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　２ 年　 ６ 月 １８ 日現在

機関番号：１２１０２
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２７８０

研究課題名（和文）ポスト量子時代をみすえた高機能暗号の安全性評価手法の確立

研究課題名（英文）Security Evaluation of High Functional Encryption toward Post-Quantum Era

研究代表者
國廣　昇（Kunihiro, Noboru）

筑波大学・システム情報系・教授

研究者番号：６０３４５４３６

交付決定額（研究期間全体）：（直接経費）　　12,800,000円

研究成果の概要（和文）：ポスト量子暗号として期待される格子暗号は，格子理論に関係する問題に安全性の根拠をおいているが，最小ベクトル問題の困難さに関して精密な評価を与えることに成功した．量子計算機の実現が，RSA暗号などの従来から使われている暗号技術に対してどのような影響を及ぼすかの評価を行った．いくつかの物理実験の包括的な理解を進め，実社会に対する影響に関して考察を与えた．ポスト量子暗号と比較して議論される従来暗号に関しても研究を行い，その安全性に関して成果を得た．

研究成果の学術的意義や社会的意義
本課題では，ポスト量子時代を見据えた暗号技術に関して研究を行った．それにより，ポスト量子暗号方式の安全性の根拠となる問題の困難さを与えるとともに，量子計算機の現代暗号に対する影響に関して成果を得た．様々な条件下でのRSA暗号を代表とする現代暗号の安全性評価も与えている．以上の成果を通して，ポスト量子時代を見据えた暗号技術の安全性評価を与えることに成功しており，安心して暗号技術を利用する基礎を与えた．

研究成果の概要（英文）：Lattice-based cryptography is expected as a post-quantum cryptosystem.Its security relies on the difficulty of lattice-related problems.We have succeeded in giving a precise analysis of its difficulty.In particular, we have obtained results on algorithms for solving the Shortest Vector Problem.We have evaluated how the realization of quantum computers affects conventional cryptographic techniques such as RSA cryptography.Specifically, we have given a comprehensive understanding of several physical experiments and discussed their effects on the real world.Furthermore, we have studied the security evaluation of conventional cryptography and have obtained results on its security.Through these results, we have succeeded in giving a security evaluation for cryptography in the post-quantum era, and have given a basis to use cryptography securely.

研究分野：暗号理論

キーワード：暗号理論　安全性評価　ポスト量子暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 研究の社会的背景

我々の生活の中に，すでに，暗号技術が広く深く浸透している．プライバシー保護の意識の高まりとともに，狭い意味での暗号（秘匿通信）だけではなく，完全準同型暗号，属性ベース暗号などの高機能な暗号の必要性が生じている．高い機能性を獲得するために，暗号構成において，本質的に多重の線形性を持つ格子理論に基づく問題に関する研究が盛んに行われている．

量子計算機が実現した場合には，素因数分解問題，離散対数問題などの従来から用いられている暗号方式は，Shor のアルゴリズムにより，量子多項式時間で破られることがわかっている．量子計算機の実現に向けて，世界中で活発に研究が進んでいるが，技術的なブレークスルーにより，近い将来に実現する可能性は否定できない．そのため，量子計算機が実現した場合にも安全な暗号（ポスト量子暗号）の構成が重要となる．ポスト量子暗号の候補として，格子理論に基づく暗号が，最も有力である．その中でも，特に，LWE 問題，LPN 問題，およびその関連問題の困難さに基づく暗号の研究が進んでいる．

ポスト量子暗号に関しては，実際に，世界中で，暗号化方式の標準化の動きがある．米国では，国家安全保障局（NSA）が，2020 年の策定を目指して，ポスト量子暗号の標準化をすることを宣言している．EU でも同様の動きが活発に行われている．その中でも，特に英国では，政府通信本部(GCHQ)も，量子暗号に向けた学術研究に研究資金を提供するなど，各国で研究が活発化している．当然のことながら，標準化をする際には，安全性の重点的な解析によるできるだけ正確な理解が必須となる．

以上より，格子問題の困難さを安全性の根拠とする暗号は，高機能暗号という側面からも，ポスト量子暗号という側面からも極めて重要であり，それを支える格子問題の困難さに対する正確な評価は，必須である．

(2) 研究の学術的背景

ポスト量子暗号，高機能暗号という観点から考えると，従来から研究が進んでいる素因数分解や離散対数問題をもとにした暗号方式では，不十分であり，格子理論に基づく暗号技術が重要となる．具体的には，Learning Parity Noise (LPN)問題，Learning with Error (LWE)問題, Ring-LWE 問題などの困難さに基づく暗号方式や，属性ベース暗号，（完全）準同型暗号などの高機能暗号が必須となる．

その一方で，格子理論に基づく問題は，2005 年の Oded Regev による提案が暗号利用のさきがけであり，比較的新しい問題である．そのため，困難さの解析は十分にされているとは言い難い．正確な困難さの評価により，安心して暗号方式を利用することが可能となる．

２．研究の目的

本研究の主たる目的は，LWE 問題，LPN 問題などの格子理論に基づく困難な問題のできるだけ厳密な困難さの評価を行うことである．格子問題は，ポスト量子暗号のみならず，完全準同型暗号などの高機能暗号の安全性の根拠となる問題として期待されている．そのため，格子問題の困難さの正確な理解は，次世代の暗号技術を考える上で必要である．さらに，LWE 問題，LPN 問題にこだわらず，幅広く格子理論に関係する問題に対して，その困難さを評価することを目的とする．この研究により，格子問題を利用して構成される暗号の正確な安全性評価が可能となり，最終的には，高機能かつ高い安全性を持つ暗号を長期にわたり，安心して，使用することが可能となる．

ポスト量子時代を考察する上で，現在利用されている暗号方式との比較は必須であり，RSA 暗号などの現在広く利用されている暗号方式の安全性評価を行うことも重要である．そのため，量子計算機実現後にどの程度，現在使われている暗号が弱くなるのかをできるだけ精密な評価をすることも目的とする．さらに，様々な状況に対する攻撃を想定することにより，RSA 暗号の安全性を明らかにするとともに，同様の攻撃手法をポスト量子暗号に対しても適用することを目指す．

３．研究の方法

研究目的を達成するために，本研究課題では，以下の方法により研究を遂行する．(i) LWE 問題，LPN 問題，最短ベクトル問題（SVP）などの格子理論に関する問題の困難さの解析を行う．(ii) ポスト量子暗号の候補として期待される暗号方式の提案，拡張を目指す．(iii) 量子計算機の実現が，現代暗号に及ぼす影響をできるだけ正確に理解するため，素因数分解，離散対数問題の Shor のアルゴリズムに対する影響の研究を進める．さらに，ポスト量子時代を見据える上で，現代暗号との性能比較や，現代暗号の安全性評価手法のポスト量子暗号への環流が必須となる．そのため，現代暗号自身に対する安全性評価も重点的に行う．具体的には，(iv) 格子理論を用いた RSA 暗号やその変種の安全性評価を行う．(v) 秘密鍵を誤り付きで得られた時の RSA 暗号の安全性評価を行う．以上を本研究課題の方法とする．

４．研究成果

大きく分けて，(1)次世代暗号の提案，安全性評価，(2)従来暗号の精密な安全性評価，に関して成果を得た．特に，後者の研究も，前述のように，次世代暗号の安全性評価や性能比較を行う際の有効な解析手法として有効であると考えるため，重要な研究課題である．

(1) ポスト量子時代を見据えた暗号の提案，安全性評価

①　格子理論に基づく困難な問題に関する評価

次世代暗号として期待されている格子暗号に対して，より精密な安全性評価を与えた．最短ベクトル探索問題の最悪時計算量の評価を異なる二つの手法に対して行っている．既存の方式では，理論的な妥当性に問題がある箇所があったが，この研究では精密な解析を行うことにより適切な評価の導出に成功している．具体的には，格子簡約基底，BKZ 簡約基底およびスライド簡約基底における短いベクトルを列挙する最悪ケースの計算量が，従来知られている Walter による評価よりも小さいことを示した．さらに，Walter のアプローチに従う限り，この評価が最適であることを示した．さらに，得られた評価を任意のブロックサイズに対して拡張している．この成果は，ブロック簡約基底の幾何学的特性を利用することにより得られている．この研究では，最悪ケースに関する解析を与えており，安全に格子暗号を使う際の指標を与えている．

最短ベクトル問題について研究を行い，成果を得た．この問題を解く際に，一般にランダムサンプリング手法が有効であるが，これまでに行われてきた解析では，得られた格子ベクトルが特定の平行多面体内に一様に分布しているという妥当性が確認されていない仮定に基づいていた．この研究では，ランダムサンプリングとその変種の一般化を行い，離散的 Pruning を伴う格子列挙手法を導入した．これは，n 次元空間の分割に基づいた新しい幾何学的記述を与えている．この結果は，ガウシアンヒューリスティックという妥当な仮定の下での，ランダムサンプリングの解析として初めてのものである．さらに，数値実験を行い，得られた解析が妥当であることを示している．ランダムサンプリングおよびその変種の成功確率を推定し，従来知られている Pruning 列挙との比較を行うことを可能にした．

格子暗号方式のうち，Ring-LWE 問題を安全性の根拠とする格子暗号方式は，数論変換(Number Theoretic Transform)を用いた効率的な実装が知られている．Ring-LWE 暗号方式は，NIST にも多数提出されており，次世代の暗号方式の有力候補である．しかし，実装された暗号方式にはサイドチャネル攻撃の脅威が存在するため，サイドチャネル攻撃の耐性を考察することが，暗号方式を安全に利用するために必要不可欠である．この研究では，数論変換実行中の演算情報を抽出する攻撃手法に着目し，秘密鍵を復元する攻撃の提案を行った．提案した秘密鍵復元手法について理論的解析を行い，提案アルゴリズムが多項式サイズ n の多項式時間となるための条件の導出に成功した．

②　同種写像に基づく暗号

ポスト量子暗号として期待される同種写像に基づいて，多人数鍵共有方式の提案を行った．従来から知られている SIDH 鍵共有方式と Burmester-Desmedt 鍵共有方式を組み合わせることにより，多人数 2 ラウンド鍵共有方式の提案に成功している．素朴な方法では，n 人での鍵共有には，n-1 ラウンド必要であったが，提案手法においては，2 ラウンドにまで削減することに成功している．この方式は，古典計算機，量子計算機両方に対しても耐性があり，耐量子暗号方式になっている．

さらに，この提案方式の実装も行った．いくつかのパラメタ選択に対して，適切なパラメタの選択法を与えるとともに，実用上十分高速であることを確認した．

さらに，提案した多人数鍵共有方式を利用した擬似乱数生成器の提案に成功している．ついで，これまで考慮されてこなかった通常同種写像上での Diffie-Hellman 鍵共有の安全性評価を行った．

③　量子計算機を用いた時の安全性

量子計算機が実現した際に，どの程度現代暗号が脆弱になるかは，ポスト量子時代の暗号を考える上で極めて重要である．RSA 暗号に関して，必要な量子的リソースおよびこれまで行われている物理実験の精密な整理を行った．これまでに数種類の素因数分解を行った物理実験が行われているが，いくつかの実験は，本来求めたい素因数を陽に利用して回路構成を行った実験であり，いくつかの実験では，特殊な合成数（これまでの実験では 15）のみに有効な回路であることを明らかにした．以上の考察により， Shor のアルゴリズムの実装として適切な回路構成はこれまでに存在しないことを明らかにしている．この成果を，国際会議（MQC2019）および国内シンポジウム（NICT サイバーセキュリティシンポジウム 2019）で招待講演を行っている．

楕円離散対数問題も，素因数分解と同様に量子計算機を用いると多項式時間で解読できることが知られている．この研究では，既存方式の拡張を行い，従来知られている回路よりも少ないリソース（量子ビット数，ゲート数）で楕円離散対数問題を解く回路構成を与えている．具体的には，逆元計算の省コスト化を行い，楕円離散対数問題を解く際の計算量削減を実現している．

共通鍵暗号において，ある特定の暗号利用モードでは，Simon のアルゴリズムにより量子多項式時間で解読されることが知られている．この研究では，精密な成功条件の評価を行い，より少ない量子ビット数で解読できることの証明を行っている．

Shor のアルゴリズムを実行する上で，量子剰余加算回路を繰り返し実行している．効率的な量子剰余加算回路の提案を行い，具体的な量子計算機のハードウェア構成を考慮した上での実装を行っている．依然，量子計算機自身にノイズが大きいため，意味のある実験結果は得られていないが，素因数分解の大規模実験に向けて準備を進めている．

これまでの研究では量子ゲート型の量子計算機を想定していたが，（量子）アニーリング計算を用いた場合の，素因数分解の評価も進めている．従来法の改良および実装の工夫を行い，アニーリング計算を用いて 32 ビット合成数の素因数分解に成功している．これは，アニーリング計算に基づく素因数分解の中では，最も大きい合成数である．

(2) 従来暗号の精密な安全性評価

ポスト量子時代を考察する上で，現在利用されている暗号方式との比較は必須であり，RSA 暗号の安全性評価も行っている．様々な状況に対する攻撃を想定することにより，RSA 暗号の安全性が明らかになったとともに，同様の攻撃法をポスト量子暗号に対しても考えることにより，これら暗号の安全性を正当に評価する助けとなる．

① 格子を使った解析

RSA 暗号に対する部分鍵漏洩攻撃は，秘密鍵 d および素因数の部分情報が攻撃者に与えられた環境下で，秘密鍵全体を復元する攻撃である．多くの研究では，格子ベースのアルゴリズムが提案されている．この研究では，いくつかの既存の攻撃シナリオを含む一般的な攻撃シナリオの定式化を行い，そのシナリオのもとで機能する攻撃の提案に成功している．この攻撃は，いくつかの既存の部分鍵漏洩攻撃を特殊なケースとして含んでいる．さらに，いくつかの特殊なケースにおいては，過去の最良の攻撃よりも優れた結果となっている．この結果は，単に既存の結果の一般化や改善だけではなく，一般的な攻撃シナリオを含んでいるため，この結果を幅広く利用することができる．

RSA の部分鍵漏洩攻撃は多くの研究がなされているが，本来は，Boneh と Durfee による Small Secret Exponent 攻撃により，部分鍵漏洩攻撃は，部分情報がなくても $d < N^{0.292}$ であれば常に機能することが望ましい．しかし，Boneh-Durfee の攻撃の性能を失うことなく，与えられた部分情報を有効に利用することは難しい課題であり，多くの既知の部分鍵漏洩攻撃では，$d < N^{0.292}$ では機能しないという問題点があった．この研究では，Secret Exponent d が小さい場合の攻撃の改良を行った．提案攻撃は，必要とする部分情報が少ないという意味で，これまでに知られているすべての攻撃よりも優れている．我々の攻撃は Boneh-Durfee bound を完全にカバーしている．

② サイドチャネル

RSA 暗号の秘密鍵がそのビットの値に応じて，何らかのアナログ値が漏洩された状況を想定する．この状況下で，どの程度情報が漏洩すると攻撃が成功するかの評価を行っている．従来提案されているアルゴリズムは，ノイズに対称性があるときに有効なものであったが，非対称なノイズの時にも有効なアルゴリズムの提案に成功した．さらに，正しいノイズの分布が未知であっても近似分布のみが得られている時に有効なアルゴリズムの提案に成功した．より広いクラスに対して適用可能なアルゴリズムの提案を行い，さらに，攻撃成功の条件を厳密に導出している．これまでに得られた秘密鍵が得られた時の安全性評価に関する一連の成果をまとめた解説論文を発表するとともに，国際会議 WICS にて，Keynote スピーチを行っている．

RSA 暗号の復号処理の演算結果が誤り付きで得られたときの安全性評価を行っている．特に，sliding window 法を用いた演算情報が誤り付きで得られた時の安全性評価を行っている．まず，w=1 という特殊な状況において，誤り付きの演算結果が得られたときの安全性評価を与えた．具体的には，誤り率が 5.8%以下であるときには，攻撃に成功することを示している．

ついで，2 以上の w に対して，誤りのない演算結果が得られた時の改良を行っている．このアルゴリズムでは，演算結果から，秘密鍵系列を部分的に復元することにより行われる．精密な評価を与えるとともに，復元ができていないビットに関する情報を利用したアルゴリズムの提案に成功している．ついで，この二つの結果を組み合わせることにより，一般の w に対して，誤り付きの状況下で有効なアルゴリズムの提案に成功している．

５．主な発表論文等

〔雑誌論文〕　計25件（うち査読付論文　25件／うち国際共著　5件／うちオープンアクセス　0件）

１．著者名 Kunihiro Noboru, Takayasu Atsushi	４．巻 277
２．論文標題 Worst case short lattice vector enumeration on block reduced bases of arbitrary blocksizes	５．発行年 2020年
３．雑誌名 Discrete Applied Mathematics	６．最初と最後の頁 198～220
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.dam.2019.09.017	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 Takayasu Atsushi, Kunihiro Noboru	４．巻 761
２．論文標題 Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound	５．発行年 2019年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 51～77
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.tcs.2018.08.021	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 Oonishi Kento, Huang Xiaoxuan, Kunihiro Noboru	４．巻 LNCS 11975
２．論文標題 Improved CRT-RSA Secret Key Recovery Method from Sliding Window Leakage	５．発行年 2020年
３．雑誌名 Proc. of ICISC2019	６．最初と最後の頁 278～296
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-40921-0_17	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 Oonishi Kento, Kunihiro Noboru	４．巻 LNCS11396
２．論文標題 Attacking Noisy Secret CRT-RSA Exponents in Binary Method	５．発行年 2019年
３．雑誌名 Proc. of ICISC2018	６．最初と最後の頁 37～54
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-12146-4_3	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	4．巻
Lu Yao, Kunihiro Noboru, Zhang Rui, Peng Liqiang, Ma Hui	LNCS11149
2．論文標題	5．発行年
Certifying Variant of RSA with Generalized Moduli	2018年
3．雑誌名	6．最初と最後の頁
Proc. of ICICS2018	598～608
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
https://doi.org/10.1007/978-3-030-01950-1_35	有
オープンアクセス	国際共著
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	該当する

1．著者名	4．巻
Furukawa Satoshi, Kunihiro Noboru, Takashima Katsuyuki	-
2．論文標題	5．発行年
Multi-party Key Exchange Protocols from Supersingular Isogenies	2018年
3．雑誌名	6．最初と最後の頁
Proc. of ISITA2018	208-212
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.23919/ISITA.2018.8664316	有
オープンアクセス	国際共著
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	－

1．著者名	4．巻
Naganuma Ken, Yoshino Masayuki, Sato Hisayoshi, Yamada Nishio, Suzuki Takayuki, Kunihiro Noboru	-
2．論文標題	5．発行年
Decentralized Netting Protocol over Consortium Blockchain	2018年
3．雑誌名	6．最初と最後の頁
Proc. of ISITA2018	174- 177
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.23919/ISITA.2018.8664259	有
オープンアクセス	国際共著
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	－

1．著者名	4．巻
Onozawa Sota, Kunihiro Noboru, Yoshino Masayuki, Naganuma Ken	LNCS11049
2．論文標題	5．発行年
Inference Attacks on Encrypted Databases Based on Order Preserving Assignment Problem	2018年
3．雑誌名	6．最初と最後の頁
Proc. of IWSEC2018	35～47
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
https://doi.org/10.1007/978-3-319-97916-8_3	有
オープンアクセス	国際共著
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	－

1．著者名 Peng Liqiang, Lu Yao, Kunihiro Noboru, Zhang Rui, Hu Lei	4．巻 LNCS10946
2．論文標題 A Deterministic Algorithm for Computing Divisors in an Interval	5．発行年 2018年
3．雑誌名 Proc. of ACISP2018	6．最初と最後の頁 3～12
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-93638-3_1	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 Zheng Mengce, Kunihiro Noboru, Hu Honggang	4．巻 LNCS10831
2．論文標題 Cryptanalysis of RSA Variants with Modified Euler Quotient	5．発行年 2018年
3．雑誌名 Proc. of Africacrypt2018	6．最初と最後の頁 266～281
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-89339-6_15	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 Kunihiro Noboru	4．巻 29
2．論文標題 Mathematical Approach for Recovering Secret Key from Its Noisy Version	5．発行年 2017年
3．雑誌名 Mathematical Modelling for Next-Generation Cryptography	6．最初と最後の頁 199～217
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-981-10-5065-7_11	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 Lu Yao, Peng Liqiang and Kunihiro Noboru	4．巻 29
2．論文標題 Recent Progress on Coppersmith’s Lattice-Based Method: A Survey	5．発行年 2017年
3．雑誌名 Mathematical Modelling for Next-Generation Cryptography	6．最初と最後の頁 297～312
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-981-10-5065-7_16	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 Zheng Mengce, Kunihiro Noboru and Hu Honggang	4．巻 10342
2．論文標題 Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference	5．発行年 2017年
3．雑誌名 Proc. of ACISP 2017	6．最初と最後の頁 324～342
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_17	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 Ying Jason H. M. and Kunihiro Noboru	4．巻 10343
2．論文標題 Solving the DLP with Low Hamming Weight Product Exponents and Improved Attacks on the GPS Identification Scheme	5．発行年 2017年
3．雑誌名 Proc. of ACISP 2017	6．最初と最後の頁 460～467
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-59870-3_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 Ying Jason H. M. and Kunihiro Noboru	4．巻 10355
2．論文標題 Bounds in Various Generalized Settings of the Discrete Logarithm Problem	5．発行年 2017年
3．雑誌名 Proc. of ACNS 2017	6．最初と最後の頁 498～517
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-61204-1_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 －

1．著者名 Aono Yoshinori and Nguyen Phong Q.	4．巻 10211
2．論文標題 Random Sampling Revisited: Lattice Enumeration with Discrete Pruning	5．発行年 2017年
3．雑誌名 Proc. of Eurocrypt2017	6．最初と最後の頁 65～102
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-56614-6_3	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 Atsushi Takayasu and Noboru Kunihiro	4．巻 100-A(1)
2．論文標題 General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA	5．発行年 2017年
3．雑誌名 IEICE Transactions	6．最初と最後の頁 50-61
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.50	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 Toru Akishita and Noboru Kunihiro	4．巻 LNCS 9689
2．論文標題 Improved Differential Fault Analysis on Camellia-128	5．発行年 2016年
3．雑誌名 Proc. of COSADE2016	6．最初と最後の頁 130-143
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-43283-0_8	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 Atsushi Takayasu and Noboru Kunihiro	4．巻 LNCS 9723
2．論文標題 Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs	5．発行年 2016年
3．雑誌名 Proc. of ACISP2016	6．最初と最後の頁 243-257
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-40367-0_15	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 Atsushi Takayasu and Noboru Kunihiro	4．巻 LNCS 9866
2．論文標題 Partial Key Exposure Attacks on CRT-RSA: General Improvement for the Exposed Least Significant Bits	5．発行年 2016年
3．雑誌名 Proc. of ISC2016	6．最初と最後の頁 35-47
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-45871-7_3	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 Atsushi Takayasu and Noboru Kunihiro	4．巻 -
2．論文標題 Small Secret Exponent Attacks on RSA with Unbalanced Prime Factors	5．発行年 2016年
3．雑誌名 Proc. of ISITA2016	6．最初と最後の頁 236-240
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 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 Hwei-Ming Ying and Noboru Kunihiro	4．巻 -
2．論文標題 Cold Boot Attack Methods for the Discrete Logarithm Problem	5．発行年 2016年
3．雑誌名 Proc. of CANDAR2016	6．最初と最後の頁 154-160
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDAR.2016.0037	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 Hwei-Ming Ying and Noboru Kunihiro	4．巻 -
2．論文標題 Decryption of Frequent Password Hashes in Rainbow Tables	5．発行年 2016年
3．雑誌名 Proc. of CANDAR2016	6．最初と最後の頁 655 - 661
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDAR.2016.0117	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 Atsushi Takayasu and Noboru Kunihiro	4．巻 LNCS10159
2．論文標題 A Tool Kit for Partial Key Exposure Attacks on RSA	5．発行年 2017年
3．雑誌名 Proc. of CT-RSA2017	6．最初と最後の頁 58-73
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_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 Noboru Kunihiro and Yuki Takahashi	4．巻 LNCS10159
2．論文標題 Improved Key Recovery Algorithms from Noisy RSA Secret Keys with Analog Noise	5．発行年 2017年
3．雑誌名 Pro. of CT-RSA2017	6．最初と最後の頁 328-343
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_19	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39件（うち招待講演　3件／うち国際学会　5件）

1．発表者名 Ryo Kurama and Noboru Kunihiro
2．発表標題 New Quantum Algorithms for Modular Inverse and Its Application on the Elliptic Curve Discrete Logarithm Problem
3．学会等名 AQIS2019 (Poster Presentation) (国際学会)
4．発表年 2019年

1．発表者名 Noboru Kunihiro
2．発表標題 Quantum Factoring Algorithm: Resource Estimation and Survey of Experiments
3．学会等名 MOQC2019（招待講演）（国際学会）
4．発表年 2019年

1．発表者名 大西健斗，梨本翔永，鈴木大輔，國廣昇
2．発表標題 Arduino Uno上に実装されたEd25519に対するマルチショット単純電力解析攻撃
3．学会等名 SCIS2020
4．発表年 2020年

１．発表者名
大西健斗，國廣 昇

２．発表標題
Sliding Window法の誤りつき演算情報を用いたCRT-RSA秘密鍵復元手法

３．学会等名
CSS2019

４．発表年
2019年

１．発表者名
Hyungrok Jo, Noboru Kunihiro, Yoshinori Yamasaki

２．発表標題
Cayley hash function-map based on LPS-type Ramanujan graphs

３．学会等名
CSS2019

４．発表年
2019年

１．発表者名
鞍馬遼，國廣昇

２．発表標題
剰余逆元計算の新しい量子アルゴリズムと楕円曲線離散対数問題への応用

３．学会等名
ISEC研究会2019年7月

４．発表年
2019年

１．発表者名
大西健斗，國廣昇

２．発表標題
Attacking Noisy Secret CRT-RSA Exponents in Binary Method (from ICISC 2018)

３．学会等名
ISEC研究会2019年5月

４．発表年
2019年

１．発表者名
カク海萍，國廣昇

２．発表標題
複数人鍵共有プロトコルSIBDの実装

３．学会等名
情報処理学会全国大会

４．発表年
2020年

１．発表者名
大西健斗，田中智樹，宇野隼平，山本直樹，國廣昇

２．発表標題
効率的な量子剰余加算回路の提案とその実装

３．学会等名
第41回量子情報技術研究会（QIT41）

４．発表年
2019年

１．発表者名
伊豆哲也，清水俊也，篠原直行，盛合 志帆，國廣 昇

２．発表標題
アニーリング計算による素因数分解について（その２）

３．学会等名
SCIS2020

４．発表年
2020年

１．発表者名
大西健斗，黄暁萱，國廣昇

２．発表標題
Sliding Window法の演算情報に基づくビット復元率の厳密な解析

３．学会等名
SCIS2019

４．発表年
2019年

１．発表者名
黄暁萱，大西健斗，國廣昇

２．発表標題
Sliding Window法からの漏洩情報を用いた秘密鍵復元アルゴリズムの改良

３．学会等名
SCIS2019

４．発表年
2019年

１．発表者名
鈴木海地，高安敦，國廣昇

２．発表標題
大きい復号鍵をもつRSA暗号に対する部分鍵導出攻撃の改良

３．学会等名
SCIS2019

４．発表年
2019年

１．発表者名
清水俊也，伊豆哲也，篠原直行，盛合志帆，國廣昇

２．発表標題
アニーリング計算による素因数分解について

３．学会等名
SCIS2019

４．発表年
2019年

１．発表者名
江利口礼央，國廣昇

２．発表標題
乗算可能な線形秘密分散法の整数計画法による構成

３．学会等名
SCIS2019

４．発表年
2019年

１．発表者名
伊藤宗一郎，勝又秀一，國廣昇

２．発表標題
準同型署名の弱安全性から強安全性への効率的な変換

３．学会等名
SCIS2019

４．発表年
2019年

１．発表者名
黄 暁萱，大西 健斗，國廣 昇

２．発表標題
Sliding window法からの漏洩情報を用いた秘密鍵復元攻撃の改良

３．学会等名
CSS2018

４．発表年
2018年

１．発表者名
大西健斗，國廣昇

２．発表標題
数論変換におけるサイドチャネル情報を用いたRing-LWE暗号方式の秘密鍵復元攻撃

３．学会等名
ISEC研究会2019年3月

４．発表年
2019年

１．発表者名
鈴木海地，高安 敦，國廣 昇

２．発表標題
RSA暗号の部分鍵導出攻撃の拡張

３．学会等名
ISEC研究会2018年7月

４．発表年
2018年

１．発表者名
安井 捷，國廣 昇

２．発表標題
安全性を高めた共通鍵暗号の量子アルゴリズムに対する詳細な安全性評価

３．学会等名
ISEC研究会2018年7月

４．発表年
2018年

１．発表者名
江利口礼央，國廣昇，岩本 貢

２．発表標題
いくつかの理想的な秘密分散法を用いた最適な複数割り当て法

３．学会等名
SITA2018

４．発表年
2018年

１．発表者名
國廣昇

２．発表標題
Shorのアルゴリズムに基づく素因数分解実験の調査

３．学会等名
QIT39

４．発表年
2018年

１．発表者名
Noboru Kunihiro

２．発表標題
Recovering RSA Secret Keys from Noisy Keys

３．学会等名
WICS（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
大西健斗，國廣昇

２．発表標題
Sliding Window法の誤りつき演算情報を用いたCRT-RSA秘密鍵復元アルゴリズム

３．学会等名
SCIS2018

４．発表年
2018年

１．発表者名
伊豆 哲也，國廣 昇

２．発表標題
素因数分解の現状

３．学会等名
SCIS2018

４．発表年
2018年

１．発表者名
小野澤 綜大，高安敦，國廣昇

２．発表標題
Edwards型楕円曲線におけるHidden Number Problem

３．学会等名
SCIS2018

４．発表年
2018年

１．発表者名
大西健斗，國廣昇

２．発表標題
2^m-ary法に基づく誤りつき演算情報を用いたCRT-RSA秘密鍵復元アルゴリズム

３．学会等名
ISEC研究会7月

４．発表年
2017年

１．発表者名
小野澤綜大，高安 敦，國廣 昇

２．発表標題
楕円曲線ディフィー・ヘルマン鍵共有に対する格子簡約攻撃

３．学会等名
ISEC研究会11月

４．発表年
2017年

１．発表者名
小野澤 綜大，高安 敦，國廣 昇

２．発表標題
楕円曲線Hidden Number Problem のEdwards 曲線への拡張

３．学会等名
応用数理学会第14回研究部会連合発表会

４．発表年
2018年

１．発表者名
Kento Oonishi and Noboru Kunihiro

２．発表標題
Recovering CRT-RSA Secret Keys from Noisy Secret Exponents

３．学会等名
IWSEC2017（国際学会）

４．発表年
2017年

１．発表者名
Noboru Kunihiro

２．発表標題
Recovering RSA Secret Keys from Noisy Keys

３．学会等名
UTokyo - IIT Madras Workshop on Theoretical Computer Science（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
高安敦，國廣昇

２．発表標題
ブロック簡約格子に対する最短ベクトル探索の最悪時計算量評価

３．学会等名
電子情報通信学会情報セキュリティ研究会

４．発表年
2016年

１．発表者名
古川悟，高安敦，國廣昇

２．発表標題
通常同種写像を用いたDH鍵共有の安全性解析

３．学会等名
電子情報通信学会情報セキュリティ研究会

４．発表年
2017年

１．発表者名
高安敦，國廣昇

２．発表標題
Slide簡約基底に対する最短ベクトル探索の最悪時計算量評価

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2017年

１．発表者名
Jason Ying. Noboru Kunihiro

２．発表標題
On the Computational Complexity of the DLP with Low Hamming Weight Product Exponents

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2017年

１．発表者名
Mengce Zheng, Noboru Kunihiro, Honggang Hu

２．発表標題
Improved Factoring Attacks on Multi-Prime RSA with Small Prime Difference

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2017年

１．発表者名
古川悟，國廣昇，高島克幸

２．発表標題
超特異楕円曲線の同種写像を用いた擬似ランダム関数の構成

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2017年

１．発表者名
大西健斗，國廣昇

２．発表標題
サイドチャネル攻撃によるCRT-RSA秘密鍵の復元

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2017年

１．発表者名
國廣昇

２．発表標題
アナログ情報からのRSA鍵復元アルゴリズムの理論解析

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2017年

〔図書〕　計1件

１．著者名 Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, and Dung Hoang Duong	４．発行年 2018年
２．出版社 Springer	５．総ページ数 368
３．書名 Mathematical modelling for next-generation cryptography : Crest Crypto-math Project	

〔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
研究分担者	ＮＧＵＹＥＮ　ＰＨＯＮＧ (NGUYEN PHONG) (80771419)	東京大学・大学院情報理工学系研究科・客員教授 (12601)	