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　　６　月　２２　日現在

機関番号：　２７３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００００２９

研究課題名（和文）対話型証明と秘密分散に基づく認証方式・署名方式の設計及び安全性評価

研究課題名（英文）Design and Security Evaluation of Authentication and Signature Schemes Based on Interactive Proof and Secret Sharing

研究代表者

穴田　啓晃（Anada, Hiroaki）

長崎県立大学・情報システム学部・准教授

研究者番号：４０７２７２０２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：IDストリングとこれに対する複数のデジタル署名の知識を識別不可能証明システムで証明するAND合成証明システムを定義し，一般的に構成する指針を与えた．キーアイデアは，IDストリングへコミットし，IDストリングとデジタル署名を証拠とし証拠識別不可能なうちに知識を証明するものである．このシステムを構成部品に用い，単一のアイデンティティのユーザが複数の権限機関から属性証明書を付与される匿名属性認証スキームのシンタックス及び安全性を定義した．また，提案スキームを構成する一般的雛形を設計し，安全性を評価した．関連研究も含み成果を雑誌論文で4件，学会で14件発表し，また国際研究集会会議録3件を編集した．

研究成果の概要（英文）：We defined an AND-composition of proof systems that prove the knowledge of an identity string and digital signatures on the string in witness-indistinguishable way. We gave a generic design of the system. The key idea is "Commit to your identity, and prove your identity and signatures by WIPoK". Moreover, by using the AND-composition of proof systems as a building block, we defined the syntax and security of an anonymous attribute-authentication scheme in which a user of a single identity is given attribute-credentials by plural authorities. Then we designed a generic template of constructing the proposed scheme, and evaluated the security. We proposed these achievements at four journal papers, fourteen conferences. We edited three lecture notes of related international workshops.

研究分野：　暗号理論

キーワード：　属性ベース認証　属性ベース署名　対話型証明　秘密分散　証拠識別不可能　属性プライバシー　コミットアンドプルーヴ　秘密鍵結託耐性

１．研究開始当初の背景

(1) 属性ベース認証・署名スキーム

暗号学（Cryptology）における 2005 年頃からの主要な研究対象に属性ベース暗号プリミティブがある．これは暗号化ファイル自身の持つ役割ベースアクセス制御機能によるデータストレージの効率の良い利用，また，ユーザの属性に基づくプライバシー保護型認証・署名機能が実現可能とされているからである．本研究は後者を研究対象としていた．

2014 年に文献①，及び，同年に本研究代表者らが発表した文献②は，共に対話型証明（図 1）を用いるアプローチで属性ベース署名スキームを構成した研究であった．その構成手順は，はじめに 3-move のプロトコル（Σプロトコル）を対話型証明に用い属性ベース認証スキームを構成し，Fiat-Shamir 変換により非対話型とするものである．

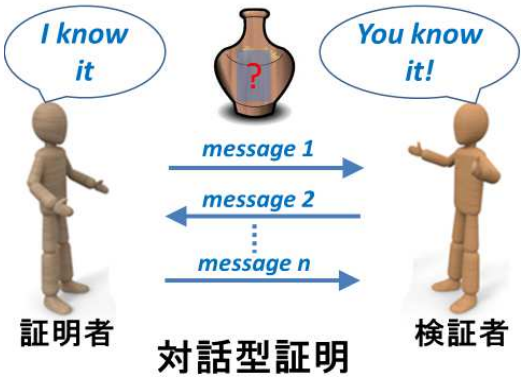

図 1

(2) 双線形群の要否という研究テーマ

属性ベース署名スキームを含む属性ベース暗号プリミティブの構成に対する研究コミュニティにおけるアプローチは，それまで 9 年程，双線形群の数学構造を用いたものであった．これに対し，2014 年の文献①，②のアプローチは双線形群を用いないアプローチであった．双線形群は現時点では楕円曲線上のペアリング演算で実現されており，そのべき乗演算は単一の巡回群のべき乗演算と比較し 10 倍程度の演算時間を要する．この処理効率から，双線形群を用いない属性ベース暗号プリミティブを構成するという問題は研究コミュニティのみならず実用システムの開発者からも関心の対象となっていた．なお，属性ベース暗号スキームの原型と考えられる ID ベース暗号スキームについては，当時既に双線形群を用いることは不可避であろうとの研究が発表されており，では属性ベース署名スキームの場合はどうなのかがこの研究上の焦点の一つとなっていた．

この焦点に関し，2014 年の文献①，②の構成は各々欠点を持っていた．文献①では属性ベース署名スキームとして扱うべき述語が閾値論理のケースに制限された形で述べられており，より一般性のあるモノトーン論理式のケースは 1994 年の文献③に依存していた．文献③ではモノトーン論理式の述語に対するΣプロトコルが提案されていたものの，プロトコルの（非自明な）アルゴリズムが記述されていなかった．一方，文献②の構成はこの点を補い，モノトーン論理式の述語に対するΣプロトコルのアルゴリズムを与えていた．しかし，属性ベース署名スキームとして有するべき属性プライバシー（図 2 Attribte-Privacy）の性質をワンタイム署名のケースしか有していなかった．

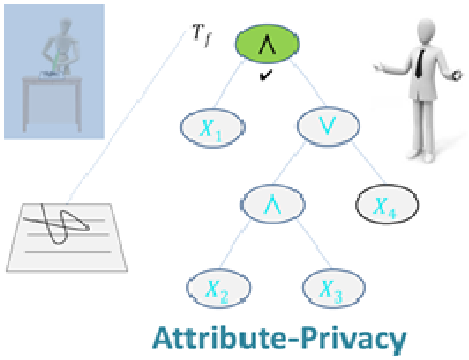

図 2

＜引用文献＞

① J. Herranz: “Attribute-based signatures from RSA”, Theory of Computer Science, vol. 527, 73-82 (2014)

② Hiroaki Anada, Seiko Arita, Kouichi Sakurai: “Attribute-based signatures without pairings via the fiat-shamir paradigm”, AsiaPKC2014

③ R. Cramer, I. Damgård, B. Schoenmakers: “Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols”, CRYPTO 1994

２．研究の目的

前節の背景を踏まえ，本研究では二つの目的を設定した．

(1) 必要な数学構造の追究

双線形群を用いない属性ベース認証・署名スキームのアルゴリズムを設計することが第一の目的であった．ただし，属性ベース暗号プリミティブの基本要件である次の三要件を満足するよう設計することが挑戦課題であった．

要件A)　述語に一般のモノトーン論理式を扱えること
要件B)　属性プライバシーを有すること
要件C)　秘密鍵結託耐性を有すること

設計においては安全性を評価することも目的とした．

(2) プライバシー保護認証システムの提案

属性ベース認証・署名スキームは証明者・検証者間で共有した述語を満足する true /false アサインメントを証明者が秘匿しつつ（上記要件 B），証明・署名プロトコルを実行する．ただし証明する内容は true アサイ

ンメントに対応する複数の属性証明書を所持していることである．本研究の第二の目的は，この性質を利用した認証システムを論文レベルで提案することであった．属性証明書は現実には多様な機関が発行しうることから，秘密鍵発行機関が複数あるスキームを設計することが挑戦課題であった．

３．研究の方法

前節の目的を達成するに当たり，本研究では大別し二つの方法を取った．第一は双線形群などの代数構造に依存しない形で対話型証明を設計する方法である．第二は従来研究の延長線上で双線形群を用い属性ベース認証・署名スキームを設計する方法である．

(1) 双線形群などの代数構造に依存しない形で対話型証明を設計する方法

先の文献③では，Σプロトコルにおける 2nd move のメッセージ，すなわち challenge message を証明者が秘密のストリングと見立て（これは本来 public coin ではあるが），これを秘密分散するアプローチで属性ベース認証・署名スキームが構成されていた．ただし，要件 C を満足しない欠点があった．本研究ではこのアプローチにコミットメントの手順を加えることで目的を追究した．これはコミットアンドプルーヴと呼ばれるもので，ただし証拠の一部分のみに対しコミットする点が新しい．

(2) 双線形群を用い属性ベース認証・署名スキームを設計する方法

この方法を検討したのは，先行研究の調査を進めるうち，暗号プリミティブの処理効率対高機能の構図（トレードオフ）を明らかにすべきと考えたからである．この方法では対話型証明を用いる前提に基づき，要件 A，B，C を満足する属性ベース認証・署名スキームを設計した．加えて，研究中に派生したアイデアに基づき，高機能を実現する属性ベース暗号プリミティブを検討することとした．

４．研究成果

前々節の目的を踏まえ前節の方法により研究を推進した結果，次の(1)から(4)に説明する成果を得た．成果物である雑誌論文・学会発表のうち主要なものについて，その概要を説明する形で報告する．

(1) 属性ベース認証・署名スキーム

学会発表⑤ “Attribute-Based Two-Tier Signatures: Definition and Construction”.

属性ベース署名方式において計算効率の向上は重要な課題である．本発表は，署名を生成する度に鍵発行センターからセカンダリキーを発行依頼する二段階署名という制約の下で，ペアリング演算を必要としない，なおかつ要件 A，B，C を満足する属性ベース署名方式を提案した．

学会発表① “Anonymous Authentication Scheme with Decentralized Multi-authorities”.

ユーザが複数の鍵発行機関から付与された複数の属性証明書で認証を受理させるサービスでは認証処理が同時に実行できる方式が望ましい．かつ，プライバシー保護の観点から，ユーザのアイデンティティが匿名となる方式が必要とされている．本発表では，ユーザのアイデンティティが識別不可能という意味において匿名性を備え，かつ，複数の属性を同時に認証する方式の安全性を定義した上で，具体的な方式を提案し安全性を証明した．かつ，属性ベース認証・署名スキームに拡張することが可能であることに触れた．ただし，要件 A，B を満足するものの要件 C は満足しない．

学会発表⑧ “バンドルされた証拠空間に対する証明システムとその複数の権限機関を伴う匿名属性認証スキームへの応用”.

証明システムの AND 合成であり，証明するステートメントの証拠の先頭要素が共通であるという制約の意味で証拠空間が個々の証拠空間の直積より狭くなった（底空間上にバンドルされた）ものを定義した．証拠識別不可能な証明システムの並列合成のケースに対し，そのプロトコルを一般的に構成した．次に，単一のアイデンティティのユーザが複数の権限機関から属性鍵を付与される匿名属性認証スキームのシンタックス及び安全性定義を提案した．更に，構成プロトコルを用い提案スキームを実現する雛形を与えた．雛形においては，証拠の先頭要素がアイデンティティストリング，残りの要素がその上のデジタル署名であり，その対が属性鍵として権限機関から与えられる．今後の課題として，提案スキームの対話型及び非対話型の実例を指摘した．なお，本発表は国内シンポジウムにおける設計指針の提起に留まった．このため，要件 A，B，C を満足する属性ベース認証スキームの構成も含め，詳細設計を今後の研究課題とする所存である．

学会発表⑪ “複数の鍵発行権限機関がある設定における匿名属性認証スキーム”.

本発表は学会発表⑧で指摘した対話型の実例である．双線形群の代数構造を用いる方法(2)による．結果，要件 A，B，C を満足する属性ベース認証・署名スキームを，述語が all-AND 論理式のケースで与えた．これはモノトーン論理式へ拡張可能である．

(2) 秘密分散法

雑誌論文② “Cross-group secret sharing scheme for secure usage of cloud storage over different providers and regions”.

本論文は方法(1)で研究を遂行した際の派生的な研究結果である．k-out-of-n 秘密分散方式で生成した n 個のシェアをクラウドファ

イルサービスのサーバに置いた際，プロバイダが k 個以上のシェアを収集しデータを不誠実に復元し情報を窃取する問題に着眼した．k-out-of-n 及び l-out-of-m の秘密分散共有を，対称鍵暗号を介して組み合わせ，l 個以上のプロバイダにまたがって k 個以上のシェアを収集しない限りデータを復元できない特徴を実現し問題を解決し，方式の安全性を証明し実装評価した．

(3) 属性ベース暗号スキーム

雑誌論文① “Short CCA-Secure Attribute-Based Encryption”.

属性ベース暗号は暗号化ファイル自身の持つ役割ベースアクセス制御機能でデータストレージの効率の良い利用を実現可能にする技術である．本論文では属性ベース暗号が選択暗号文攻撃に対し安全になるよう変形する際に暗号文長が長くなる問題に着眼した．従来方法が一般的変換に依存するのに対し，提案方法は個々の属性ベース暗号個別の変形手法でより短い暗号文長を実現できることを，典型的な属性ベース暗号方式に対し示した．

(4) 応用

学科発表③ “Expressive Rating Scheme by Signatures with Predications on Ratees”.

五つ星評価による評定とコメントなどの例に見られる評判ボードは，製品についての有用な情報を消費者に提供する利便性から親しまれている．本発表では評判ボードのためのスキームの一種を提案した．これは AND, OR, NOT の演算子を用いることで，従来スキームと比較し表現豊かに評定するのを可能にする．この表現豊かな評定スキームのシンタックスの定義を与えた上で，属性ベース署名方式を用いた一般的構成を提案した．特に，前者の関連付け可能という性質を，後者の二重評定抑止という性質へ反映させた点が理論的貢献と考えている．

雑誌論文④ “Generic Construction for Attribute-Based Identification Schemes Secure against Reset Attacks”.

スマートカードを挿抜する手法等によるリセット攻撃は本人認証方式に対する脅威である．本論文は属性ベース認証方式のケースにおいてリセット攻撃を定義した．また，リセット攻撃に対し安全となるよう改良するための複数のアプローチをまとめた．このサーベイの後，リセット攻撃に対し安全で，かつ，計算効率の優れたアプローチの方式を，暗号学的コミットメントを構成部品に用いることで構成し，なおかつ安全性を証明した．

雑誌論文③ “A Hybrid Encryption Scheme with Key-cloning Protection: User / Terminal Double Authentication via Attributes and Fingerprints”.

属性ベース暗号は復号者の属性を認証し，ただし復号者の ID 情報を暗号文や復号処理から漏らさない性質が長所となっている．逆に，この性質ゆえ秘密鍵の複製を検出できない問題がある．本論文はネットワーク端末機器のフィンガープリント情報を用い RSA 暗号を端末認証しこの問題を解決する方法を提案した．

５．主な発表論文等

〔雑誌論文〕（計 4 件）

① Hiroaki Anada, Seiko Arita: “Short CCA-Secure Attribute-Based Encryption”, Advances in Science, Technology and Engineering Systems Journal,3(1), 261-273 (2018) （査読有），
https://astesj.com/v03/i01/p32/

② Hiroaki Anada, Junpei Kawamoto, Chenyutao Ke, Kirill Morozov, Kouichi Sakurai: “Cross-group secret sharing scheme for secure usage of cloud storage over different providers and regions”, The Journal of Supercomputing,73(10), 4275-4301 (2017) （査読有），
https://link.springer.com/article/10.1007%2Fs11227-017-2009-7

③ Chunlu Chen, Hiroaki Anada, Junpei Kawamoto, Kouichi Sakurai: “A Hybrid Encryption Scheme with Key-cloning Protection: User / Terminal Double Authentication via Attributes and Fingerprints”, Journal of Internet Services and Information Security, 6(2), 23-36 (2016) （査読有），
http://isyou.info/jisis/vol6/no2/jisis-2016-vol6-no2-02.pdf

④ Ji-Jian Chin, Hiroaki Anada, Seiko Arita, Kouichi Sakurai, Swee-Huay Heng, Raphael Phan: “Generic Construction for Attribute-Based Identification Schemes Secure against Reset Attacks”, International Journal of Cryptology Research 5(1): 28-44 (2015) （査読有），
https://mscr.org.my/data/journal/journal-20180121010542.pdf

〔学会発表〕（計 14 件）

① Hiroaki Anada, Seiko Arita:Anonymous Authentication Scheme with Decentralized Multi-Authorities. SMARTCOMP 2017,
https://ieeexplore.ieee.org/document/7946989/

② Hiroaki Anada, Seiko Arita: “Short CCA-Secure Ciphertext-Policy Attribute-Based Encryption”, SMARTCOMP 2017,
https://ieeexplore.ieee.org/document/7947045/

③ Hiroaki Anada, Sushmita Ruj, Kouichi Sakurai：“Expressive Rating Scheme by Signatures with Predications on Ratees”, NSS 2016,
https://link.springer.com/chapter/10.1007%2F978-3-319-46298-1_24

④ Chenyutao Ke, Hiroaki Anada, Junpei Kawamoto, Kirill Morozov, Kouichi Sakurai：“Cross-group Secret Sharing for Secure Cloud Storage Service”, ACM IMCOM2016,
https://dl.acm.org/citation.cfm?doid=2857546.2857610

⑤ Hiroaki Anada, Seiko Arita, Kouichi Sakurai: “Attribute-Based Two-Tier Signatures: Definition and Construction”, ICISC2015,
https://link.springer.com/chapter/10.1007%2F978-3-319-30840-1_3

⑥ Chunlu Chen, Hiroaki Anada, Junpei Kawamoto, Kouichi Sakurai ：“Hybrid Encryption Scheme using Terminal Fingerprint and its Application to Attribute-based Encryption without Key Misuse”, AsiaARES2015,
https://link.springer.com/chapter/10.1007%2F978-3-319-24315-3_26

⑦ Ji-Jian Chin, Hiroaki Anada, Syh-Yuan Tan ：“Reset-Secure Identity-Based Identification Schemes Without Pairings”, ProvSec2015,
https://link.springer.com/chapter/10.1007%2F978-3-319-26059-4_13

⑧ 穴田啓晃,有田正剛: “バンドルされた証拠空間に対する証明システムとその複数の権限機関を伴う匿名属性認証スキームへの応用”, 暗号と情報セキュリティシンポジウム 2018

⑨ 穴田啓晃,有田正剛: “効率が良く追跡可能な属性ベース署名”, 暗号と情報セキュリティシンポジウム 2017

⑩ 穴田啓晃, ルジ・スシミタ, 櫻井幸一 “被評定者の属性に基づく表現豊かな評定スキーム”, 暗号と情報セキュリティシンポジウム 2016

⑪ 穴田啓晃,有田正剛: “複数の鍵発行権限機関がある設定における匿名属性認証スキーム”,電子情報通信学会 ISEC 研究会, 2017 年 11 月

⑫ 穴田啓晃,有田正剛: “対角線上証拠識別不可能な証明システム”, 電子情報通信学会 ISEC 研究会, 2017 年 3 月

⑬ 穴田啓晃,有田正剛: “知識の証明のバンドリングとそのデジタル署名への応用”, 電子情報通信学会 ISEC 研究会, 2016 年 9 月

⑭ Hiroaki Anada, Seiko Arita, Kouichi Sakurai:“Attribute-Based Two-Tier Signatures”, 電子情報通信学会 ISEC 研究会, 2015 年 7 月

〔その他〕(会議録編集３件. 組織委員として企画・運営した国際研究集会のもの)

① Kirill Morozov, Hiroaki Anada, Yuji Suga(ed.): “Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling”. MI Lecture Note Vol.80, Institute of Mathematics for Industry, Kyushu University (2018). Publisher: Institute of Mathematics for Industry, Kyushu University, ISSN: 2188-1200,
http://www.imi.kyushu-u.ac.jp/files/imipublishattachment/file/math_5acd74ff3090d.pdf

② Hiroaki Anada, Kirill Morozov, Yuji Suga, Shinya Okumura, Kouichi Sakurai(ed.) “Secret Sharing for Dependability, Usability and Security of Network Storage and Its Mathematical Modeling”. MI Lecture Note Vol.73, Institute of Mathematics for Industry, Kyushu University (2017). Publisher: Institute of Mathematics for Industry, Kyushu University, ISSN: 2188-1200,
http://www.imi.kyushu-u.ac.jp/files/imipublishattachment/file/math_58d8ad2f89418.pdf

③ Hiroaki Anada, Takanori Yasuda, Kouichi Sakurai and Isamu Teranishi (ed.) “Next-generation Cryptography for Privacy Protection and Decentralized Control and Mathematical Structures to Support Techniques”. Mathematics for Industry Research No.4, Institute of Mathematics for Industry, Kyushu University (2016). Publisher: Institute of Mathematics for Industry,

Kyushu University, ISSN: 2188-286X, http://www.imi.kyushu-u.ac.jp/files/imipublishattachment/file/math_56b29fcacd1eb.pdf

６．研究組織

(1)研究代表者
穴田　啓晃（ANADA, Hiroaki）
長崎県立大学・情報システム学部・准教授
研究者番号：４０７２７２０２

(2)研究分担者
有田　正剛（ARITA, Seiko）
情報セキュリティ大学院大学・情報セキュリティ研究科・教授
研究者番号：５０３８７１０６

(3)研究協力者（海外）
ルジ・スシミタ（RUJ, Sushmita）
Indian Statistical Institute, Assistant Professor
https://www.isical.ac.in/~sush/