Development of a New Open-source Evaluation Board Designed for Side-channel Analysis

Ryotaro Oohara[1], Haruka Hirata[2], Kazuhide Uchiyama[2],
[1] Kobe University, Hyogo, Japan
[2] The University of Electro-Communications, Tokyo, Japan

RISC-V day 2023 summer

サイドチャネル解析

電子デバイスの消費電力、計算時間などを**サイドチャネル情報**と呼び、
サイドチャネル情報を解析して**暗号化鍵を不正に取得**する攻撃が存在する

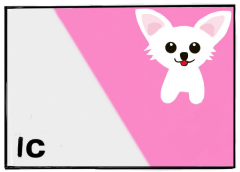
これらの攻撃は計算がハードウェア上で行われる限りは避けられないため、
対策手法と併せて重要視されている研究課題である

- 対策手法の安全性はどのように証明する？

理論的な証明はもちろんのこと、**実験的な証明も求められる**

研究者がそれぞれ好きな機材で実験してもいいのだろうか・・？

世界共通の評価用ボードがあると嬉しい！！



SAKURA-Gが抱える問題

評価ボードの必要性

・サイドチャネル解析への対策技術の安全性を示すには実験による評価が必須

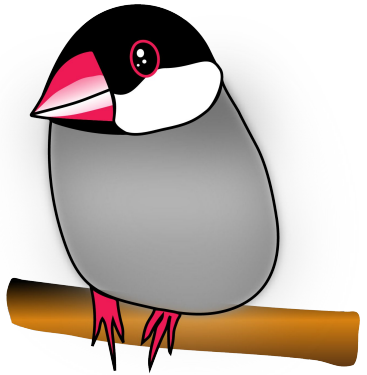
・業界ではSAKURA-Gを使った評価実験が一般的

暗号化と通信用に2機のFPGAを搭載することで低ノイズの測定が可能

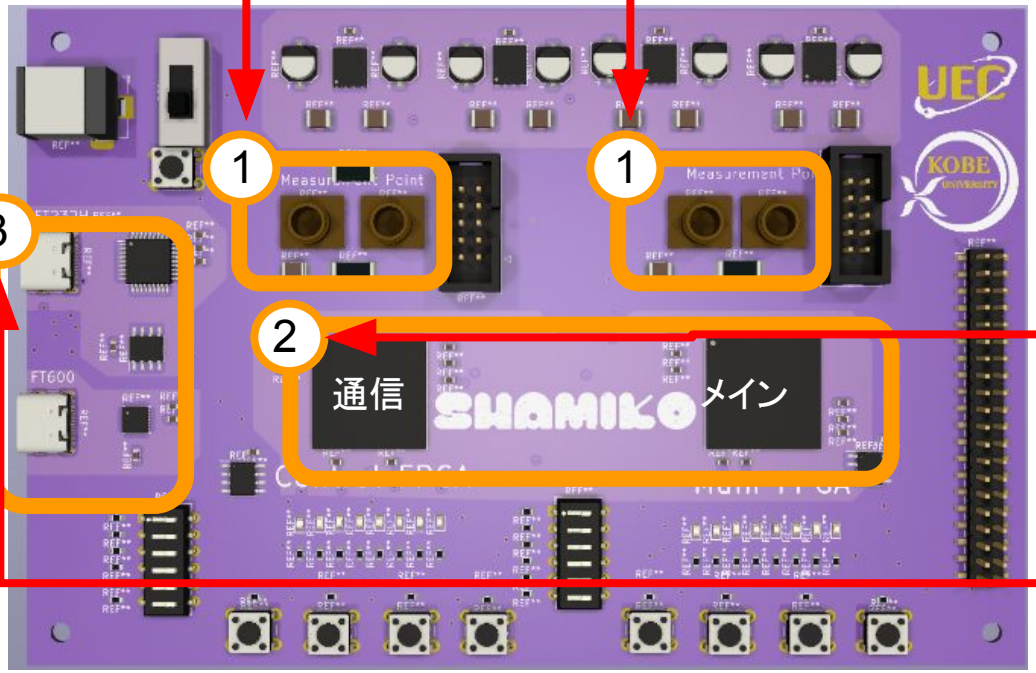
SAKURA-Gの問題

10年前に開発されたまま更新が止まっているため、
開発ツールが古いものしか使えない (SystemVerilogも・・)

→ アイデアの提案から実装・評価実験までのサイクルが遅延し、
暗号ハードウェア分野の研究が停滞するおそれがある



次世代のサイドチャネル解析評価ボードSHAMIKOを提案



①電力計測ポイント
SHAMIKOはFPGAの**コア電源の**
電力計測ポイントを複数持つ

②FPGA
2035年までサポートされている
Spartan™ 7、Artix™ 7を搭載

③USBインタフェース
USB2.0、USB3.0の両方のポート
を持ち、互換性を維持しつつ従来よ
り大きな通信帯域を提供

※画像はイメージです。

Side-cHannel Attack experiMents and Implements Kindly bOard

SHAMIKOの開発方針

SHAMIKOはOSSとして継続したサポートと高い入手性を目指す

完全なオープンソース

- SHAMIKOはフリーウェアのKiCADで設計
- 設計データはオープンソースとして公開

改造してFPGAをASICに置き換えることも容易

アクセシビリティ

- 基板実装サービスに発注可能な設計
- 販売終了したとしても
  容易に入手可能

誰でもFusionPCBAで製造可能

SHAMIKOの開発ロードマップ

7月中旬：仕様策定
現在各所に仕様検討に関してディスカッションを行っている

8月末：回路図完成
回路図完成時点で一度、専門家とレビューを行う

10月中旬：基板設完了
設計完了後レビューを行いFusionPCBAに製造を依頼

11月初頭：基板評価開始
- 基板の基本的な動作検証を行う。
- 各種ソフトウェア資産をSHAMIKOに移植、評価を行う

2024~:Release
フィードバックを反映させSHAMIKO1.0をリリース

まとめ･ご支援のお願い

SHAMIKOとは

SAKURA-Gの代替となる次世代のサイドチャネル解析評価ボード

最新の開発環境　＋　オープンソース　＋　高い入手性

支援のお願い

SHAMIKO projectは支援を募集しています。

- **スポンサー**　:SHAMIKOは資金獲得の目途が立っておりません
- **設計協力等**　:回路レビューや電源回路設計等