

暗号理論とその応用

教授　尾形　わかは

研究分野：暗号、署名、暗号プロトコル

ホームページ: http://www.crypt.ict.e.titech.ac.jp/

●研究内容・目的

　情報化社会においては、情報を秘匿するための暗号、通信相手を確認するためのエンティティ認証、伝送される情報の完全性を保証するためのメッセージ認証が不可欠であり、すでにインターネットや携帯電話において情報やユーザの安全性を守るために、暗号技術が広く利用されています。また近年では、ブロックチェーン技術を用いた暗号資産など、単に情報を暗号化したり、相手を認証するためだけでなく、様々な機能の実現に暗号技術が応用されています。当研究室では、より高い安全性と利便性を持ったサービスを実現するためには、どのように暗号技術が利用可能であるのか、また、どのような弊害が起こり得るのか、それを解明する研究を行っています。

●主な研究テーマ

１．セキュアな委託計算

情報

情報を外部サーバへ

預けることで

利便性が増す

外部サーバから

情報が漏洩

○

×

通常の情報保存

サーバ管理組織に

対しても情報の

漏えいを防ぐ

○

検索などの操作が  
できない（利便性低下）

×

暗号化して保存

　近年では、多くの個人や企業が大量の情報を外部サーバに預けて保管し、またその情報の処理（検索や加工など）も外部の計算資源を利用して行うことが主流となりつつあります。ただ、組織における機密情報や、個人のプライバシー情報を外部に保存する場合は、外部サーバ管理者への漏えいリスクも考慮する必要があります。このような漏えいリスクは、情報の暗号化によって軽減することが可能ですが、一般に、暗号化された情報は、情報の検索や加工などの処理が不可能となり、利便性が大幅に低下します。

このような問題を解決する技術として、検索用インデクスを検索可能な状態で暗号化する検索可能暗号方式や、暗号化したままデータ処理が可能な準同型暗号などがあります。当研究室では、類似度の高い文書を検索する方式の安全性解析[2]や、完全準同型暗号を利用したプライバシー保護型データマイニングの研究などを行っています。また、暗号化した情報へのアクセスパターン解析による情報漏洩を防ぐための技術であるOblivious RAM方式に関する研究も行っています。

２．秘密分散法の応用

情報の紛失に備えるための一般的な方法としては、情報のバックアップがありますが、バックアップ数を増やすほど情報漏えいのリスクは増大します。秘密分散法とは、情報の紛失と漏えいを同時に防ぐことのできる暗号技術です。典型的な秘密分散共有法である「しきい値法」では、秘密情報から生成される複数の「シェア」は次の２つの性質を満たします。(a)あらかじめ定められた数（しきい値）のシェアからは元の秘密情報を復元できる、(b)しきい値未満のシェアからは元の秘密情報について何もわからない。このように生成したシェアを別々のサーバに保管することで、サーバに対するサイバー攻撃や災害の際にも、情報漏洩や情報紛失を防ぐことができます。

各情報を

復元することなく

統計量のみを復元

秘密分散法は、情報を安全に保存するだけでなく、分散された複数の情報の操作（統計処理など）ができるという利点も持っており、完全準同型暗号と同様に、プライバシーを保護したデータマイニングサービスなどへ応用可能です。尾形研究室では、決定木による分類を行う効率的な方式の構築[3]などを行っています。

３．高機能暗号・高機能署名の研究

　上で紹介した暗号技術以外にも、様々な付加的な機能の付いた公開鍵暗号やディジタル署名があります。当研究室では、秘密鍵の部分情報が漏えいしても高い安全性を保つことのできるIDベース暗号（メールアドレス等を公開鍵の代わりに用いることのできる暗号方式）[1]や、多数の署名を集約することで署名長を節約できる署名方式[4]などの研究を行っています。

●教員からのメッセージ

　安全な暗号方式を設計するには、必要な機能と攻撃者のモデル化、それらに基づいた厳密な証明が欠かせません。これらの暗号理論研究で得た能力は、暗号研究者だけでなく様々な分野の研究者や技術者になった時に役立つと思います。

●関連する業績、プロジェクトなど：

1. T. Tomita, W. Ogata, K. Kurosawa, R. Kuwayama, “CCA-Secure Leakage-Resilient Identity-Based Encryption without q-type Assumptions,”　IEICE Trans. on Fundamentals, Vol.E103-A, No.10, pp.1157-1166 (2020.10)
2. W. Ogata, T. Otemori, “Security analysis of secure kNN and ranked keyword search over encrypted data.” Int. J. Inf. Secure., vol. 19, issue 4, pp.419-425 (2020.8)
3. Ichikawa, W. Ogata, K. Hamada, R. Kikuchi, “Efficient Secure Multi-Party Protocols for Decision Tree Classification,”　Proc. of ACISP 2019: Information Security and Privacy, LNCS vol. 1547, pp. 362-380 (2019.7)
4. K. Hashimoto, W. Ogata, “Unrestricted and Compact Certificateless Aggregate Signature Scheme,” Inf. Sci., Vol.487, pp.97-114 (2019.6)