様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

2013 年 5 月 16 日現在

機関番号：22604
研究種目：挑戦的萌芽研究
研究期間：2011～2012
課題番号：23654014
研究課題名（和文）　数体上の量子公開鍵暗号の鍵生成と安全性の研究

研究課題名（英文）　Research on key generation and security of quantum public key cryptosystems over number fields

研究代表者
中村 憲（NAKAMULA Ken）
首都大学東京・理工学研究科・客員教授
研究者番号：80110849

研究成果の概要（和文）：　量子公開鍵暗号系の具体的方式として提案された，数体を利用したナップサック暗号系 OTU2000 を拡張した．秘密鍵を次数や整数基底の制限なしに多項式時間で生成する方法を提案し，より広い秘密鍵空間が取れる様に条件を緩和し，実際に公開鍵も生成する事に成功した．その方法を定式化した論文は JSIAM Letters に掲載された．これは当初に予想した以上の成果を挙げる事ができ，任意の数体を利用する OTU2000 の拡張に関して現実的で良質な鍵生成法を確立した．

研究成果の概要（英文）：　We have extended OTU2000 which is a knapsack base cryptosystem utilizing number fields proposed as an explicit model of quantum public key cryptosystems. We have proposed a method of generating secret keys without any restriction on degrees or integral basis, given a weaker condition for secret keys to obtain them from wider area, and actually succeeded in generating public keys also.　The method has been formulated and published as a paper in JSIAM Letters.　The result is more than what we expected at the beginning, and has established a good practical method of key generation for an extension of OTU2000 over arbitrary number fields.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	1,400,000	420,000	1,820,000

研究分野：数物系化学
科研費の分科・細目：数学・代数学
キーワード：(1) 数体，(2) ナップサック暗号，(3) ナップサック問題，(4) 量子公開鍵暗号，(5) 低密度攻撃，(6) 国際研究者交流（ドイツ）

１．研究開始当初の背景

量子計算機実現により殆どの既存公開鍵暗号の安全性が脅かされる．その事態を克服する為に，量子計算機でも解決困難と考えられているナップサック問題に基いて発明された，数体上の量子公開鍵暗号を研究する事とした．

公開鍵暗号の発明によって，我々が享受しているインターネット環境の安全性が保証されている．しかしながら，この様な安全性は量子計算機が出現すれば保つ事ができない．その理由は，現存する公開鍵暗号の殆どが整数分解問題か離散対数問題の古典計算機による解決困難性に根拠を置いているが，この二つの問題は量子計算機を用いれば多項式時間で解かれてしまう事が示された

からである.

そこで提案されたのが, 逆に量子計算機で数体の剰余体の離散対数問題を解いて秘密鍵から公開鍵を生成し, それから量子計算機でも解読困難なナップサック問題による暗号文を作成するという, 量子公開鍵暗号系のモデルで通常 OTU2000 と呼ばれている. これは量子計算機を本格的に使う初の方式で理論的に国際的注目を集めているが, 鍵生成に量子計算機が必要で計算機実験が容易でなく, これ迄に安全性や実用性の研究は数える程しかなかった. 利用している数体も有理数体が殆どで, せいぜい虚二次体までに限られていた. しかし有理数体だけではOTU2000 の「用いる数体は秘密」という安全性の根拠が崩れる. 類数が小さい虚二次体も極めて限られている. ところが数体の類数が大きいと, 鍵生成に必要なパラメタ条件から暗号文のナップサック問題が低密度となり, 各種の格子最短ベクトル問題を解く低密度攻撃に対して弱い.

我々も主に虚二次体上の OTU2000 に対し秘密鍵生成効率化やナップサック問題高密度化の研究をしてきていた. またパラメタを制限した虚二次体上の OTU2000 の公開鍵を比較的高次元 (約 500) で生成し, それに対して攻撃実験をしてきた. しかしながら上述した要請から, 使える数体を実二次体以上に広げることは重要な問題として残されていた.

２．研究の目的

目標の一つは鍵生成効率化を計り古典計算機に於る実現可能性も追求する事で, もう一つは暗号文から生ずるナップサック問題の困難性を評価する事である. これにより量子計算機の将来は当然ながら, 現在の古典計算機に於ても有益な, 新しい暗号系の安全性に関する研究に貢献する. しかも実現された暗号系は量子計算機の攻撃に対する耐性を持つ.

虚二次体上での研究の発展としての本研究は, 実二次体と三次以上の数体に対して OTU2000 の鍵生成効率化を実現し, そのナップサック問題に基く安全性を評価する事を当初の目的としていた.

実二次体等で鍵生成できていなかった一つの理由はパラメタ条件を簡単に確認できなかった所にある. 最初に, この問題は適切な整数基底にを取れば解決する手法がある事に気付いた. そこで適切な整数基底を構築する手段の定式化を目標とした. 実二次体では標準的基底も適切であるが, それ以外の候補をも検討する事とした. また, 高次元のナップサック問題を考えるには位数の大きい剰余体の離散対数問題を解く必要があり, これはパラメタの制限なしには古典計算機でできない. そこで無限個あると思われる類数 1 の実二次体等で, パラメタを制限して暗号文のナップサック問題が高密度な公開鍵を生成し, 数体が秘密である利点が通用するかどうか計算機実験等で検証する事とした. 一年目には実二次体上の OTU2000 を対象と考え, 二年目には三次以上の数体, とりわけ巡回三次体を対象とする事とした. 巡回三次体には標準的な整数基底があり共役元を含む為パラメタの候補が多い.

３．研究の方法

数体の整数を整数基底で表した係数の絶対値が, 積により増(減)する様子を考察するのか基本である. それを適用して, 前述の**適切な**整数基底の中で最適なものを確定する. その際に, 公式として評価を精密化するだけでなく, 少ない計算量で確認できる事を重視する. ところが, その考察をしている過程で幸運にも問題解決手段は, 適切な整数基底でなくても, **任意の**整数基底に対して存在する事を発見した. それは公式による係数成長評価ではなく, 数論アルゴリズムの常套手段である計算過程による評価である. その為に, 新たに代数的整数の★演算を導入して解答を得た. これについて以下で説明する.

先ず, 長さ n 重み k のナップサック問題に対応する公開鍵生成の為に, 適当な次数 r の数体 F の整数環 $\mathbf{Z}_F$ の素イデアル P を取り, その剰余体 $\mathbf{Z}_F/P$ の完全代表系 $R(P)$ を固定する必要があるが, これは $\mathbf{Z}_F$ の適当な基底を取り, それに関する係数の絶対値を抑えるのが普通である. 次に, パラメタとして「二個ずつ互いに素」な $p_1, \ldots, p_n \in \mathbf{Z}_F$ を, 条件

- 任意の相異なる k 個の p_i 達の積が $R(P)$ に属する

が充される様に取らなくてはならない. 条件を充すパラメタ p_i 達が取れれば秘密鍵は生成できる. しかし, この条件を n 個から k 個を選ぶ組合せについて全部確めていては, 計算量が膨大になり使えない. 虚二次体や有理数体の場合は, その十分条件がノルムを評価する形で与えられ簡単に確認できた. ところが他の場合はノルムや絶対値を抑えても整数基底に関する係数の絶対

値は抑えられない．そこで p_i 達に対して，それ等 k 個の積の整数基底に関する係数の絶対値が評価できる別の条件を考える．その為に，具体的には書かないが，各 $a, b \in \mathbf{Z}_F$ に対し，整数基底 $w_1, \ldots, w_r$ に依存する（正確には多元環 $\mathbf{Z}_F$ の基底 $w_1, \ldots, w_r$ の構造定数に依存する）新しい★演算により，その★積 $a★b \in \mathbf{Z}_F$ を定義した．この★演算は一般には結合法則を満足しないので，演算の順序に注意をする必要がある．しかし，どの様な順序で積を取っても，係数成長評価に有効な手段となる次の性質を持つ．例えば $c = w_1 + \cdots + w_r$ を，任意の順序で k 個★演算して得られた★冪 $c^{★k} = c★\cdots★c$ の $w_1, \ldots, w_r$ に関する係数の絶対値が z 以下の時，

- もし p_i 達の $w_1, \ldots, w_r$ に関する係数の絶対値が y 以下なら，それ等 k 個の通常の積は $w_1, \ldots, w_r$ に関する係数の絶対値が $y^k z$ で抑えられる

という性質を持つ．故に $c^{★k}$ を反復平方法などで一回だけ計算しておけば，どの範囲で p_i 達を取れば，それ等のうち k 個の通常の積が $R(P)$ に属するか判る．この★演算を適用した p_i 達の通常の積による係数成長評価で，これまでは困難であった秘密鍵生成が可能である．

係数成長を評価する為に★演算を適用する方法は他にもあるから，どれが最良か研究する事が問題として残されている．また★演算は基底 $w_1, \ldots, w_r$ に依存するから，その変更による評価の最適化も依然として残された問題である．例えば，実二次体 $F = \mathbf{Q}(\sqrt{7})$ では，整数基底 $1, \sqrt{7}$ より整数基底 $1, -2+\sqrt{7}$ の方が優れている．

得られた整数基底から生成した秘密鍵に関して，対応するナップサック問題が持つ密度の下界を求める．ここ迄は公開鍵の生成が不必要で量子計算機を使わない．

次に，現存する計算機でも秘密鍵から公開鍵が計算可能な様にパラメタを制限して，それにより生ずる理論的弱点を検討するとともに，実際に暗号文を作成して各種の格子最短ベクトル問題解法算法で攻撃する．以上全過程で理論的考察と実験的検証を何度も反復する．

４．研究成果

上述した★演算を適用する方法は，任意次数の数体に対して OTU2000 の秘密鍵を生成可能である．しかも，これによる秘密鍵の生成は多項式時間でできる事が証明できている．

これに加えてパラメタ $p_1, \ldots, p_n \in \mathbf{Z}_F$ は「二個ずつ互いに素」より弱い条件で十分な事も示した．それは暗号文を平文に複合する時の一意性を保証できれば良い事を観察して得られたものである．即ち，これにより OTU2000 の鍵空間を格段に広げる事ができた．

そこで当初の方針を変更して，一般の数体についての鍵生成プログラムを計算代数システム MAGMA 実装し，それによる鍵生成実験を実行した．その結果OTU2000 の鍵生成に関しては，公開鍵も計算可能な様にパラメタを少し制限すれば，実用化可能な段階に到達したと言える．実際 $n = 1000$ 程度 $k \leqq 50$ 程度なら，数体 F の定義方程式を与えれば数秒以内に秘密鍵を生成できる．公開鍵生成には少し時間がかかるが，それでも数分程度である．

また，新たに MAGMA の開発者でもあるドイツの Kaiserslautern 大学の Claus Fieker 教授との共同研究により，我々の鍵生成法は計算法が簡単であるだけでなく最良に近い鍵が得られる事と，新たに確率的観点を導入した係数成長評価をすれば更に効率的な鍵生成が可能である事が判明した．これらの観点を加えたプログラム作成は今後の課題として残されている．

これ迄生成した秘密鍵に関して，対応するナップサック問題の密度は十分高いという実験結果を得ている．しかしながら，擬密度は必ずしも高くないという実験結果を得ている．そこで生成された公開鍵を用いた具体的暗号文を作成し，それに対して実際に低密度攻撃をして強度を検証する必要がある．また公開鍵を生成する為に秘密鍵の一つに制限を加えて，量子計算機なしに離散対数問題を解いている．そこで，この制限による攻撃に対する脆弱性や鍵生成効率への影響と，有限体の離散対数問題を解く指数計算法の実装による制限緩和等を理論的・実験的に考察する必要がある．同時に，研究期間内では任意次数の数体での鍵生成法に研究を集中した為，当初予定した低次数の数体での鍵生成に関する最適化のが遅れている．そこで，この問題を実可換 2, 3, 4 次体に対して，より詳細に研究する事を予定している．

残された問題は，実際に生成した鍵や暗号文の安全性に関する理論的・実験的な研究が第一である．これと連携しながら，更に適

切な鍵生成が第二の課題である． 本研究の開発した手法にも改良の余地がある． 係数成長評価は反復平方法の他にも幾つか手段があるから，その中で最適な手段を探る事は技術的な改良として引き続き追究する必要がある． 整数基底に何を選択すればよいのかという問題に関しても，秘密鍵生成の過程に確率的観点を導入する事に関しても，それと同様の事が言える． これらに成果が得られれば，拡張 OTU2000 は鍵生成だけでなく安全性に関しても量子計算機耐性を持つ暗号系として実用化の段階に入る事ができる.

本研究の主題とは直接は関係しないが，導入した★演算を用いた積による整数基底の係数成長評価は，方法が単純だから数体の整数の冪検出など他の問題への応用も広く期待される． 他方で評価自身は未だ荒く，類似の演算など手法の改善を図ることも必要であろう． これ等の問題も余裕があれば研究してみたい.

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２件）

[1] MIYAMOTO, Yasunori, NAKAMULA, Ken, Improvement of key generation for a number field based knapsack cryptosystem, JSIAM Letters, 査読有, Vol.5 (2013), 45--49.

[2] 中村 憲, 数論システム NZMATH の使い方, 計算機代数システムの進展, 九州大学マス・フォア・インダストリ研究所, 査読無, 2011 年 11 月 30 日, pp.77--89.

〔学会発表〕（計５件）

[1] 中村 憲, 数論システム NZMATH の有効活用について (3), 日本応用数理学会 2012 年度年会, 2012 年 8 月 29 日, 稚内 全日空ホテル.

[2] 宮本 泰徳, 中村 憲, ナップサック暗号の数体を利用した鍵生成法の改良と考察, 日本応用数理学会 研究部会 連合発表会 (第 8 回), 2012 年 3 月 9 日, 九州大学.

[3] 平野 正樹, 中村 憲, 平方 Weil ペアリングと簡約 Tate ペアリングの計算量評価と数値実験, 日本応用数理学会 研究部会連合発表会 (第 8 回), 2012 年 3 月 9 日, 九州大学.

[4] 田中 覚, 中村 憲, 宮本 泰徳, 平野 正樹, 数論システム NZMATH の有効活用について (2), 日本応用数理学会 2011 年度年会, 2011 年 9 月 16 日, 同志社大学.

[5] 中村 憲, 数論システム NZMATH の使い方, 研究集会 計算機代数システムの進展, 2011 年 8 月 29 日, 九州大学.

６．研究組織

(1)研究代表者
中村 憲 (NAKAMULA Ken)
首都大学東京・理工学研究科・客員教授
研究者番号：80110849

(2)研究分担者
なし

(3)連携研究者
なし