様式Ｃ－１９

# 科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　25　年　6　月　6　日現在

機関番号：12601
研究種目：若手研究（B）
研究期間：2010　～　2012
課題番号：22700006
研究課題名（和文）　公開鍵暗号に対する安全性評価理論の確立

研究課題名（英文）　Research on Security Analysis of Public Key Cryptosystems

研究代表者
國廣　昇　（KUNIHIRO NOBORU）
東京大学・大学院新領域創成科学研究科・准教授
研究者番号：60345436

研究成果の概要（和文）：
本研究課題の目的は，公開鍵暗号に対する安全性評価理論の確立である．主に，格子理論を駆使した安全性評価を行った．その結果，RSA 暗号やナップザック暗号などの公開鍵暗号の安全性に付随した様々な問題に対して，より正確な求解の条件を求めることに成功し，その結果，暗号自身の安全性評価をより正確に与えることに成功した.この成果により,安全かつ適切に,暗号技術を用いることが可能である.

研究成果の概要（英文）：
Our research goal is to establish theories on security analysis of public key cryptosystems. We employ the lattice theory for its analysis. We succeeded in obtaining more accurate conditions for solving some problems related to public key cryptosystems such as RSA scheme and knapsack scheme. Then, we succeeded in providing more accurate security analysis for such schemes. These results enable us to use cryptographic technologies more securely and adequately.

交付決定額

（金額単位：円）

| | 直接経費 | 間接経費 | 合　計 |
|---|---|---|---|
| 2010 年度 | 1,200,000 | 360,000 | 1,560,000 |
| 2011 年度 | 900,000 | 270,000 | 1,170,000 |
| 2012 年度 | 1,000,000 | 300,000 | 1,300,000 |
| 年度 | | | |
| 年度 | | | |
| 総　計 | 3,100,000 | 930,000 | 4,030,000 |

研究分野：暗号理論
科研費の分科・細目：情報学・情報学基礎
キーワード：公開鍵暗号，安全性評価，格子理論

## １．研究開始当初の背景

(1) 研究の社会的背景

暗号技術は，すでに電子商取引などで幅広く使われている．安全に取引を行う上で，使用する暗号の安全性が保証されている必要がある．そのため，新しい暗号方式を作る以上に，現在，広く使われている暗号方式の安全性を評価することが重要である．例えば，安全であると評価され，広く使われてしまった方式が，実はある種の実現可能な攻撃に脆弱であることがわかってしまうような事態は避けなくてはならない．その評価をする際，場当たり的な評価ではなく，数学などの理論

に基づき，体系的に安全性の評価がされなくてはならない．しかし，暗号の安全性評価は一般的に複雑で面倒な作業であり，間違いが混入されやすい．また，ad hoc な研究が多く，職人芸な側面が強い．本研究課題では，職人芸からの脱却をはかるため，暗号の安全性評価に関する一般理論の構築を目指すことを目標とする．その際，攻撃評価手法自身の能力が非力であれば，それは実際の評価の局面ではあまり役にたたない．汎用的ではあるが，実用に耐えうる攻撃手法の提案が目標である．

(2) 研究の学術的背景

暗号の安全性を評価する際に用いる道具としては，ありとあらゆる数学を用いることが可能であるが，整数論を高度に用いた攻撃だけでなく，直接的に関係がないと思われていた「格子理論」に基づく攻撃手法が，近年，注目を浴びている．しかしながら，格子理論の暗号への応用に関しては，歴史は浅く，未だ，その理論整備は不十分である．本研究課題では，主に，格子理論に基づく暗号の安全性評価理論の確立を学術的な目標とする．暗号の安全性を解析する上で，完全に暗号が解読されてしまうという，いわゆる全面解読だけでなく，何らかの要因により部分情報が漏れてしまった上での安全性解析も重要となる．処理時間やメモリサイズの制限などにより，方式を少し変更して仕様を策定してしまうことが現実にはよくおこる．暗号方式自身は何ら欠陥がなかったとしても，これまでにも，「不適切な仕様」や「仕様通りではない実装」により，部分情報が漏れてしまい，その情報をもとに解読を行う攻撃法が提案されている．そのため，様々な状況を考えた上で解析を行う必要がある．

２．研究の目的

暗号を安心して使うためには，暗号の安全性を正確に評価することが，きわめて重要である．暗号が安全であることを示す一つの方法は，想定しうる強力な攻撃に対して，破られないことを示すことである．そのため，攻撃手法の研究がきわめて重要となる．これまでに，多くの攻撃手法が考案されているが，その中でも，格子理論は，安全性の評価を行う強力な数学的な理論として，近年，注目を浴びている．格子理論自身の研究に関しては，その歴史は古く 19 世紀から始まっているが，暗号の安全性解析の道具として使われ始めたのはごく最近であり，理論整備はまだ進んでいない．この分野のこれまでの主な研究は，
Type1: 強力であるが，特定の暗号方式に特化しており，汎用性のない攻撃(代表例：Boneh-Durfee, Durfee-Nguyen, Itoh らの結果など)
Type2: 汎用的であるが，暗号解読の場面では非力な攻撃（代表例：Jochemz-May の結果）
のいずれかに大別される．すなわち，汎用的であり，なおかつ，強力な攻撃はこれまでに提案されておらず，個別の暗号の安全性を評価するためには，問題に応じた煩雑な議論をそのつど行う必要がある．

この問題点を解決して，汎用的であり強力な攻撃手法を提案するのが本研究の主たる目的である．

３．研究の方法

(1) 研究計画のポイント

一般に，格子理論による暗号の安全性解析は，次の手順により行われる．① 暗号の解読問題を，ある種の代数方程式の求解問題に変換する．② この代数方程式を基に，ベクトルの集合を構成する．③ このベクトルの線形和の長さが最小（もしくはかなり短いベクトル）となるものを見つける．④ 得られたベクトルをもとの暗号の解読問題の解へ変換することにより，秘密情報を求める．最短ベクトル探索問題は，NP 困難な問題であり，問題のサイズが十分大きい場合には，効率的に解くことが困難であるが，LLL アルゴリズムや BKZ アルゴリズムなどの基底簡約アルゴリズムにより，比較的高次元であっても，有効であることが各種の実験により確認されている．

① に関しては，秘密情報の漏れ方に基づいて，代数方程式の導出のさいに，工夫が必要であり，適切な変換を導出する必要がある．② に関しては，従来の研究では，ad hoc な構成しかなされて来なかったが，本研究課題では，組織的な構成を目指す．

(2) 具体的な研究手順

① 既存の研究を包含する一般理論の構築
多くの格子理論に基づく安全性解析が提案されているが，以下の二つに大別される．
Type1: 強力であるが，汎用性のない攻撃
Type2: 汎用的であるが，非力な攻撃
まずは，これら一連の研究の網羅的な調査を行う．

ついで，一般理論の構築を行う．具体的な研究は以下の二つの方向より行う．(1) いくつかの単発的に行われている強力な攻撃の本質を抽出する．(2) 逆に，汎用的ではあるが，実際の場面では非力である方式のチューニングも行う．すなわち，実際の暗号解読での状況を考慮して，詳細な条件付け，もしくは制限付けを行う．これにより，これまでの攻撃を全て特殊ケースとして含むような一般理論を構築する．すなわち，これまでの攻

撃が，適切にパラメタ設定をすることにより含まれるような理論体系の構築を行う．この二つのアプローチにより，実際の暗号解読に適した方法を提案する．

② 構築した一般理論の理論的な性能評価
一般理論の構築後は，性能の理論的評価を行う．既存の研究では，この種の理論的な評価は個別の暗号解読に対してのみ有効であり，一般論としての理論評価は行われていない．そのため，どの手法にも適用しうる理論評価をまず行う必要がある．ついで，個別の問題に適用した時の評価も行い，既存研究との差異を考察する．この差異が小さいことが期待されるが，差異が無視できないくらい大きい場合には，その原因の調査を行い，その結果を① の一般理論の構築にフィードバックし，より洗練された理論の構築を目指す．

４．研究成果

(1) 平成 22 年度の成果
① ナップザック暗号に対する安全性評価を行った．具体的には，新たな密度の定義 $d=n\mathrm{H}(p)/\log A$ を導入し，ナップザックの密度があるしきい値以下であれば，一回の SVP オラクルの呼び出しで，解読できることを証明した．既存の攻撃では，平文がランダムな場合か，低重みの時にのみ有効であったが，提案した攻撃法では，平文がどのような重みであっても有効である．また，重みが小さい安全なナップザック暗号を構成することは，極めて困難であることを明らかにした．（文献⑪）

② Small Inverse Problem を拡張した Generalized Small Inverse Problem を導入し，この問題に対する効率的なアルゴリズムを示した．さらに，この問題が多項式時間で解けるための条件を具体的に導出した．具体的には，基となる部分問題の格子を利用することにより，より難しい問題に対する格子を構成している．この問題は，RSA 暗号に関連した多くの問題から帰着されるため，RSA 暗号の安全性評価に対して有効である．（文献⑩）

③ 具体的な RSA 暗号の変種に関する安全性評価を行った．具体的には，Takagi による変種に対して，秘密鍵が小さい時の解読を示した．具体的には，秘密鍵がある値以下であるときには，この方式は多項式時間で破られることを証明した．得られた結果を合成数が２つのときに，適用すると，既存の結果が得られるため，我々の結果は自然な形で既存の結果を含んでいる．ついで，数値実験により，提案アルゴリズムの有効性を示した．（文献⑨）

(2) 平成 23 年度の成果
① RSA 暗号において，秘密鍵 $d$ が小さく設定されている時には，効率的に攻撃が行われることが知られている．いくつかの攻撃がこれまでに単発的に行われているが，本研究では，これらの攻撃を部分クラスとして含むフレームワークの導入を行った．ついで，このフレームワークにおいて，最適なパラメタの設定を解析的に求めることに成功した．この算出において，2 変数の高次方程式を解く必要があるが，この求解は一般に困難である．解の導出時において，グレブナ基底を道具として用いている．最適なパラメタを導出した結果，既存の結果：Boneh と Durfee による限界 $d<N^{0.292}$ が，このフレームワークにおいても，やはり，最適であることの厳密な証明に成功した．このフレームワークは，極めて広いクラスであると考えられるため，Boneh-Durfee の限界をこれ以上，拡張できないのではないかという予想を強くサポートする結果となっている．（文献⑦）

② ナップザック暗号においても，格子理論を用いた安全性評価手法の改良を行った．この改良は，ナップザックの重さが一様分布に従っていない場合でも適用できるという従来の研究にはない特徴がある．この改良の結果，密度の評価において，重要なのは，重さの調和平均であることが明らかになった．この結果は，一様分布である場合を純粋に含んだ結果となっている．（文献⑥）

(3) 平成 24 年度の成果
① RSA 原理に基づく暗号である複数素数 RSA-OAEP に関する評価を行い，安全性が担保される範囲を詳細に評価した．その結果，従来の研究では，安全とされていたパラメタ設定は，不適当であることを示し，より適切な限界を提示した．具体的に，安全性を保証するためには，より小さい $e$ を選択する必要があることを明らかにした．さらに，用いる素数の数が増えた時の漸近的な評価も行い，従来のアルゴリズムよりも，速い速度で限界に到達していることを示した．（文献①④）

② RSA 暗号に対する攻撃の一つ，「小さい秘密鍵に対する攻撃」に関する評価を行った．従来の問題を含む，より広いクラスの問題を定義し，その問題を多項式時間で解くアルゴリズムを提案した．さらに，適切な仮定の下での，提案アルゴリズムの最適性を示した．この仮定は，近似 GCD 問題が解ける範囲の限界に関するものである．この２つの限界に関しては，これまでは独立のものであると考えられてきたが，この成果により，密接に関連

があり，どちらかが改良されれば，自動的に，もう片方の限界も改良されることを明らかになった．（文献③）

③ RSA 暗号の秘密鍵が，消失および誤りが乗った状態で得られた時に，元の秘密鍵を完全に復元するアルゴリズムの提案を行った．さらに，提案アルゴリズムにより，鍵の復元が可能となる範囲の詳細な評価を行った．具体的な範囲は，消失の確率をδ，誤りの確率がεであるとすると，$\varepsilon + \delta/2 < 1/2 - \sqrt{(1-\delta)\ln 2/(2m)}$ で与えられる．ついで，原理的に，解を復元できるための理論限界を示し，提案アルゴリズムは，2 次の近似項まで，理論限界を達成していることを明らかにした．（文献②）

以上の成果の一部を，解説論文という形でまとめ，電子情報通信学会 Fundamentals Review 誌で出版をしている．

以上の成果は，RSA 暗号やナップザック暗号などの公開鍵暗号の安全性に付随した様々な問題に対して，より正確な暗号の安全性評価を与えており，より安全に，適切に，暗号技術を用いることが可能となった．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 27 件）


① A. Takayasu and N. Kunihiro, “Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors,” in Proc. of ACISP2013, 掲載決定，査読有り，2013.

② N. Kunihiro, N. Shinohara and T. Izu, “Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors,” in Proc. of PKC2013, LNCS 7778, pp. 180-197, 2013. 査読有り．

③ N. Kunihiro, “On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree,” in Proc. of ISC2012, LNCS 7483, pp. 55-69, 2012, 査読有り．

④ K. Tosu and N. Kunihiro, “Optimal Bounds for Multi-Prime Phi-Hiding Assumption,” in Proc. of ACISP2012, LNCS7372, pp. 1-14, 2012, 査読有り．

⑤ Y. Nagashima and N. Kunihiro, “Faster Algorithm for Solving Hard knapsacks for Moderate Message Length,” in Proc. of ACISP2012, LNCS7372, pp. 43-56, 2012, 査読有り．

⑥ J. Kogure, N. Kunihiro and H. YAMAMOTO, “On the Hardness of Subset Sum Problem from Different Intervals,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E95-A, No.5, pp. 903-908, 2012, 査読有り．

⑦ N. Kunihiro, N. Shinohara and T. Izu, “A Unified Framework for Small Secret Exponent Attack on RSA,” in Proc. of SAC2011, LNCS7118, pp. 260-277, 2011, 査読有り．

⑧ 國廣昇, “格子理論を用いた暗号解読の最近の研究動向，”電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol. 5, No. 1, pp. 42-55, 2011.（査読なし，解説論文）

⑨ N. Kunihiro, “Solving Generalized Small Inverse Problems,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E94-A, No.6, pp. 1274-1284, 2011, 査読有り．

⑩ N. Shinohara, T. Izu and N. Kunihiro, “Small Secret CRT-Exponent Attacks on Takagi’s RSA,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E94-A, No.1, pp. 19-27, 2011, 査読有り．

⑪ N. Kunihiro, “New Conditions for Secure Knapsack Schemes against Lattice Attack,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E93-A, No.6, pp. 1058-1065, 2010, 査読有り．


〔学会発表〕（計 30 件）


(1) 國廣昇, “チュートリアル：格子簡約を用いた RSA 暗号への攻撃，” Lattice Crypto Day 2012 Japan (LCD2012J) , IIJ, 2012 年 3 月 15 日（査読なし，依頼講演）.

(2) 國廣昇, “格子簡約アルゴリズムを用いた暗号の安全性解析，” 第３回暗号及び情報セキュリティと数学の相関ワークショップ，中央大学，2011 年 12 月 21 日，（査読なし，依頼講演）.

６．研究組織

(1)研究代表者

國廣　昇　（KUNIHIRO NOBORU）
東京大学・大学院新領域創成科学研究科・
准教授
研究者番号：60345436