3-3-2　耐量子計算機暗号の安全性評価
3-3-2　Security Evaluation of Post-Quantum Cryptography

伊藤 琢真　青野 良範　黒川 貴司　篠原 直行
ITO Takuma, AONO Yoshinori, KUROKAWA Takashi, and SHINOHARA Naoyuki

量子コンピュータ開発の進展に伴い、現在使用されている RSA 暗号などの公開鍵暗号が解読される危険性が高まっている。そのため古典と量子の両方のコンピュータでも解読が困難な暗号である耐量子計算機暗号の標準化が進められている。本稿では耐量子計算機暗号の候補である多変数公開鍵暗号と格子暗号を中心に暗号の安全性評価について述べる。

As quantum computing advances, the vulnerability of current public key cryptosystems, such as RSA, increases. Consequently, the standardization of post-quantum cryptography (PQC), which is resilient against both classical and quantum computing attacks, is being actively pursued. This paper presents the security evaluation of cryptography, focusing on multivariate public key cryptosystems and lattice-based cryptography, which are prominent PQC candidates.

1　まえがき

量子コンピュータの技術開発により様々な技術革新が期待される中、その卓越した計算能力によって、現在使用されている RSA 暗号や楕円曲線暗号などの代表的な公開鍵暗号方式が解読されてしまうことが懸念されている [1]。公開鍵暗号方式は情報通信社会を支えるための基盤技術であるため、量子コンピュータ時代が到来しても安全に運用可能な新しい暗号方式、すなわち古典と量子と両方のコンピュータに対して解読が困難と期待される暗号方式である耐量子計算機暗号（PQC、(Post-Quantum Cryptography)）の標準化が世界的に進められている。米国 NIST（National Institute of Standards and Technology）では、世界中から様々な PQC を募り、それらの選定と標準化に向けて動いている。

公開鍵暗号方式は幾つかの数学的問題の困難性を利用して構築されている。PQC には多変数多項式を用いた方式や、格子を用いた方式などがあり、セキュリティ基盤研究室ではこの二つの方式の安全性評価に力を入れている。本稿ではそれらの研究成果について述べる。

2　暗号の安全性評価

一般的に、暗号方式のパラメータ評価は以下の二段階に分けられる。まず、暗号方式を破ることが計算問題を解くことと同等かそれよりも困難であるという安全性証明を行う。この計算問題を安全性の根拠となる問題と呼ぶ。次に、計算問題をコンピュータで解いた場合に、どの程度の計算時間などのコストがかかるのかを見積もり、その値が基準値を超えるようなパラメータを逆算する。この二段階の分業により、様々な暗号方式の安全性が一つの計算問題を調べることで評価可能となる。本稿ではこのコスト評価を安全性評価と呼ぶが、広義には計算アルゴリズムの改良から実装バグの検出等のより広い範囲を含めることもある。なお、この基準値には 2^{128} などの大きな値が用いられ、基準値を 2^b としたパラメータを b ビットセキュリティと呼ぶ。例えば、A と B の 2 つの文字から成る b 桁のパスワードは 2^b 通りあり、事前情報無しにこのパスワードを突破するためには、最大で 2^b 回の試行が必要であり、この試行回数を基準値とするのであれば、このパスワードの安全性は b ビットセキュリティと言えるだろう。

3　多変数公開鍵暗号

多変数公開暗号は主に非線形な連立方程式の求解が困難であることなどを利用して構築されている。有限体上の多変数連立代数方程式の解を求める問題は MP（Multivariate Polynomial）問題と呼ばれており、非線形多項式で構成される MP 問題を解くことは NP−困難 [2] であると知られている。現在、古典・量子の双方の

コンピュータにおいてMP問題を多項式時間で解くための手法が発見されていないことから、多変数公開鍵暗号はPQCとして期待されている。MP問題のうち、連立方程式を構成する全ての多項式が二次多項式である問題はMQ（Multivariate Quadratic）問題と呼ばれている。多項式の全次数が大きいほど項の個数も多くなる傾向にあるため、多くの多変数公開鍵暗号では秘密鍵や公開鍵のデータ量を削減するために、二次多項式が用いられている。公開鍵には、線形変換と秘密鍵との合成写像がよく使われるため、MQ問題を効率良く解く研究のほかに、公開鍵を秘密鍵かそれと同等の性能をもつ多項式系へと変換できるかというIP（Isomorphism of polynomials）問題の研究も進められている。

最初の多変数公開鍵暗号方式は1988年に提案された松本今井暗号[3]と言われている。この暗号方式は既に解読されているが[4]、その後様々な多変数公開鍵暗号が提案されるており、現在では代表的なものとして、UOV[5]やHFE[6]が挙げられ、それらの亜種の提案と研究が続けられている。MQ問題を効率良く解ければ、大抵の多変数公開鍵暗号方式を解読できるようになるため、実際にどの程度の難しさまでのMQ問題を解けるのかを調査するための国際コンテストFukuoka MQ Challengeが開かれており、そこでの記録は安全な多変数公開鍵暗号を設計するための重要な指標となる。

3.1　多変数公開鍵暗号のパラメータ設定

多変数公開鍵暗号の安全性は主にMQ問題とIP問題に依存する。ここではMQ問題でよく使われる解き方とその計算コストについて紹介する。はじめに、MQ問題の求解において重要な指標となる正則次数について紹介する。体$\mathbb{F}$係数とするn変数多項式をm個持つ集合をFとし、各多項式の全次数を$d_1, \ldots, d_m$とする。多項式集合Fから生成されるイデアルを$\langle F \rangle$と書く。

Fの全ての多項式が斉次多項式の場合、Fの正則次数Dを次のように定義する。

$$D = \min\{d \geq 0 \mid \dim_{\mathbb{F}}(\{f \in \langle F \rangle, \deg(f) = d\}) = \binom{n+d-1}{d}\} \cdots\cdots\cdots (1)$$

正則次数Dは、Fが半正則という性質を満たすときに、次の式$H(z)$から求められる[7]。

$$H(z) = \frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1-z)^n} \cdots\cdots\cdots (2)$$

この式$H(z)$を$\sum_{k\geq 0} c_k z^k$という形で表したときに、$c_k \leq 0$となる最小のkがDと一致する。Fの多項式がランダムに選択されている場合はFが半正則になる傾向が高いことが知られており、またFが非斉次多項式を含む場合でも上記の式(2)が用いられる。

以下では、Fの条件として、変数の個数nが多項式の個数mより少ない場合（$n < m$）を想定するが、$n \geq m$の場合はいくつかの変数に適当な値を代入して方程式を場合分けすることで、変数nを$m-1$に置き換えた問題として扱う。この条件下では連立方程式の解が一つ以下となる傾向にある。MQ問題を解く代表的な方法として、XLアルゴリズム[8]による求解とグレブナ基底の計算による求解が挙げられる。まず一つ目のXLアルゴリズムについて述べる。XLアルゴリズムは、Fの多項式にたくさんの単項式が掛けられた多項式から成る集合Gを作り、GのMacaulay行列を掃き出すことにより、線形方程式を得て解を求める手法である。与えられた多項式よりも低い次数の多項式を得る必要があるため、大抵の場合において、Gを全次数がD以上の多項式を持つように作らなければならない。n変数D次単項式の総数は$\binom{n+D}{D}$であるから、GのMacaulay行列のサイズは$\mathcal{O}\left(\binom{n+D}{D}^2\right)$となり、この行列の掃き出しに必要な計算量は

$$\mathcal{O}\left(\binom{n+D}{D}^{\omega}\right), (2 \leq \omega \leq 3) \cdots\cdots\cdots (3)$$

となる。

次に二つ目のグレブナ基底の計算による求解について紹介する。グレブナ基底とは端的に表現すると、イデアルの基底のうち、便利な性質を持つ基底である。$\langle F \rangle$のグレブナ基底から、Fに対する連立方程式の解を求めることは（比較的）容易とされている。グレブナ基底を計算するアルゴリズムにはBuchbergerのアルゴリズム[9]、F4[10]、F5[11]、M4GB[12]など様々なものが提案されている。グレブナ基底の計算はXLアルゴリズムと類似している部分があり、それを基準に説明する。Fの多項式に次数が1以下の単項式を掛けて多項式集合G_1を作り、G_1のMacaulay行列の掃き出しにより多項式集合$\widetilde{G_1}$を求める。先の手順と同様に今度は$\widetilde{G_1}$に対して単項式を掛けてG_2を作り、その行列の掃き出しにより$\widetilde{G_2}$を求める。この手順を繰り返すことで最終的にグレブナ基底となるG_lを求めることができる。グレブナ基底の計算はそれが求まるまでに、D次の多項式が必要になると考えられており、そのため、XLアルゴリズムと同様に計算量の式(3)がよく使用される。

以上のことから、n変数m多項式で構成される暗号方式の安全性の基準値には式(3)が利用されている。例えば、$n = 95, m = 96$というMQ問題は$D = 49$となり、$\omega = 2$とすると式(3)の$\mathcal{O}$の内部は、$\binom{n+D}{D}^{\omega} \fallingdotseq 2^{258.75}$となり、258ビットセキュリティとなる。

より厳密な安全性を評価するために。理論的に考えられる計算量に加えて、実際にどの程度の時間で解読できるのかという数値も重要な指標となる。多変数公開鍵暗号の分野では、どの程度までの難しさの MQ 問題を解けるのかという国際コンテスト、Fukuoka MQ Challenge が開かれており、そこでは暗号方式用と署名方式の 2 種類、そして係数体が GF (2)、GF (256)、GF (31) の 3 種類、合わせて計 6 種類の問題が用意されている。あるパラメータの問題を解くために、どのようなアルゴリズムで、どのようなスペックの計算機を使用して、どのくらいの時間を要して解けたのかが記録されている。

3.2　多変数公開鍵暗号の安全性評価に関する研究成果

我々は MQ 問題をグレブナ基底の計算で解く方法について研究し、無駄な行列の掃き出しをある条件で省けることを発見し、従来の方法よりも効率よく MQ 問題を解けるようになった (図 2)。またその結果として、解読に 4 年以上は要すると想定されていた問題を 2 か月程度で解くことに成功した [13]。この結果は Fukuoka MQ Challenge に掲載されている。

元々、グレブナ基底を計算する過程で、無駄な多項式を処理してしまう、すなわち、行列を掃き出したときに零となる行が現れるのはよく知られている。我々は、ランダムに生成された MQ 問題に対して数値実験を繰り返すうちに、零となる行が連続して続いていることを発見し、その性質を利用することで、行列の無駄な掃き出しを大幅に削減することに成功した。

今後の課題には、この効率化されたアルゴリズムを用いた場合に、理論的にどの程度の計算時間がかかるのかといった計算量評価の厳密化が挙げられる。

4　格子暗号

格子とはユークリッド空間内に規則的に並んだ点の集合で、コンピュータの中では基底ベクトルの集合 $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ により集合 $L=\{a_1\boldsymbol{b}_1 + \cdots + a_n\boldsymbol{b}_n : a_i \in \boldsymbol{Z}\}$ を表現する。格子の世界においてベクトルと点は同一視される。格子の性質に関する研究の歴史は少なくとも 100 年以上続いているが、公開鍵暗号の構成要素としては Ajtai-Dwork による国際会議 STOC1997 での発表 [14] が起点となり注目を集めた。その後、最短ベクトル問題等の格子に関する計算問題が NP- 困難であり、かつ平均的に難しいという暗号応用に向いた性質が発見され研究が進められた。特に、2000 年代には Regev [15] による LWE (Learning With Errors) 問題に基づく格子暗号の構成、Gentry [16] によるイデアル格子問題に基づく完全準同型暗号の構成など、基礎・応用ともに大きな進展があり、それに伴い安全性評価の研究も深化した。2024 年現在、格子問題を効率的に解く量子アルゴリズムが発見されていないことから格子暗号は代表的な耐量子計算機暗号のカテゴリとして知られており、古典・量子の双方のコンピュータにおいて適切な実装・パラメータ設定のための安全性評価が進められている。本節では、格子暗号の安全性評価手法である格子点探索アルゴリズムの概要と近年の進展について述べる。

4.1　格子暗号のパラメータ設定

格子暗号のパラメータ設定について述べる。多くの格子暗号は安全性証明の帰着先が LWE 問題、SIS (Short Integer Solution) 問題、NTRU 問題及びその変種であり、これらの問題を解くコスト評価に関する研究が活発に行われている。上記の計算問題は基底ベク

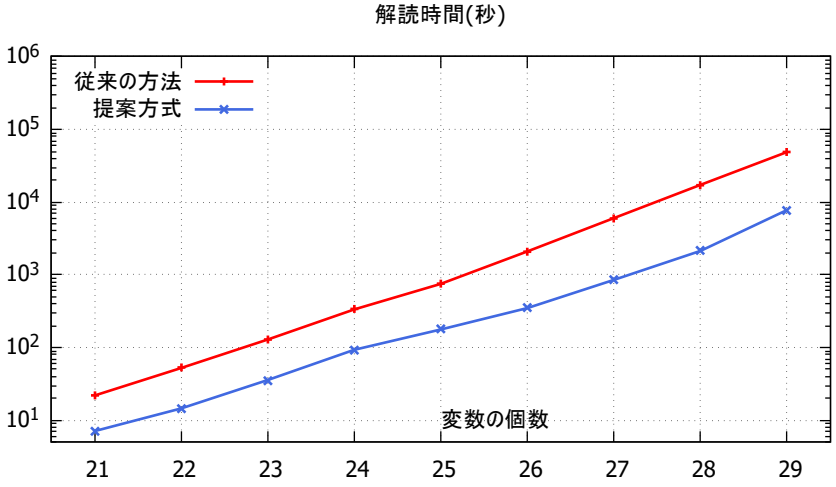

図 1　MQ 問題 ($m = 2n$) 求解の実験結果

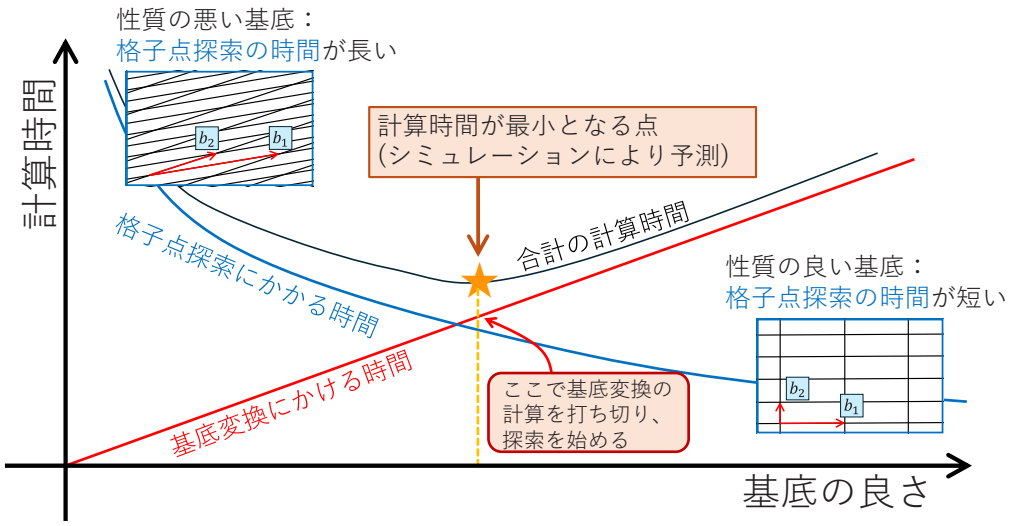

図 2　格子暗号評価の一般的なフレームワーク

トルの集合Bとして与えられた格子Lの中から、条件を満たす格子点を発見する計算問題として統一的に捉えることができる。この枠組みの中で計算問題のコスト評価に用いられる標準的な手法は、格子基底簡約アルゴリズムにより基底Bを別の良い基底B'に変換し、篩(ふるい)アルゴリズム (Sieve algorithm) または格子点探索アルゴリズム (ENUM algorithm) により目標の点を発見する 2 段階フレームワークである (図 2)。計算コストを最小化するため、前半の格子基底簡約アルゴリズムをどこで打ち切り、後半の篩または格子点探索を開始するかが重要となる。打ち切りタイミングの設定には、前半の格子基底簡約における計算時間と基底B'の関係、後半の入力基底B'と目標の点を発見するまでの計算時間の関係を評価することが必要になり、そのためのシミュレーターの開発が重要となる。

次に、代表的な格子点探索アルゴリズムである格子点探索アルゴリズムの近年の進展について概説する。なお、このアルゴリズムは格子簡約アルゴリズムのサブルーチンとしても用いられており、格子に関するアルゴリズムの中で最も基本的なものの一つと考えられている。

最短ベクトル問題を例にとり格子点探索アルゴリズムの解説を行う。最短ベクトル問題とは与えられた基底$B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$に対して格子点集合$L$の中で最も短い非ゼロベクトルを求める問題であり、NP 困難であることが知られている。最短ベクトルを求めるため、格子点探索アルゴリズムでは入力の基底Bに対して以下の深さnの探索木を考える。

・各ノードには格子点がラベル付けされており、根にはゼロベクトルが対応する
・深さkのノードには$\boldsymbol{v} = \sum_{i=n-k+1}^{n} a_i \boldsymbol{b}_i$の形のベクトルが対応し、その子ノードは$\boldsymbol{v} + a_{n-k}\boldsymbol{b}_{n-k}$の形のベクトルが対応する

この木を根から深さ優先探索を用いて探索することで、最短ベクトルを求めることができる。具体的には最短ベクトルの長さが上から$\sqrt{n} \cdot \det(B)^{1/n}$で押さえられるため、深さ$k$のノードにおいてその射影長$|\pi_{n-k+1}(\boldsymbol{v})|$が$R$よりも大きい場合には枝刈りを行うことで探索範囲を有限に押さえることができる。このアルゴリズムは長さR以下の全ての格子点を列挙することが保証されているため、その中で非ゼロの一番短いものを取ることで最短ベクトルとなる。実際には計算の効率化のため、$|b_1|, \dots, |b_n|$の中で上記上界よりも小さいものが存在した場合には初期値として利用し、Rよりも小さい長さの格子点が発見された時点でRの値を更新する等の改良が考えられる。

格子点探索アルゴリズムの改良の中で最も実用的なものは、探索半径$R_1, \dots, R_n$を個別に設定し深さkのノードを$|\pi_{n-k+1}(\boldsymbol{v})| > R_k$の条件で枝刈りする Gama-Nguyen-Regev [17] の手法であり、論文では最短ベクトルの発見確率pとコストNを評価する公式が以下のように与えられた。

$$p = \frac{\mathrm{vol}(C_n)}{|b_1| \cdots |b_n|} \quad , \quad N = \sum_{k=1}^{n} \frac{\mathrm{vol}(C_k)}{|b_{n-k+1}^*| \cdots |b_n^*|} \cdots\cdots\cdots (4)$$

ただし、C_kはk次元物体

$$C_k = \{(x_1, \dots, x_k) : x_1^2 + \cdots + x_j^2 \le R_j^2 \text{ for all } j\}$$

であり、正確な体積の計算は容易ではないが、良い近似を計算するアルゴリズムが知られている。確率を一定値以上に保ったままコストを最小化する問題は、$R_1, \dots, R_n$に関する最適化問題として定式化できるため、格子点探索アルゴリズムを実行する前に最適な探索半径を事前計算することが可能となる。

4.2　格子暗号の安全性評価に関する研究成果

我々は格子点探索アルゴリズムの研究を進め、上記計算コストの下限に関する結果とコスト評価の問題点の修正を行った。

まず、計算コストの下限について説明する。前節で述べた格子点探索アルゴリズムのコスト評価は計算量の上界であり、格子基底簡約アルゴリズムの出力基底B'の Gram-Schmidt 基底に大きく依存する。そのため、将来的なアルゴリズムの進化により計算量が大きく削減された場合、暗号方式のパラメータを再調整する必要がある。このような場合、長期的な安全性の担保に支障が出る可能性がある。この問題に対処するため、最短ベクトルの発見確率pを固定したときの計算コストNの下限を求める公式を導出した [18]。この式と格子基底簡約アルゴリズムが出力する最良の格子基底に対応する Gram-Schmidt 基底を組み合わせることで、格子点探索アルゴリズムがどのように進化してもそれ以上は攻撃計算量を下げることができないという限界を導出することが可能である。

次にコスト評価の問題点の指摘について説明する。これまでコスト評価の公式 (4) はどのような場合についても良い近似を与えると考えられてきたが確率pが非常に低い場合に最適化問題を解いて求めた$R_1, \ldots, R_n$に対して、正確なコスト評価を与えておらず現実のコストよりも低い値となることが明らかとなった。我々はこの問題を修正する方法を提案し、上記計算コストの下限を求める関数を修正した [19]。

図 3 に公式から導かれる格子の次元と古典・量子における計算コストの下限を示す。横軸が格子の次元、縦軸が計算コストである。黄色、赤色で示した線がそれぞれそれまでの研究によるコストの下限と修正後の下限である。大体 5 ～ 10 ビット程度上昇している。また、水色の点線は最新の篩アルゴリズムによる計算量評価の上界であるが、メモリアクセスのモデルの仮定により評価が分かれている。大枠では篩アルゴリズムの方の性能が上回っているが、巨大なメモリ空間が物理的に用意可能であるかどうか等の現実的な制約を考えることで関係が反転するため、両者を組み合わせたハイブリッドアルゴリズムや、物理的な制約を加味した安全性評価などを続けていくことが今後の課題となる。

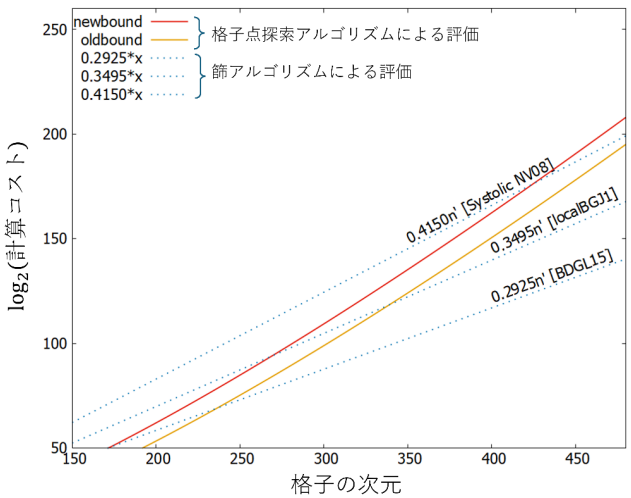

図 3　格子点探索の計算コストの評価

5　まとめ

本稿では PQC の候補である多変数公開鍵暗号と格子暗号を例に、暗号の安全性評価について記し、そこでは、暗号を実用化するためのパラメータの設計には、理論値だけでなく実験値も重要な指標となることについて述べた。本研究室では引き続き、数学的問題を解くための手法を含めた計算の改良に取り組み、PQC の実用化、標準化に向けて、暗号の安全性評価に関する研究開発を行っていく。

【参考文献】

1 P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Review, 41, pp.303–332,1999.
2 M. R. Garey and D. S. Johnson, “Computers and Intractability: A Guide to the Theory of NP-completeness,” W. H. Freeman and Co., New York, 1979.
3 T. Matsumoto and H. Imai, “Public quadratic polynomial-tuples for efficient signature verification and message-encryption,” in EUROCRYPT 1988. Lecture Notes in Computer Science, vol.330, (Springer, Heidelberg), pp.419–553, 1988.
4 J. Patarin, “Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt’88,” in CRYPTO 1995, Lecture Notes in Computer Science, vol.963 (Springer, Berlin), pp.248–261,1995.
5 A. Kipnis, J.-J. Patarin, and L. Goubin, “Unbalanced oil and vinegar schemes,” in International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 1999). Lecture Notes in Computer Science, vol.1592, (Springer, Berlin), pp.206–222, 1999.
6 J. Patarin, “Hidden field equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms,” International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 1996). Lecture Notes in Computer Science, vol.1070, (Springer, Berlin), pp.33–48, 1996.
7 Keith Pardue, “Generic sequences of polynomials,” Journal of Algebra, vol.324, no.4, pp.579–590, 2010.
8 N. Courtois, A. Klimov, J. Patarin, and A. Shamir. “Efficient algorithms for solving overdefined systems of multivariate polynomial equations,” EUROCRYPT 2000, pp.392–407, Springer, 2000.
9 B. Buchberger, “Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal,” Ph.D. thesis, Universitat Insbruck, 1965.
10 J. C. Faugère, “A New Efficient Algorithm for Computing Gröbner Bases (F4),” Journal of Pure and Applied Algebra, 139, pp.61–88, 1999.
11 J. C. Faugère, “A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)”. ISSAC 2002, pp.75–83. ACM, 2002.
12 R. H. Makarim and M. Stevens, “M4GB: An Efficient Gröbner Basis Algorithm,” Proc. of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, pp.293–300, Association for Computing Machinery, 2017.

13 T. Ito, N. Shinohara, and S. Uchiyama, “An efficient F4-style based algorithm to solve MQ problems,” Advances in Information and Computer Security - 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, August 28-30, 2019, Proceedings, ed. N. Attrapadung and T. Yagi, Lecture Notes in Computer Science, vol.11689, pp.37–52, Springer, 2019.
14 M. Ajtai and C. Dwork “A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence,” Proc. of ACM STOC 1997.
15 O. Regev “On lattices, learning with errors, random linear codes, and cryptography,” Journal of the ACM, vol.56, no.6, pp.1–40.
16 C. Gentry “A fully homomorphic encryption scheme,” Ph. D. Thesis, Stanford University, 2009.
17 N. Gama, P. Q. Nguyen, and O. Regev “Lattice Enumeration Using Extreme Pruning,” Proc. of Eurocrypt 2010, LNCS 6110, pp.257–278, 2010.
18 Y. Aono, P. Q. Nguyen, T. Seito, and J. Shikata “Lower Bounds on Lattice Enumeration with Extreme Pruning,” Proc. of CRYPTO 2018, LNCS 10992, pp.608–637, 2018.
19 青野　良範，フォン　グエン“格子の Extreme Pruning における計算コストのずれについて，”日本応用数理学会第 19 回研究部会連合発表会，2018.

伊藤 琢真（いとう たくま）
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究員
博士（理学）
暗号技術の安全性評価
【受賞歴】
2019 年　The 14 th International Workshop on Security（IWSEC 2019）Best Paper Award 受賞

青野 良範（あおの よしのり）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（理学）
公開鍵暗号の安全性評価
【受賞歴】
2023 年　IEEE Signal Processing Society Best Paper Award
2021 年　科学技術分野の文部科学大臣表彰 若手科学者賞
2017 年　情報処理学会コンピュータセキュリティ研究会（CSEC）優秀研究賞

黒川 貴司（くろかわ たかし）
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究技術員
博士（工学）
暗号技術の安全性評価

篠原 直行（しのはら なおゆき）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士（数理学）
暗号に関する数理学
【受賞歴】
2019 年　The 14th International Workshop on Security（IWSEC 2019）Best Paper Award
2013 年　第 12 回（2013 年）ドコモ・モバイル・サイエンス賞先端技術部門優秀賞
2008 年　日本数式処理学会第 17 回大会 2008 年度奨励賞