様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　１１　日現在

機関番号：　１７１０２
研究種目：　挑戦的萌芽研究
研究期間：　2013～2014
課題番号：　２５５４０００４

研究課題名（和文）確率検査証明理論に基づく非対話型ゼロ知識証明の構成理論と暗号系への実用強化

研究課題名（英文）Building non-interactive zero-knowledge proof from probabilistically checkable proof and its application to practical cryptosystems

研究代表者

櫻井　幸一（SAKURAI, KOUICHI）

九州大学・システム情報科学研究科（研究院・教授

研究者番号：６０２６４０６６

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：ペアリング暗号によってしか実現できていない、効率的な非対話型ゼロ知識証明の実現を、RSAをはじめとする他の暗号系でも実現し、応用システムの対象範囲を広げることを目指した。ID(個人情報)ベース暗号の発展系の１つである属性(attribute)情報ベース暗号でも、既存方式はペアリング技術を利用している。本研究では課題であった、ペアリングを利用しない属性ベース電子署名を構成することに成功した。この成果をACM AsiaPKC2014で発表した。

研究成果の概要（英文）：Our target here was the realization of the effective non-interactive zero-knowledge proof system, which had been realized only by the pairing-based construction, in the other construction (with the RSA) that yield benefit of enlarging its applied area. It is worth noting that existing work in the field of attribute-based encryption scheme that is one of the extensions of ID-based encryption scheme owes its construction to the pairing technique. Our research succeeded to construct an attribute-based signature scheme that does not utilize the pairing technique, which was the problem in our study. We presented this result in ACM AsiaPKC2014.

研究分野：　情報セキュリティ

キーワード：　暗号　認証　ゼロ知識証明　確率検査証明　証明可能安全性　RSA暗号　属性情報ベース電子署名　Fiat-Shamir変換技法

１．研究開始当初の背景

1980 年代 Blum 学派によっては始まったゼロ知識対話型証明 (Zero-Knowledge Interactive Proof: ZKIP)は，その後２つの流れをとる：一つは認証など暗号応用としてのゼロ知識(Zero-Knowledge)理論の展開，もう一つは確率的対話型証明(Interactive Proof，IP)モデルに関する計算量理論的研究である．1990 年になると後者の IP モデルから証明の検証を確率的に行う確率検査証明 (Probabilistically Checkable Proof: PCP) へと展開する．PCP 理論自体はその後，近似アルゴリズムの理論的限界の解明など，驚くべき結果を生み出していく．

計算量理論の立場から，Kilian らMIT 学派 [STOC’97]は確率検査証明に含まれる知識複雑性の計算量的解明を試み，多くの確率検査証明がゼロ知識証明(ZK-PCP)に変換できることを示した．この結果の変換では，証明者の能力が多項式時間以内という現実制約には適用できずに，実際の暗号メカニズムの設計には直接適用できない．これに対して，2012 年 Ishai らは，暗号理論への応用を想定した，NP 証明者に制限したモデルで，ゼロ知識確率検査証明を構成した[On Efficient Zero-Knowledge PCPs．TCC 2012]．

その一方で，これも Blum が発見した，対話型でないゼロ知識非対話型証明 (Non-Interactive ZK: NZK)の研究がある．証明者と検証者とで共通の乱数列を事前に共有するモデル下での証明技法であり，安全な電子署名設計の基盤となっている．しかし，この技法も NP 完全問題への還元など変換自体が非効率であり，RSA 暗号など実用的な方式への適用が課題となっている．これに解決の糸口を付けたのが Gross-Sahai [Eurocrypt2008]である．彼らは回路還元を用いずに，効率的な非対話型ゼロ知識証明の構成に成功した．この研究を構造維持型電子署名へと発展させた研究が，NTT 阿部らのグループより精力的に行われている．しかし，日本国内で，非対話型ゼロ知識証明との関係はおろか，ゼロ知識確率検査証明を研究しているものは皆無の現状にある．

本研究では，つぎの３つの挑戦課題を設定した．

(1)非対話型証明と確率検査証明のモデルの違いと共通点の明確化
(2) ２つのモデル間の違いを結びつける媒体の提案
(3) ペアリングに依存しない現実的な非対話型ゼロ知識証明の構成（特に RSA 暗号系）

２．研究の目的

暗号理論で基本的な役割を果たす非対話型ゼロ知識証明とその応用である安全な電子署名など暗号機能の構成に対して，理論計算機分野の基礎である確率検査証明がいかに有効であるのか，またその限界の解明も重要である．

特に，現在ペアリング暗号によってしか実現できていない，効率的な非対話型ゼロ知識証明の実現を，RSA をはじめとする他の暗号系でも実現するという課題に挑戦し，応用システムの対象範囲を広げることを目指した．

３．研究の方法

「安全な電子署名の構成に，確率検査証明が有効である」というアイデアは，本研究代表者の 20 年前の研究に起源をもつ[Digital Signature with User-Flexible Reliability，1993 年暗号と情報セキュリティシンポジウム SCIS1993]．ここでは，確定的な検証のみの電子署名に対して，ゼロ知識非対話型証明の乱数利用に着目し，確率的検証技法を導入することで，検証の信頼性に利用する乱数ビットの個数で制御可能にしている．

その一方で，確率検査証明に含まれる知識複雑性を解析し，冗長な情報はもらさないゼロ知識確率検査証明の研究が展開された[Kilian et.al STCO’97]．しかし，計算量クラスの特徴付けにとどまり，電子署名など実用的な暗号系への応用にまでは至っていない現状にある．

本研究では，このギャップをうめるべく，確率検査証明と非対話型証明，およびそれらのゼロ知識性との関係を探索した．非対話型証明と確率検査証明のモデルは，どちらも乱数が利用されるが，あきらかにモデルが異なることに注意する．

研究代表者のプログラムにもっとも近いのは Valiant[TCC2008]である．Valiant は，ブートストラップ手法を用いて，NIZK の効率を改善している．また Gennaro らにより，確率検査証明ではなく，スパンプログラムを用いた効率よい非対話型ゼロ知識証明の構成が提案された[Gennaro et al.: Quadratic Span Programs and Succinct NIZKs without PCPs．IACR Cryptology ePrint Archive 2012: 215 (2012)]．ここでは，スパンプログラムを用いたクラス NP の特徴付けなど，確率検査証明を用いない試みをとっている．しかし，Gennaro らの研究は，Gross-Sahai の延長にあり，やはりペアリングに依存したままである．

これに対して，本研究での新たな試みは，PCP と NZKP の差をうめる中間媒体の導入を検討した．この媒体は，ある種の耐タンパデバイスなどハードウエア的なモデルを仮定する．また，ハード的な物理道具の付加にたよらず，完全にソフトウエア的な手法のみでの

解決は挑戦課題である．これに関しては難読化プログラムモデルなどの適用を試みた．

４．研究成果

4.1 解決できた課題

３つ目の挑戦課題に関しては，代表者が室長を兼務する九州先端科学技術研究所の穴田研究員との共同研究で，具体的な結果を得，ACM 系国際会議に投稿し査読をへて採択，発表する成果をおさめた．

“Attribute-Based Signatures without Pairings via the Fiat-Shamir Paradigm” Hiroaki Anada, Seiko Arita, Kouichi Sakurai (ACM AsiaPKC2014)

3-move かつ公開コイン（検証者の使う乱数が公開）のプロトコルで対話型の知識のゼロ知識証明を構成する研究が，1990 年代に暗号と計算量理論の研究者の間で進められてきた．Schnorr は整数論上の離散対数の概念に基づき，今日 Schnorr プロトコルと呼ばれる対話型の知識の証明を提案した[Schnorr, “Efficient Identification and Signatures for Smart Cards”, CRYPTO `89]．ただし，ゼロ知識証明の性質は限定的，すなわちプロトコルに従って（正直に）振る舞う検証者に対してのみゼロ知識性が保証されているので，対話型の知識の 正直検証者ゼロ知識証明と呼ばれている．この提案方式はΣプロトコルとして抽象化され定式化された．

Σプロトコルを witness-indistinguishable（証拠が識別不可）な証明システムに拡張する着想は，その原型が次の論文で述べられている：Cramer, Damgard, Schoenmakers: "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols", CRYPTO `94. すなわち，この論文では，対話型の知識の証明において，知識 1 と知識 2 のどちらかを有していることを証明する，いわゆる OR 証明の設計が示されている．更に，AND と OR の論理演算子を任意個含むブール式についても，秘密分散の技術を適用することで，3-move で witness-indistinguishable な設計が言及されている（しかし具体的な設計は与えられなかった）．また，1986 年に提案され現在は標準的手法にまで整備された Fiat-Shamir 変換を当該認証方式に適用することで，署名方式も得られることが述べられている．これらの手法による認証方式及び署名方式は，理論上も実用上も重要なペアリングフリー (pairing-free)の性質を達成し，なおかつ属性ベース化できる可能性があるため，注目すべきと考えてきた．

本研究では属性ベース署名方式を提案した．属性ベース署名方式とは，ユーザの属性が署名ポリシを満足する場合にのみデジタル署名を生成可能にするデジタル署名方式の一種である．ここで，ユーザの属性は，例として{A 社員，B 部門}等の，認証された所属・資格の形式を指し，署名ポリシは，例として [A 社員 AND [B 部門 OR C 部門]]等の，属性についてのブール式を指す．本論文は，属性ベース署名方式を，1990 年代よりよく研究されてきたΣプロトコルを拡張するアプローチにより，実現した．

先のΣプロトコルは，叙述についての知識を有することを証明者が検証者に証明する証明システムである．我々は，先述の OR 証明を解析し，そのアイデアを活用し，ブール式 f を満足するという叙述についての知識を有することの，3-move で witness-indistinguishable な証明システムのΣプロトコル $\boldsymbol{\Sigma}_f$ を与えた（次の定理 1）．

定理 1. （本論文で構成した）$\boldsymbol{\Sigma}_f$は，Σプロトコルタイプのブール証明システムである．

しかし，この $\boldsymbol{\Sigma}_f$は，属性ベース認証方式としては十分ではなく，従って，$\boldsymbol{\Sigma}_f$ を Fiat-Shamir 変換（従来技術）して得られる署名方式も属性ベース署名方式になり得ない．というのも，一般に属性ベース方式であるためには，次の(1)(2)(3)の性質，特に(1)を有することが必要だからである（上記の $\boldsymbol{\Sigma}_f$は(1)を有さない）： (1)秘密鍵の収集についての結託攻撃に対する耐性； (2)ユーザの匿名性； (3)属性プライバシー．この状況に対し，本論文では属性ベース署名の先行研究（Maji, Prabhakaran, Rosulek: “Attribute-Based Signatures”, CT-RSA 2011, pp. 376-392）で用いられていた署名バンドルのアイデアを用い，上記の $\boldsymbol{\Sigma}_f$を属性ベース認証方式に拡張した（本論文では ABID と呼んでいる）．この ABID の基本性質を述べたのが次の定理 2 である．

定理 2. 提案属性ベース認証方式 ABID はΣプロトコルである．

ABID の署名バンドルに Fiat-Shamir 署名を用いる，更に Fiat-Shamir 変換を適用し属性ベース署名方式 ABS を得るなど，Fiat-Shamir パラダイムで提案方式を発展させて性質を述べたのが次の定理 3 及び定理 4 である．

定理 3. 用いた Fiat-Shamir 署名が選択メッセージ攻撃に対し存在的偽造不可ならば，提案属性ベース認証方式 ABID は同時発生的攻撃に対し安全である．

定理 4. ABID に Fiat-Shamir 変換を適用し得られた属性ベース署名方式 ABS は，ランダムオラクルモデルにおいて，ABID の受動的攻撃に対する安全に基づき，選択メッセージ攻撃に対し存在的偽造不可である．

4.2 最新の研究動向と残された課題

２つ目の課題「PCP と NZKP の差をうめる中間媒体の導入」を考えている．この媒体は，

ある種の耐タンパデバイスなどハードウエア的なモデルを仮定する．また，ハード的な物理道具の付加にたよらず，完全にソフトウエア的な手法のみでの解決は挑戦課題である．これに関しては難読化プログラムモデルなどの適用を試みる.」に関しては,近年進展した識別不可能性難読化，indistinguishability obfuscator（iO）の理論がある[Garg,Gentry, Halevi, Raykova, Sahai, and Waters.Candidate indistinguishability obfuscation and functional encryption for all circuits. In FOCS, 2013].
この iO 理論は属性ベース署名への適用の研究が期待できる，これに関し，最近次の論文が発表された：Ramchen, Waters: "Fully Secure and Fast Signing from Obfuscation", ACMCCS2014[*3]．この iO に基づく署名方式を属性ベースへ拡張することが理論上も実用上も重要である．というのも，iO の技術はペアリングフリーを実現する可能性が期待できるからである．

また，ゼロ知識証明と難読化に関する研究も発表されている[Omkant Pandey, Manoj Prabhakaran, Amit Sahai: Obfuscation-Based Non-black-box Simulation and Four Message Concurrent Zero Knowledge for NP. TCC (2) 2015: 638-667]．ここでは，従来の PCP 理論を iO 理論で置き換えており，本研究の第一挑戦課題へのアプロートに示唆を与えている．

iO を用いて，長く未解決だった否認可能な暗号の具体的な構成に成功した研究も発表された[Amit Sahai, Brent Water “How to use indistinguishability obfuscation: deniable encryption, and more,” Proc. STOC '14 Proceedings of the 46th Annual ACM Symposium on Theory of Computing, pp. 475-484 (2014).].
研究代表者も，Jian Weng (中国・Jinan 大 NICT 招聘プログラム支援で九大に滞在)との共同研究により，この iO 理論を用いて，代理人再暗号化に関する成果を得た[SCIS2015 で発表].

Fiat-Shamir 技法による署名設計の限界の１つにランダムオラクルの必要性がある．今回，穴田研究員らと設計した属性署名もランダムオラクルモデル下での安全性証明を与えている．この仮定を取り除く技法はすでにいくつかしられており，現在も検討中である．

５．主な発表論文等

〔雑誌論文〕（計　　１件）

Hiroaki Anada, Seiko Arita, Kouichi Sakurai: “Attribute-Based Signatures without Pairings via the Fiat-Shamir Paradigm”, In Proc. of 2nd ACM ASIA Public-Key Cryptography Workshop (ASIAPKC 2014), Kyoto, Japan, June 2014, pp. 49-58 [査読あり]

〔学会発表〕（計　　３件）

1. Hiroaki Anada, Seiko Arita, Kouichi Sakurai: “Boolean Formula-Proof and Its Application to Attribute-Based Identifications and Signatures”, 火の国情報シンポジウム，大分，2014 年 3 月，予稿論文集，1B-2 [査読なし]
2. Hiroaki Anada, Seiko Arita, Kouichi Sakurai: “Attribute-Based Identification Schemes of Proofs of Knowledge”, 第 31 回暗号と情報セキュリティシンポジウム (SCIS2014)，鹿児島，2014 年 1 月，予稿論文集，3E3-3 [査読なし]
3. Junzuo Lai,Xianping Mao, Qixiang Mei, Kouichi Sakurai, Jian Weng “CCA-Secure Multi-hop Unidirectional Proxy Re-Encryption from Indistinguishability Obfuscation” SCIS 2015 The 32nd Symposium on Cryptography and Information Security, Kokura, Japan, Jan. 20 - 23, 2015 [査読なし]

〔その他〕
ホームページ等
研究代表者研究室
http://itslab.inf.kyushu-u.ac.jp/
大学 HomePage:
http://hyoka.ofc.kyushu-u.ac.jp/search/details/K000220/

６．研究組織

(1)研究代表者

櫻井幸一（SAKURAI Kouichi）
九州大学大学院システム情報科学研究院
研究者番号：60264066

以上．