次世代暗号の解読で世界記録を達成

ーペアリング暗号の安全性を確立し次世代暗号の標準化に貢献ー

篠原 直行（しのはら なおゆき）
ネットワークセキュリティ研究所 セキュリティ基盤研究室 研究員

大学院博士後期課程修了後、2009年、NICTに入所。公開鍵暗号の安全性評価に関する研究に従事。
博士（数理学）。

はじめに

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。例えば、ネットショッピングでクレジットカード決済をする場合、利用者はクレジットカード番号などの機密情報を入力しクレジットカード会社へ送信します。この際にカードの機密情報を保護するために公開鍵暗号などの暗号化技術が使用されます。従って、このような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、利便性が高く、様々なサービスに応用可能な、クラウドに適した新しい暗号として、「ペアリング暗号[*1]」を応用した「関数型暗号」や「検索可能暗号」などの研究が盛んに行われています（図1）。例えば、クラウドストレージを利用したメールサービスにおいて、利用者の大量のメールが暗号化されてクラウド上に保持されているとします。それらのメールに対してキーワード検索をする場合に検索可能暗号を使用すれば、キーワードもメールも暗号化されたまま、一度も復号されることなく検索が実行されるため高度なプライバシー保護を実現できます。クラウドに適したこれらの暗号技術は従来の公開鍵暗号[*2]では実現困難であったため、ペアリング暗号は次世代の公開鍵暗号として注目されています。

ペアリング暗号の安全性とその評価方法

ペアリング暗号では、その高速実装技術や、「検索可能暗号」などの応用技術に関する研究成果が多く報告されているのに対して、その安全性の検証は十分になされていませんでした。そこで、NICT はペアリング暗号の実用化のために必要不可欠である安全性検証の研究を九州大学、（株）富士通研究所と共同で行いました。

ここでは、ペアリング暗号の安全性とその評価方法を簡単に説明します（図2）。ペアリング暗号の安全性は、離散対数問題[*3]を解く時間で見積もられます。特に、その安全性に関わる要素として、計算能力、解読理論、解読時間、鍵サイズがあります。計算能力とは計算機性能を示すもので、計算機の台数やコア数・コア性能で決定されます。また、鍵サイズはペアリング暗号のセキュリティパラメータで、鍵サイズが大きいほどペアリング暗号の解読に必要な時間が大きくなります。例えば計算能力が低い計算機環境で、効率の悪い解読理論を用い、解読にかける時間も短ければ解読する能力は

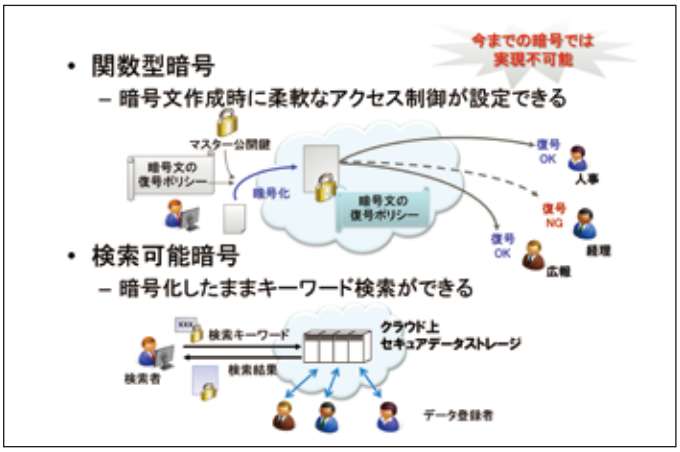

図1●ペアリング暗号への期待: クラウドへの応用

図2●ペアリング暗号の安全性評価（1）

図3●ペアリング暗号の安全性評価（2）

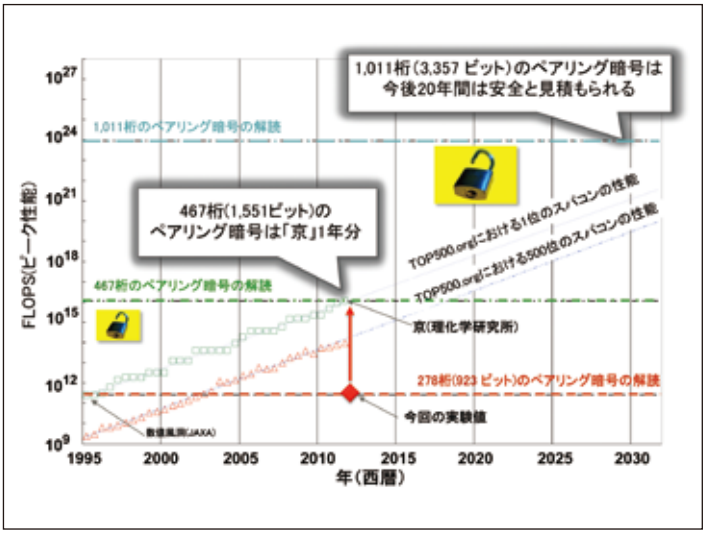

図4●安全なペアリング暗号の鍵サイズは?

小さいため小さい鍵サイズのペアリング暗号しか破ることができません。逆に計算能力が高く、解読理論の効率が良く、解読する時間も十分確保できれば大きな鍵でもペアリング暗号を解読することができます。そこで、安全な鍵サイズとは何かということになりますが、一般的には「世界最速のスーパーコンピューター」と「高性能な解読理論」を用いて「1年の解読時間」を要しても解読できない鍵サイズが安全な鍵サイズとされています（図3）。この安全な鍵サイズを見積もるために、具体的にはまず高性能な計算機を可能な限り集め、「高性能な解読理論」を構築し、可能な限り大きな鍵サイズに対して解読実験を行う、これはすなわち解読の世界記録の樹立に挑戦することになります。そしてそのときの計算時間や、そのとき使用した計算機環境と「世界最速のスーパーコンピューター」との比から、現時点で解読できる最大の鍵サイズが判明し、そのサイズより大きい鍵が安全な鍵であることが分かります。

ペアリング暗号の安全な利用を目指し、解読世界記録に挑戦

ペアリング暗号の安全な鍵サイズを見積もるために、我々は、これまで解読に数十万年かかり解読不可能と考えられてきた 278桁（923ビット）の鍵サイズを持つペアリング暗号の解読に挑戦しました。そして、新たな数学的な理論や高速実装技術を創出することで解読理論を改良し、汎用計算機21台（252コア）を用いて148.2日でそのサイズのペアリング暗号を解読することに成功しました。この世界記録達成の解読実験で得られたデータによって、現時点では467桁より大きい鍵サイズが安全であることが分かりました。さらに図4に示したように、今後の計算機性能の上昇予測を考慮すると、1,011桁の鍵サイズを持つペアリング暗号が今後20年間は安全であることが分かります。

今後の展望

今回の成果は、ペアリング暗号解読の世界記録が達成されただけでなく、安全なペアリング暗号の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。また、本成果は、わが国の電子政府や暗号に関する国際標準化機関等において、安全な暗号技術を利用するための根拠として活用され、次世代の暗号の標準化に役立てられます。

用語解説

＊1 ペアリング暗号
離散対数問題を安全性の根拠とする、2001年に開発された公開鍵暗号。従来の公開鍵暗号では実現困難であった、クラウドに適した様々な利便性の高い応用を、ペアリングと呼ばれる双線形写像を利用することで可能にしたため、次世代の暗号方式として注目されている。

＊2 公開鍵暗号
1976年にDiffieとHellmanによって提案された暗号。暗号化に用いる鍵と復号に用いる鍵を別に用意することで、暗号化に用いる鍵を公開（公開鍵と呼ばれている）することができる。代表的な方式としてRSA暗号や楕円曲線暗号がある。

＊3 離散対数問題
与えられた数値gとaに対し、gのd乗がaと等しくなるような整数d（対数値）を求める問題。