様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　５　月　１９　日現在

機関番号：　２２６０４
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５４０００１９

研究課題名（和文）数体を用いた量子計算機耐性を持つ公開鍵暗号の実現

研究課題名（英文）Realization of public key cryptosystems using number fields with registance to quantum computers

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

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：量子計算機耐性数体利用暗号系 OTU2000 の古典計算機による実用化を考察した．数体 F で暗号の効率的鍵生成をするには，整数基底で F の整数を表した係数の大きさの積による成長評価が要る．そこで F に新しい乗法を導入し，部分和問題に基く効率的鍵生成プログラムを実装した．更に高密度部分和問題を持つ公開鍵を生成し，暗号文の平文復号攻撃を行う計画を立てた．実際に計算機実験を進めると，高密度部分和問題を持つ鍵生成には時間が掛り過ぎ，予定した平文復号攻撃は挫折した．この問題点は量子計算機実現で解決されるから，それ以外の鍵生成を効率化した事は一定の実用的意味を持つ．

研究成果の概要（英文）：We studied realization by classical computers for the cryptosystem OTU2000 using number fields with registance to quantum computers. We need to estimate the growth of the size of coefficients of the product of integers written by an integral base of a number field F. So we introduced a new multiplication on F, and implemented efficient programs to generate keys for the cryptosystems based on subset sum problems. We planed to generate public keys with high density subset sum problems, and to attack by decrypting cipher texts generated by those keys. As a result of computer experiments, it took too much time to generate public keys with high density subset sum problems, hence we have not been able to try the attacking at the moment. This problem is solved by the realization of quantum computers, therefore it is useful that our study have made key generation more efficient except for this part.

研究分野：　数物系科学

キーワード：　数体　数論アルゴリズム　公開鍵暗号　量子計算機　国際研究者交流（フランス，ドイツ）

１．研究開始当初の背景

量子計算機が実現されると，これ迄使われている殆どの公開鍵暗号は安全性が脅かされる．　その事態を考慮して 2000 年に，量子計算機でも解決困難と考えられている部分和問題に基いて，数体を利用した量子公開鍵暗号モデルが量子計算機を用いて提案された．　この方式は量子計算機を必要とする為，現時点での実用化は考えられていない．　そこでこれを改良して古典計算機による実現可能性を検討する事とした．

公開鍵暗号の発明により，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き，これらは量子計算機により容易に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乗法群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部分和問題に基いた暗号文を作成するという，量子公開鍵暗号系のモデルで，これは通常 OTU2000 と呼ばれている．　そ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い．　利用する数体も有理数体が殆どで，せいぜい虚二次体に限られる．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の一つが崩れる．　また類数が小さい虚二次体も極めて限られるが，もし数体の類数が大きいと暗号文に対する部分和問題の密度が低くなる傾向があり，格子最短ベクトル問題を解く攻撃に対して弱くなる．

これ迄に我々も，主に虚二次体を利用した OTU2000 に関して，秘密鍵生成の効率化や部分和問題の高密度化を研究した．　また，虚二次体を利用した OTU2000 に関して，比較的高次元 (約 500) で条件付ながら秘密鍵から公開鍵を生成し，それに対する攻撃実験をしてきた．　その発展として，科研費挑戦的萌芽研究「数体上の量子公開鍵暗号の鍵生成と安全性の研究」(2011～2012 年度，課題 ID 11017200) では，更に実二次体や三次以上の数体を利用する OTU2000 に関して，秘密鍵生成の効率化と部分和問題の密度評価を研究してきた．　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 に関して，極めて高速な秘密鍵生成が可能になり，鍵の一つである剰余体の乗法群の位数が滑らかという条件付ながら秘密鍵から公開鍵生成もする事ができた．

２．研究の目的

本研究では以上の背景と成果を引継いで，実際に OTU2000 を古典計算機だけで利用できる様にする事が主要な目的である．　具体的には，第一に鍵生成の効率化による現存する古典計算機だけ用いた実現可能性の追求で，第二に暗号文から生ずる部分和問題の困難性評価による安全性の確認である．　これが成功すれば，量子計算機が実現されるであろう将来は勿論，古典計算機だけの現在に於ても，新しい有益な暗号系の誕生に貢献する事ができる．　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．　より具体的には以下の目標を達成する．

第一に，更なる秘密鍵生成の効率化を計る．これ迄，有理数体や虚二次体でなければ秘密鍵生成すら困難であった理由の一つは，パラメタ条件確認に必要な，**代数的整数の積による整数基底に関する係数の絶対値の変化や増大度**を簡単に評価できなかった所にあった．　この問題は，実二次体の標準基底を含め適切な条件を充す整数基底に対して解決できる事を発見した．　そこで適切な整数基底を構築する手段の定式化を試みたが，その過程で幸運にも問題解決手段は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，新たに後述する代数的整数の★二項演算という積を導入して解答を得た．　しかし，この★演算を適用して評価を得るには，どの整数に対して積を計算すれば最適なのか不明である．　現時点では整数基底の和に反復平方法を適用した評価で鍵生成しているが，それ以外の効率的な場合があるかどうか研究したい．　また★演算は整数基底に依存するから，整数基底選択の問題も依然として残されている．　そこで，併行して最適な整数基底を理論的考察と計算機実験により決定したい．

第二に，高次元の部分和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，これは条件付の秘密鍵でなければ古典計算機では困難である．　これ迄の実験では，条件付の秘密鍵から公開鍵を生成しても，そこそこ高密度な部分和問題の暗号文が作成できているが，まだ不十分である．　そこで，これ等が実際に格子最短ベクトル問題を解く低密度攻撃に耐性を持つかどうか，計算機実験により検証したい．　同時に，秘密鍵に条件を付けた事が OTU2000 に与える影響 ― 鍵生成の効率や攻撃に対する脆弱性等 ― についても，数体が秘密である利点が通用するかどうかを含めて，検討する必要

がある．更に最重点としては，より高密度の部分和問題を持つ秘密鍵・公開鍵の生成を目指す．

また秘密鍵生成に於る手法の改良は代数的整数の冪検出等への応用も考えられる．

３．研究の方法

前述した様に，一般の数体 F に対して設計されている OTU2000 が，有理数体や虚二次体に対してしか実装されなかったのは，鍵生成に必要なパラメタが充す条件を，他の数体では簡単に確認できなかった事である．この問題を克服する為に我々は以下の手法を採用した．

先ず，長さ n 重み k の部分和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ろうとも，係数成長評価に有効な手段となる次の様な性質を持つ:
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，どんな積の順序で得られた★冪であろうとも，

- 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，例えば反復平方法などで，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．

その際にどの順序で★冪を計算するのが最良か検討する必要がある．係数成長を評価する為に★演算を適用する方法は★冪の他にもあるから，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．

この方法により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．それを適用して，前述した最適な★演算適用法と最適な整数基底を確定する．その際に，より良い評価を精密に求めるだけでなく，少ない計算量で確認できる事を重視する．得られた最適な★演算適用と整数基底を用いた場合の，部分和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，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．これ等の鍵生成に成功した場合についていえば，どの★演算適用法にも極端に大きな差は無く，また整数基底の違いによる係数成長評価の違いも殆ど重視する必要が無い事が判明した．以上により鍵生成効率化という第一の目標は，それなりの成果を得る事ができた．

しかしながら第二の目標である我々の方法が実用化可能な程度に安全かどうかは計算機実験すらできていない．その検証の為に**擬密度**が高い部分和問題を持つ公開鍵を生成し，それによる暗号文の平文復号攻撃を行う計画を立てた．ところが実際に計算機実験を進めると幾つか問題点が判明した．初めに一方で，古典計算機で離散対数問題を解く為，秘密鍵の一つである F の素イデアル P を選ぶとき，剰余体 $\mathbf{Z}_F/P$の乗法群が位数滑らかな必要がある．しかし k が少し大きいと，その様な P の発見に時間が掛り困難となる．次に他方で，暗号文の耐性を保証する部分和問題の強度を上げる為に擬密度を高める必要がある．有効なのは k を $n/2$ に近く大きくする事だが，その時は最初の問題点が障害となり鍵生成が困難である．更に離散対数問題を解くのにも時間が掛り過ぎる．以上により予定していた，擬密度が高い部分和問題を持つ暗号文に対する攻撃は前段階で挫折した．但し上記問題点は量子計算機実現で解決されるから，それ以外の鍵生成を効率化した事は一定の実用的意味を持つ．

また，ドイツから Claus Fieker，フランスから Andreas Enge 両教授を，国際研究集会「代数学と計算 2015」に招聘し特別講演・招待講義・ゼミで集中的共同研究をした．その中で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て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，対応する部分和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も得られている．そこで既に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，この制限を原因とする攻撃に対する脆弱性や鍵生成効率への影響と，有限体の乗法群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必要がある．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　1　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.

〔学会発表〕（計　0　件）

〔図書〕（計　1　件）

[1] 日本応用数理学会 監修／薩摩順吉・大石進一・杉原正顯(分担執筆／中村憲)，応用数理ハンドブック，朝倉書店，2013，704pp.

〔産業財産権〕
○出願状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：

国内外の別：

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
量子公開鍵暗号の Magma による実装
http://tnt.math.se.tmu.ac.jp/labo/master/2011/miyamoto/

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

(3)連携研究者