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

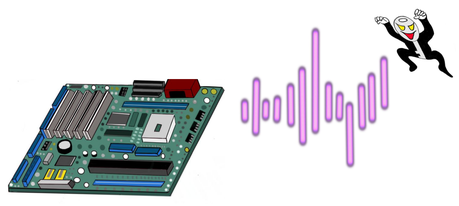
Ryotaro Oohara[1], Haruka Hirata[2], Kazuhide Uchiyama[2],
[1] Kobe University, Hyogo, Japan
[2] The University of Electro-Communications, Tokyo, Japan

What is Side-channel Analysis?

Attacks against cryptographic devices

Cryptographic devices such like smart cards and credit cards are widely used in the world. Of course, cryptography is very important when you see web services.

The encryption algorithm which is used in such services and devices must be theoretically proven. However, can we say the algorithm is secure what if someone accesses directly the hardware devices?
The encryptions which is theoretically proven, e.g., Advanced Encryption Standards, have potential to be exploited as long as it works on the hardware.



Side-channel analysis

Leakage such link time, power consumption, and electromagnetic radiation are **effective information to extract a secret key** used in the encryption for an attacker. Researchers call them “side-channel” while input/output is called main-channel. Attacks using side-channel information is called Side-channel attacks (SCAs).
For instance, we measure much amount of traces of the power consumption with an oscilloscope. Then we statistically analyze them and obtain the secret keys.

Figure 1 shows an example of simple power analysis. If a process branches depending on the certain bit, i.e., 0 or 1 (do nothing when 0), the attacker obtains information that the process was taken or not taken.

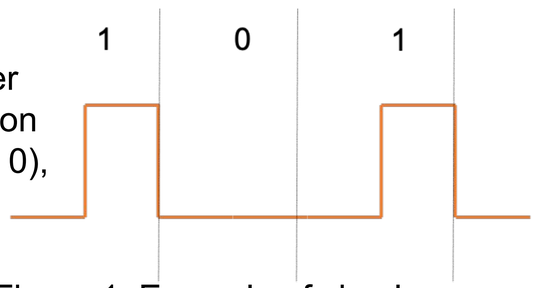


Figure 1: Example of simple power analysis.

Background of our proposal

Security evaluation for the countermeasure

To protect devices many countermeasures against side-channel attacks have been proposed ever. To confirm their security, those proposed countermeasures must be practically evaluated.

In the experimental evaluation, the SAKURA-G board [1], which has two FPGA and is designed for side-channel experiments is widely used around the world.
The board is proposed by Japanese researchers, and thanks to having two FPGAs that one is used for encryptions and another one is used for communications we get ultra-low noise power traces.

Problems of SAKURA-G

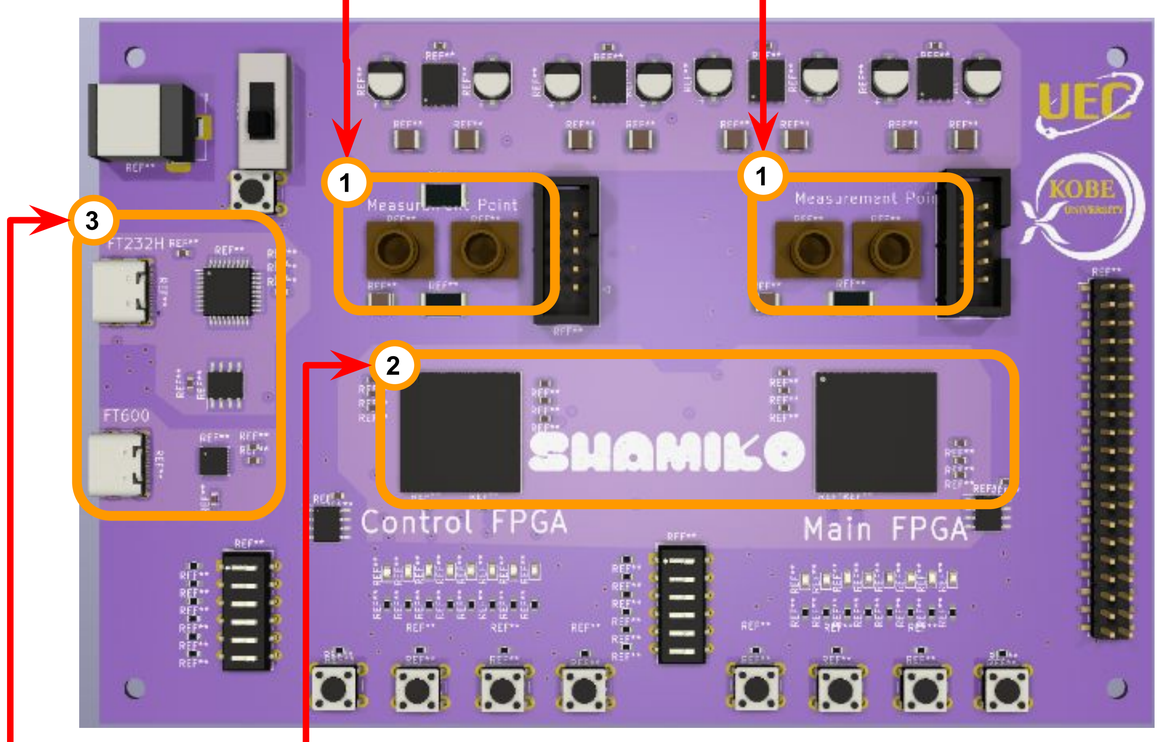
The SAKURA-G is originally proposed a decade ago and is not updated for a long time.
That’s why, installed FPGAs is very old there are some problems, e.g, developing tools is restricted (we are enforced to use Xilinx ISE instead of VIVADO), it does not run on Windows 11 or newer OS. Moreover, Xilinx stooped developing/updating the ISE. Hence this field of research would be waning.

To conquer this situation, we launched the SHAMIKO project, the successor to SAKURA project.

Our Proposal: SHAMIKO

Rendering Image

①Power measurement point
SHAMIKO has several power measurement points with **shunt resistors** insert **core power supply lines** to measure the power consumption of **target logics** in the FPGA.



②FPGA
Employs **Spartan™ 7** or **Artix™ 7**, **<u>supported until 2035</u>**

③USB Interface
SHAMIKO has both **USB 2.0** and **USB 3.0** ports, providing both **compatibility** and **faster communication** than conventional devices.

Design concept of SHAMIKO

・Completely open source

SHAMIKO is being designed in **KiCAD**, an open source CAD system. The **design project files** will be provided as **open source**. If you can use **KiCAD**, you can easily replace the **Main FPGA** with **your ASIC** by modifying SHAMIKO.

・Accessibility

We are planning to build all SHAMIKO parts in Digikey and the **Fusion Open Part Library**.This will allow anyone to manufacture by **only sending BOMs and Gerbers to SeeedStduio Fusion**.

Road map

Mid Jul.：Specification development
We are currently discussing the specifications with hardware security researchers.

Late Aug.：Schematic design complete
Review with a circuit design expert.

Mid Oct. ：PCB design complete
PCB design expert review and manufacturing by FusionPCBA.

Early Nov.：Start of Prototype evaluation.
- Verify the basic behaviour of the prototype SHAMIKO.
- Port the software assets to SHAMIKO and evaluate them.

2024～ ：Release
SHAMIKO 1.0 will be released based on the feedback from the prototype SHAMIKO.

REFERENCES：
[1] https://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html

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

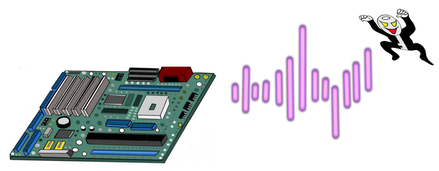
Ryotaro Oohara[1], Haruka Hirata[2], Kazuhide Uchiyama[2],
[1] Kobe University, Hyogo, Japan
[2] The University of Electro-Communications, Tokyo, Japan

What is Side-channel Analysis?

暗号デバイスへの攻撃

情報化が進む現代では、Webショッピングやクレジットカード、ICカードなど暗号機能を搭載したサービスやデバイスをいたるところで目にします。

これらのサービスでは、理論的な安全性が証明された暗号アルゴリズムを使うことが当たり前ですが、「デバイスに物理的にアクセスできる人」がいたらどうでしょうか。理論的には安全とされている暗号アルゴリズムも、ハードウェア上で動作する限りは物理アクセスによって破られてしまうおそれがあります。



サイドチャネル解析

暗号化計算にかかる時間や計算中の消費電力、電磁波など、入出力（暗号化んにおいては平文と暗号文）以外から漏えいする情報のことを**サイドチャネル情報**と呼びます。サイドチャネル情報を用いて解析・攻撃するので、サイドチャネル解析・攻撃といいます。

たとえば、デバイスの消費電力を用いたサイドチャネル解析では、オシロスコープを使って電力波形を測定し、統計的に解析することで暗号化に使用された秘密鍵を不正に取得します。

右図に単純な電力解析の例を示します。
あるビットが0か1かで処理が分岐
（0のときはなにもしない）する場合、
電力波形を見るだけでどちらの分岐に
進んだかを知ることができます。

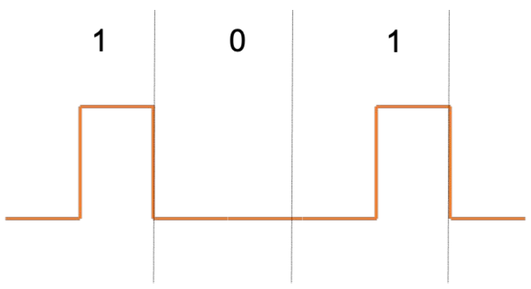


図: 単純な電力解析の例

Background of our proposal

対策技術の安全性評価

サイドチャネル解析への対策技術は、理論的に安全性を示しただけでは不十分です。対策によって攻撃がどの程度難しくなるのか、消費電力を測定するなどの評価実験を行う必要があります。
評価実験には、FPGAが2つ搭載された専用の評価ボード（SAKURA-G [1]）を使うことが多く、世界中で広く使用されています。

SAKURA-Gは日本で開発されたボードで、2機のFPGAを暗号化処理とインタフェースとで使い分けています。これによって、暗号化中の消費電力を低ノイズで得ることができ、信頼度の高い評価実験を実現します。

SAKURA-Gの課題

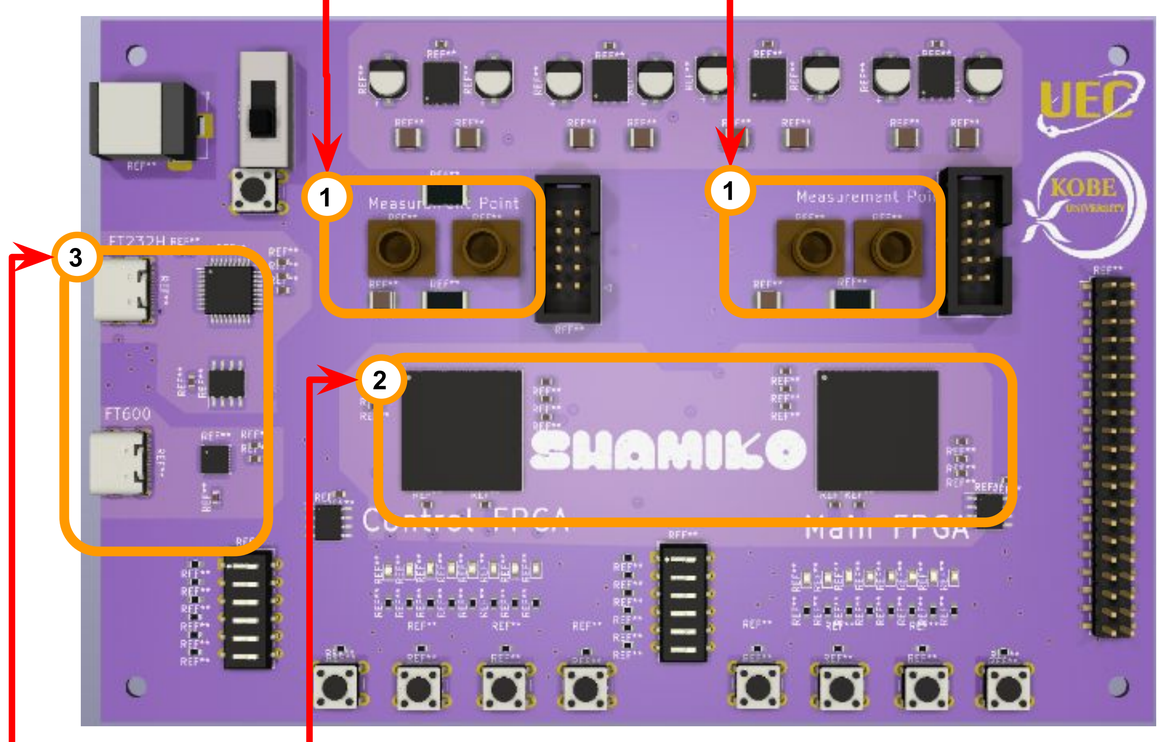
SAKURA-Gは歴史が古く、10年前に開発されたボードです。しかしながら、開発時から現在に至るまで更新が行われておらず、古いFPGAを使い続けている状況です。そのため、開発環境がXilinx ISE（現在は後継としてVIVADOがXilinxから提供）に制限されてしまっています。

ISEの開発が既にストップしている、Windows 11では動かないなど、SAKUGA-Gは様々な問題点を抱えています。
このままでは暗号ハードウェアセキュリティ分野が衰退してしまうと危機を感じ、SAKURAの後継となる、SHAMIKOプロジェクトを立ち上げました。

Our Proposal: SHAMIKO

イメージ図

①電力計測ポイント
電力解析攻撃では、プロセッサの内部ロジックの消費電力を計測します。
SHAMIKOはFPGAの**コア電源ライン**に対して、**シャント抵抗**を挿入した電力計測ポイントを複数持ちます。



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と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も大きな通信帯域を提供

SHAMIKOの設計指針

完全なオープンソース

SHAMIKOはオープンソースのCADであるKiCADで設計しており、最終的なプロジェクトファイルごとオープンソースとして公開する予定です。
KiCADさえ使えればSHAMIKOを改造してFPGAをASICに置き換えることも容易です。

アクセシビリティ

SHAMIKOは全ての部品をDigikeyとFusionPCBAの提供する**Fusion Open Part Library**で構成する計画です。これにより、誰でもSeeedStduioやその他PCB組み立てサービスにBOMとガーバーを送るだけで製造可能です。

Road map

7月中旬：仕様策定
現在各所と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

REFERENCES：
[1] https://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html