格子と暗号に関する研究動向について
-暗号攻撃、格子暗号、完全準同型暗号-

Research Trend in Lattice and Cryptography
-Cryptanalysis, Lattice-Based Cryptography, Fully Homomorphic Encryption-

深瀬道晴[*]
Masaharu Fukase

Email: fukase@dokkyo.ac.jp

格子を用いる暗号は、整数論を用いる暗号に対して、いくつかの利点を有しているが、実際に実用されているのは後者である。しかし、最近、格子を用いる暗号が、今日、及び、次世代のネットワーク社会に資する潜在性を持つことが再認識されてきている。本稿では、格子と暗号に関する最近の研究動向を要約する。本稿で取り上げる事項は、(1)格子を用いる暗号攻撃、(2)格子暗号、(3)完全準同型暗号の 3 つである。(1)については、暗号攻撃に用いられることの多い LLL アルゴリズムと BKZ アルゴリズムについて、また、RSA 暗号攻撃の概要について述べる。(2)については、1990 年代後半に提案された代表的な格子暗号について述べる。(3)については、主に、格子を用いる Gentry の完全準同型暗号について述べる。

Although lattice-based cryptography has several advantages over number-theory-based cryptography, the latter has most usage. However, many researchers have gotten new understandings of the potential of lattice-based cryptography, which is supposed to contribute to the present and future networked society. In this paper, we summarize research trend in lattice and cryptograhy. We concentrate on 1.lattice-based cryptanalysis, 2.lattice-based cryptography, and 3.fully homomorphic encryption. First, we discuss LLL algorithm and BKZ algorithm, which have wide usage as tools of cryptanalysis, and lattice-based attacks on RSA(1). Second, we discuss some representative lattice-based cryptosystems, which were proposed in the late 1990s(2). Third, we mainly discuss Gentry's fully homomorphic encryption, which is based on lattices(3).

*: 獨協大学経済学部

1. はじめに

格子は、線形独立なベクトルの集合によって定義される加群である。格子は、暗号攻撃と暗号構成の双方に用いられてきた。

格子を暗号攻撃の手段として用いる場合、1982年に提案されたLLLアルゴリズム[14]が良く用いられる。LLLアルゴリズムは、ナップザック暗号や特殊なパラメータを用いる場合のRSA暗号に適用されてきた。特に、ナップザック暗号はLLLアルゴリズムに対して耐性が非常に低いことが示された。

一方、格子は、1996年にAjtaiによって初めて暗号構成に用いられた[1]。また、その後、格子を用いる暗号がいくつも構成された。これは、格子の暗号攻撃への応用と逆の方向性を持つ応用といえる。ここで、暗号攻撃自体は、暗号研究において必須のテーマである。なぜなら、現代暗号はそれ以前の暗号と異なり、暗号アルゴリズムが公開されており、暗号の安全性に重大な欠陥が存在しないことを絶え間なく検証しなければならないからである。しかし、暗号攻撃の研究が、暗号構成の研究と同程度には必ずしも肯定的な印象を与えない場合がある。このため、Ajitai以降いくつも格子を応用する暗号システムが構築されたことは、格子の研究においてより肯定的な結果といえる。

格子暗号は、Kuo等に指摘されているように、素因数分解問題や離散対数問題等の整数論を応用する暗号方式に対して以下の利点を持っている[13]。

1. 量子アルゴリズム攻撃への耐性を有する(post-quantum)
2. 一部の暗号の安全性が最悪計算量に基づいて証明されている(worst case hardness assumption)
3. 完全準同型暗号の構成に応用された(construction of fully homomorphic encryption)

特に、完全準同型暗号が格子を用いて構成された結果は、格子の分野だけでなく暗号研究にとって極めて重要な結果と見なされている。完全準同型暗号の構成という問題は、RSAが発表された直後に遡り、多くの応用可能性が指摘されてきた。特に、完全準同型暗号は、来るクラウド環境において機密データの安全な処理を可能にすると考えられている。そのため、上記3つの利点のうち、3は今日のネットワーク社会において特に重要である。また、次世代コンピューターとされている量子コンピューターの実用レベルでの開発を想定する場合、2は重要である。なぜなら、そのとき、RSA等の整数論を応用する暗号は安全ではないからである。

以上において、格子と暗号の関わりを概観した。本稿では、次のように格子と暗号に関する最近の研究動向を要約する。第2章において、格子に関する諸概念を述べる。第3章において、格子を応用する暗号攻撃について述べる。第4章において、1990年代から2000年代初頭において提案された格子暗号方式のいくつかのこれまでの経緯と最近の動向について述べる。第5章において、完全準同型暗号についての動向を述べる。そして、第6章において、本稿を要約する。

2. 格子に関する諸概念

この章では、格子に関する諸概念を述べる。

2.1 格子と基底

格子は、Z^mにおける線形独立なベクトルの組$b_1, \dots, b_n$についての整数係数による全ての線形結合の集合である。このように、線形結合の際に整数係数に限ることで、格子は離散構造となる。そして、ベクトルの組$b_1, \dots, b_n$を格子の基底という。格子の基底は、1つに限られない。また、nを格子の次元という。

2.2 基底簡約

現基底簡約の本質は、基底を構成するベクトルを相互に直行に近づけることである。基底を構成するベクトルを相互に直行に近づける目的は、様々な問題に対する解を導きやすくすることである。一般に、基底を完全に直行化することはできないが、これは格子が離散構造であることに起因する。

2.3 SVP(the shortest vector problem)

SVP(the shortest vector problem＝最短ベクトル問題、または、最小ベクトル問題)は、格子における零でない最も短いベクトルを求める問題である。SVPは、計算困難な問題として知られており、効率的な解法は見つかっていない。しかし、格子の次元が十分に低いとき、基底簡約によってSVPの厳密解が求まる場合が多い。

3. 暗号攻撃

この章では、格子を用いる暗号攻撃に際してのツールや計算資源等について述べた後、RSA暗号攻撃について概要を述べる。また、量子コンピューターモデルにおけるアルゴリズムの可能性について述べる。

3.1 暗号攻撃に用いるツール等

(1) LLLアルゴリズム

LLLアルゴリズムは、基底簡約アルゴリズムである。LLLアルゴリズムは格子を用いた暗号攻撃という観点において、非常に重要な結果である。また、暗号攻撃だけでなく、LLLアルゴリズムは、多項式素因数分解、整数計画法、信号処理など、

幅広く応用されている。LLL アルゴリズムの本質的なアイディアは、Gram-Schmidt 直行化の演算を整数演算で近似することである。LLL アルゴリズムは後述の NTL(Number Theory Library)[24]に実装されており、NTL における LLL の実装が事実上の標準である。

(2) BKZ アルゴリズム[23]

第 4 章で述べる格子暗号の安全性評価は、LLL アルゴリズムの拡張型である BKZ アルゴリズムを用いて行われてきた。BKZ アルゴリズムは、メインルーチンとしての LLL アルゴリズムに ENUM という探索のサブルーチンを加えたものである。BKZ アルゴリズムは後述の NTL に実装されており、NTL における BKZ の実装が事実上の標準であった。

しかし、最近、Chen 等は NTL における BKZ の実装は最適でないこと、及び、NTL の BKZ を用いて評価された格子暗号の安全性は正確でないことを指摘した[5]。Chen 等は、BKZ のサブルーチンである探索において新しい枝狩り法を採用した。その結果、例えば後述の NTRU 暗号は従来主張されていたよりも低い安全性しか持たないことが示された。

(3) NTL(Number Theory Library)

NTL において実装されている BKZ アルゴリズムは広く用いられてきて、前述のように事実上の標準であったが、Chen 等によって必ずしも最適でないことが指摘された。NTL はこれまでに何度も変更が加えられてきたが、最後に変更が加えられたのは 2009 年 8 月である(2012 年 8 月現在)。今後、NTL に Chen 等の方法が実装されるかは不明である。

3.2 マルチ CPU、GPU、クラウド等の計算資源

今日、マルチ CPU、GPU などの大きな計算資源が入手可能である。また、来るクラウド社会においてはさらに大きな計算資源が利用できるようになる。暗号の安全性評価においては、利用可能な計算資源を考慮に入れなければならない。例えば、クラウド社会においては、敵がクラウドの莫大な計算資源を用いることを想定しなければならない。

Kuo 等は、GPU、及び、クラウドサービスを格子暗号の基礎となる SVP 求解に利用した[13]。そして、SVP 求解に要する労力を、アメリカ合衆国ドルに換算して提示した。これらの試みは、2 つの観点において新しい試みである。まず、急速に需要が高まりつつあるクラウドサービスを暗号攻撃実験に用いたこと、次に、暗号攻撃に要する労力を従来よりも実用的な指標によって提示したことである。Kuo 等の新しい指標による提示の試みは、ほぼ同時期に発表された Kleinjung 等の指標に非常に近いものである[12]。

従来は、暗号攻撃実験は研究者がそれぞれ個別のハードウェアを用いて行い、低いセキュリティパラメーターにおける計算時間から外挿法により高いセキュリティパラメーターにおいて要する計算時間が見積もられる場合が多かった。このような方法においては、提示される安全性評価について、追試をすることが一般的に困難である。Kuo 等や Kleinjung 等の試みは、この観点からもより正確な安全性評価を可能にするものと思われる。

3.3 RSA 暗号攻撃について

格子を用いる暗号攻撃として、RSA に対する暗号攻撃が知られている。ここでは、國廣[25]の解説論文に従って、その概要を説明する。

RSA 暗号の暗号化と復号は、次のようになる：異なる素数p, qに対して、$N = pq$とする。自然数eを選び、$ed \equiv 1 \bmod (p-1)(q-1)$となる自然数$d$を計算する。ここで、公開鍵は$(e, N)$、秘密鍵は$d$である。平文$m$に対する暗号文$c$は、$c = m^e \bmod N$である。復号は、$m = c^d \bmod N$で行う。尚、RSA 暗号はこの暗号化の仕方から、5 章で述べるように、準同型性を有する。

上記から、ある自然数kに対して、$ed = 1 + k(p-1)(q-1)$となる。$s = p + q$，$A = N + 1$とおき、整理すると、$ed - 1 - k(A - s) = 0$となる。今、e、Aが既知の値であり、d, k, sが未知の値である。pqの値は既に分かっているので、$s = p + q$の値がさらに分かれば、p, qの値を知ることができる。このとき、$ed \equiv 1 \bmod (p-1)(q-1)$から、$d$を計算することができる、すなわち秘密鍵を計算することができる。

$ed - 1 - k(A - s) = 0$について、$\bmod e$をとると、$k(A - s) + 1 \equiv 0 \bmod e$である。ここで、2 変数法付方程式$x(A + y) + 1 \equiv 0 \bmod e$を考えれば、その解の 1 つは、$(x, y) = (k, -s)$であり、$s$が求まる。

しかし、上記の 2 変数法付方程式のように非線形方程式は、取り扱いが困難である。そこで、非線形項のxyについて$xy = z$とおき、線形化する方法がある。このように線形化すれば、問題は法付き線形方程式の問題に変換される。

ここで、格子を用いて法付き線形方程式を解く方法が知られている。具体的に、法付き線形方程式の各項の情報に従い、格子の基底を生成し、その格子の最短ベクトルを求める。このとき、(1)SVP オラクルが存在する、(2)格子における最短ベクトルが（符号の違いを除き）ただ一つに限られる、という仮定の下で、最短ベクトルの係数が、法付き線形方程式の解となっている。より詳しい解説については、國廣[25]の解説論文を参照された

い。

上記のような方法が適用できるのは、$d = N^{\delta}$としたとき、δが小さいときである。現在、RSA暗号攻撃において、δを$\delta = 0.292$まで大きくできることが知られている。RSA暗号攻撃の研究において、重要な未解決の問題として、このδをどこまで大きくできるのかという問題がある。δをどこまで大きくできるのか、または、$\delta = 0.292$が限界なのかを示すことは今後の重要な課題である。

3.4 量子アルゴリズムについて

現在までに、格子暗号に対する量子コンピューターモデルにおける効率的なアルゴリズムは発見されていない。RSA等の整数論を用いる暗号については、量子コンピューターモデルにおける効率的なアルゴリズムが発見されているため、格子暗号は”post quantum”の暗号とされている。

格子暗号に対する量子コンピューターを用いる攻撃法の研究について、Ludwig によって基底簡約に量子アルゴリズムである Grover の探索アルゴリズムを適用できることが示された[15]。しかし、Bennett 等は Grover の探索アルゴリズムは指数関数的な効率向上をもたらすものではないことを示している[3]。このため、Ludwig の結果は、格子暗号の量子コンピューター耐性を直ちに弱めるものではない

4. 代表的な格子暗号

この章では、1990 年代後半において提案された代表的な格子暗号の特徴を述べた後、それらに対する暗号攻撃や標準化について述べる。

4.1 暗号化、復号等の特徴

(1) Ajtai-Dwork 暗号[1]

Ajtai 等の公開鍵暗号システム構成の結果は、格子を暗号攻撃だけでなく暗号構成にも用いることができることを示しただけでなく、ある問題の最悪の場合の困難性に基づいて安全性が証明される初めての公開鍵暗号システムを構成したという点においても重要である。Ajtai-Dwork 暗号において、平文はビット毎に暗号化される。秘密鍵は超平面[1]であり、公開鍵は超平面に近いベクトルである。0 は、公開鍵を用いて超平面に近いベクトルに変換される。一方、1 は、任意のベクトルが選ばれる。そして、復号においては、超平面に近いベクトルは 0 に変換され、そうでないベクトルは 1 に変換される。

Ajtai-Dwork 暗号において、任意の暗号文についてそれが 0 の暗号文であるか 1 の暗号文であるかということを効率的に計算できるならば、特殊な格子の SVP の最悪の場合が効率的に解けることが示されている。したがって、特殊な格子の SVP の最悪の場合が計算困難であることを仮定することで、Ajtai-Dwork 暗号の安全性が保証される。このような、安全性証明が行われている暗号として、他に Regev[22] と Peikert[20]の暗号が知られている。

(2) GGH 暗号[10]

格子暗号の特徴の 1 つは、暗号化と復号の仕組みが視覚的に理解できることである。これは、整数論に基づく暗号にはない特徴であり、例えば、Micciancio が述べるように素因数分解の過程を視覚的に理解することは難しい[17]。GGH の暗号化と復号の仕組みは、格子暗号の中でも特に直感的に理解しやすいものである。GGH 暗号において、平文、暗号文はベクトルであり、秘密鍵、公開鍵は格子の基底である。平文は、公開鍵によって、格子上のベクトルではないが格子上のあるベクトルに近いベクトルに変換される。そのベクトルが、暗号文となる。そして、暗号文のベクトルは、秘密鍵によって、暗号文のベクトルに近い格子上のベクトルを求めることによって復号される。

(3) NTRU 暗号[11]

格子暗号において唯一標準化されているのが、NTRU 暗号である。NTRU 暗号の安全性は格子の計算困難な問題に依存しているが、一方で、暗号化関数と復号関数は多項式環[2]における特殊な演算である。そして、Ajtai-Dwork 暗号や GGH 暗号と異なり、NTRU の暗号化と復号の仕組みを視覚的に理解することは困難である。

4.2 これまでの経緯と最近の動向

Ajtai-Dwork 暗号と GGH 暗号は、Nguyen の暗号攻撃によって、実用的なセキュリティレベルで使用するには非常に非効率であることが示された[18][19]。その後、Ajtai-Dwork 暗号は Ajtai 等によって、GGH 暗号は Micciancio によって改良され、効率が向上した[2][16]。NTRU 暗号は、上の 2 つの暗号とは異なり、実用的なセキュリティレベルでの使用を困難にするような暗号攻撃を受けていない。そして、上の 2 つの暗号の改良後のものを含めても、最も効率が良く、実用性を備えている[21]。また、NTRU 暗号は IEEE 標準であり、商業的に用いられている。

また、これらの暗号は、暗号攻撃に用いられる LLL アルゴリズム等の基底簡約アルゴリズムの性能を示す際に、非常に良く用いられてきている。例えば、Chen 等の基底簡約アルゴリズムの最近の結果においても、NTRU 暗号に対する攻撃実験

[1] 超平面とは、平面がn次元空間において一般化された概念である.

[2] 環とは、和と積について閉じている代数構造である.

が行われている[5]。

5. 完全準同型暗号

完全準同型暗号の構成は、RSA が発表された直後に既に重要な未解決問題として提起されていた。RSA 暗号は、偶然にも積演算について準同型性[3]を有していたからである。積演算だけでなく、和演算、そして、任意の演算について準同型性を有している暗号を構成することができた場合、非常に有用な応用可能性が指摘されてきた。そのような暗号は、完全準同型暗号と呼ばれている。しかし、この未解決問題は約 30 年間解決されることはなかったが、2009 年 Gentry によって初めて解決された[9]。

完全準同型暗号は、復号鍵を用いることなく、暗号化データを入力とする任意の関数を計算することを可能にする。すなわち、平文$m_1, \dots, m_t$に対応する暗号文$E(m_1), \dots, E(m_t)$が与えられたとき、復号鍵を用いることなく、$E(f(m_1, \dots, m_t))$を計算することを可能にする。ここで、Eは暗号化関数、fは効率的に計算できる任意の関数である。

このような演算を可能にする完全準同型暗号は、様々な応用をもたらす。例えば、ユーザーが検索エンジンに暗号化されたクエリーを投げ、検索エンジンは暗号化された検索結果を返すという応用である。このとき、検索エンジンはユーザーのクエリーの中身を知る必要がない。

Gentry の完全準同型暗号は、暗号化と復号に格子を利用する。これは、完全準同型暗号において、特に、復号に要する演算の複雑さが低い必要があるためである。格子における演算は、それほど大きくない整数の和や積の演算であるため、整数論を応用する暗号と比較して、演算が複雑ではない（整数論を応用する暗号は、大きな整数の指数演算を要するため、演算がより複雑になる）。そして、Gentry の完全準同型暗号の安全性は、格子における計算困難な問題に依存する。

一方、Dijk 等は格子ではなく、剰余計算のみを用いるより単純な方法で完全準同型暗号を構成した[8]。Dijk 等の目的は、より単純な暗号を構成することであった。Dijk 等の完全準同型暗号の安全性は、Approximate GCD の計算困難性に依存する。ここで、Approximate GCD とは、大きな素数pを、与えられた$x = pq_i + r_i$から求める問題である。ここで、q_iは大きな整数、r_iは小さな整数である。また、これに近い問題に基づく完全準同型暗号が、Coron 等によって構成されている[6]。

現在までに、完全準同型暗号として、Gentry の暗号のように格子に関連するもの、Dijk の暗号のように整数環に関連するものが知られている。Gentry や Dijk 以外にもいくつかの完全準同型暗号が発表されており、例えば、格子に関連する完全準同型暗号として、Brakerski 等の暗号が知られている[4]。

完全準同型暗号の実用までの大きな課題は、その効率である。現時点では、計算時間と鍵サイズの両方において非常に非効率である。効率に関して、最新の研究では、例えば、Coron 等が鍵サイズを小さく抑える手法を発表している[7]。

6. まとめ

本稿では、格子と暗号に関する最近の研究動向を要約した。本稿で取り上げた事項は、(1)格子を用いる暗号攻撃、(2)格子暗号、(3)完全準同型暗号の 3 つである。特に、(3)については、暗号に関する代表的な学会である CRYPTO と EUROCRYPT において、2009 年以降例年完全準同型暗号に関するいくつかの論文が採択されている。完全準同型暗号の構成に用いられるいくつかの問題、暗号の効率や暗号攻撃等のテーマについて、今後も多くの研究成果が発表される見込みである。

本稿において、格子に基づく暗号が、量子コンピューター耐性、安全性証明、完全準同型暗号の構成という観点で、様々な利点を持つことを述べた。しかし、格子に基づく暗号は多くの場合、これらの利点を相殺しかねない効率の悪さを抱えている。このため、今後の格子と暗号に関連する研究において、格子に基づく暗号の効率化は特に重要な課題と考えられる。

謝辞

本研究の一部は、情報学研究所研究助成によるものである。

参考文献

(1) Ajtai, M., Dwork, C.:"A Public-Key Cryptosystem with Worst-case/Average-case Equivalence.", Proceedings of STOC'97, ACM, pp.284-293 (1997)

(2) Ajtai, M., Dwork, C.:"The First and Fourth Public-Key Cryptosystems with Worst-case/Average-case Equivalence.", ECCC, TR07-097 (2007)

(3) Bennett, C., Bernstein, E., Brassard, G., Vazirani.:"Strength and Weaknesses of Quantum Computation.", Special Issue on Quantum Computation of the Siam Journal of Computing, (1997)

(4) Brakerski, Z., Vaikuntanathan, Vinod.:"Efficient fully homomorphic encryption from (standard) LWE.", Ost11, pp.96-106 (2011)

(5) Chen, Y., Nguyen, P.Q.:"BKZ2.0: Better Lattice Security Estimates.", Proceedings of ASIACRYPT'2011, pp.1-20 (2011)

(6) Coron, J.-S., Mandal, A., Naccache, D.,

[3] 複数の対称について、写像で移す前の演算が写像で移した後の演算と対応しているとき、それらは準同型写像を持ち、準同型であるという.

Tibouchi, M.:”Fully Homomorphic Encryption over the integers with shorter public-keys.”, Proceedings of CRYPTO 2011, LNCS, vol.6841, pp.487-504 (2011)
(7) Coron, J.-S., Naccache, D., Tibouchi, M.:”Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers.”, Proceedings of EUROCRYPT 2012, LNCS, vol.7237, pp.446-464 (2012)
(8) Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.:”Fully Homomorphic Encryption over the Integers.”, Proceedings of EUROCRYPT’2010, pp.24-43 (2010)
(9) Gentry, C.:”A Fully Homomorphic Encryption Using Ideal Lattices.”, PhD thesis, Stanford University, http://crypto.stanford.edu/craig/. (accessed 15 December 2012)
(10) Goldreich, O., Goldwasser, S., Halevi, S.:”Public-Key Cryptosystems from Lattice Reduction Problems.”, Advances in Cryptology - CRYPTO'97, vol. 1294 of LNCS, Springer-Verlag, pp. 112-131, (1997).
(11) Hoffstein, J., Pipher, J., Silverman, J.H.:”NTRU: A Ring-Based Public Key Cryptosystem.” Proceedings of ANTS III, vol. 1423 of LNCS, Springer-Verlag, pp. 267-288(1998)
(12) Kleinjung, T., Lenstra, A.K., Page, D., Smart, N.P.:”Using the Cloud to Determine Key Strength.”, Cryptology ePrint Archive, Report 2011/254 (2011)
(13) Kuo, P., Schneider, M., Dagdelen, O, Buchmann, J., Cheng, C., Yang, B.:”Extreme Enumeration on GPU and in Clouds - How Many Dollars You Need to Break SVP Challenges –.” CHES 2011, vol 6917 of LNCS, pp. 160-175, (2011)
(14) Lenstra, A.K., Lenstra, H.W., Lovasz, L.:”Factoring Polynomials with Rational Coefficients.”, Mathematische Ann., Vol. 261, pp.513-534 (1982)
(15) Ludwig, C.:“Practical Lattice Basis Sampling Reduction.”, PhD thesis, TU Darmstadt, http://elib.tu-darmstadt.de/diss/000640/ (accessed 15 December 2012)
(16) Micciancio, D.:”Improving Lattice Based Cryptosystems Using the Hermite Normal Form.”, Silverman, pp.126-145 (2001)
(17) Micciancio, D.:”The Geometry of Lattice Cryptography.”, FOSAD’2011, pp.185-210 (2011)
(18) Nguyen, P.Q., Stern, J.: “Cryptanalysis of the Ajtai-Dwork Cryptosystem.” Advances in Cryptology - Crypto'98, vol. 1462 of LNCS, Springer-Verlag, pp. 223-242 (1998)
(19) Nguyen, P.Q.: “Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto'97.” Advances in Cryptology - Crypto'99, vol. 1666 of LNCS, Springer-Verlag, pp. 288-304, (1999)
(20) Peikert, C.:”Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem.”, extended abstract, STOC 2009, pp.333-342 (2009)
(21) Perlner, R.A., Cooper, D.A.:”Quantum Resistant Public Key Cryptography: A Survey”, Proceedings of IDtrust 2009, Vol.373, pp.85-93 (2009)
(22) Regev, O.:”New Lattice-Based Cryptographic Constructions.”, J.ACM, 51(6), pp.899-942 (2004)
(23) Schnorr, C.P., Euchner, M.:”Lattice Basis Reduction: Improved Practical Algorithms and Soving Subset Sum Problems.”, Math. Programming, Vol. 66, pp.181-199 (1994)
(24) Shoup, V.:”NTL – A Library for Doing Number Theory.” http://www.shoup.net/ntl/index.html (accessed 15 December 2012)
(25) 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 Fundamental Review, Vol.5, No.1, pp.42-55 (2011)

(2012 年 9 月 21 日受付)
(2012 年 12 月 19 日採録)