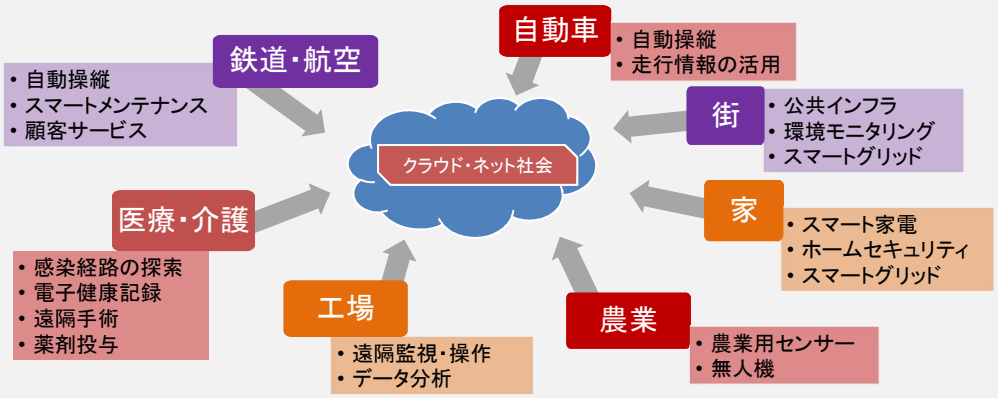
センサ・制御データのセキュアかつ高信頼な通信処理

Secure and highly reliable communication processing of a sensor and a control data

岡山大学　野上 保之　日下 卓也　梶谷 翔馬　城市 翔　生田 健

アルゴリズムレベルの安全設計

身の回りのあらゆる“モノ”がインターネットにつながる時代

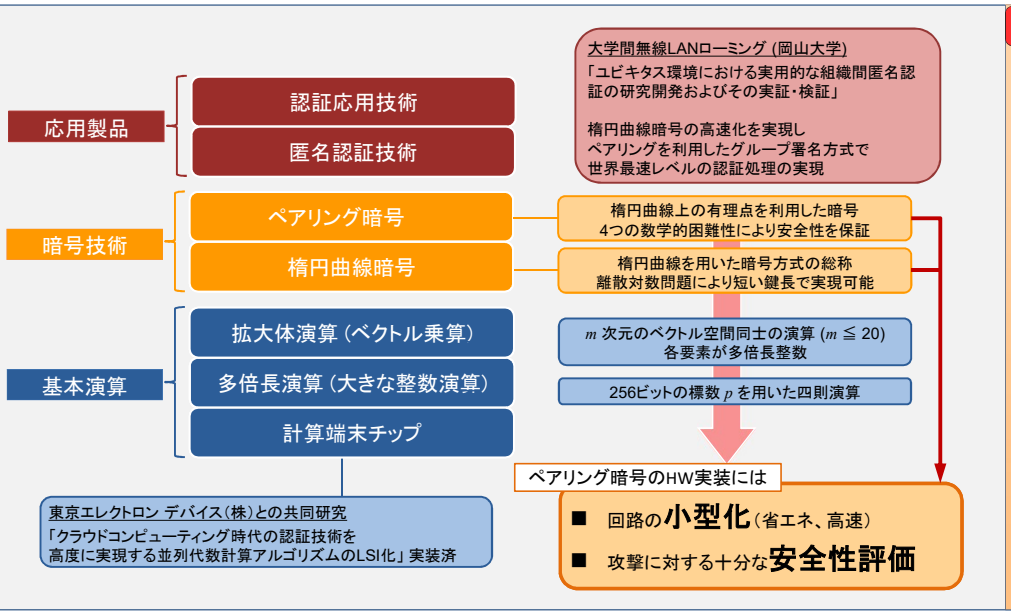


セキュリティ脅威

IoTデバイスの乗っ取り

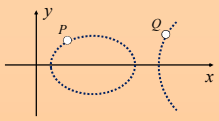
安全に情報を処理する技術が重要

複雑な数学



数学を用いた暗号

楕円曲線暗号

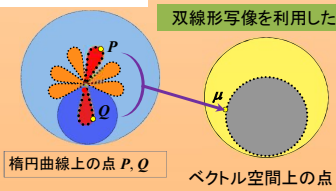


楕円曲線上の
離散対数問題により
安全性が保証される

$$y^2 = x^3 + ax + b$$

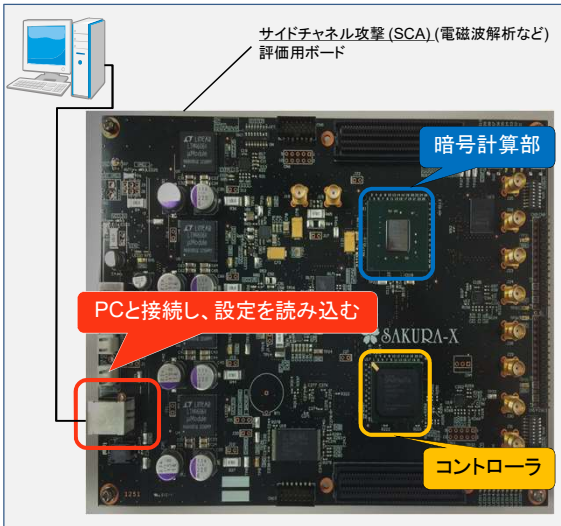
ペアリング暗号

双線形写像を利用した暗号



楕円曲線上の点 P, Q　　ベクトル空間上の点 μ

これら暗号技術の実用化に向けて
実際のHWを用いた安全性評価が必要



東京エレクトロン デバイス社製
暗号シミュレーションボード SAKURA-X

回路に含まれるアルゴリズム

CVMA
20次元までのベクトル乗算を求める

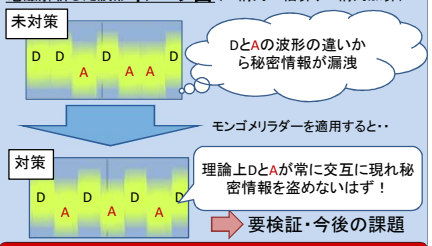
楕円スカラ倍算
楕円曲線上の有理点に対する演算
アフィン座標、射影座標、ヤコビアン座標に対応

モンゴメリラダー
アルゴリズム対称化によるSCA対策

幅広い埋め込み次数（1～20）の
セキュアなTatepペアリング暗号を実現

サイドチャネル攻撃対策

電磁解析した波形**イメージ図**（D:楕円二倍算、A:楕円加算）



開発状況と今後のスケジュール

楕円曲線暗号・ペアリング暗号　‥‥実装済

HW上でのデータを計測し、
理論値との比較を行う

安全性評価・活用へ

研究開発用に回路データ(verilog)を
無料公開予定！

安全性評価のための楕円曲線暗号攻撃実験

ECDLP（楕円曲線離散対数問題）

楕円曲線$E: y^2 = x^3 + ax + b \quad a, b \in F_p$

Eを満たす有利点の集合をG_rとすると

$G_r \triangleq \{(x, y) | x, y, a, b \in F_p, y^2 = x^3 + ax + b\}$

点$P, Q \in G_r$について
$Q = [s]P$を満たすsを求めること

$$[s]P = \underbrace{P + P + P + \cdots + P + P}_{s\text{ 個の }P}$$

計算が非常に困難

解読手法

PollardのRho法

ランダムウォークによる点生成をおこない
秘密鍵 s を求める

$$R_n = \begin{cases} [a_n]P + [b_n]Q & 0 \le n < l \\ R_{n-1} + R_{f(R_{n-1})} & l \le n \end{cases}$$

$f(x) \in [0, l-1]$

$$if: R_n = R_m \quad s = \frac{a_m - a_n}{b_n - b_m} \quad (b_n \neq b_m)$$

期待値：$\sqrt{r}$

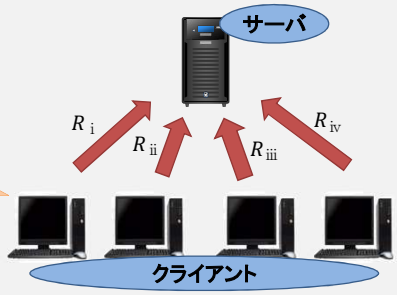
（ランダムスカラ法における期待値：$\frac{r}{2}$ ）

PollardのRho法を用いた暗号攻撃プログラム

Rho法の特徴
- 点生成1回の計算量が楕円加算1回
- **並列化が容易**
- 効率的な手法とされている

暗号攻撃プログラム
1. クライアント側でランダムな点生成を行い生成した点をサーバ側に送る
2. サーバ側で送られてきた点を保存しこれまでに保存した点と衝突判定を行う
3. 点が衝突するまで1,2を繰り返す

並列化
各クライアントPCにそれぞれ異なるランダムな初期点を与えることで各PCが別々のランダムウォークを行うため並列化による点生成が容易に可能



成果と現行の実験

暗号攻撃プログラムの効率化
楕円加算における
Montgomery Multiplication を最適化
=> **従来より性能が26%改善！**

他大学と連携した大規模実験
大学の長期休暇等を利用し
岡山大学のPC（約500コア）と
北九州市立大学のPC（約1000コア）を暗号攻撃実験に使用

解読に成功すれば世界記録となる114bitのECDLPに対して攻撃実験を実施中

今後の予定

NICT（国立研究開発法人情報通信研究機構）総合テストベッドとの連携により
最大2000コア程度の計算リソースを用いた大規模暗号攻撃実験を計画中

新たな暗号攻撃手法

Webベース暗号攻撃

Webページを開くだけで攻撃に参加可能
- 攻撃プログラムをWebアプリとしてWebブラウザ上で実行
- 計算機のプラットフォームに非依存

攻撃プログラムのWebアプリ化
暗号攻撃プログラムを
Webブラウザ上で実行可能な形式で実装
=> **Native Client** を利用して高速化

Native Client によるWebアプリの高速化
- C/C++のコードを専用のコンパイラを用いてブラウザ上で実行可能な形式に変換
- クライアント計算環境のOSに依存せず実行可能
- JavaScriptによる実装と比較して**約6倍高速**に実行可能

スマートフォンアプリを利用した攻撃

攻撃プログラムのスマートフォンアプリ化
- 暗号攻撃プログラムをスマートフォン上で実行可能なJavaで書き換える
- 点生成をスマートフォン上で行う

暗号攻撃プログラムの効率化
ランダムな点生成において楕円加算を効率的に行うための手法として
Montgomery Multiplication と
Montgomery Trickを用いた
=>**27bitにおける計算時間を約1/2に短縮**

PCとの比較
PCと比べるとスマートフォンでは暗号解読にかかる時間が約100倍遅くなった
=> **Androidアプリを C/C++で実装することにより高速化が期待できる**

※本パネル研究の成果の一部は「文科省科研費基盤（A）『IoT時代の遠隔操作型・自律型移動システムにおける安全かつ高信頼な通信の実現』」の助成による。

お問合せ先：岡山大学大学院自然科学研究科　氏名　野上 保之
TEL:086-251-8127　E-mail yasuyuki.nogami@okayama-u.ac.jp
岡山大学 OKAYAMA UNIV.