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　３ 年　 ６ 月　 ９ 日現在

機関番号：１２６１２
研究種目：若手研究(B)
研究期間：2017～2020
課題番号：１７Ｋ１２６９７

研究課題名（和文）鍵漏洩に耐性のあるIDベース暗号の高安全かつ高効率な実現

研究課題名（英文）Improvement of security and efficiency of identity-based encryption schemes resilient to key leakage

研究代表者

渡邉　洋平（Watanabe, Yohei）

電気通信大学・大学院情報理工学研究科・助教

研究者番号：４０７９２２６３

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究では，メールアドレス等の個人を識別できる任意の文字列（その意味でIDと呼ぶ）を公開鍵として利用可能な公開鍵暗号であるIDベース暗号（Identity-Based Encryption: IBE）について，各種の鍵漏洩耐性を持つIBEの高安全かつ高効率な方式の実現，及び実社会の状況に鑑みた上での本質的に必要な鍵漏洩耐性を持つIBEを新たに定式化・実現することを目指した．結果として，鍵失効機能付きIBE及び鍵隔離型IBEについて様々な成果を得たと共に，新たな鍵漏洩耐性を有するIBEについての定式化も行った．

研究成果の学術的意義や社会的意義
通常のIBEにおいても高い安全性及び高い効率性を両立することは容易ではなく，近年やっと体系化されてきた研究指針である．しかし，機能付きIBEは通常のIBEとは枠組みから異なるため，IBEにおける指針がそのまま適用できる場合は少なく，学術的な工夫が必要であった．また情報漏洩インシデントは今もなお数多く起きており，そのような漏洩に耐性のある暗号技術の研究には社会的および学術的な意義があると考えられる．

研究成果の概要（英文）：Identity-based encryption (IBE) is public-key encryption that enables us to use arbitrary strings, such as e-mail addresses, for public keys. In this project, we aimed to improve IBE schemes with various secret-key leakage resilience properties so that simultaneously achieve strong security levels and high efficiency, and to realize a new model of secret-key leakage resilience for IBE. We finally obtained various results on revocable IBE and key-insulated IBE, and formalized a new model of secret-key leakage resilience.

研究分野：暗号理論

キーワード：暗号理論　IDベース暗号　鍵漏洩耐性

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ID ベース暗号（Identity-Based Encryption: IBE）は任意の文字列（より正確にはメールアドレス等の個人を識別できる任意の文字列であり，その意味で ID と呼ぶ）を公開鍵として利用可能な PKE であり，2000 年代初頭に初めて実用的な IBE が楕円曲線上のペアリング演算を用いることで実現された．それ以降，IBE は現代暗号理論分野における中心的な暗号要素技術の一つとして注目され，非常に多くの研究がなされると共に，IETF RFC 5091，ISO/IEC 18033-5，IEEE 1363.3 等で標準化も進められてきた．それにもかかわらず，実社会では IBE それ自体の利用があまり進んでいない．その理由のひとつとして，秘密鍵漏洩時の対応策が不十分であること，特に IBE の元々のメカニズムでは効率的な鍵無効化機能が実現できないことが挙げられる．IBE では，個人を識別できる任意の文字列を公開鍵にできることから，PKE のように「各公開鍵/秘密鍵に“鍵証明書”を発行してその正当性を別途保証する」といった機構が必要ない．この点がしばしば IBE の最大の特長として挙げられ，IBE が高い利便性を有していると言われている所以であるが，これは PKE と同様の鍵無効化機能は実現できないことも意味している．具体的には，PKE では鍵漏えいが起こった際にはその鍵の証明書を失効することで鍵無効化を実現しており，鍵証明書が不要な IBE では当然同様の方法を取ることができない．実際，2015 年 12 月に米 Microsoft 社がゲームサイト “Xbox Live” 用の秘密鍵を漏洩させた際にも，鍵証明書を失効することで対応を行っており，IBE を実利用する場合にも鍵漏洩時に実用的かつ迅速に対応できるような機構が必要不可欠である．国内で暗号技術評価を行うプロジェクトである CRYPTREC の報告においても，鍵漏洩時の対応策の実現が IBE 実利用に向けた重要な課題のひとつだとされている．

これまでにも，鍵漏洩問題の解決に向けた理論的な先行研究が行われてきた．効率的な鍵無効化機能の実現に向け，鍵無効化機能付き IBE（Revocable IBE: RIBE）が盛んに研究されており，また異なるアプローチで鍵漏洩問題の解決を図っているものとして，鍵隔離機能付き IBE（Key-Insulated IBE: KI-IBE），耐部分漏洩機能付き IBE（Leakage-Resilient IBE: LR-IBE）が知られている．KI-IBE は鍵を定期的に更新することで，また LR-IBE は秘密鍵が部分的に漏れても安全性に影響がないような構造を持つことで，鍵漏洩問題の解決を図っている．しかしながら，既存の RIBE，KI-IBE，LR-IBE はいずれも(1)高安全かつ(2)高効率なものが実現できていない．これらの機能付き IBE が(1)高安全であるとは，①適応的安全性と呼ばれる実用的に必要だと考えられている安全性を持ち，また②その安全性が弱い（多項式時間で解くことができないと広く信じられている）計算量仮定のもとで数学的に証明されていることを指し，(2)高効率であるとは，①方式の各パラメータ長が短く，特にどのパラメータ長も ID の長さに依存せず，及び②安全性を証明する際に根拠とする計算問題を解く難しさと方式の安全性を破る難しさがほぼ同等に近いことを指す．

２．研究の目的

本研究では，各種の鍵漏洩耐性を持つ IBE の高安全かつ高効率な方式を実現すること，更には実社会の状況を鑑みた上で，本質的に必要な鍵漏洩耐性を持つ IBE を新たに定式化・実現することを目指す．

まず，RIBE，KI-IBE，LR-IBE それぞれに関して(1)及び(2)の両方を達成する方式を実現する．具体的には，各機能付き IBE において，(1)当該分野で“弱い”，すなわち“解かれないだろうと強く信じられている”計算量仮定の下で適応的安全性を持ち，(2)鍵長が ID のビット長に依存しない効率的なパラメータ長を持ち，証明の帰着効率が緊密である構成法を提案する．

更に，各機能性（鍵無効化，鍵更新，耐部分漏洩）から実社会で最低限要求される中心的な要素だけを抽出し，実用的な安全性レベルは持ちつつも今までより広い範囲の鍵漏洩耐性をカバーする定義を新たに与え，それまでの知見を活かし(1)及び(2)を達成する方式を具体的に構成する．

３．研究の方法

まず，RIBE，KI-IBE，LR-IBE それぞれに関して(1)及び(2)の両方を達成する方式の実現に向け，以下の方針で研究を行う．

最初に，これまでに精力的に研究を行ってきた RIBE について，(1)高安全かつ(2)高効率を満たすものの実現を目指す．具体的には，通常の IBE における高安全かつ高効率の両立を実現するアプローチとして知られる“Dual System Encryption（DSE）”手法を適用し，構成を試みる．しかしながら，DSE 手法は RIBE にそのまま適用できないことが知られているため，種々のアプローチでもってその問題の回避を試みる．また，最初に(1)及び(2)を達成する IBE を DSE 手法を用いて構成し，その IBE の安全性に RIBE の安全性を帰着させるという，ある種のモジュラーアプローチにも並行して取り組む．また，量子計算機の実現にも耐え得る RIBE の実現や拡張概念である階層型 RIBE の高安全および高効率な実現にも取り組む．

次に，KI-IBE について，RIBE 研究方法と同様に(1)高安全かつ(2)高効率なものの実現を目指

す．KI-IBE には 2 種類の秘密鍵が存在し，補助鍵と呼ばれる鍵を平時はインターネットから隔離して保存しておき，必要に応じて補助鍵を用いて復号鍵を更新することで，漏洩時のリスクを最小限に抑えることのできる有用な方式である．KI-IBE は RIBE とメカニズムが比較的似ているため，RIBE 構成時に取ったアプローチを応用することで(1)及び(2)を両立した方式を実現できるだろうと予想される．

続いて，LR-IBE について，これまでと同様に(1)高安全かつ(2)高効率なものの実現を目指す．LR-IBE は秘密鍵が部分的に漏れても安全性を保証可能な IBE であり，基本的に通常の IBE と同様のメカニズムを持つため，通常の IBE に用いられるテクニックの応用が可能だと考えられる．しかしながら，基礎として用いる IBE が(1)及び(2)を実現できるものだとしても，部分漏洩耐性と相性が良いかどうかを良く見極めなければならない．従って，まずは既存の LR-IBE を良く調査し，部分漏洩耐性を持たせるためにはどのような特徴を持った構成がふさわしいのかを理解することに努め，その後，(1)及び(2)を両立する LR-IBE の実現を目指す．

なお，適当なタイミングで方式ごとにこれまでの進捗状況を振り返り，(1)①②及び(2)①②までの全ての要件を満たすのが難しいと判断した場合には，どの要件を妥協するかを的確に判断した上で，できる限り望ましい要件を満たす方式の実現に切り替える．

上記研究を進めながら，最終目標である「新たな鍵漏洩耐性を持つ IBE の定式化」を見据え，暗号技術の実利用状況やセキュリティインシデントの状況を，CRYPTREC 等の団体が発表している文書から調査，また専門家からの聞き取りを進めていく．そして，新たな鍵漏洩耐性を持つ IBE の定式化，及びその安全性を満たす方式の構成を行う．RIBE，KI-IBE，LR-IBE それぞれにおいて，強い安全性を持ちながら効率的にすることが難しい事実からもわかる通り，各機能性を愚直に組み合わせたとしても，効率的な構成の実現は難しいと考えられる．そこで，各機能付き IBE から出来る限り機能性を抽出し，弱めていく方針を取る．ここまでに調査してきた暗号技術の実利用状況やセキュリティインシデントの状況から，実際どの程度の鍵漏洩耐性があれば実用上問題ないのかを導き出す．例えば，調査結果から，実用においては想定する鍵漏洩回数は無制限ではなく高々数十個程度で十分である等の結論が考えられる．鍵漏洩耐性を“出来る限り広く，問題ないレベルで浅い”ものにし，効率的でありながら，従来のものより（実用的な意味で）強い鍵漏洩耐性を持つ IBE を定式化する．その後，ここまでに方式ごとに研究してきた過程で得た知見を活用し，できる限り(1)及び(2)を両立する方式の構成を目指す．

４．研究成果

まず，RIBE に関する成果についてまとめる．RIBE，及びその拡張である階層型 RIBE について，(1)高い安全性を有し，かつ(2)効率的な方式を提案した．具体的には，次の３つの方式を提案し，査読付学術英文論文誌等で発表した．まず，(1)最も望ましいと考えられている適応的安全性及び鍵漏洩耐性を満たし，(2)各パラメータが短く，特に ID の長さに依存しない方式を初めて提案した．また，(1)量子計算機でも破ることのできない適応的安全性及び鍵漏洩耐性を，(2)比較的効率的に実現し，査読付学術英文論文誌等で発表した．さらに，階層型 RIBE について，(1)最も望ましいと考えられている適応的安全性及び鍵漏洩耐性を満たし，(2)既存方式に比べ各パラメータが最も短い方式を提案し，査読付学術英文論文誌等で発表した．最後の構成法は任意の IBE を構成要素として使うことができるため，その IBE の具体的な構成によって，より効率的な方式や量子計算機に耐性のある方式等，様々な方式が実現可能である．

続いて，Key-Insulated Identity-Based Encryption (KI-IBE) について，高安全かつ高効率なものの実現を目指し，研究を行った．具体的には，以前提案した KI-IBE 方式の安全性証明の不備を発見し，元々の高い効率性を損なうことなく新たに構成を提案，査読付国際論文誌にて論文発表を行った．また，その構成テクニックを応用し，鍵隔離機能を有する公開鍵暗号 (Key-Insulated Public-Key Encryption: PK-KIE) の提案も併せて行っている．提案 PK-KIE 方式も，高い効率性及び高い安全性を達成している．また，IBE から構成可能な検索可能暗号（暗号化したまま検索が可能な暗号技術）について，鍵隔離耐性を含む鍵漏洩耐性を実現する方式を初めて実現し，査読付き学術論文誌等で発表した．具体的には，IoT 環境での利用を想定し，秘密鍵が漏洩しても更新することで安全性を維持可能な検索可能暗号の構成を提案，また Raspberry Pi を用いた実装も行い，IoT 環境で利用可能であることを示した．

上記の研究を進めている中で，研究時間の配分を考え，LR-IBE に関する(1)及び(2)を達成する方式の研究よりも最終目標である「新たな鍵漏洩耐性を持つ IBE の定式化」に向けた研究を優先することとした．RIBE，KI-IBE，LR-IBE 以外の鍵漏洩耐性を有する暗号技術として，鍵の分散管理を行うことで漏洩リスクの軽減を図るしきい値公開鍵暗号についても研究を行い，より弱い計算量仮定から強い安全性を証明可能かつ効率的な方式を提案し，国内会議及び査読付国際会議にて論文発表を行い，国内会議で優秀論文賞を受賞した．また，実社会で広く利用されている AES の鍵漏洩耐性について解析も行い，国内会議及び査読付国際会議で発表を行った．最終的に，LR-IBE と KI-IBE を組み合わせたモデルを考え，(1)高い安全性と(2)高い効率性を両立するよう，単純に組み合わせたモデルではなく，実用的に十分な安全性レベルとなるようなモデルを検討し，そのモデルを実現する効率的な方式を構成した．研究期間内に成果発表には至らなかったが，論文執筆を進めている．

５．主な発表論文等

〔雑誌論文〕　計21件（うち査読付論文　11件／うち国際共著　2件／うちオープンアクセス　2件）

１．著者名 M. Ebina, J. Mita, J. Shikata, and Y. Watanabe	４．巻 －
２．論文標題 Efficient Threshold Public Key Encryption from the Computational Bilinear Diffie-Hellman Assumption	５．発行年 2021年
３．雑誌名 Proceedings of ACM APKC 2021	６．最初と最後の頁 23－32
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3457338.3458296	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 K. Emura, A. Takayasu, and Y. Watanabe	４．巻 －
２．論文標題 Adaptively secure revocable hierarchical IBE from k-linear assumption	５．発行年 2021年
３．雑誌名 Designs, Codes and Cryptography	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） 10.1007/s10623-021-00880-w	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 K. Emura, J.H. Seo, and Y. Watanabe	４．巻 863
２．論文標題 Efficient revocable identity-based encryption with short public parameters	５．発行年 2021年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 127－155
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2021.02.024	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 A. Takayasu and Y. Watanabe	４．巻 849
２．論文標題 Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more	５．発行年 2021年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 64－98
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2020.10.010	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 T. Uemura, Y. Watanabe, Y. Li, N. Miura, M. Iwamoto, K. Sakiyama, and K. Ohta	4．巻 －
2．論文標題 A Key Recovery Algorithm Using Random Key Leakage from AES Key Schedule	5．発行年 2020年
3．雑誌名 Proc. of ISITA 2020	6．最初と最後の頁 382－386
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-10	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 植村 友紀，渡邉 洋平，李 陽，三浦 典之，岩本 貢，崎山 一男，太田 和夫	4．巻 －
2．論文標題 AES鍵スケジュールからの固定ビット数漏洩を用いた鍵復元アルゴリズムの性能評価	5．発行年 2021年
3．雑誌名 SCIS 2021予稿集	6．最初と最後の頁 2B3-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 H. Anada, A. Kanaoka, N. Matsuzaki, and Y. Watanabe	4．巻 19
2．論文標題 Key-Updatable Public-Key Encryption with Keyword Search (Or: How to Realize PEKS with Efficient Key Updates for IoT Environments)	5．発行年 2020年
3．雑誌名 International Journal of Information Security	6．最初と最後の頁 15－38
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-019-00441-2	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 K. Emura, S. Katsumata, and Y. Watanabe	4．巻 LNCS 11736
2．論文標題 Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices	5．発行年 2019年
3．雑誌名 Proceedings of ESORICS 2019	6．最初と最後の頁 113－133
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-29962-0_6	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 Junji Shikata and Yohei Watanabe	４．巻 87(5)
２．論文標題 Identity-based Encryption with Hierarchical Key-insulation in the Standard Model	５．発行年 2019年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 1005－1033
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-018-0503-4	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 Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki, and Yohei Watanabe	４．巻 10946
２．論文標題 Key-updatable Public-key Encryption with Keyword Search: Models and Generic Constructions	５．発行年 2018年
３．雑誌名 Information Security and Privacy	６．最初と最後の頁 341－359
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-93638-3_20	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 高安敦，渡邉洋平，江村恵太	４．巻 －
２．論文標題 より効率的で適応的に安全な鍵失効機能付きIDベース暗号の構成	５．発行年 2019年
３．雑誌名 暗号と情報セキュリティシンポジウム2019（SCIS 2019）予稿集	６．最初と最後の頁 2A3-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 江村恵太，勝又秀一，渡邉洋平	４．巻 －
２．論文標題 鍵生成センタに対して安全なIDベース暗号	５．発行年 2019年
３．雑誌名 暗号と情報セキュリティシンポジウム2019（SCIS 2019）予稿集	６．最初と最後の頁 2A3-1
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 海老名将宏，渡邉洋平，四方順司	４．巻 －
２．論文標題 探索問題の困難性に基づく効率的なしきい値公開鍵暗号の構成	５．発行年 2019年
３．雑誌名 暗号と情報セキュリティシンポジウム2019（SCIS 2019）予稿集	６．最初と最後の頁 2A4-4
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 海老名将宏，渡邉洋平，四方順司	４．巻 －
２．論文標題 CBDH仮定に基づく効率的な閾値公開鍵暗号	５．発行年 2018年
３．雑誌名 コンピューターセキュリティシンポジウム2018（CSS 2018）予稿集	６．最初と最後の頁 746－753
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 松崎なつめ，穴田啓晃，金岡晃，渡邉洋平	４．巻 －
２．論文標題 鍵更新機能付き検索可能暗号：効率化に向けた一工夫	５．発行年 2018年
３．雑誌名 コンピューターセキュリティシンポジウム2018（CSS 2018）予稿集	６．最初と最後の頁 814－821
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 A. Takayasu and Y. Watanabe	４．巻 LNCS 10342
２．論文標題 Lattice-Based Revocable Identity-Based Encryption with Bounded Decryption Key Exposure Resistance	５．発行年 2017年
３．雑誌名 Information Security and Privacy	６．最初と最後の頁 184－204
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-60055-0_10	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 Y. Watanabe, K. Emura, and J. H. Seo	4．巻 LNCS 10159
2．論文標題 New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters	5．発行年 2017年
3．雑誌名 Topics in Cryptology - CT-RSA 2017	6．最初と最後の頁 432－449
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-52153-4_25	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 該当する

1．著者名 松崎なつめ，穴田啓晃，金岡晃，渡邉洋平	4．巻 －
2．論文標題 鍵更新機能付き検索可能暗号の一般的構成	5．発行年 2018年
3．雑誌名 暗号と情報セキュリティシンポジウム 2018（SCIS 2018）予稿集	6．最初と最後の頁 4A2-6
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 渡邉洋平，穴田啓晃，松崎なつめ	4．巻 －
2．論文標題 鍵更新機能付き検索可能暗号：鍵隔離モデルによる実現	5．発行年 2017年
3．雑誌名 コンピュータセキュリティシンポジウム 2017（CSS 2017）予稿集	6．最初と最後の頁 741－748
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 松崎なつめ，穴田啓晃，渡邉洋平	4．巻 －
2．論文標題 鍵更新機能付き検索可能暗号：公開鍵更新モデルによる実現	5．発行年 2017年
3．雑誌名 コンピュータセキュリティシンポジウム 2017（CSS 2017）予稿集	6．最初と最後の頁 734－740
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 松崎なつめ，穴田啓晃，渡邉洋平	４．巻 －
２．論文標題 鍵更新機能付き検索可能暗号の一提案 ～検索可能代理人再暗号化の適用について～	５．発行年 2017年
３．雑誌名 電子情報通信学会情報セキュリティ研究会，ISEC2017-5	６．最初と最後の頁 1－6
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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10件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Yohei Watanabe
２．発表標題 Efficient Threshold Public Key Encryption from the Computational Bilinear Diffie-Hellman Assumption
３．学会等名 ACM APKC 2021（国際学会）
４．発表年 2021年

１．発表者名 Keita Emura
２．発表標題 Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices
３．学会等名 ESORICS 2019（国際学会）
４．発表年 2019年

１．発表者名 Yohei Watanabe
２．発表標題 Key-updatable Public-key Encryption with Keyword Search: Models and Generic Constructions
３．学会等名 ACISP 2018（国際学会）
４．発表年 2018年

１．発表者名
高安敦

２．発表標題
より効率的で適応的に安全な鍵失効機能付きIDベース暗号の構成

３．学会等名
暗号と情報セキュリティシンポジウム2019（SCIS 2019）

４．発表年
2019年

１．発表者名
江村恵太

２．発表標題
鍵生成センタに対して安全なIDベース暗号

３．学会等名
暗号と情報セキュリティシンポジウム2019（SCIS 2019）

４．発表年
2019年

１．発表者名
海老名将宏

２．発表標題
探索問題の困難性に基づく効率的なしきい値公開鍵暗号の構成

３．学会等名
暗号と情報セキュリティシンポジウム2019（SCIS 2019）

４．発表年
2019年

１．発表者名
海老名将宏

２．発表標題
CBDH仮定に基づく効率的な閾値公開鍵暗号

３．学会等名
コンピューターセキュリティシンポジウム2018（CSS 2018）

４．発表年
2018年

１．発表者名
松崎なつめ

２．発表標題
鍵更新機能付き検索可能暗号：効率化に向けた一工夫

３．学会等名
コンピューターセキュリティシンポジウム2018（CSS 2018）

４．発表年
2018年

１．発表者名
Yohei Watanabe

２．発表標題
New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters

３．学会等名
RSA Conference 2017, Cryptographers' Track, CT-RSA 2017（国際学会）

４．発表年
2017年

１．発表者名
渡邉洋平

２．発表標題
鍵更新機能付き検索可能暗号：鍵隔離モデルによる実現

３．学会等名
コンピュータセキュリティシンポジウム 2017（CSS 2017）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
研究代表者ウェブページ
https://iw-lab.jp/users/watanabe/

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