StarBEDを活用した並列解読攻撃による次世代暗号「楕円ペアリング暗号」の安全性評価

研究テーマ　114ビット位数の楕円ペアリング暗号に対する大規模解読実験

研究実施機関　岡山大学

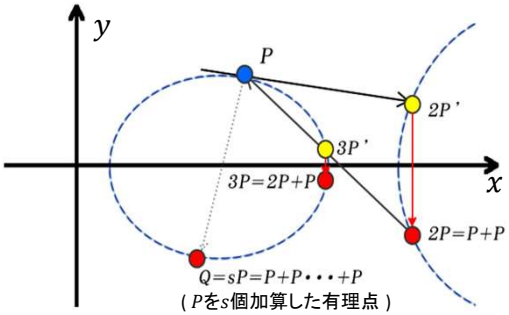
研究の概要

Internet of Things(IoT)の時代が到来し、小型デバイスの利用増加に伴って安全性担保の重要性が高まっている。
しかし、現在主流の公開鍵暗号であるRSA暗号で安全性を担保するために要求される暗号鍵の鍵長は非常に長いため、計算リソースが少ない小型デバイスに搭載する暗号としては適していない。そこで、小型デバイスでも実装可能な鍵長で安全性を担保することのできる楕円曲線暗号に対し、鍵長を114bitとして並列攻撃して安全性評価を行った。

NICT総合テストベッドを活用した研究成果

StarBED利用規模
物理ノード310台

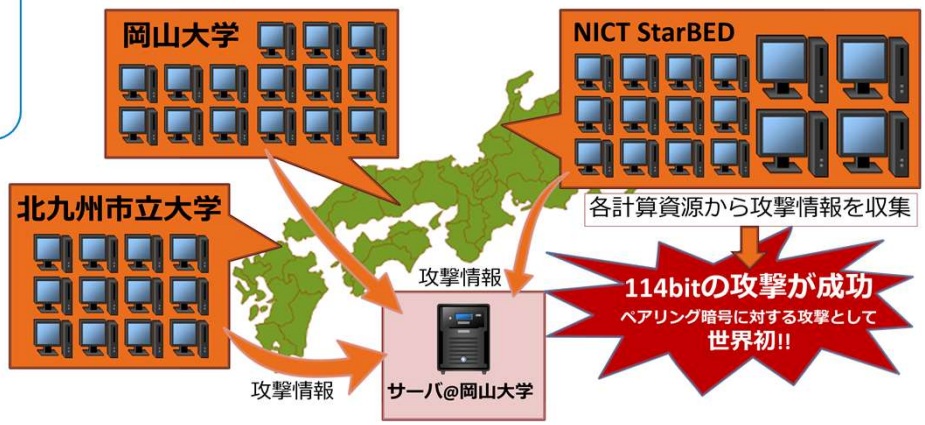
＜楕円曲線暗号の安全性＞



有理点の加算結果は2点を通る直線，または1点における接線と楕円曲線の交点のx軸上の対称の点

有理点PとQからsを求めるのは困難（楕円離散対数問題）

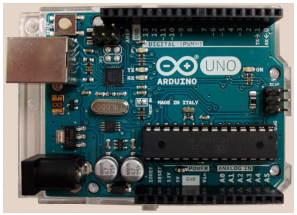
＜114bit楕円曲線暗号の解読攻撃＞



＜IoTデバイスへの搭載＞

	RSA暗号	**楕円曲線暗号**
鍵長	長い	**短い**
IoTデバイスに	搭載が困難	**搭載が容易**

IoTデバイスの一例



8bit汎用マイコンボード
「Arduino Uno」

今後の展望

114bitや112bitの実験結果を基に116bit位数の楕円ペアリング暗号に対する大規模な攻撃実験を行い，考察を深め，より緻密な安全性評価を行う。