様式 C-19

科学研究費補助金研究成果報告書

平成　23　年　6　月　10　日現在

機関番号：８２６２６
研究種目：研究活動スタート支援
研究期間：2009～2010
課題番号：２１８０００９４
研究課題名（和文）情報漏洩に強く実用的な検索可能公開鍵暗号方式に関する研究

研究課題名（英文）　On the Study of Practical Searchable Public-key Encryption with Leakage-Resilience

研究代表者
崔　洋　（SAI YOU）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・産総研特別研究員
研究者番号：５０５５１０２４

研究成果の概要（和文）：
誤り訂正符号を用いた秘密分散法を使用することによって、情報漏洩を防ぐ暗号が構成できることを示した。また本手法に基づいて構成された確定論的な暗号(Deterministic Encryption)が、ある種の情報漏洩を防ぐ性質を持つ、すなわち、秘密鍵の分散化によって部分的な情報漏洩に耐性を持たせることができる、ことを証明した。本確定論的な暗号を Private Information Retrieval（PIR）のデータベース検索技術に応用することで、検索速度等において、従来法よりも暗号化されたデータを効率的に検索できることを示した。

研究成果の概要（英文）：
By employing secret sharing techniques in terms of error-correcting codes, it is shown that the property of leakage-resilience could be achieved. As well, it is beneficial to make use of Deterministic Encryption to prevent information leakage. Provably in a mathematics way, Deterministic Encryption derived from error-correcting codes, is resistant to partially information leakage, because it is built in a secret sharing way. Furthermore, it is also shown that the new approach has achieved higher efficiency with PIR-based database searching techniques.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,130,000	339,000	1,469000
2010 年度	980,000	294,000	1,274,000
年度			
年度			
年度			
総　計	2,110,000	633,000	2,743,000

研究分野：工学
科研費の分科・細目：情報学基礎
キーワード：暗号と情報セキュリティ

１．研究開始当初の背景

近年、クラウドコンピューティングに代表される、大規模データベースのサービス提供やデータ保存アウトソーシングなどが、管理コストの削減やエネルギー消費削減の面から大変注目されている。現在、その普及の障害となっているのが、情報セキュリティに関する懸念である。企業の機密情報や個人情報を外部に配置し、他社に管理をゆだねることは、例えばデータベースの管理者が不十分な管理を行ったり、データを悪用したりするなどの問題が生じる可能性を意味している。現状、クラウド業者との契約による担保でこの問題への対処がなされているが、例えば情報漏洩事故が起きると、ネットワークに流出した個人情報は完全に消すことが事実上不可能であるなど、一旦事故が起こった場合に企業や個人が受けるダメージが大きいため、技術を用いた本質的な解決法がユーザサイドから強く望まれている。

本研究が対象としている、**検索可能公開鍵暗号方式**とは、例えばデータベースの外部サーバへの設置等で利用できる暗号方式である。この場合、サービスが提供される外部サーバには暗号化されたデータベースを置いて、サーバ事業者にはデータを読めない状態にしつつ、サーバ事業者がユーザから暗号化されたキーワード検索命令を受け取ると、ユーザが所望の対応するデータの暗号文を検索でき、ユーザに送り返すことができる、といった機能が実現できる。研究開始当時、本暗号方式についても盛んに研究が行われており、いくつかの方式が提案されていた。しかし、その内容は理論的なものにとどまっており、暗号方式導入による通信コスト増の評価等は十分でなく、それらのデメリットとアウトソースしたことのメリットの総合評価も明らかではなかった。

２．研究の目的

本研究の目的は、大規模データベースにおける管理者の不注意による情報漏洩や管理者自身の内部犯行に十分に対処できない問題に対し、耐情報漏洩（Leakage-Resilience）性質を満たし、かつ実用的な検索可能公開鍵暗号方式を構築することにある。本目的が達成されることにより、ユーザの持っているクラウドデータベースサービス等への懸念が払しょくできると考えられる。結果として、データベースのアウトソースが促進され、その市場の拡大、サーバ配置の最適化等による管理コストの減少、消費エネルギーの減少等が期待できる。

３．研究の方法

本研究では、まず現実の使用環境に即した問題設定における最強の安全性を定義する。次にその安全性を満たす確定論的な暗号の構成法について検討する。さらに実際に暗号を構成し、その暗号の効率を向上させる方法について検討する。

そしてこれら考察に基づいて構成された確定論的な暗号を、Private Information Retrieval（PIR）のデータベース検索技術に応用することで、従来法よりも暗号化されたデータを効率的に検索できる、検索可能公開鍵暗号方式を構成する。検索可能公開鍵暗号方式の安全性定義についても検討を行い、提案暗号方式が従来よりも高度な安全性を持っていることを数学的に証明する。

４．研究成果

本研究では、Boneh らによる PIR 手法とさまざまな組み合わせ論的手法を用いて構成された、これまで提案された中で最良と考え

られていた方式が、理論的には興味深い成果ではあるものの、特に計算コストの面で実際の使用環境では実装できない非常に効率の悪い方式であることを明らかにした。

現実の使用環境に即した問題設定における最強の安全性を定義し、その安全性を満たす効率のよい暗号の構成法について、IDベース暗号と呼ばれる特殊な公開鍵暗号、RFID (Radio Frequency IDentification) 等の非常に制限された計算資源でも実装可能な暗号技術等、いくつかの場合について検討を行った[2,3]。さらにその暗号の効率を向上させる方法について検討し、格子問題および符号理論問題に基づく暗号を構成した[5]。誤り訂正符号を用いた秘密分散法を使用することによって、情報漏洩を防ぐ暗号が構成できることを示した。また本手法に基づいて構成された確定論的な暗号が、ある種の情報漏洩を防ぐ性質を持つ、すなわち、秘密鍵の分散化によって部分的な情報漏洩に耐性を持たせることができる、ことを証明した。

本研究の主要な成果である、IEEE Globecom 2010で発表された論文“Practical Searching Over Encrypted Data By Private Information Retrieval”では、PIR のデータベース検索技術を用いて、符号理論に基づく秘密分散法を使用し構成された暗号化データベースの情報検索技術は、暗号化されたデータのまま、キーワードを効率的に検索できることを示した。また、計算速度も従来法より劇的に速いものであり、数学的に耐情報漏洩性が示されており、安全性と効率性を両立する非常に有用な技術である。本成果により、検索可能公開鍵暗号がより現実的なものとなったと言える。これは、本研究が行われたことにより、情報のアウトソースが安全に可能となったことを意味しており、安全・安心なネットワークサービス実現に大きな貢献を果たす重要な基礎技術であると結論付けられると考える。

その他、本研究の実行において、主要な目的以外にもいくつかの成果を挙げることができた。効率的な暗号の構成法の検討の中で、RFID のプライバシー保護技術の効率化や、中間者攻撃と呼ばれる能動的な攻撃にも安全な RFID 認証方式の提案[6]、確定論的暗号の一般的な構成法の提案[7]も行うなど、当初の予定よりも研究範囲を広げることができた。

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 7 件）

1. 吉田 怜、崔 洋、関野 智啓、繁富 理恵、大塚 怜、今井 秀樹、Practical Searching Over Encrypted Data By Private Information Retrieval 、 IEEE Press (Communications Society)、査読有、P1-5、2010.12

2. 関野 智啓、崔 洋、古原 和邦、今井 秀樹、Privacy Enhanced RFID Using Quasi-Dyadic Fix Domain Shrinking 、 IEEE Press (Communications Society)、査読有、1-5、2010.12

3. 阿部 正幸、崔 洋、今井 秀樹、Eike Kiltz、Efficient Hybrid Encryption from ID-Based Encryption、Designs, Codes and Cryptography、Vol.54、No.3、pp.205-240、査読有、2010.03

4. 関野 智啓、崔 洋、古原 和邦、今井 秀樹、Flexible Quasi-Dyadic の実装・評価に関する考察、IEICE Technical Report、2011.01

5. 関野 智啓、崔 洋、古原 和邦、今井 秀樹、プライバシを考慮した RFID 向け個別化公開鍵暗号方式の新たなモード、IEICE Technical Report、2011.01

6. 岡田 知己、崔 洋、古原 和邦、今井 秀樹、中間者攻撃に対して安全な HB＃ 認証方式の改良、IEICE Technical Report、2011.01

7. 崔 洋、Kirill Morozov、古原 和邦、今井 秀樹 、 Generic Constructions of Deterministic Encryption、IEICE Technical Report、2010.01

〔学会発表〕（計 2 件）

1. Practical Searching Over Encrypted Data By Private Information Retrieval、マイアミ、

IEEE Globecom 2010、2010 年 12 月
2. Generic Constructions of Deterministic Encryption、高松、2010 年 1 月

〔図書〕（計　1　件）
崔　洋、花岡　悟一郎、Applications of Signcryption　章、＜Practical Signcryption＞ Yuliang Zheng & Alex Dent、 Springer-Verlag、1st Edition.、XVIII、278p.
ISBN: 978-3-540-89409-4, November 2010.

〔その他〕
SCIS （Symposium on Cryptography and Information Security）2010年度、最優秀論文賞（Best Paper Award）

６．研究組織
(1)研究代表者
崔　洋　　（SAI YOU）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・産総研特別研究員
研究者番号：５０５５１０２４

(2)研究分担者
なし

(3)連携研究者
なし