

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.security.mot.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、これらの技術が利用されています。このような暗号技術は、単に情報を暗号化したり、相手を認証するだけでなく、様々な機能の実現に応用することができ、一見、実現不可能であると思えることも可能となります。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。

●研究テーマ

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

○

検索できない

（利便性低下）

×

暗号化して保存

１．検索可能暗号方式の構築と評価

　近年では、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が、外部サーバに情報を保存することにより、情報漏洩のリスクが高まります。特に、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出す場合は、サーバ管理者への漏洩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、通常の暗号方式によって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ものの一つとして、情報の検索が可能であるように暗号化する検索可能暗号があります。

　当研究室では、サーバ管理者による検索結果の改ざんを検出可能な検索可能暗号や構築に関する研究や、安全性を段階的に定義し、各安全性レベルが保証される具体的な方式の構築を試みる研究などを行っています。

２．秘密分散法の安全性強化や応用研究

機密情報から複数の

シェアを作成し，

分散管理する．

一つのシェアが

紛失しても

機密情報は

復元可能

個々のシェアからは

機密情報は漏洩しない

情報の紛失に備えるための一般的な方法は、幾つかのコピーを保存しておくこと（バックアップ）ですが、コピーの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、秘密情報から幾つかの補助的な情報（＝シェア）が次の２つの性質を満たすように作成されます。(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。例えば、しきい値法を用いて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アタックや災害の際にも、情報漏洩や情報紛失を防ぐことができます。当研究室では、秘密分散法にユーザ認証の仕組みを組み込んだパスワード認証付き秘密分散法や、サーバによる情報改竄の検知などの機能を持つ秘密分散法の構築を行っています。

何らかの通信を

行うことで，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、保存し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、プライバシーを保護したデータマイニングなどのサービスへの応用が期待されています。原理的にはどんな演算も可能ですが、実用的には計算コストがかかりすぎるなどの問題点があるため、漏洩する情報を抑えつつ効率よく必要な演算を行う方法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

学術論文：

1. S. Taketani, W. Ogata, “Improvement of UC Secure Searchable Symmetric Encryption Scheme," Advances in Information and Computer Security, the 8th International Workshop on Security, IWSEC 2015, LNCS Vol. 9241, pp.135-152 (2015)
2. W. Ogata, H. Eguchi, “Cheating Detectable Threshold Scheme against Most Powerful Cheaters for Long Secrets,” Designs, Codes and Cryptography, Vol.71, No.3, pp.527-539 (2014)
3. T. Araki, W. Ogata, “A Simple and Efficient Secret Sharing Scheme Secure against Cheating,” IEICE Trans. on Fundamentals, Vol.E94-A, No.6 pp.1338-1345 (2011)