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　 ９ 月 １９ 日現在

機関番号：１２１０１
研究種目：基盤研究(C)（一般）
研究期間：2012～2015
課題番号：２４５００００４

研究課題名（和文）秘密鍵の漏洩に対し安全な公開鍵暗号系に関する研究

研究課題名（英文）Study on leakage resilient public-key encryption schemes

研究代表者
黒澤　馨（Kurosawa, Kaoru）

茨城大学・工学部・教授

研究者番号：６０１５３４０９

交付決定額（研究期間全体）：（直接経費）　　4,000,000円

研究成果の概要（和文）：秘密鍵の一部が漏洩したとしても安全性が保たれるような暗号方式を、leakage resilient 暗号方式という。本研究では、まず、universal hash proof systemを基に、leakage resilient でかつCCA安全（選択暗号文攻撃に対し安全）な公開鍵暗号方式を構成する一般的な方法を示した。次に、漏洩レートがほぼ1となるCPA安全（選択平文攻撃に対し安全）なIDベース暗号方式、および内積暗号方式を開発した。さらに、それらを連続メモリleakageモデルに拡張した。また、上記の成果を基に、従来より効率のよい匿名IDベース暗号方式を開発した。

研究成果の概要（英文）：An encryption scheme is called leakage resilient if it is secure even if a part of the secret key is leaked.
First I showed a general construction method of leakage resilient CCA secure (secure against chosen ciphertext attack) public-key encryption schemes based on universal hash proof systems. Next I constructed a CPA secure (secure against chosen plaintext attack) ID-based encryption scheme and an inner product encryption scheme such that the leakage rate is almost 1. They are generalized to the continuous memory leakage model. Further based on these results, I showed an efficient anonymous ID-based encryption scheme.

研究分野：現代暗号理論

キーワード：公開鍵暗号　IDベース暗号　内積暗号　鍵漏洩

１．研究開始当初の背景

暗号装置の動作状況を様々な物理的手段で観察することにより、装置内部の秘密鍵情報を盗みとろうとする敵の攻撃方法を、サイドチャンネル攻撃と呼ぶ。具体的には、装置の計算時間を解析しそれから秘密鍵情報を盗み取るタイミング攻撃、消費電力を解析する電力解析攻撃、レーザー光線などで一時的に装置を誤動作させそれを利用して秘密鍵情報を盗み取る故障利用攻撃、装置から発生する電磁波を解析する電磁波解析攻撃、キャッシュメモリの状態を解析するキャッシュ攻撃などが知られており、1990 年代後半から盛んに研究されている。

サイドチャンネル攻撃の研究が始まった初期のころ、理論研究者はこれを自分たちの研究分野とはみなさず、冷淡であった。しかし、2009 年に Goldwasser らは、秘密鍵の漏洩量がある値以下であるならば、格子理論に基づく Regev の公開鍵暗号及び Gentry らの ID ベース暗号は、どのようなサイドチャンネル攻撃に対しても安全であることを理論的に証明した。このように、どのようなサイドチャンネル攻撃に対しても安全であることが理論的に証明された暗号方式は、leakage resilient な暗号方式と呼ばれる。2009 年以降、leakage resilient な暗号方式の研究が活発かしてくる。

上記で述べた格子理論に基づく暗号方式は、公開鍵サイズ、暗号文サイズが大きく、効率が非常に悪い。これに対し、たとえば、Naor と Segev は、実用的な効率性を有する leakage resilient 公開鍵暗号方式をいくつか構成した。

２．研究の目的

本研究の目的は、従来より効率的、かつ漏洩レート（＝漏れてもよい秘密鍵のビット数/秘密鍵のビット数）が１に近いような公開鍵暗号方式、ID ベース暗号方式、および機能型暗号方式を開発することである。

３．研究の方法

日頃、共同研究を行っている情報通信機構(NICT)の野島良研究員や Le Trieu Phong 研究員らと密接に議論を重ね、研究打ち合わせを行うことにより、研究目的を達成する。また、現代暗号理論に関するトップレベルの国際会議に出席して最新の研究成果を収集すると共に、当分野における一流の研究者と討論を行う。

４．研究成果

(1) Leakage resilient な公開鍵暗号方式の開発

0 の暗号文と 1 の暗号文を区別できないような公開鍵暗号方式を、選択平文攻撃(Chosen Plaintext Attack)に対し安全な(IND-CPA 安全な)暗号方式、敵が復号オラクルにアクセスできたとしても 0 の暗号文と 1 の暗号文を区別できないような公開鍵暗号方式を、選択暗合文攻撃(Chosen Ciphertext Attack)に対し安全な(IND-CCA 安全な)暗号方式という。

さらに、秘密鍵の一部が漏洩したとしても IND-CPA 安全な公開鍵暗号方式を IND-lrCPA 安全、秘密鍵の一部が漏洩したとしても IND-CCA 安全な公開鍵暗号方式を IND-lrCCA 安全と呼ぶことにする。

Naor と Segev は、判定 Diffie-Hellman 仮定(DDH 仮定)に基づき、 IND-lrCPA 安全な公開鍵暗号方式、および IND-lrCCA 安全な公開鍵暗号方式を示した[1]。彼らは、まず、ユニバーサル１ハッシュ証明システムを利用し、IND-lrCPA 安全な方式を構成した。次に、IND-CPA 安全な公開鍵方式から IND-CCA 安全な公開鍵暗号方式を構成する一般的な方法である Naor-Yung パラダイムを基に、IND-lrCPA 安全な方式から IND-lrCCA 安全な方式を構成する一般的な方法を示した。

しかし、後者の方法は、非対話型ゼロ知識証明を利用するため、非常に効率が悪い。そこで、彼らは、DDH 仮定の下で IND-CCA 安全な実用的公開鍵暗号方式である Cramer-Shoup 暗号について検討し、この方式が 1/6 の漏洩レートを有する IND-lrCCA 安全な公開鍵暗号方式であることを示した。

Dodis らは、漏洩レートが１に近い IND-lrCCA 安全な公開鍵暗号方式示したが、効率は非常に悪い[2]。

本研究では、まず、ユニバーサル 1 ハッシュ証明システムの拡張である「補助入力を有するユニバーサル 2 ハッシュ証明システム」から IND-lrCCA 安全な公開鍵暗号方式を構成する一般的な方法を示した。

次に、それを基に、判定合成数剰余仮定（Decision composite residuosity 仮定、DCR 仮定）に基づく方式と、判定線形仮定（Decision Linear 仮定、DLIN 仮定）に基づく方式の２つを具体的に示した。

前者は、DCR 仮定に基づく世界初の IND-lrCCA 安全な公開鍵暗号方式である。後者は、ペアリングという計算量の大きい演算を用いないという意味において世界初の DLIN 仮定に基づく IND-lrCCA 安全な公開鍵暗号方式である。

これらの方式は、Dodis らの方式[2]に比べると、漏洩レートは小さいものの、はるかに効率がよい。比較を表１に示す。

ただし、漏洩レートは、（漏洩してもよいビット数）/（秘密鍵のサイズ）によって定義される。また、δは 0 に近い実数である。

方式	漏洩レート	仮定
Naor-Segev [1]	1/6	DDH
Dodis ら [2]	1-δ	DLIN （ペアリング有り）
本研究(1)	1/12	DCR
本研究(2)	1/18	DLIN（ペアリ

		ング無し)

表 1. IND-lrCCA 安全な公開鍵暗号方式の比較

(2) Leakage resilient な ID ベース暗号および内積暗号の開発

ID ベース暗号方式(IBE)においては、任意のビット列を公開鍵として利用できる。この分野は非常に活発に研究されてきており、ペアリングに関連する仮定、平方剰余仮定、格子に関連する仮定などの下でいくつかの IBE 方式が提案されている。Akavia ら、および Alwen らは、これらの IBE 方式を少し変形すると、leakage resilient になることを示した。しかし、その安全性は、ランダムオラクルモデルか、標準モデルにおける非静的仮定に基づいてのみ証明されている。また、Chow らは、仮定の下で漏洩レートが 1/3 となる leakage resilient な IBE 方式を示している[3]。

内積暗号方式(IPE)は、IBE の拡張であり、受信者の秘密鍵は述語ベクトル id に依存し、送信者は平文および属性ベクトル u をもとに暗号文を計算する。受信者は、u と id の内積がセロのときのみ、正しく復号できる。id=id'となることと(1,id)と (id',-1)の内積が 0 となることは等価なので、IPE を基に IBE を構成することができる。IPE は、IBE のみならず、多くの応用を有することが知られており、機能型暗号と呼ばれる暗号方式のクラスの重要な一部を形成している。

本研究では、まず、DLIN 仮定の下で、漏洩レートが 1 に近い IBE を開発した。従来の leakage resilient IBE との比較を表 2 に示す。

IBE 方式	仮定	漏洩レート
Chow ら[3]	DBDH	1/3-o(1)
Lewko ら[4]	1,2,3	1/3-o(1)
本研究	DLIN	1-o(1)

表 2. Leakage resilient IBE

次に、leakage resilient な IPE を世界で初めて構成した。漏洩レートは 1 に近く、DLIN 仮定の下で selectively-secure である。

一方、Brakerski らは、連続漏洩モデル(continual memory leakage model, CML model)を導入し、同モデルにおいて selectively secure IBE 方式を示した[5]。本研究では、上記の本 IBE 方式を少し修正すると、CML モデルで fully secure になることを示した。同様に、CML モデルで selectively secure となる IPE 方式を示した。

方式	安全性	漏洩レート
Brakerski ら[5]	selective	1/2-o(1)
本研究	full	1/2-o(1)

Table 3. IBE in the CML model

Boneh, Raghunathan および Segev は、本研究で開発した leakage resilient な IBE 方式を基に、function private IBE を構成している [6]。

(3) k-LIN 仮定に基づく効率のよい ID ベース暗号の開発

k-LIN 仮定は DLIN 仮定の一般化であり、k=2 の場合が DLIN 仮定に一致する。従来、k-LIN 仮定に基づく IBE においては、秘密鍵、および暗号文のオーバーヘッドは 2k+2 個の群要素[8]、または 2k+1 個の群要素[9]を必要とする。

一方、各 ID の秘密鍵から ID に関する情報が漏れないような IBE 方式を function-private IBE (FP-IBE)方式という。Boneh らは、DLIN 仮定の下、秘密鍵、および暗号文のオーバーヘッドが 6 個の群要素となる FP-IBE 方式を示した[6]。

本研究では、(2)で開発した IBE 方式を基に、k-LIN 仮定の下、秘密鍵、および暗号文のオーバーヘッドが 2k 個の群要素となる IBE 方式を開発した。同様に、DLIN 仮定の下、秘密鍵、および暗号文のオーバーヘッドが 4 個の群要素となる FP-IBE 方式を示した。

方式	暗号文サイズ	仮定
Lewko [7]	$6\|G\|+\|G_T\|$	2-LIN
Kurosawa ら[8]	$6\|G\|+\|G_T\|$	2-LIN
Blazy ら[9]	$(2k+1)\|G\|+\|G_T\|$	k-LIN
本研究	$2k\|G\|+\|G_T\|$	k-LIN

Table 4. IBE 方式の比較

方式	暗号文サイズ	仮定
Boneh ら[6]	$8\|G\|+\|G_T\|$	2-LIN
本研究	$4\|G\|+\|G_T\|$	2-LIN

Table 5. FR-IBE 方式の比較

<引用文献>

[1] M. Naor and G. Segev, Public-key cryptosystems resilient to key leakage, in:CRYPTO 2004, pp.18-35.

[2] Y. Dodis, K. Haralambiev, A. López-Alt and D. Wichs, Efficient public-key cryptographyin the presence of key leakage, ASIACRYPT 2010), pp.613-631.

[3] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters. Practical leakage-resilient identity-based encryption from simple assumptions. ACM CCS 2010, pp.152-161.

[4] A. B. Lewko, Y. Rouselakis, and B. Waters. Achieving leakage resilience

through dual system encryption. In TCC 2011, pp.70-88.
[5] Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, Vinod Vaikuntanathan: Overcoming the Hole in the Bucket: Public-Key Cryptography Resilient to Continual Memory Leakage. FOCS 2010: pp.501-510
[6] Dan Boneh, Ananth Raghunathan, Gil Segev: Function Private Subspace Membership Encryption and Its Applications. ASIACRYPT (1) 2013, pp. 255-275
[7] A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. EUROCRYPT 2012, pp.318-335
[8] Kaoru Kurosawa, Le Trieu Phong: Leakage Resilient IBE and IPE under the DLIN Assumption. ACNS 2013, pp.487-501
[9] Olivier Blazy, Eike Kiltz, Jiaxin Pan: (Hierarchical) Identity-Based Encryption from Affine Message Authentication. CRYPTO (1) 2014, pp.408-425.

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 Kaoru Kurosawa, Ryo Nojima, Le Trieu Phong: New leakage-resilient CCA-secure public key encryption. Journal of Mathematical Cryptology, 査読有, 7(4), pp.297-312 (2013)

〔学会発表〕（計 3 件）

① Kaoru Kurosawa, Le Trieu Phong: IBE Under k -LIN with Shorter Ciphertexts and Private Keys. ACISP 2015, 査読有, pp.145-159 (2015)
② Kaoru Kurosawa, Le Trieu Phong: Kurosawa-Desmedt Key Encapsulation Mechanism, Revisited. AFRICACRYPT 2014, 査読有, pp.51-68 (2014)
③ Kaoru Kurosawa, Le Trieu Phong: Leakage Resilient IBE and IPE under the DLIN Assumption. ACNS 2013, 査読有, pp.487-501 (2013)

６．研究組織

(1)研究代表者

黒澤　馨（KUROSAWA, Kaoru）
茨城大学・工学部・教授
研究者番号：60153409