114bit楕円曲線暗号の攻撃実験成功と今後の展望

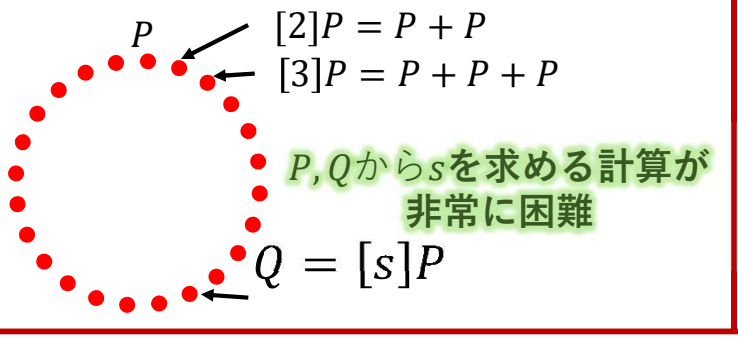
Successful attack experiment of 114 bit elliptic curve cryptography and Future work

岡山大学　野上 保之　日下 卓也　城市 翔　生田 健　小林 航也
北九州市立大学　上原 聡
東京農工大学　山井 成良

楕円曲線暗号の安全性の根拠

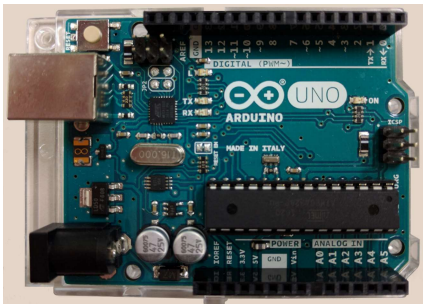
ECDLP（楕円曲線離散対数問題）

楕円曲線上の点P, Qについて
$Q = [s]P$を満たすsを求めること



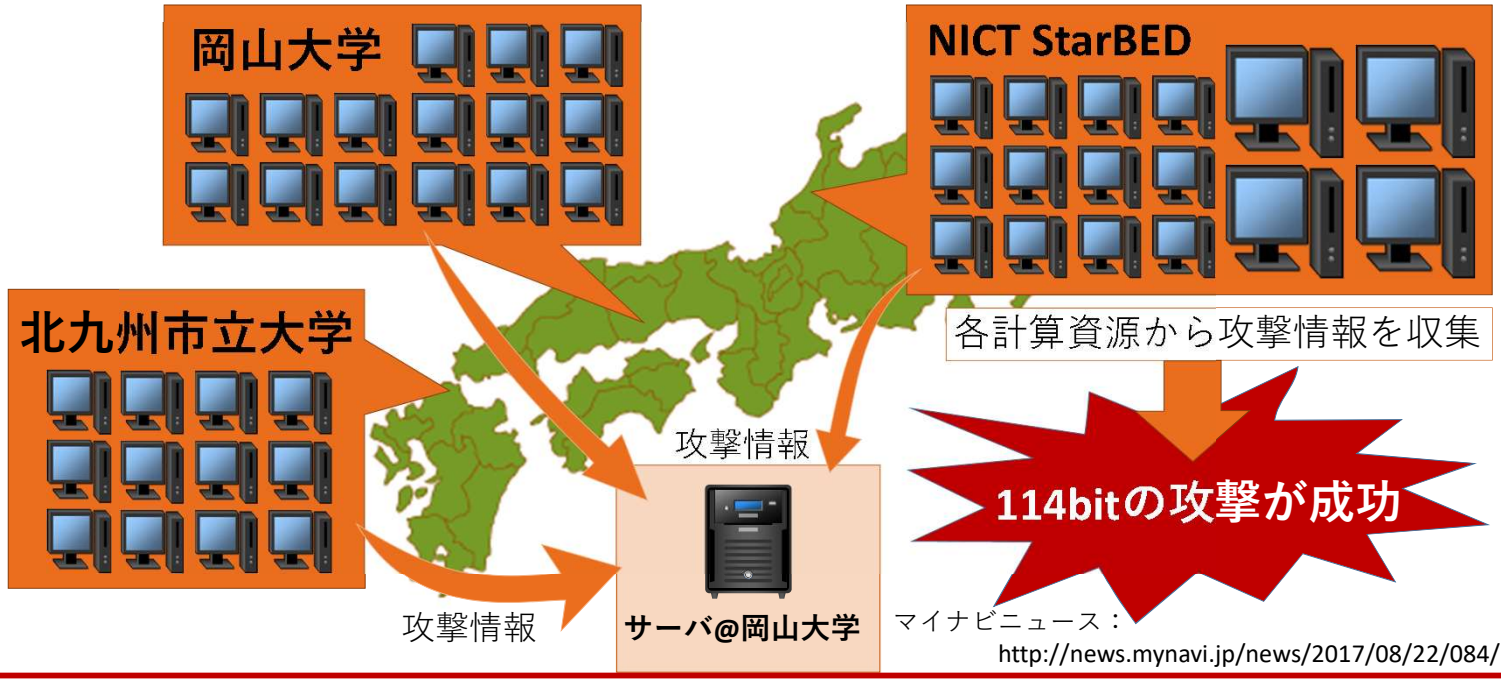
IoTデバイスへの搭載

	RSA暗号	楕円曲線暗号
鍵長	長い	短い
IoTデバイスに対し	搭載が難しい	**搭載が容易**



8bit汎用マイコンボード「Arduino uno」

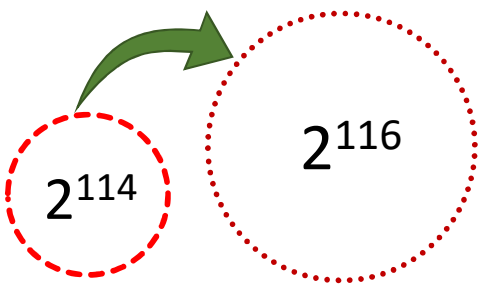
114bit楕円曲線暗号の攻撃実験



マイナビニュース：
http://news.mynavi.jp/news/2017/08/22/084/

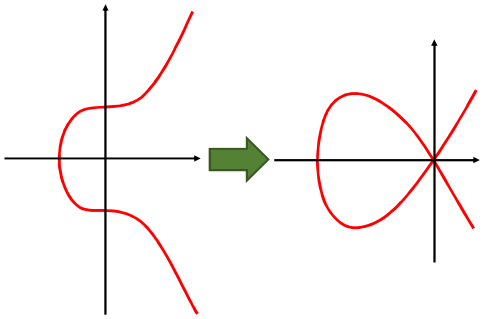
今後の展望

116bitの楕円曲線暗号に対する攻撃実験



Montgomery Curve など別の曲線に対する攻撃実験

(今回はBarreto-Naehrig Curveを使用)



Deep Learning を用いた秘密鍵の推定