デジタル署名方式の効率性を担保したまま、安全性を大幅に向上させることが可能である。

(３)安全性と効率性を両立する ID ベースデジタル署名方式の開発
上記（２）の結果を応用し、属性ベース署名方式の特別な場合である ID ベース型デジタル署名について、高い効率性を持つことで知られている Galindo-Garcia ID ベース署名について、その方式を改良し、従来よりも高い安全性を持つ ID ベース型デジタル署名の開発を行った。
提案方式は、既存の Galindo-Garcia 方式が loose 安全性と呼ばれる弱い安全性しか満たしていないのに対し、tight 安全性と呼ばれる非常に強固な安全性を満たしていることが証明されている。また、公開鍵サイズなどの効率性については Galindo-Garcia 方式よりもおおよそ 2 倍程度の低下となってしまうが、実際の署名生成時の効率は同程度であり、元々高い効率性を持つ Galindo-Garcia 方式のことを鑑みると、現実的には十分に許容範囲であるといえる。

(４)集約機能を持つ属性ベースデジタル署名方式の開発
デジタル署名の発展技術である、属性ベースデジタル署名について、多数の署名を同時に検証可能な、集約機能つき属性ベース署名方式のフレームワークを考案した。これは本研究で提案するまで知られていなかった結果であり、今後集約機能を持つ属性ベース署名方式の研究を進める上での重要な基礎を固めたといえる。また、考案したフレームワークの条件を満たす具体的な構成方式を初めて構築した。本研究で構成した集約機能付き属性ベース署名方式は、多線形写像と呼ばれる、近年最も注目されている暗号技術を使用している。この多線形写像については、その安全性に問題がある報告もなされているため、これを使用しない集約機能付き属性ベース署名方式を考案することは今後の大きな課題である。

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 7 件）

① Masayuki Fukumitsu、Shingo Hasegawa、Black-Box Separations on Fiat-Shamir-Type Signatures in the Non-Programmable Random Oracle Model、IEICE Trans. Fundamentals, Special Section on Cryptography and Information Security、査読有、E101-A(1)、77-87、2018 年

② Masayuki Fukumitsu、Shingo Hasegawa、A Galindo-Garcia-like Identity-Based Signature with Tight Security Reduction、CANDAR'17、査読有、87-93、2017 年

③ Masayuki Fukumitsu、Shingo Hasegawa、Impossibility of the Provable Security of the Schnorr Signature from the One-More DL Assumption in the Non-programmable Random Oracle Model、ProvSec2017、査読有、LNCS 10592、201-218、2017 年

④ Masayuki Fukumitsu、Shingo Hasegawa、A Generic Construction of Tight Security Signatures in the Non-Programmable Random Oracle Model、ISITA2016、査読有、96-100、2016 年

⑤ Shingo Hasegawa、Shuji Isobe、Eisuke Koizumi、Hiroki Shizuya、Ryo

Takahashi 、 A Construction of Attribute-based Aggregate Signatures、ISITA2016、 査読有、76-80、2016 年

⑥ Masayuki Fukumitsu 、 Shingo Hasegawa、 Impossibility on the Provable Security of the Fiat-Shamir-Type Signatures in the Non-programmable Random Oracle Model、ISC2016、査読有、LNCS 9866、389-407、2016 年

⑦ Masayuki Fukumitsu 、 Shingo Hasegawa、 Black-Box Separations on Fiat-Shamir-Type Signatures in the Non-Programmable Random Oracle Model、ISC2015、 査読有、LNCS 9290、3-20、2015 年

〔学会発表〕（計 4 件）

① 福光正幸、長谷川真吾、NPROM における一般的な暗号学的な仮定からの Fiat-Shamir 型署名の安全性証明不可能性について、2018 年暗号と情報セキュリティシンポジウム、2018 年

② 福光正幸、長谷川真吾、Schnorr 署名の One-More DL 仮定からの安全性証明不可能性について、2017 年暗号と情報セキュリティシンポジウム、2017 年

③ 福光正幸、長谷川真吾、Non-Programmable Random Oracle Model における Fiat-Shamir 型署名の安全性証明不可能性の再考察、2016 年暗号と情報セキュリティシンポジウム、2016 年

④ 福光正幸、長谷川真吾、Non-Programmable Random Oracle モデル上で安全性証明可能な Fiat-Shamir 型署名、コンピュータセキュリティシンポジウム 2015、2015 年

６．研究組織

(1)研究代表者

長谷川　真吾（HASEGAWA, Shingo）
東北大学・教育情報基盤センター・助教
研究者番号：80567214