次世代暗号の安全性解析と高速実装アルゴリズムの開発

九州大学　マス・フォア・インダストリ研究所　教授
高木　剛

研究の背景

現代暗号は、インターネット上の電子決済やDVDの著作権保護技術など、安全な情報システムに不可欠な技術として広く普及しています。情報技術の飛躍的進歩に伴い、必要とされる暗号技術もより高度になっていますが、その中に、既存の方式では実現できなかった機能を備えたセキュリティ応用技術が達成可能となる「ペアリング暗号」があります。例えば、ペアリング暗号ではデータを秘匿したままキーワードを検索できるため、クラウドコンピューティングやビックデータの時代に適した暗号として産業界でも研究開発が活発に行われています。このように、ペアリング暗号への期待は大きいものがありますが、2001年の提案後も、(1)安全性の詳細な解析、(2)高速実装アルゴリズムの開発、の2課題の克服が実用化に向けての大きな障壁と考えられていました。

研究の成果

(1)安全性の詳細な解析：ペアリング暗号の安全性を解析することを目的に、最新の暗号解読アルゴリズムを用い、数百CPUコアレベルの大規模解読実験を行いました。解読に数十万年かかると見積もられていた923ビットのペアリング暗号を解読することに成功し、攻撃者の解読能力限界を見積ることが可能となりました。これは、2005年のフランス国防省等の解読記録を大幅に更新する、暗号解読の世界記録樹立となりました(図1,2)。

(2)高速実装アルゴリズムの開発： ペアリング暗号は既存暗号と比較して10倍以上も演算コストの負荷が大きいと報告されていました。本研究課題では、ペアリング暗号の数学構造に対して計算整数論の手法を駆使して、高速な演算方法を構築しました。汎用計算機、携帯端末、センサー端末などの実環境で高速実装可能なアルゴリズムを提案し、実際に高速に動作する実験データを得ました。

今後の展望

この成果は、一般ユーザーがネットショッピングやネットバンキング等のサービスをより安全に利用するための重要な一歩といえます。今回の暗号解読は、ペアリング暗号の安全な鍵長の詳細な評価や適切な暗号鍵の交換時期を見積もるための技術的根拠として活用できます。これにより、暗号に関する国際標準化機関等において安全な鍵長が決定され、産業界や電子政府において、将来に向けて安心したペアリング暗号が利用可能となります。また、多様な計算機環境の高速実装アルゴリズムの開発により、ペアリング暗号の実用化への道が拓かれました。

関連する科研費

平成22-24年度　挑戦的萌芽研究「大規模解読実験による公開鍵暗号の安全性解析」
平成22-24年度　基盤研究(B)「ペアリング暗号方式の基礎数理および実装方法の研究」

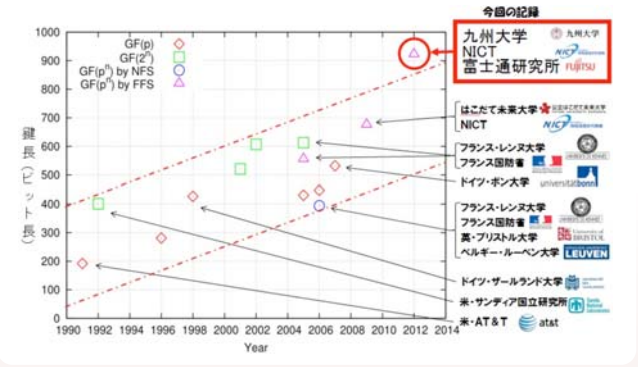

図1　ペアリング暗号解読世界記録の推移

図2　解読に用いた計算機

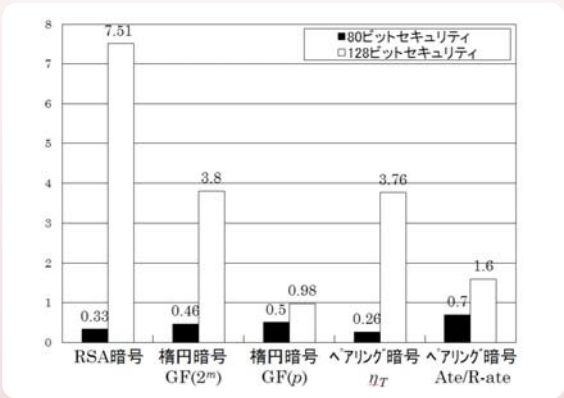

図3　携帯電話上(ARM9 225MHz)でのペアリング暗号の実行速度(秒)

(記事制作協力：日本科学未来館　科学コミュニケーター　小宮山　貴志)