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　２ 年　 ６ 月 ２４ 日現在

機関番号：３２７２１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ０５３５３

研究課題名（和文）準同型暗号の高速化に関する研究

研究課題名（英文）Study on speeding up homomorphic encryption

研究代表者
有田　正剛（Arita, Seiko）

情報セキュリティ大学院大学・その他の研究科・教授

研究者番号：５０３８７１０６

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究は、データマイニングやAI技術におけるデータプライバシーの保護を目的として、それらの技術における諸アルゴリズムを、データを暗号化したままで実行することを目的として、準同型暗号を効率化することを目標とする。一般の準同型暗号は、円分体と呼ばれる代数的数体を用いて構成されるが、本研究では、円分体ではなく、その(素数2に関する)分解体Zを用いることで、平文構造として（有限体ではなく）2のべき乗数を法とする整数環が現れる状況を実現し、これによって準同型暗号の数倍から数十倍程度の高速化を実現した。

研究成果の学術的意義や社会的意義
現代社会ではスマートフォンなどの各種デバイスを通して各種データを収集し、得られたビックデータをA Iに学習させることで、様々な高度な社会サービスが実現されつつある。しかしながら、これら収集されたビックデータとその処理により、人々のプライバシーが危険な状態に晒されている。本研究はデータを暗号化したままで処理することを可能とし、人々のプライバシーを守りつつ高度なA Iサービスを実現するための基盤となる技術の一つである。

研究成果の概要（英文）：The purpose of this research is to improve the efficiency of homomorphic encryption in order to protect the data privacy of data mining and AI technology through executing the algorithms in those technologies only on encrypted data. General homomorphic encryption schemes are constructed by using an algebraic number field called a cyclotomic field, but in this research, the decomposition field Z (for prime number 2) is used instead of the cyclotomic field. We have realized a situation where an integer ring modulo a power of 2 appears as a plaintext structure (rather than a finite field), and as a result, we have achieved several times to several tens of times the speedup of homomorphic encryption.

研究分野：暗号理論

キーワード：準同型暗号　データプライバシー

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

完全準同型暗号は、暗号化したままで凡ゆる計算を可能とする暗号方式である。Genrty [1]によってブレークスルーがもたらされて以来、理論的に洗練され、より安全でより効率的な方法が考案されてきた。中でも、Ring-LWE 問題と呼ばれる問題の困難性に基づく方法は、安全性を理論的に証明することができ、効率の面からも比較的優れている。しかしながら、一般的な暗号に比べ、完全準同型暗号は暗号文サイズが非常に大きくなり、準同型演算（暗号化したままでの加算や乗算）、特に準同型乗算のコストが大きい。

そこで、実用化の鍵になる方法として、Smart ら [2]によって平文パッキングの手法が提案された。この手法は、上記 Ring-LWE 問題をベースとする完全準同型暗号に適用される。それらの完全準同型暗号は、円分環と呼ばれる代数的整数の成す環を用いるが、その円分環の代数的構造を利用して、単一の暗号文に複数の平文をパッキングして暗号化することができる。これにより、単一の暗号文に対する演算によって、それに含まれる複数の平文（以下、平文スロット）に対して同時並列に準同型演算を行うことができ、準同型演算のスループットを著しく向上させることが可能となった。

上記平文パッキングの手法を用いた、Ring-LWE 問題ベースの完全準同型暗号は、HElib や SEAL 等のオープンソースライブラリによって実装され、これらを用いて遺伝子情報、医療情報、金融情報等を対象として、プライバシーを保護しつつ、データマイニングや学習アルゴリズムを適用するための研究が進んでいる。

２．研究の目的

本研究の目的は、上記平文パッキングの手法を改良し、より小さな暗号文により多くの平文をパッキングすることで、スループットにおいて完全準同型暗号文の効率化を達成し、完全準同型暗号の実用化に貢献することである。

３．研究の方法

完全準同型暗号は円分整数を用いて実現される。これを改良するには、まず、ベースとなっている代数的整数論をしっかり理解する必要がある。今まで共同研究を行ってきた、情報セキュリティ大学院大学の半田沙里研究員や小﨑俊二研究員と定期的に代数的整数論に関するセミナーを行った。その上で、暗号理論に関する国際会議に出席し、最新の研究成果を収集し、研究打ち合わせを行い、議論を重ね、研究目的を達成した。

４．研究成果

（１）　準同型暗号と円分体

Ring-LWE 問題に基づく完全準同型暗号（以下、環準同型暗号）は円分整数の数理に基づく。円分整数aとは１の原始m乗根ζを用いて$a = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}$と表される代数的整数である。ここで、各$a_i$は通常の整数であり、$n = \varphi(m)$である。

一般に環準同型暗号では暗号化対象の平文は何らかの小さな素数pを法とした円分整数でエンコードされる。素数pを法とした円分整数は、ある次数dに関するガロア体$\mathrm{GF}(p^d)$の要素を複数並べたベクトルとなる。小さな素数pについて、この次数d $(> \log_p(m))$は小さくない。このようにして、環準同型暗号ではその平文は複数の平文スロットの組みとして表され、各平文スロットは大きな次数dをもつガロア体$\mathrm{GF}(p^d)$の要素を表す。つまり、複数の平文データ（＝平文スロット）が一つの暗号文にまとめて暗号化されることとなるが、これを平文パッキングと呼ぶ。平文どうしの加算や乗算は、各平文スロットにおける、ガロア体$\mathrm{GF}(p^d)$の要素としての加算や乗算となり、複数の平文スロットの同時並列演算となる。

このような平文構造はガロア体の要素を用いるアプリケーション、例えばエラー訂正符号や AES 暗号等には適するが、一般的なアプリケーションには不都合である。一般的なアプリケーションでは、各平文スロットの構造は、ガロア体$\mathrm{GF}(p^d)$よりも素数冪p^lを法とした剰余環$\mathbb{Z}_{p^l}$が自然だからである。実際、従来の環準同型暗号をアプリケーションへ応用する際、平文スロットのガロア体構造をあえて消去するために、d次元あるスロットのうち（定数項に相当する）わずか１次元分のみしか使われないことが多く、平文パッキングの並列性を著しく損ねていた。

（２）　分解体の利用

本研究は、素数冪p^lを法とする整数スロットで構成される平文構造をもつ環準同型暗号を実現す

るために、円分環Rの代わりに、素数pに関する分解環R_Zを使用する。

ζを 1 の原始m乗根とする。 m番目の円分環$R = \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_i \in \mathbb{Z}\}$は、$\zeta$によって生成される、すべての円分整数から成る環である。ここで、$n = \varphi(m)$は、mにおけるオイラー関数φの値である。環準同型暗号の平文空間は、小さな素数pを法とする円分整数の空間$R_p = R/pR$となる。円分環Rでは、素数pは（一般に）素ではなく、整数nのある約数gについて、g個の素イデアル$\wp_i$の積に分解されることが知られている：$pR = \wp_0\wp_1 \cdots \wp_{g-1}$. 各素イデアル$\wp_i$の剰余体$R/\wp_i$は環準同型暗号の平文スロットの空間に他ならず、剰余次数$d = n/g$のガロア体$\mathsf{GF}(p^d)$に同型である。このようにして平文空間R_pは以下のように分解される：

$$R_p \simeq R/\wp_0 \oplus \cdots \oplus R/\wp_{g-1} \simeq \mathsf{GF}(p^d) \oplus \cdots \oplus \mathsf{GF}(p^d).$$

前述のように、素数pを法とする整数演算としては、各d次元スロット$\mathsf{GF}(p^d)$中、1 次元部分空間$\mathsf{GF}(p) = \mathbb{Z}_p$しか使用できない。

素数pに関する分解環R_Zは、素数pが円分環Rにおいてと同じ形の素イデアル分解を持つような、円分環Rの最小の部分環である。すなわち、

$$pR_Z = \wp_{Z,0}\wp_{Z,1} \cdots \wp_{Z,g-1}.$$

ここで、因子の個数gは円分環Rのときと同一である。分解環R_Zの上記の最小性より、各因子$\wp_{Z,i}$の剰余体$R_Z/\wp_{Z,i}$は 1 次元、つまり素体$\mathbb{Z}_p$に同型でなければならない。 したがって、分解環R_Zの平文空間は

$$(R_Z)_p \simeq R_Z/\wp_{Z,0} \oplus \cdots \oplus R_Z/\wp_{Z,g-1} \simeq \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p.$$

となる。ここで、素数pに関するヘンゼルリフトをl回繰り返すことにより、$q = p^l$について、$(R_Z)_q \simeq \mathbb{Z}_q \oplus \cdots \oplus \mathbb{Z}_q$が得られる。 したがって、分解環$R_Z$は、期待通り、素数冪$q = p^l$を法とする整数の平文スロットを実現する。これにより、分解環R_Zのすべての次元を素数冪qを法とする整数の平文スロットとして使用できることになる。前述したように元々の剰余次数dは小さくはないので、スロット構造のこのスリム化により、素数冪qを法とする整数平文の同時並列な操作が大幅に効率化される。

ただし、円分環Rには、要素の加算/乗算とノイズ処理の双方をそれぞれ効率的に実装できる、魅力的な（ベクトル空間としての）基底が存在する。円分環Rの代わりに分解環R_Zを使用しても、同様のことができるだろうか？

円分環Rの実装上の優れた特性は、2 種類の基底の存在に集約される [3]。

- パワフル基底：互いにほぼ直交する短いベクトルで構成される。円分有理数を最も近い円分整数に丸め込むときに使用される。
- CRT 基底：FFT 変換と乗算に関連する。 2 つの円分整数が、それぞれ CRT 基底に関する係数ベクトルとして与えられると、それらの 2 つの円分整数の積は、成分ごとの積として効率的に計算できる。

我々は、Lyubashevsky、Peikert、および Regev [3]による、円分環を対象とした方法を拡張し、分解環R_Zの構造を調べ、その 2 種類の基底を構成した。η 基底と ξ 基底と呼ぶ。それぞれ円分環のパワフル基底と CRT 基底を置き換えることを意図している。 円分環Rから分解環R_Zへのトレース写像を用いて、分解環R_Zの構造を円分環Rの像として捉え、その平坦性（剰余次数$d = 1$）から現れる現象を観察した。 また、 [3]に従って、分解環R_Z内の要素の代数的操作（特に乗算）に伴うノルムの増加についてもその特性を明らかにした。

（3） 暗号の構成

上記の検討に基づいて、我々は分解環R_Z上の環準同型暗号スキームを構成した。分解環R_Z上で FV スキーム [4]を実現した DR-FV スキームと、分解環R_Z上で BGV スキーム [5]を実現した DR-BGV スキームからなる。 上記 η 基底と ξ 基底を用いて具体的にアルゴリズムを記述した。暗号文の準同型演算により増加するノイズの上限を示し、提案 DR-FV スキームと DR-BG スキームが共にセキュリティパラメーター λ について$q = O(\lambda \log\lambda)$の暗号文モジュラスを使用すれば、FV スキームや BGV スキームがそうであるように、完全準同型であることを証明した [4]。

安全性証明のためには、分解環上の決定バージョンの Ring-LWE 問題の困難性が必要となる。Ring-LWE 問題のサーチバージョンは、Lyubashevsky、Peikert、および Regev によって、すでに任意の数体のイデアル格子の近似最短ベクトル問題からの量子多項式時間の帰着があることが証明されている [5]。 彼らは、円分環についてのみ、Ring-LWE 問題のサーチバージョンと決定バージョン間の等価性を証明した。 ただし、分解環の場合も、円分環のときと同じ形の、素数の素イデアル分解をもつことから、サーチバージョンと決定バージョン間の等価性は同様に証明できる。以上より、分解環上の決定バージョンの Ring-LWE 問題は円分環上のそれと同等の困難性をもつことが期待できる。

（４） 実装とベンチマーク

C++言語を使用して提案準同型暗号化スキーム DR-FV および DR-BG を実装し、さまざまなパラメーター（表１）を使用していくつかの実装実験を行った。 その結果、本研究のη基底とξ基底が円分環のパワフル基底と CRT 基底を十分に置き換えることができ、提案準同型暗号化スキーム DR-FV（表３）および DR-BG（表４）が素数冪p^lを法とする整数演算について、従来の環準同型暗号スキームライブラリ HElib（表２）よりも、同程度のセキュリティパラメータにおいて数倍速いことが確認された。 実際、表 4 の par-131071 は、セキュリティパラメータλ= 84 の単一の DR-BGV 暗号文で 7710 個の2^lを法とする整数平文スロットを以下の速度で演算できることを示している：

（30.14、29.35、3.70、282.11、1678.52）.

一方、表 2 の par-8191 は、セキュリティパラメータλ= 92 で 7710/630=13 個の暗号文を用いて、同じ個数 7710 個の2^lを法とする整数平文スロットを演算できることを示しているが、これを 13 倍すると、

（395.85、2740.01、10.92、1397.89、6664.32）

となる。以上より、同程度のセキュリティパラメータの下で、DR-BGV スキームは HElib ライブラリよりも数倍高速であることがわかる。分解環のスロット構造に無駄がなく、並列性が数倍向上していることの効果である。

表１　選択パラメータ

	m	g	d	l	r (DR-FV)	r (DR-BGV)	r (HElib)
par-127	127	18	7	8	162	189	135
par-8191	8191	630	13	8	210	247	250
par-43691	43691	1285	34	8	234	258	256
par-131071	131071	7710	17	8	242	261	-

表２　HElib 実行速度

	λ	Enc	Dec	Add	Mult	Exp-by-2^8
par-127	26	0.23	0.18	0.00	0.66	4.78
par-8191	92	30.45	210.77	0.84	107.53	512.64
par-43691	237	268.00	5158.44	4.74	634.69	4187.81
par-131071	-	-	-	-	-	-

表３　DR-FV 実行速度

	λ	Enc	Dec	Add	Mult	Exp-by-2^8
par-127	-	0.14	0.12	0.00	0.57	4.47
par-8191	29	7.39	7.37	0.03	39.43	318.65
par-43691	32	17.38	17.19	0.11	92.14	741.42
par-131071	91	104.33	103.93	0.97	574.44	4620.22

表４　DR-BGV 実行速度

	λ	Enc	Dec	Add	Mult	Exp-by-2^8
par-127	-	0.06	0.08	0.00	0.54	3.53
par-8191	29	2.49	2.35	0.24	21.23	127.34
par-43691	32	5.17	5.19	0.59	50.85	293.52
par-131071	84	30.14	29.35	3.70	282.11	1678.52

一般に、環準同型暗号では、ノイズの大きさが関係する処理はパワフル基底で逐次的に計算し、乗算等の代数演算は成分毎の演算が可能な CRT 基底で行うというように、基底を変換しながら暗号化・復号・準同型演算を行う。分解環を用いる我々の方式では、従来の環準同型暗号に比べ、この基底変換が簡略化されるものの、やはり最もコストのかかる演算である。そこで、提案方式について、基底変換の FPGA 実装による高速化を目指し、実際に小規模の次元と暗号文モジュラスのケースを対象として基底変換処理の FPGA 実装を行った（表５）。その結果、ソフトウェアによる基底変換処理と比較したところ、わずかながら高速化を確認できた。次元を上げることにより、並列化の効果は顕著になることが期待される。

表５　FPGA による基底変換処理の実行

順序	処理内容	処理時間	詳細
1	初期化	0.255 ms	デバイスファイル Open write 制御コマンド 3 つ送信 デバイスファイル Close
2	計算対象ベクトルデータの送信	0.282 ms	デバイスファイル open write データコマンド送信 デバイスファイル close
3	基底変換計算の完了	0.389 ms	FPGA からの割り込み信号を受信
4	計算結果の受信	0.276 ms	デバイスファイル Open read データコマンド送信 デバイスファイル Close
	合計	1.202 ms	

引用文献

[1] C. Gentry, Fully homomorphic encryption using ideal lattices, Proc. Forty-first Annual ACM Symposium on Theory of Comput ing, STOC ’09, 2009.

[2] F. V. N. P. Smart, Fully homomorphic SIMD operations, Designs, Codes and Cryptography, April 2014, Volume 71, Issue 1, pp 57-81, 2014.

[3] C. P. O. R. Vadim Lyubashevsky, A Toolkit for Ring-LWE Cryptography, EUROCRYPT 2013, LNCS 7881, pp 35-54, 2013.

[4] J. F. a. F. Vercauteren, Somewhat practical fully homomorphic encryption, IACR Cryptology ePrint Archive, 2012-144, 2012.

[5] C. G. a. V. V. Zvika Brakerski, (Leveled) fully homo- morphic encryption without bootstrapping, ITCS, pages 309-325. ACM, 2012.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 ARITA Seiko、HANDA Sari	４．巻 E103.A
２．論文標題 Fully Homomorphic Encryption Scheme Based on Decomposition Ring	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 195～211
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019CIP0027	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 Arita S., Handa S.	４．巻 LNCS 10779
２．論文標題 Subring Homomorphic Encryption	５．発行年 2018年
３．雑誌名 In: Kim H., Kim DC. (eds) Information Security and Cryptology - ICISC 2017.	６．最初と最後の頁 112-136
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-78556-1_7	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0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

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	半田　沙里 (Handa Sari) (10748479)	情報セキュリティ大学院大学・その他の研究科・研究員 (32721)	
研究分担者	小崎　俊二 (Kozaki Shunji) (80626961)	情報セキュリティ大学院大学・その他の研究科・研究員 (32721)	