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

令和　６ 年　 ６ 月 １４ 日現在

機関番号：８２６２６
研究種目：若手研究
研究期間：2018～2023
課題番号：１８Ｋ１８０５５

研究課題名（和文）ネットワーク上のプライバシ保護に適する匿名認証付匿名ルーティングの研究

研究課題名（英文）Anonymously Authenticated Anonymous Routing for Privacy Protection in Networks

研究代表者
坂井　祐介（Yusuke, Sakai）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：４０７５０６５９

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：　本研究課題においては、ゼロ知識証明とその周辺技術について研究を進め、匿名認証付き匿名ルーティング構成のための基盤となる技術の整備を行った。具体的には、グループ署名に関して効率性の改善と安全性の強化および権限の一極集中の緩和、属性ベース署名について取り扱えるポリシーのクラスの拡張および効率性の改善、様々な暗号要素技術の安全性概念の再検討、追跡可能集約署名の定式化、タイトに安全な2ラウンド多重署名の構成、という成果を得た。

研究成果の学術的意義や社会的意義
　本研究課題において得られた新たな方式たちはいずれも方式の実用性を改良するものであり、より実用性の高い方式を社会で利用できるようになるという社会的意義がある。それら方式たちを得るために開発した新たな技法はいずれも他の文脈でも活用可能なことが期待され、暗号理論研究を更に進展させることが期待できるという学術的意義がある。
　本研究課題で行った安全性概念の再検討は、広く使われている安全性概念が真に実際上の脅威を捉えていることの傍証の一つを与えるものであり、その安全性概念を用いることでより信頼性の高い暗号技術が得られるという社会的・学術的意義がある。

研究成果の概要（英文）：In this project, we conducted research on zero-knowledge proofs and related topics and paved the way for constructing anonymously authenticated anonymous routing. More concretely, we obtained the following results: Efficiency and security improvements in group signatures, relaxation of centralization of power in group signatures, expressiveness and efficiency improvements in attribute-based signatures, reconsideration of security notions of multiple cryptographic primitives, formalization of aggregate signatures with interactive tracing, and construction of tightly secure two-round multi-signatures.

研究分野：暗号理論

キーワード：ゼロ知識証明　グループ署名　属性ベース署名　安全性概念　集約署名　多重署名

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネットの発展に伴い、社会の様々な仕組みがコンピュータ化され、社会全体で多大な利便性を享受できている。しかしながら、そのような社会インフラとしてのインターネット上の情報サービスがごく少数の IT 企業により提供されていることによる弊害も指摘されている。そのような弊害としては、サービス利用者の**プライバシ情報**がそれら少数の IT 企業に集約されてしまうことが挙げられる。これにより、それら個人情報が利用者の意図しない形で利用される危険性が生じる。追跡型広告（ある Web ページの閲覧履歴を基に、他の Web ページでもその閲覧履歴と関連した内容の広告を表示するもの）はそのような意図しない利用の典型的な例である。プライバシ保護の観点からそうした利用者追跡を敬遠する利用者も増加してきており、実際に米 Apple 社はそのような広告を動的に分析し広告の表示される頻度を適切なものに調整する、Intelligent Tracking Prevention という機能を Web ブラウザへ実装している（https://webkit.org/blog/7675/intelligent-tracking-prevention/）。また、このような状況の下、個人情報漏洩の際の被害が著しく甚大化しており、最近では例えば、米 Yahoo!より 5 億件のパスワードが漏洩した（https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security）。この件数は米国全人口の約 1.6 倍に当たる。

こうした問題の根本的な理由の一つとして、インターネットの利用の際に利用者のある種の識別情報がアクセス先へ自動的に送信されてしまうということが挙げられる。この問題を解決し得る技術として、Tor に代表される**匿名ルーティング**の技術がある（https://www.torproject.org/）。この技術は、通信路上のデータを暗号学的に攪乱しながら複数の中継サーバに中継させ、それによって通信の送信者や受信者、更には通信の存在そのものを秘匿するという技術である。しかしながら、この匿名ルーティング技術の大きな問題として、利用者の**認証**の機能を持たないという点が挙げられる。この認証機構の欠如のため例えば、悪意の利用者による技術の濫用を防ぐことができないという問題が生じる。ここで注意すべきは、通常の利用者認証の技術は利用者の一意特定を前提とするため、匿名ルーティングと単純に組み合わせることはできないということである。つまり、利用者認証により送信者が正規の利用者であることを確認する際にはその送信者の識別情報を中継サーバへ開示する必要があり、従って中継サーバに対して利用者の匿名性が保たれないことになる。ここから言えることは、前述のインターネットにおけるプライバシ問題を解決するためには、匿名ルーティング技術よる匿名性と、利用者の匿名性を損なわない認証とを**両立**させる必要があるということである。

一見すると、**匿名認証**との併用が問題の解決に有用であると思われる。匿名認証とは、利用者がある特定のグループに属することを利用者の識別情報を一意に特定することなしに認証できる技術である。具体的にはこの技術は、当該の利用者がグループに所属することを、識別情報に対するそれ以上の情報を一切漏洩させることなしに認証することができる。匿名ルーティングの利用に際してこの匿名認証を用いて利用者を認証することで、利用者の匿名性を保護しつつ、悪意の利用者を防ぐことが可能になると思われる。しかしながら、この匿名認証の技術もそのままでは匿名ルーティングには適用できない。匿名ルーティングに匿名認証を組み合わせる場合、通信の開始時に認証を行い、その認証の履歴も同時に中継サーバが中継していくことになる。このとき、匿名認証は認証の履歴を攪乱する機能を持たないため、この認証の履歴を遡ることで送信元を特定することができてしまう。

もし、この認証の履歴すらも匿名ルーティングの技術によって暗号学的に攪乱することが可能であれば、上記問題を解決し、匿名ルーティングによる通信の存在すら秘匿した通信を匿名認証における匿名性を損なわないままに行うことができるものと期待される。すなわち、匿名ルーティングと匿名認証という異なる目的を持った要素技術を**統合**して通信の秘匿化と利用者の認証とを同時に実行できる要素技術を実現することにより、上述のインターネットにおけるプライバシ問題を解決することが可能になると考えられる。このときに問題となるのが、匿名ルーティングによる通信の秘匿性と匿名認証による通信の検証可能性との**対立**である。概して言えば、通信を秘匿するということは通信の内容を第三者から見て無意味な内容に変換するということであり、それに対して、通信の正当性を検証可能にするということは通信の内容を（少なくとも一部を)第三者から見ても有意味な内容にするということである。このように匿名ルーティングと匿名認証とは根本的に相反する目的を持った技術であり、そのために両技術の統合には原理的な困難さが存在する。

２．研究の目的

本研究は、この匿名ルーティング、匿名認証の両技術を統合した、インターネット上のプライバシ問題の解決に向けた**匿名認証付匿名ルーティング**の創出を目的とする。本技術によれば、匿名ルーティングと同様にしてネットワーク上で送信元・送信先・通信の存在を秘匿したままの通信が行え、更に通信の開始時に匿名認証と同様にして匿名性を維持したまま認証を行え、加え

てその認証の履歴が追跡され匿名ルーティングによる匿名化が無効化されることもないような通信を実現することが可能となる。本技術によれば、インターネット上での匿名での通信が汎用的に行えるようになり、具体的には下記のような効果が期待される。まず、この技術を用いれば、前述の追跡型広告について通信の送信元を利用した利用者の追跡が不可能となり、これにより追跡型広告を提供すること自体が技術的に困難となるという形でインターネット利用者のプライバシを保護することが可能となる。また、個人情報漏洩についても、情報サービス提供者が利用者についての通信の送信元に基づく過剰に詳細な情報を収集することが技術的に不可能となり、それにより万一の個人情報漏洩の際の被害を軽減することが可能となる。

３．研究の方法

この技術の実現に向けて本研究では、プライバシを保護した形での通信を行える暗号要素技術である匿名ルーティングとプライバシを保護した形での利用者認証を行える暗号要素技術である匿名認証とを統合するというアプローチを取るが、このアプローチには上述の通り、相反する目的を持った二つの暗号要素技術の統合という原理的な困難さが存在する。本研究では、その困難さを克服するために、**Groth-Sahai 証明系**という技術の数学的構造に着目する。Groth-Sahai 証明系はゼロ知識証明と呼ばれる要素技術の一方式であり、単にゼロ知識証明であるという以上の種々の優れた性質を持つ。そのような性質の一つで、本研究においても有用であるのが再ランダム化可能性という性質である。ゼロ知識証明とは、秘密の情報がある条件を満たすことを、その秘密に関して当該の条件を満たすこと以上の一切の情報を漏洩させずに第三者に証明できる技術である。また再ランダム化可能性とは、既に実行された証明の履歴を変換することで、証明がもう一度実行し直されたかのような新たな証明の履歴を得ることができる性質である。前者のゼロ知識証明としての性質は、匿名ルーティング、匿名認証いずれにも非常に有用な性質であり、本研究でもその性質を活用して研究を進める計画である。また、再ランダム化可能性は、匿名ルーティングにおける通信データの攪拌に非常に有用な技術である。これらの性質を活用して最終的な目標である匿名認証付匿名ルーティングの実現に取り組む計画であるが、その時さらに、上で述べた単純な並列利用の場合のような、匿名ルーティングとしては十分な機能を達成していたとしてもそれを匿名認証と組み合わせたゆえに全体としては十分な機能を達成していない（あるはその逆の）状況を避けるため、二つを不可分な形に結び付ける必要がある。そのためには、二つの機能それぞれに対して個別に Groth-Sahai 証明系を設計するのではなく、全体を単一の Groth-Sahai 証明系として構成するというアプローチを取る計画である。

これまで述べてきたように匿名ルーティング、匿名認証はいずれも単独ではプライバシを保護したインターネット上での通信を実現するには不十分であることに着目したこと、その二つを統合することでプライバシ保護に汎用的に利用可能な情報通信システムを実現しようとすることが本研究の独自性である。またそれに向けて、Groth-Sahai 証明系という両要素技術の構成にあたり共通して有用な暗号要素技術に着目したこと、また、Groth-Sahai 証明系を利用するにあたり匿名ルーティングのための Groth-Sahai 証明系、匿名認証のための Groth-Sahai 証明系と個別設計せず、両機能を同時に実現する単一の Groth-Sahai 証明系を設計しようとすることも本研究の独自性である。

４．研究成果

(1) 平成 30 年度

平成 30 年度は、匿名認証付き匿名ルーティング実現のための重要な要素技術であるゼロ知識証明について研究を進め、特に、ゼロ知識証明を用いた匿名認証技術の一種である属性ベース署名に関して以下のような成果を得た。

属性ベース署名とは、署名の発行者が自身がある属性を有することを第三者に証明できる暗号要素技術であり、そのとき、署名者の属性がある条件を満たしていることのみが証明され、そのような条件を満たすもののうちいずれであるのかについては秘匿されるという性質を持つものである。この要素技術において、利用できる条件をより広いものに拡張していくことは、同要素技術の研究において中心的な課題の一つである。本研究では、任意のチューリング機械を用いて条件を記述でき、属性として長さに制限のない任意の文字列を利用できる属性ベース署名方式を設計した。この成果は、国際会議 Asiacrypt 2018 へ採録となっている。

また、同じくゼロ知識証明を用いた匿名認証技術の一種であるグループ署名について、以下のような成果を得た。グループ署名とは、グループに所属する各利用者が、自身がそのグループに所属することを第三者に証明できる暗号要素技術である。このとき、第三者には、署名者がグループに属していることのみが開示され、署名者の具体的な ID については秘匿されるという性質を持つ。この要素技術において、署名者のグループからの脱退は重要な課題の一つである。特に、脱退を可能にするためのアプローチとして検証者ローカル失効と呼ばれるものが知られているが、このアプローチでは署名者の鍵が漏洩したときに ID の秘匿性が必ずしも保たれないことが知られていた。本研究では、鍵漏洩下でも ID が秘匿される、初めての検証者ローカル失効グループ署名方式を設計した。この成果は、国際会議 SCN 2018 へ採録となっている。

(2) 令和元年度

令和元年度は、匿名認証付き匿名ルーティングの重要な要素技術であるグループ署名について研究を進め、以下のような成果を得た。

上述のグループ署名において、グループの管理者のみは、非常時には証明を実行した履歴から証明を実行した利用者の ID を特定することが可能である。この利用者の ID を特定できる権限は濫用されると利用者のプライバシ侵害につながる強大な権限であり、権限の行使を適切に制限できることが望まれる。本年度は、管理者の権限の行使を制限できる第三者機関を設定可能なグループ署名方式の提案を行った。この方式では、第三者機関は特定の条件を満たす証明の履歴についてのみ ID の特定を認めるという形で一括して管理者の権限の行使を許可でき、一旦許可したのちは管理者と第三者機関との間で通信を行うことなく管理者は権限を行使できるという特徴がある。この成果は、英文論文誌 Security and Communication Networks に採録となっている。

また、上述の通り、グループ署名における署名者の脱退は重要な問題である。実用上重要であるのみならず、理論的にも、グループへの所属を証明する際はそれを実行している利用者はすでに脱退した利用者ではないことを確認しなければならないが、これは利用者の ID を部分的に漏洩させることを意味するため、グループ署名の利用者の ID を一切秘匿するという機能とは相反する。そのため、既存の方式のアドホックな拡張では達成が極めて困難である。この問題について、本年度は、理論上の漸近的な性能と実運用の際の具体的な性能とを両立させるグループからの脱退の可能なグループ署名方式を設計した。この成果は、英文論文誌 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences に採録となっている。

(3) 令和 2 年度

令和 2 年度は、本研究の目標である匿名認証付き匿名ルーティングのあるべき安全性概念について研究を進め、複数の成果を得た。

匿名通信においては、暗号化された通信内容をネットワーク上で中継していく際に各暗号文が中継されていった経路を秘匿する必要がある。そのためには、暗号文の「再ランダム化」と呼ばれる、暗号文を、暗号化された内容を変えずに元々の暗号文とは無関係な暗号文に見えるよう改変する操作が中心的である。この操作と両立する(知られている中で)最も安全性のレベルの高い安全性概念が RCCA 安全性である。RCCA 安全性は、暗号文の再ランダム化のみは許容し、暗号文へのそれ以外の意味のある操作は一切許容しないという直観を定式化することを意図したものである。これに関して本研究では、RCCA 安全性が必ずしも上述の直観を忠実に定式化しておらず、技術的な取り扱いの容易さが先行している可能性を指摘した。さらに、上述の直観をより忠実に定式化した新たな安全性概念を定義し、その安全性概念が従来からの RCCA 安全性と等価であることを示した。この成果は、英文論文誌 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences に採録となっている。

同様の視点から、ID ベース暗号と呼ばれる高機能暗号技術における受信者の ID の秘匿性(匿名性)についても、この性質に関する標準的な安全性概念が受信者の ID に関する情報が一ビットも漏洩しないという直観を忠実に定式化していない可能性を指摘した。同様に、この直観をより忠実に定式化した安全性概念を新たに定義し、その安全性概念が標準的な安全性概念と等価であることを示した。この成果は、匿名認証付き匿名ルーティングに ID ベース暗号を組み込む際に、両者の円滑な接続を可能にすると期待される。この成果は、国際会議 ESORICS 2020 に採録となっている。

これ以外にも、匿名認証付き匿名ルーティングにおいて中心的である、意味のある改変を、かつそれのみ許容するゼロ知識証明について研究を行い、それを応用して集約署名という暗号技術に関する成果も得ている。この成果は、国際会議 ProvSec 2020 へ採録となっている。

(4) 令和 3 年度

令和 3 年度は、本研究の目標である匿名認証付き匿名ルーティングのあるべき安全性概念について研究を進め、以下の成果を得た。

匿名通信においては、ネットワーク上の複数の参加者が動的に結託することが想定される。そうした結託を適切にモデル化することは、安全な匿名通信技術を設計するにあたって非常に重要である。本年度は、この点に関して検討を進め、同じくネットワーク上の複数の参加者が動的に結託することが想定される暗号要素技術である、追跡可能集約署名という暗号技術について以下の成果を得た。集約署名とは、複数の署名者による(一般には異なる文書に対する)デジタル署名をコンパクトな表現に圧縮でき、圧縮したまま、元となったデジタル署名全てについての検証を一括して行える暗号要素技術である。この技術の課題として、ここのデジタル署名を圧縮する際に単体のデジタル署名として検証に通過しない不正なデジタル署名が混入すると、圧縮後の表現の検証は失敗してしまい、かつ、どのデジタル署名が正当であってどのデジタル署名が不

正であったかを確認できなくなってしまうというものがある。この課題を解決するのが追跡可能集約署名であり、この暗号要素技術は、圧縮後の表現からどの(圧縮前の)デジタル署名が不正であったかを確認することができるものである。

この追跡可能集約署名においても、個々の署名者が動的に結託し、圧縮された表現の検証や不正署名の追跡を妨害してくることが想定される。この点に関して、匿名通信において検討を進めてきた参加者の動的な結託に関する知見を追跡可能集約署名へ応用し、署名者の動的な結託に耐えられる追跡可能集約署名を提案した。この成果は、国際会議 ACNS Workshop SCI 2021 へ採録となっている。

(5) 令和 4 年度

令和 4 年度は、本研究の目標である匿名認証付き匿名ルーティングの実現に向けて研究を進め、以下の成果を得た。

上述の属性ベース署名において、署名者の属性に対する条件として論理回路の様な記述力の高い計算モデルを許容する方式は、署名データのサイズが条件の記述長に応じて長くなるものか、そうでなければ、その様な大きなデータサイズを回避するために、Karp 帰着と呼ばれる複雑で高コストな計算を用いるものしか存在していなかった。本研究では、署名データのサイズが条件の記述長に依存せず、かつ、Karp 帰着の様な高コストな計算を必要としない、初めての方式を提案した。そのための構成要素として、constraint SNARK と呼ばれる非対話ゼロ知識証明の新たな変種の概念と構成法を提案し、それを用いて上述の性質を持つ属性ベース署名方式を提案した。この成果は、国際会議 SCN 2022 へ採録となっている。

ここで得た新たな非対話ゼロ知識証明は、本研究の目標である匿名認証付き匿名ルーティングの効率的な構成に活用できると期待される。

(6) 令和 5 年度

令和 5 年度は、本研究の目標である匿名認証付き匿名ルーティングの実現に向けて研究を進め、成果をあげた。

具体的には、匿名認証付き匿名ルーティングの重要な構成要素であるゼロ知識証明について研究を進め、ゼロ知識証明を応用した認証技術の一種である多重署名について以下の成果を得た。多重署名とは、ある文書に対して複数の署名者間で対話的に通信を行うことで、それら署名者がそれぞれその文書に対して署名を発行したことを検証できる、小さな署名データを生成できる暗号要素技術である。また、(計算量的安全な)暗号要素技術はある計算問題の計算量的な困難さに基づいて安全性が証明されることが通例であるが、このとき、計算問題の計算量的な困難さと、暗号要素技術への攻撃の計算量的な困難さにはギャップがある場合がある。このギャップが大きい場合、暗号要素技術の攻撃の困難さを十分に高く設定するためには、より困難さの高い計算問題を用いる必要がある。このようなより困難さの高い計算問題を用いた場合、暗号要素技術の効率性が低下してしまう。このような問題を避けるためには、暗号要素技術への攻撃の困難さと、計算問題の困難さとの間にギャップの少ない方式が望ましい。そのようなギャップの小さな方式は、タイトに安全な方式と呼ばれる。本年度は、多重署名について、判定 Diffie-Hellman 問題と呼ばれる問題に基づく、通信ラウンド数が 2 回に抑えられる、タイトに安全な多重署名方式を提案した。この成果は、英文論文誌 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences へ採録決定済みである。

ここで得た新たなゼロ知識証明は、匿名認証付き匿名ルーティングのタイトに安全な方式の構成にも活用できると期待される。

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Sakai Yusuke	４．巻 13409
２．論文標題 Succinct Attribute-Based Signatures for Bounded-Size Circuits by Combining Algebraic and Arithmetic Proofs	５．発行年 2022年
３．雑誌名 Security and Cryptography for Networks, 13th International Conference, SCN 2022, Amalfi (SA), Italy, September 12-14, 2022, Proceedings	６．最初と最後の頁 711～734
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-14791-3_31	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ishii Ryu、Yamashita Kyosuke、Sakai Yusuke、Matsuda Takahiro、Teruya Tadanori、Hanaoka Goichiro、Matsuura Kanta、Matsumoto Tsutomu	４．巻 12809
２．論文標題 Aggregate Signature with Traceability of Devices Dynamically Generating Invalid Signatures	５．発行年 2021年
３．雑誌名 Applied Cryptography and Network Security Workshops - ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21-24, 2021, Proceedings	６．最初と最後の頁 378～396
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-81645-2_22	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 HAYATA Junichiro、KITAGAWA Fuyuki、SAKAI Yusuke、HANAOKA Goichiro、MATSUURA Kanta	４．巻 E104.A
２．論文標題 Equivalence between Non-Malleability against Replayable CCA and Other RCCA-Security Notions	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 89～103
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0015	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kazuma Ohara, Keita Emura, Goichiro Hanaoka, Ai Ishida, Kazuo Ohta, Yusuke Sakai	４．巻 E102-A
２．論文標題 Shortening the Libert-Peters-Yung revocable group signature scheme by using the random oracle methodology	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1745-1337
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1101	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, Kazuma Ohara, Kazumasa Omote, Yusuke Sakai	4．巻 2019
2．論文標題 Group Signatures with Message-Dependent Opening: Formal Definitions and Constructions	5．発行年 2019年
3．雑誌名 Security and Communication Networks	6．最初と最後の頁 ―
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2019/4872403	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 ―

1．著者名 TAKEMURE Kaoru、SAKAI Yusuke、SANTOSO Bagus、HANAOKA Goichiro、OHTA Kazuo	4．巻 ―
2．論文標題 More Efficient Two-Round Multi-Signature Scheme with Provably Secure Parameters for Standardized Elliptic Curves	5．発行年 2023年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 ―
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2023EAP1045	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 ―

〔学会発表〕　計9件（うち招待講演　1件／うち国際学会　9件）

1．発表者名 Sakai Yusuke
2．発表標題 Succinct Attribute-Based Signatures for Bounded-Size Circuits by Combining Algebraic and Arithmetic Proofs
3．学会等名 SCN 2022（国際学会）
4．発表年 2022年

1．発表者名 Ishii Ryu、Yamashita Kyosuke、Sakai Yusuke、Matsuda Takahiro、Teruya Tadanori、Hanaoka Goichiro、Matsuura Kanta、Matsumoto Tsutomu
2．発表標題 Aggregate Signature with Traceability of Devices Dynamically Generating Invalid Signatures
3．学会等名 ACNS Workshop SCI（国際学会）
4．発表年 2021年

１．発表者名
Goichiro Hanaoka, Misaki Komatsu, Kazuma Ohara, Yusuke Sakai, Shota Yamada

２．発表標題
Semantic Definition of Anonymity in Identity-Based Encryption and Its Relation to Indistinguishability-Based Definition

３．学会等名
ESORICS 2020（国際学会）

４．発表年
2020年

１．発表者名
Kaoru Takemure, Yusuke Sakai, Bagus Santoso, Goichiro Hanaoka, Kazuo Ohta

２．発表標題
Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers

３．学会等名
ProvSec 2020（国際学会）

４．発表年
2020年

１．発表者名
Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka

２．発表標題
Fully Anonymous Group Signature with Verifier-Local Revocation

３．学会等名
11th Conference on Security and Cryptography for Networks (SCN 2018)（国際学会）

４．発表年
2018年

１．発表者名
Yusuke Sakai, Shuichi Katsumata, Nuttapong Attrapadung, Goichiro Hanaoka

２．発表標題
Attribute-Based Signatures for Unbounded Languages from Standard Assumptions

３．学会等名
24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018)（国際学会）

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関