様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月　 １ 日現在

機関番号：３２６８６
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ０３４３２

研究課題名（和文）グレブナー基底計算アルゴリズムの深化

研究課題名（英文）Further development of algorithms for Groebner basis computation

研究代表者
横山　和弘（YOKOYAMA, Kazuhiro）

立教大学・理学部・教授

研究者番号：３０３３３４５４

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：グレブナー基底は多項式イデアルのよい性質をもつ基底で、純粋数学から工学等の応用まで幅広く用いられている。しかし、グレブナー基底計算の効率化には未だに問題が残っている。本研究ではSBAと呼ばれる効率化技法に関して、その理論の完成と高速化を実現できる実装を行なった。理論研究では、互換性と呼ばれる項順序に関する条件の下でSBAの正確な正当性・停止性の証明に成功した。実装実験により、SBAの優位性を活かせる基底変換計算などのアルゴリズムを構築した。応用研究では、暗号の安全性研究でのグレブナー基底計算法の適用実験や理論解析行なった。

研究成果の学術的意義や社会的意義
グレブナー基底は多項式イデアルのよい性質をもつ基底で、連立代数方程式の求解に留まらずに、解の代数的構造などが計算によりわかることから、純粋数学から情報（暗号理論等）や工学（制御・最適化等）への応用まで幅広く用いられている。本研究によるグレブナー基底計算の高速化により、その適用範囲が広がることで、さらなる数学研究の進展や情報・工学での活用が期待される。

研究成果の概要（英文）：Groebner bases, bases of polynomial ideals, have useful computational properties and used in a various areas such as mathematics and engineering science. However, there still remains a problem on their computational efficiency. In this project, focusing an efficient technique named SBA, we succeeded in completing its theoretical correctness and termination, and an efficient its implementation on a
real computer. As a theoretical result, under a reasonable condition "compatibility" on monomial orders, the correctness and termination of our SBA are theoretically guaranteed. By its implementation on a real computer, we devised several algorithms based on SBA, which have certain superiority to existing algorithms. As application study, we applied Groebner basis computation to analyze the security level of public key cryptosystems.

研究分野：計算機代数

キーワード：グレブナー基底　計算機代数　F5アルゴリズム　F4アルゴリズム　公開鍵暗号　計算可換環論　計算代数幾何

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

グレブナー基底は多項式イデアルのある種のよい性質をもつもので、その計算可能性により純粋数学から工学等の応用まで幅広く用いられている。研究代表者と分担者は長期に渡り、グレブナー基底計算の高速化とそれの応用研究を行ってきたが、大規模な計算には未だ困難さが残っている。グレブナー基底を計算するアルゴリズムでは、その基本的な枠組みとして、発見者のブッフバーガーによるアルゴリズムがあり、その改良としてフォジェールによる F4 アルゴリズムが代表的なものとなっている。これまで数多くの改良や実装が行われてきたが、効率化には未だ問題が残っている。大きな要因の一つとして、グレブナー基底計算では S 多項式というものを大量に生成し、それに対して、別の多項式の除算を行って得られる余りを集めるが、余りが 0 となってしまう「無駄」な S 多項式が現れることである。2002 年にフォジェールにより提案された F5 アルゴリズムでは、「理想的な場合」にはこのような無駄な S 多項式を全て排除できるとされ、極めて高速な実行結果が示されたが、理論的には不完全であった。フォジェールの F5 アルゴリズムの発表以後十数年にわたり様々な研究や改良が行われ、これらのアルゴリズムを総称して signature based algorithm(SBA)と呼ぶようになったが、未だ高速な実装を可能にするような決定版ともいえるアルゴリズムは見つかっておらず、不完全さは解消されていない。

２．研究の目的

signature based algorithm(SBA)と呼ばれる F5 アルゴリズムの発展形について以下を行う。

(1)理論的な完全性、即ち、いかなる入力に対してもアルゴリズムの停止性が保証され、さらに結果が正しいという正当性も保証され、しかも不要な S 多項式を可能な限り排除する理論を構築する。

(2)完成された理論を基として、従来の計算法より高速にグレブナー基底を計算できる具体的なアルゴリズムを構築し、その高速な実装も計算機上で実現する。

(3)理論と高速実装を検証するために、いくつかの応用計算トピックを選び、実際の問題に適応することも行う。ここでは、公開鍵暗号の安全性解析で現れる連立代数方程式がどこまでグレブナー基底を用いて計算できるか、を主として扱う。また、純粋数学に有用なイデアル計算にも適用する。

３．研究の方法

(1) 研究グループは３名からなり、分担して研究を行う。

①研究代表者(横山) は研究の統括を行う。また、既存のグレブナー基底計算アルゴリズムの理論的な解析を行い、SBA の完全な理論の構築とそれに基づく基本アルゴリズムの提案を行う。また、検証実験として、および暗号研究への応用についての研究を行う。

②野呂は理論研究を受けて、既存および新アルゴリズムの実装法、計算機実験、および SBA を取り入れた F4 アルゴリズム実装のさらなる高速化についての研究を行う。その他の SBA の効率的な実装に役立つ部品の改良も行う。計算機代数システム Risa/Asir を実装のプラットフォームとする。

③篠原は、検証実験として、暗号の安全性研究へのグレブナー基底計算の応用についての研究を行う。

(2) 研究グループで定期的にセミナーを行い、情報を共有する。また、海外の研究者と密に研究交流・情報共有を行い、理論・アルゴリズム研究の進展の動力とする。

４．研究成果

(1)理論研究では、第１段階・第２段階に分けて段階的に行い、最終的に「互換性」と呼ばれる項順序に関する妥当な条件の下で SBA 理論の正確な正当性・停止性の証明に成功した。結果として得られるアルゴリズムでは、従来提案されている SBA に対して、新たに追加する計算が不要であり、理論的な正当性のための処理が計算効率を阻害することがないことも示された。ここで、第１段階を斉次イデアルの場合とし、第２段階を一般のイデアルとした。従来の SBA 理論の詳細な検討を行い、その特性を明確にした上で、項順序における妥当な条件下で正当性・停止を正しく示すことに成功したが、ここでの鍵となるアイデアは研究代表者と海外研究者との共同研究で得られた知見である minimal signature の採用とイデアルの生成集合の syzyzy 加群を利用してイデアルの元の signature を明快に識別できる標準表現であった。

(2)アルゴリズム・高速実装研究は、理論の完成と並行して行われ、当初は部品となる計算の高速化を行い、理論の完成により、それらの統合が行われた。実際には、計算機代数システム Risa/Asir を実装のプラットフォームとし、部品となる計算の高速化を行った。例えば、SBA の高速化・改良に重要な役割を持つと思われる生成集合の syzygy 加群やそこから計算される自由分解に関し、最も効率的と考えられている Schreyer 分解とそれを計算する La Scala-Stillman 法を調査し、効率的な実装方法を考察し Risa/Asir システム上で実装した。これらを有効にと統合して、理論研究で得られた SBA のアルゴリズム化とその実装に成功した。数式処理システム Risa/Asir 上での計算機実験により、いくつかの例では、従来の計算法を凌駕するパフォーマン

スが得られた。
(3) 応用計算による実証研究では、暗号の安全性検証でグレブナー基底計算を行った。多変数公開鍵暗号の暗号化方式で扱われる連立代数方程式に特化して、SBA を用いずに可能な限り改良を進めた F4 アルゴリズムの性能の理論的な解析と数値実験を行った。その結果、上記の連立代数方程式を解くコンテストにおいて世界記録を更新した。SBA と F4 アルゴリズムを融合したアルゴリズムの性能を評価する上で、本方式は重要な指標の一つとなるものと考える。また、純粋数学への応用として、グレブナー基底を利用したイデアル計算として同種写像の公式計算や準素分解の高速化などを行なった。

５．主な発表論文等

〔雑誌論文〕　計11件（うち査読付論文　10件／うち国際共著　3件／うちオープンアクセス　2件）

１．著者名 Takahashi Yasushi、Kudo Momonari、Fukasaku Ryoya、Ikematsu Yasuhiko、Yasuda Masaya、Yokoyama Kazuhiro	４．巻 15
２．論文標題 Algebraic approaches for solving isogeny problems of prime power degrees	５．発行年 2020年
３．雑誌名 Journal of Mathematical Cryptology	６．最初と最後の頁 31～44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/jmc-2020-0072	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Ishihara Yuki、Vaccon Tristan、Yokoyama Kazuhiro	４．巻 -
２．論文標題 On FGLM algorithms with tropical Groebner bases	５．発行年 2020年
３．雑誌名 ISSAC '20: Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation	６．最初と最後の頁 257-264
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3373207.3404037	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Ikematsu Yasuhiko、Fukasaku Ryoya、Kudo Momonari、Yasuda Masaya、Takashima Katsuyuki、Yokoyama Kazuhiro	４．巻 -
２．論文標題 Hybrid Meet-in-the-Middle Attacks for the Isogeny Path-Finding Problem	５．発行年 2020年
３．雑誌名 APKC '20: Proceedings of the 7th ACM Workshop on ASIA Public-Key Cryptography	６．最初と最後の頁 36-44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3384940.3388956	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Noro Masayuki, Yasuda Masaya, Yokoyama Kazuhiro	４．巻 68
２．論文標題 Symbolic Computation of Isogenies of Elliptic Curves by Velu ' s Formula	５．発行年 2020年
３．雑誌名 COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI	６．最初と最後の頁 93-130
掲載論文のDOI（デジタルオブジェクト識別子） 10.14992/00020348	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名	4．巻
ITO Takuma、SHINOHARA Naoyuki、UCHIYAMA Shigenori	E104.A
2．論文標題	5．発行年
Solving the MQ Problem Using Groebner Basis Techniques	2021年
3．雑誌名	6．最初と最後の頁
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	135～142
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1587/transfun.2020CIP0025	無
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Vaccon Tristan、Verron Thibaut、Yokoyama Kazuhiro	102
2．論文標題	5．発行年
On affine tropical F5 algorithms	2021年
3．雑誌名	6．最初と最後の頁
Journal of Symbolic Computation	132～152
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1016/j.jsc.2019.10.012	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	該当する

1．著者名	4．巻
Nagashima Saki、Shinohara Naoyuki、Uchiyama Shigenori	11
2．論文標題	5．発行年
Quadratic Frobenius pseudoprimes with respect to $x^{2}+5x+5$	2019年
3．雑誌名	6．最初と最後の頁
JSIAM Letters	53～55
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.14495/jsiaml.11.53	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Ito Takuma、Shinohara Naoyuki、Uchiyama Shigenori	11689
2．論文標題	5．発行年
An Efficient F_4 -style Based Algorithm to Solve MQ Problems	2019年
3．雑誌名	6．最初と最後の頁
Lecture Notes in Computer Science	37～52
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1007/978-3-030-26834-3_3	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

１．著者名 Takemura Yusuke、Hakuta Keisuke、Shinohara Naoyuki	４．巻 -
２．論文標題 ECC Atomic Block against Strong Side-Channel Attacks Using Binary Curves	５．発行年 2019年
３．雑誌名 2019 Seventh International Symposium on Computing and Networking Workshops	６．最初と最後の頁 387~393
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW.2019.00073	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Vaccon Tristan, Verron Thibaut, Yokoyama Kazuhiro	４．巻 -
２．論文標題 On Affine Tropical F5 Algorithms	５．発行年 2018年
３．雑誌名 Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation	６．最初と最後の頁 383-390
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3208976.3209012	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Aoyama Toru, Noro Masayuki	４．巻 -
２．論文標題 Modular Algorithms for Computing Minimal Associated Primes and Radicals of Polynomial Ideals	５．発行年 2018年
３．雑誌名 Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation	６．最初と最後の頁 31-38
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3208976.3209014	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計19件（うち招待講演　7件／うち国際学会　5件）

１．発表者名 野呂正行，横山和弘
２．発表標題 Signature based algorithm による change of ordering
３．学会等名 Risa/Asir Conference 2021
４．発表年 2021年

１．発表者名
伊藤琢真，篠原直行，内山成憲

２．発表標題
多変数公開鍵暗号の安全性評価におけるグレブナ基底計算での多項式選択

３．学会等名
2021 Symposium on Cryptography and Information Security

４．発表年
2021年

１．発表者名
野呂正行，横山和弘

２．発表標題
Implementation of a signature based algorithm in Risa/Asir

３．学会等名
RIMS Symposium Computer Algebra - Theory and its Applications

４．発表年
2020年

１．発表者名
篠原直行

２．発表標題
量子コンピュータ時代にむけた暗号技術の研究開発と標準化

３．学会等名
サイバーセキュリティシンポジウム道後2020（招待講演）

４．発表年
2020年

１．発表者名
横山和弘

２．発表標題
signature を用いたグレブナー計算アルゴリズム

３．学会等名
計算代数夏の学校2019（招待講演）

４．発表年
2019年

１．発表者名
横山和弘

２．発表標題
signature-based algorithm の停止性と正当性について

３．学会等名
2019年度理論分科会＆システム分科会合同研究会

４．発表年
2019年

１．発表者名
Yasushi Takahashi, Momonari Kudo, Yasuhiko Ikematsu, Masaya Yasuda, Kazuhrio Yokoyama

２．発表標題
Algebraic approaches for solving isogeny problems of prime power degrees

３．学会等名
MathCrypt 2019（国際学会）

４．発表年
2019年

１．発表者名
Masayuki Noro

２．発表標題
A computer algebra system Risa/Asir and an infrastructure for mathematical software OpenXM

３．学会等名
Differential systems: from theory to computer mathematics（招待講演）

４．発表年
2019年

１．発表者名
野呂正行

２．発表標題
種々のグレブナー基底計算法とその実装および性能について

３．学会等名
シミュレーションとモデリングのための計算代数 2020（招待講演）

４．発表年
2020年

１．発表者名
Ito Takuma、Shinohara Naoyuki、Uchiyama Shigenori

２．発表標題
An Efficient F_4 -style Based Algorithm to Solve MQ Problems

３．学会等名
IWSEC 2019（国際学会）

４．発表年
2019年

１．発表者名
Takemura Yusuke、Hakuta Keisuke、Shinohara Naoyuki

２．発表標題
ECC Atomic Block against Strong Side-Channel Attacks Using Binary Curves

３．学会等名
CANDAR Workshops 2019（国際学会）

４．発表年
2019年

１．発表者名
Vaccon Tristan, Verron Thibaut, Yokoyama Kazuhiro

２．発表標題
On Affine Tropical F5 Algorithms

３．学会等名
2018 ACM International Symposium on Symbolic and Algebraic Computation（国際学会）

４．発表年
2018年

１．発表者名
阿部拓実，篠原直行，野呂正行，Vaccon Tristan，横山和弘

２．発表標題
F5-style algorithm の正当性と停止性について

３．学会等名
Risa/Asir Conference 2019

４．発表年
2019年

１．発表者名
横山和弘

２．発表標題
Computer Algebra, the recent topic and future

３．学会等名
RIMS Symposium "Computer Algebra-Theory and its Applications"（招待講演）

４．発表年
2018年

１．発表者名
Aoyama Toru, Noro Masayuki

２．発表標題
Modular Algorithms for Computing Minimal Associated Primes and Radicals of Polynomial Ideals

３．学会等名
2018 ACM International Symposium on Symbolic and Algebraic Computation（国際学会）

４．発表年
2018年

１．発表者名
野呂正行

２．発表標題
Groebner basis computation in Risa/Asir

３．学会等名
RIMS Symposium "Computer Algebra-Theory and its Applications"（招待講演）

４．発表年
2018年

１．発表者名
野呂正行

２．発表標題
グレブナー基底の計算法とその応用

３．学会等名
応用特異点論研究集会，神戸大学理学部（招待講演）

４．発表年
2018年

１．発表者名
野呂正行

２．発表標題
Risa/asir 2018-2019

３．学会等名
Risa/Asir Conference 2019

４．発表年
2019年

１．発表者名
緑川輝，篠原直行，内山成憲

２．発表標題
F4-style アルゴリズムの実装について

３．学会等名
日本応用数理学会2018年度年会

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Page personnelle de Tristan Vaccon
http://www.unilim.fr/pages_perso/tristan.vaccon/recherche.html

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	野呂　正行 (NORO Masayuki) (50332755)	立教大学・理学部・教授 (32686)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	篠原　直行 (SHINOHARA Naoyuki) (70565986)	国立研究開発法人情報通信研究機構・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 (82636)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
フランス	University of Limoges			