PRESS RELEASE

岡山大学
OKAYAMA UNIVERSITY

岡山大学記者クラブ
文部科学記者会
科学記者会　　御中

平成２９年８月１８日
岡　山　大　学

世界初！　IoT 時代の次世代暗号の解読で、114 ビット位数の楕円ペアリング暗号曲線に対する攻撃に成功

現代社会では機密情報を扱うことが多く、機密情報保護のために暗号技術が使われています。広く使われているRSA暗号※1や楕円曲線暗号※2は、大規模な解読実験によって安全性の厳密な評価がされてきました。IoT時代が到来した今、IoT機器などの相互認証を簡便にできたり、暗号化したままでデータ検索ができたりするなど、クラウドに適した次世代暗号技術として、楕円ペアリング暗号※3が注目され、IoT機器への実装が期待されています。しかしながら、その安全性について、大規模な解読実験による厳密な評価がこれまでされていませんでした。

岡山大学大学院自然科学研究科の野上保之教授、北九州市立大学の上原聡教授、東京農工大学の山井成良教授らの研究グループは、楕円ペアリング暗号について約3000コアもの計算機を用いた大規模な解読実験を実施。2^{114}（114ビット、10進数で35桁ほど）の大きさをもつペアリング曲線上の楕円離散対数問題※4の解読に成功しました。楕円ペアリング暗号を実現する楕円曲線を対象としたこの規模の解読成功は世界初です。本研究成果によって、楕円ペアリング暗号のさらに厳密な安全性の評価がなされることや、セキュリティ関連製品に搭載される暗号技術のセキュリティレベルの検討が必要になります。今回の解読攻撃成功の報告は、IoT時代を担う小型デバイスなどの情報セキュリティ確保に対して大きな一石を投じるものになります。

＜本研究成果のポイント＞

・情報セキュリティを高度かつ多機能に実現する次世代の暗号技術「楕円ペアリング暗号」の IoT 機器への実装が期待されている。一方、安全性の厳密な評価がされていなかった。
・本研究グループが楕円ペアリング暗号の大規模な暗号解読実験を実施。2^{114} の大きさをもつペアリング曲線上の楕円離散対数問題の解読に世界で初めて成功した。
・解読を成功したことで、今後は楕円ペアリング暗号のさらに厳密な安全性の評価がなされることや、セキュリティ関連製品に搭載される暗号技術のセキュリティレベルの検討が必要になる。IoT 時代を担う小型デバイスなどの情報セキュリティ確保に対して、大きな一石を投じるものになる。

＜背　景＞

現代社会の情報セキュリティ、とりわけユーザや機器を電子的に認証する機能を実現する暗号技術として楕円曲線暗号があります。その安全性の評価は、多数の計算機を並列に用いた楕円離散対数問題と呼ばれる数学的にも計算量的にも難解な問題の解読攻撃の成否

により評価されます。楕円離散対数問題は楕円曲線暗号の安全性の根拠でもあります。楕円曲線暗号に用いられる楕円曲線の中には、素数 2 を使う二値データをベースにするものと、それ以外の奇数素数を使う多値データをベースにするものがあり、とくに後者の分類での安全性の評価について、これまでに解読できた最大の大きさとして、探索対象の個数を 2^{113}（113 ビット、10 進数で 34 桁ほど）もつ楕円離散対数問題の解読に成功したという報告があります（2014 年、Erich Wenger, Paul Wolfger, Graz University of Technology）。

そして次世代の暗号技術、とりわけ IoT 機器への実装が期待される暗号技術として、楕円曲線暗号を高度に拡張したのが、楕円ペアリング暗号です。一方、楕円ペアリング暗号について、楕円離散対数問題の解読による厳密な安全性の評価報告はこれまでありませんでした（図１）。

＜業　績＞

本研究グループは、岡山大学や北九州市立大学、情報通信研究機構（NICT）StarBED の計算資源を活用して、楕円ペアリング暗号を実現する楕円曲線を対象に、探索対象の個数を 2^{114}（114 ビット、10 進数で 35 桁ほど）もつ楕円離散対数問題の解読に成功しました（図２）。楕円ペアリング暗号は、図３に示される (1) ～ (4) の 4 つの難問でその安全性が実現されていますが、楕円ペアリング暗号を実現する楕円曲線を対象とした (1) の問題に対しての、この規模の解読成功報告は世界初です。この解読攻撃の成功により、より厳密な安全性の評価がなされるとともに、セキュリティ関連の製品に搭載される暗号技術のセキュリティレベルの検討が必要になります。そのような意味でも、今回の解読攻撃成功の報告は、IoT 時代を担う小型デバイスなどの情報セキュリティ確保に対して大きな一石を投じるものになります。

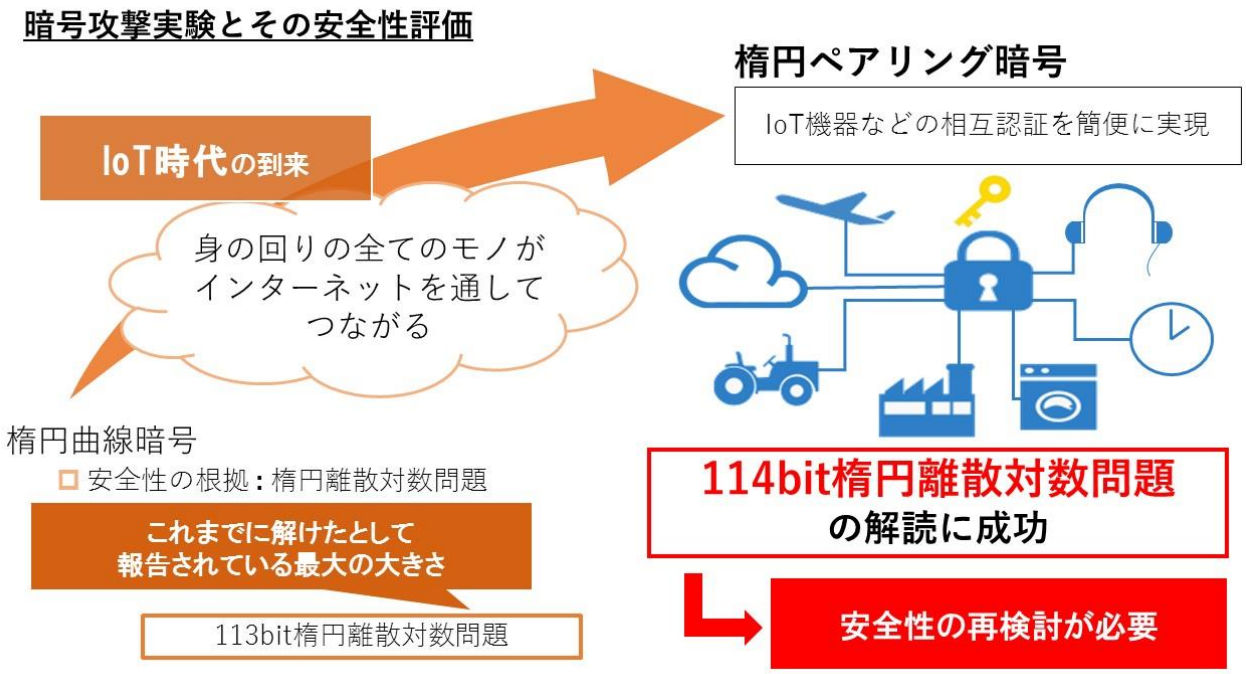

図１：IoT 時代を支える暗号技術

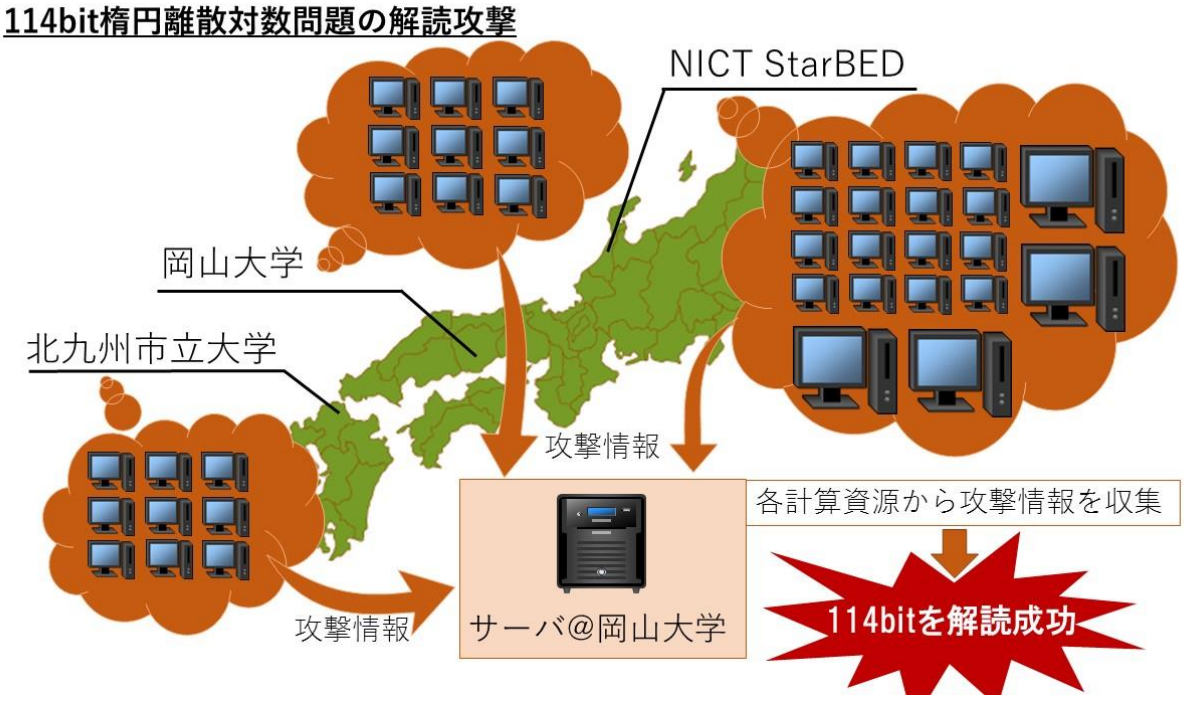

図２：本研究による大規模な並列解読攻撃

ペアリング暗号の安全性を支える 4つの数学的・計算量的な難問

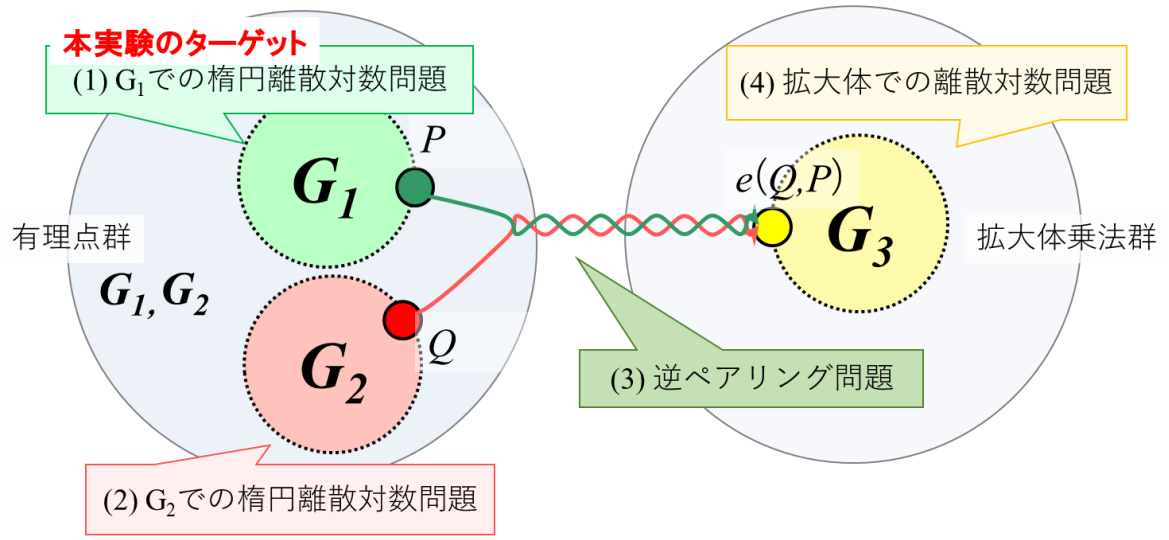

図３：楕円ペアリング暗号の安全性の根拠と本解読実験のターゲット

＜補足・用語説明＞

1）RSA 暗号

これまで広く活用されてきている公開鍵暗号の一つで、ユーザ認証など電子認証技術に活用されている。安全性の確保には、数千ビットという大きな空間が必要となる。素因数分解問題の困難性によってその安全性が担保されている。

2）楕円曲線暗号

RSA 暗号に比べ、数百ビットという小さな空間でも十分な安全性を担保できるとして、とりわけ IoT 時代のセキュリティ技術としてその活用が進んでいる。二値の数値空間を用いるものと、奇数素数を用いる多値の数値空間を用いるものに大別される。楕円離散対数問題の困難性によってその安全性が担保されている。

3）楕円ペアリング暗号

楕円曲線暗号を高度に拡張して実現される暗号であり、ID ベース暗号（メールアドレスなどで認証可能）、検索可能暗号（データを暗号化したままでのキーワード検索が可能）、匿名認証（個人情報を介さずにユーザを認証可能）などが実現できる。楕円離散対数問題など、4 つの数学的・計算量的な問題の困難性によってその安全性が担保されている。

4）楕円離散対数問題

楕円曲線暗号や楕円ペアリング暗号の安全性を担保するための数学的・計算量的に解くことが困難とされる問題である。これを現実的に解読が困難とするためには、2^{200} ～ 2^{300}（200～300 ビット、10 進数で 60～90 桁ほど）という大きな数値空間（その程度の大きな数値により加減乗除を行う空間）が必要となる。

本研究は、科学研究費補助金（25280047、研究リーダー：野上保之）による支援を受け、実施しました。

＜お問い合わせ＞
岡山大学大学院自然科学研究科（工）
教授　野上　保之
（電話番号）086-251-8127