参考資料

本研究の意義:

ネットショッピングやネットバンキング、公的機関への電子申請など、現代の情報システムでは機密情報を扱う場面が非常に多くなっています。これらのサービスを安心して利用できるようにするためには、暗号技術による情報セキュリティの確保が欠かせません。

近年、従来の公開鍵暗号では実現困難だった利便性が高く、様々なサービスに応用可能な新しい暗号として、「ペアリング暗号」を応用した「ID ベース暗号」や「検索可能暗号」、「関数型暗号」などの研究開発が盛んに行われています。一方で、ペアリング暗号はまだ歴史が浅く、安全性については検討が十分ではありませんでした。この暗号を安心して使うには、計算機の進歩などを考慮した上で、いつまで安全に利用できるかを精密に評価する必要があります。そのためには、暗号の安全性の根拠である「離散対数問題」について、解読に必要な計算資源や時間の検証・評価を理論・実験の両面から精密に行い、その結果から暗号の安全性を正確に知ることが必要です。

我々が挑戦した 278 桁長(923 ビット)のペアリング暗号は、従来、解読不可能と考えられており、開発段階で利用・普及への取組が数々行われていました。今回解読に成功したことで、278 桁長の鍵は脆弱であり、より大きな鍵を採用すべきことを意味すると同時に、解読に必要な計算資源や時間が正確に見積もられたことで、安全な暗号の選択や適切な鍵の交換時期を見積もるための技術的根拠となる、貴重なデータが得られたことを意味しています。今後、安心して使える暗号の境界値の導出については、引き続き研究を進めていく予定です。

図 1　既存暗号技術と新しい暗号技術の安全性

解読実験内容:

今回の離散対数問題の解の計算では、現時点で、最も高速な手段として知られている「関数体篩(ふるい)法」をベースとして用いました。この最新の解読技術に改良を加え、さらに利用する計算機の性能を最大限活かした実装を行うことで、解読に成功しました。今回の技術の特徴は、以下のとおりです。

1. 数式を使って初期値を最適化する技術

   実験に先立って、解読までに必要な計算機のパワーを、理論的に見積もることができる数式を新たに提案し、数多くの初期値から、最も少ないパワーで済むと予想される初期値を選択しました。

2. データ探索を二次元空間に拡張する技術

解読するには、答えの種となるデータを大量に探索する必要があります。このデータの探索に対し、従来の世界記録では「線形篩法」と呼ばれる一次元の空間を探索する手段が用いられていましたが、今回は、これを二次元空間の探索に拡張した「格子篩法」と呼ばれる方法に、更に独自に改良を施すことで、数十倍の高速化が得られました。

3. 膨大な数値データから方程式の解を高速に計算する技術

膨大な数値データから導かれる巨大な方程式について、「ランチョス法」と呼ばれる方法を使って解を求めました。計算機の性能に合わせてプログラムを最適化することで、数倍の高速化が得られました。

4. 計算機が持つパワーを限界まで引き出す並列プログラミング技術

最新の汎用計算機に搭載されている SIMD 演算を利用し、処理の並列度を限界まで高めたプログラミングを行いました。これによりおよそ数倍の高速化が得られました。

利用した計算機は NICT、九州大学、富士通研究所のサーバ 21 台、252 コアで、トータル 148.2 日間で解読に成功しました。これは、Intel Xeon プロセッサ 1 コアで、およそ 102 年の計算時間に相当します。

従来の結果との比較:

離散対数問題の解読は、従来から国内外のグループが挑戦してきました。下記の図は、主要なグループである「フランスの国防省及びレンヌ数学研究所のグループ」、「NICT 及びはこだて未来大学」について、解読に成功したビット数を今回の結果とともに一覧にまとめたものです。縦軸は、解読する問題の難しさを数式を使って算出した値です。このように、今回我々が計算に成功した記録 278 桁（923 ビット）は、従来の計算記録 204 桁（676 ビット）に比べ、およそ数百倍の難しさを持つ問題であり、従来の記録を大きく上回る結果となっています。

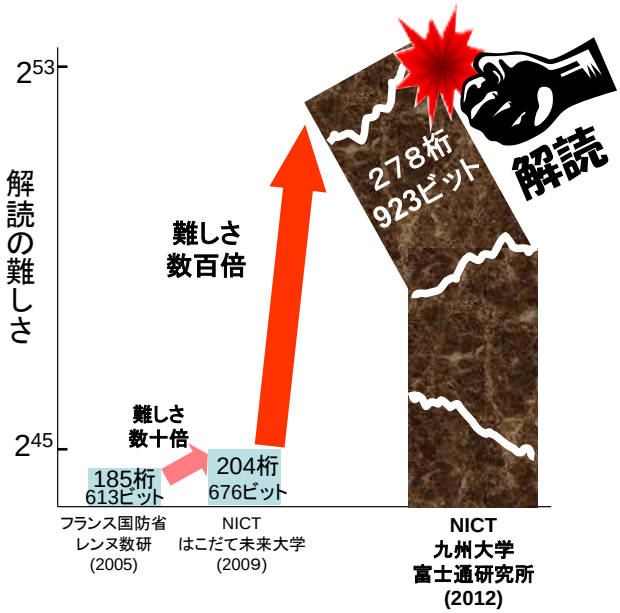

図2 離散対数問題ベース暗号解読世界記録

問題設定と解読結果:

問題の設定としては、まず、有限体 $GF(3^{97})$ を $GF(3)[x]/(x^{97}+x^{16}+2)$ として定め、超特異楕円曲線 $E(GF(3^{97}))$ $y^2=x^3-x+1$ 上の離散対数問題から、η_T ペアリングを用いて有限体 $GF(3^{582})$ 上の離散対数問題に変換したものを用います。次に、楕円曲線上の点を $Q_\pi=(Int(\pi)+4, y_\pi)$, $Q_e=(Int(e)+15, y_e)$ とします。ただし、$Int(\pi)$, $Int(e)$ は、それぞれ円周率 $\pi=3.14159...$、ならびに自然対数の底 $e=2.71828...$ を3進展開した値であり、Q_π, Q_e は、各々楕円曲線上の点の条件を満たす最も近い値を求めたものです。これは、問題の恣意性(問題の答えが事前に分かっていることが疑われる設定)を排除するために行いました。

以上の準備の下、η_T ペアリングの値を計算し、以下に示す有限体 $GF(3^{582})$ 上の離散対数問題の解読実験を実施しました。

$$\eta_T(Q_\pi, Q_e)^d = \eta_T(Q_\pi, Q_\pi)$$

計算機21台252コアを用い、148.2日かけて解読実験を行った結果、2012年4月24日に、以下の結果を得ることに成功しました。

$$d = 175279958485066813773020730619813142455096730 0$$

各組織の主な役割分担:

組織ごとの主な役割分担は、以下のとおりです。

1. NICT:計算時間短縮の理論構築・解読アルゴリズムのパラメータ最適化・計算機導入
2. 九州大:プロジェクト推進管理・プログラミング・計算機管理・実験実施
3. 富士通研:解読アルゴリズム設計・プログラム並列化・解読実験進捗管理

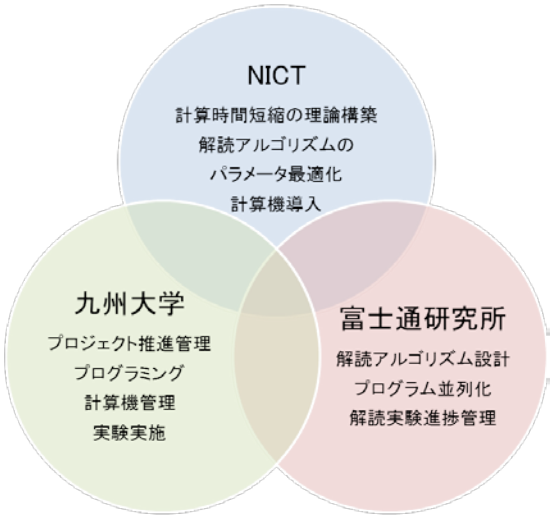

図 3 各組織の主な役割分担(産学官連携)