

研究概要

情報セキュリティは、情報社会を支える情報技術 (IT) の中で最も重要な要素技術の一つである。特に暗号技術を応用することにより、安全な通信インフラとして使われる暗号プロトコルを構築できる。例えば実際に使われている暗号プロトコルとして、SSL, IPsec, SSH などが有名である。これらを狭義的に見れば単なる安全な通信路にすぎないが、広義的な暗号プロトコルは実に多くの応用技術を持っている。例えば、電子決済方式、時刻認証システム、位置情報認証方式、電子公証人、電子投票/入札システムなどがある。これらの技術により、我々の社会活動がインターネット上などで電子的に実現され、より便利で豊かな電子社会が達成できる。

これらのセキュリティパラダイムを実現するために必要不可欠な技術として、公開鍵暗号とデジタル署名が上げられる。この2個の技術をなくして、上で述べた実りある応用技術を実現することはできない。面白いことに、これらのセキュリティコンセプトの安全性は、ある種の数学問題が困難であることに支えられている。例えば、素因数分解問題、楕円曲線上の離散対数、格子理論での最小ベクトル決定問題などが使われている。もし仮にこの基本問題が何らかの理由で破られた場合、この問題を基にして構成されているセキュリティシステム全体は全く安全でなくなることを意味する。情報セキュリティにおいて最も重要な研究テーマは、これらの数学問題の安全性を検証し、それらの問題がどのように暗号プロトコルにおいては情報セキュリティに影響を及ぼすかを考察することである。

セキュリティ技術を実社会で実現する際、安全なデバイスを用いてシステムを構築することが望まれる。特に、秘密鍵はICカードのような耐タンパー性に優れているデバイスに格納されることが多い。ここでデバイス上の実装が注意深く行われなかったとすると、攻撃者はデバイス内の秘密情報を簡単に破ることができるため、セキュアデバイス上での安全な実装技術もまた重要な研究テーマである。本研究室では、特に以下のトピックスについて研究を進める。

(1) ペアリング暗号 ペアリング暗号は従来の公開鍵暗号では実現が困難であった新たなセキュリティパラダイムが構成できるため、世界中で活発に研究が進展している分野である。代表的な例として、暗号文に含まれるキーワードを検索する技術 (暗号文キーワード検索技術)、暗号文の大きさが受信者の数によらず一定となるブロードキャスト暗号 (効率的なブロードキャスト暗号)、参加者のIDを利用して柔軟に暗号通信を行う技術 (ID ベース暗号) などがある。本研究では、ペアリング暗号の安全性および効率性を評価する。

(2) 安全性証明技術 暗号プロトコルの安全性を正確に判断するには、セキュリティモデルが必要となる。標準的なモデルとして、セマンティックセキュリティ (Semantic Security) が上げられる。安全性証明可能暗号とは、このようなモデルの上で数学的にその安全性が証明できるシステムのことを指す。安全性証明技術は、考察されるセキュリティモデル内では攻撃が不可能という保障があるため、理論的な意味を持つばかりでなく実用的にも重要な研究である。本研究では、現在および将来に使われる暗号プロトコルの安全性を研究する。

(3) 高速実装技術 我々はユビキタスコンピューティング世代の始まりに立っている。ユビキタスコンピュータは暗号技術と融合することにより、実りある応用技術をもたらしてくれると予想されている。だが、ユビキタスコンピュータは計

算資源が乏しいため (IC カードや RFID など)、セキュリティシステムで使われるメモリと速度をユビキタスデバイス向けに最適化する努力が必要である。本研究では、ユビキタスコンピュータ向けの新しい効率的な暗号アルゴリズムを設計することを目標とする。

「マス・フォア・インダストリ」にかかわる H20, 21 年度の研究実績概要

次世代の公開鍵暗号方式として、楕円曲線上の双線形写像を利用したペアリング暗号が注目を集めている。2008 年以降ペアリング暗号は、RFC5091, ISO/IEC15946-5, IEEE 1363.3 などの国際標準機関で標準化が進められてきた。ペアリング暗号の安全性は、楕円曲線上および有限体上の離散対数問題 (DLP) の計算量的困難性を根拠としている。本研究では、有限体上の DLP を漸近的に最も高速に計算可能な関数体篩法 (入力ビット長に対して準指数時間) を考察し、DLP の安全性の理論的解析および解読実験を行った。PC クラスタ (96 コア) を利用し、位数が 676 ビットの有限体 $GF(3^{426})$ 上の DLP を約 30 日で解読することに成功した。本解読結果は、2005 年の Joux-Lercier の従来記録を大幅に更新する解読世界記録であり、ペアリング暗号の電子政府への導入時期を検討するための重要な技術的根拠となった。

研究業績

1. Toshiya Nakajima, Tetsuya Izu, Tsuyoshi Takagi, “Reduction Optimal Trinomials for Efficient Software Implementation of the EtaT Pairing”, IEICE Transaction, Vol.E91-A, No.9, pp.2379-2386, 2008.
2. Jean-Luc Beuchat, Nicolas Brisebarre, Jeremie Detrey, Eiji Okamoto, Masaaki Shirase, and Tsuyoshi Takagi, “Algorithms and Arithmetic Operators for Computing the EtaT Pairing in Characteristic Three”, IEEE Transactions on Computers, Vol.57, No.11, pp.1454-1468, 2008.
3. 石黒司, 白勢政明, 高木剛, “ATmega128L 上でのペアリング暗号の高速実装”, 情報処理学会論文誌, Vol.49, No.11, pp.3743-3753, 2008.
4. Fagen Li, Masaaki Shirase, Tsuyoshi Takagi, “Certificateless Hybrid Signcryption”, The 5th Information Security Practice and Experience Conference, ISPEC 2009, LNCS 5451, Springer-Verlag, pp.112-123, 2009.
5. Eun-Kyung Ryu, Tsuyoshi Takagi, “A Hybrid Approach for Privacy-Preserving RFID Tags,” Computer Standards & Interfaces, Vol.31, No.4, pp.812-815, Elsevier, 2009.
6. 中島俊哉, 伊豆哲也, 高木剛, “素体上の超特異楕円曲線におけるペアリング暗号の効率的な計算手法”, 情報処理学会論文誌, Vol.50, No.7, pp.1745-1756, 2009.
7. 林卓也, 白勢政明, 高木剛, “ $GF(3^n)$ 上の関数体篩法の実装実験”, 情報処理学会論文誌, Vol.50, No.9, pp.1956-1967, 2009.
8. Kaoru Kurosawa, Tsuyoshi Takagi, “One-Wayness Equivalent to General Factoring”, IEEE Transactions on Information Theory, Vol.55, No.9, pp.4249-4262, 2009.
9. Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, Tsuyoshi Takagi, “Solving 676-bit Discrete Logarithm Problem in $GF(3^{6n})$ ”, 13th International Conference on Practice and Theory in Public Key Cryptography, PKC 2010, LNCS, Springer-Verlag, 2010.

プレプリント他

10. 古林靖規, 高木剛, “種数の大きな超楕円曲線上の指数計算法の計算機実験”, 情

- 報処理学会 コンピュータセキュリティシンポジウム, CSS 2009, pp.27-32, 2009.
11. 早坂健一郎, 高木剛, “素体 $GF(p)$ 上の数体篩法における多項式選択方法”, 情報処理学会 コンピュータセキュリティシンポジウム, CSS 2009, pp.33-38, 2009.
 12. 片山貴充, 高木剛, “連接キーワード検索可能な ID ベース暗号文キーワード検索可能暗号方式”, 情報処理学会 コンピュータセキュリティシンポジウム, CSS 2009, pp.577-582, 2009.
 13. 井山政志, 清本晋作, 福島和英, 田中俊昭, 高木剛, “BREW 携帯電話における R-ate ペアリングの実装”, 情報処理学会 コンピュータセキュリティシンポジウム, CSS 2009, pp.343-348, 2009.
 14. 丹羽弘和, 高木剛, 高橋修, “サーバなりすまし攻撃に対し安全な RFID セキュリティ方式”, 情報処理学会 コンピュータセキュリティシンポジウム, CSS 2009, pp.505-510, 2009.
 15. 坂本恭一, 林卓也, 高木剛, “オラクルを利用した離散対数問題に対する解読アルゴリズムの実装”, 2010 年暗号と情報セキュリティシンポジウム, SCIS2010, 4D2-4, 2010.
 16. 古林靖規, 高木剛, “種数の大きな超楕円曲線上の指数計算法の計算機実験”, 情報処理学会 コンピュータセキュリティシンポジウム, CSS 2009, pp.27-32, 2009.
 17. 佐々木廉, 丹羽弘和, 高橋修, 高木剛, “フォワードセキュアな RFID 距離制限プロトコルの提案”, 2010 年暗号と情報セキュリティシンポジウム, SCIS2010, 3E2-2, 2010.
 18. 早坂健一郎, 高木剛, “低 Hamming 重み標数の素体上における数体篩法の計算機実験”, 電子情報通信学会情報セキュリティ研究会, IEICE-ISEC2009-87, pp.53-60, 2010.

講演

1. 次世代 IT 社会のための暗号と情報セキュリティ技術に関する日台共同研究, 福岡, 2008 年 10 月.
2. グローバル COE 「計算世界観の深化と展開」発足イベント、暗号理論, 東京, 2008 年 12 月.
3. 安全な社会基盤への計算量的数論の応用, 福岡, 2009 年 3 月.
4. 電子情報通信学会情報通信基礎サブサイエティ合同研究会, 函館, 2009 年 3 月.
5. 中国電子科技大学情報科学部, 成都, 2009 年 4 月.
6. 暗号フロンティア研究会第 1 回研究会, JAIST, 2009 年 8 月.
7. 2009 International Workshop on Cryptography and Network Security, 台北, 2009 年 12 月.
8. 2009 Joint Meeting of the Korean Mathematical Society and the American Mathematical Society, ソウル, 2009 年 12 月.
9. Institute for Infocomm Research, シンガポール, 2010 年 1 月.

学位

Dr.rer.nat. (ダルムシュタット工科大学)

受賞歴

2009 年 4 月 船井情報科学振興賞

研究集会の主催

The 4th International Workshop on Security, IWSEC2009, TOYAMA Interna-

tional Conference Center, Toyama, Japan, October 28-30, 2009.

その他の特記事項

- ・2008-2009 年度 電子情報通信学会情報セキュリティ研究会専門委員
- ・2008-2009 年度 情報処理学会コンピュータセキュリティ研究会専門委員/運営委員
- ・2008-2009 年度 電子情報通信学会和文論文誌 A 編集委員
- ・2008-20010 年度 情報処理学会論文誌編集委員
- ・2008 年度 科学研究費補助金 第 1 段審査 (書面審査) 委員
- ・2008 年度 CRYPTREC ID ベース暗号 WG 主査
- ・2009 年度 CRYPTREC リストガイド WG 主査
- ・2009 年度 特許出願技術動向調査 (暗号技術) 委員
- ・国際会議プログラム編集委員 (26 件)

PKC2008, ANTS2008, ACISP2008, Pairing2008, SECRCRYPT2008, WISA2008, ACM-DIM2008, ICICS2008, CANS2008, ICISC2008, ARES2009, ISPEC2009, Pairing2009, SECRCRYPT2009, IWSEC2009, ProvSec2009, WISA2009, ACM-DIM2009, CANS2009, ICICS2009, ICISC2009, ACNS2010, SecureComm2010, CHES2010, IWSEC2010, ACM-DIM2010.