6ZC-08

SAKURA-Gにおける VITI センサーの実装

内山 一秀 †　　李 陽 ‡
電気通信大学 †　電気通信大学 ‡

1　はじめに

現在, AWS F1 インスタンスのように, クラウド上にも FPGA が存在している. このようなクラウド上の FPGA に対してサイドチャネル攻撃を行う場合, FPGA への物理的なアクセスを用いた攻撃手法を使うことが出来ないため, それらに頼らない攻撃手法が必要になる. そこで提案されたのが Remote Power Analysis (RPA) Attack である. RPA Attack では, クラウドの FPGA 上に攻撃対象のモジュールがあると仮定し, その FPGA にディジタル回路で構成された電力センサーを設置する. 攻撃者はセンサーが記録した値を読むことで, あるタイミングでの消費電力の増減を取得し, CPA 等に利用することが出来る.

従来の電力センサーに用いられている部品には欠点が存在しており, それらの部品を用いない新たな電力センサーが, Udugama らが提案した VITI センサー [5] である.

本研究では SAKURA-G ボードにこの VITI センサーを実装し, 評価することを目標としている.

2　従来の電力センサー

従来の電力センサーには, Ring Oscillator (RO)[1] や Time to Digital Converter (TDC)[2] が用いられているが, これらにはそれぞれ欠点が存在している. RO は組み合わせ回路のループで構成されており, これは FPGA にダメージを与える可能性が存在するため, クラウドの規約で禁止されている場合がある [3]. また TDC は内部でラッチを必要とするため, FPGA 側でラッチを持つ回路を拒否すれば TDC を持つ電力センサーを排除することが出来てしまう [4]. 以上より RO も TDC も用いないセンサーが必要となる.

そこで Udugama らが提案したのが, Voltage Induced Time Interval (VITI) Sensor である [5]. VITI センサーは FPGA の Power Delivery Network (PDN) に負荷が掛かる, すなわち消費電力が大きくなると論理素子の伝達遅延が増加することを利用しており, その構造や回路サイズ, データの正確性等に既存の電力センサーと比較して利点を持つ.

3　VITI センサーの構造と動作原理

VITI センサーは AND 回路, FF, メモリ, CALIBRATION 回路で構成されている (図 1). AND 回路の連なりの始端にクロックを入力し, 各 AND 回路の出力を FF に入力する. そして FF の出力をメモリに格納する. 例として, AND 回路が 4 つ連なっている場合の動作を説明する. 通常時, AND 回路には伝達遅延が存在しているため, 連なりの最後までには信号が到達しない, よってメモリに $1110_{(2)}$ が格納されるとする. 攻撃対象のモジュールの消費電力が増えると, PDN に負荷が掛かり伝達遅延が増加するため, 更に手前の AND 回路にしか信号が到達しなくなり, メモリに $1100_{(2)}$ が格納されるようになる. このメモリの値を読むことで, 攻撃対象のモジュールの消費電力の変化を記録することが可能となる.

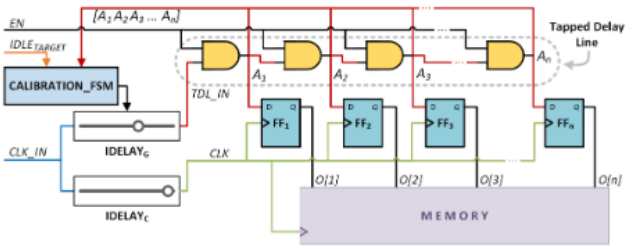

図 1　VITI センサーの構造 ([5] から引用)

4　VITI センサーの利点

この VITI センサーは内部で RO も TDC も必要とせず, また構造が単純であるので回路サイズが小さい. また, 既存のセンサーに比べて正確なデータが取

Implementation of VITI sensor in SAKURA-G
† Kazuhide Uchiyama, The University of Electro-Communications
‡ Li Yang, The University of Electro-Communications

れるため, より少ないパワートレースで鍵復元が可能となっている (図 2).

Sensor	4-bit VITI	RO[1]	TDC[2]
Slice	8	128	34
1 Power Trace (256サンプル)	256 Bytes	16,384 Bytes	256 Bytes
パワートレース数(KR=2^{75})[5]	13,000	100,000	29,000

図 2　各センサーの回路サイズ ([5] を元に作成)

5　実装の進捗

現在, VITI センサーの再現実験を行っている. 図 3 が再現実験環境のブロック図である。SAKURA-G ボードのメイン FPGA には AES モジュールと VITI センサーを実装し, コントローラ FPGA にはシリアル通信用モジュールとメイン FPGA の制御用モジュールを実装した.

使用者はシリアルコンソールを用いたコマンドの手動入力による制御と, Python のシリアル通信用ライブラリを用いたスクリプトによる制御を行うことが可能である.

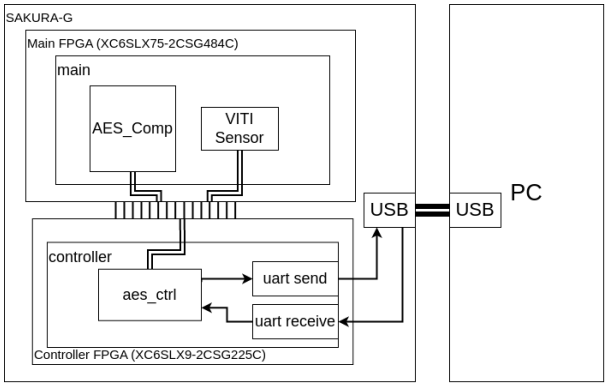

図 3　再現実験環境のブロック図

本実験環境では PC から SAKURA-G へ 128bit の鍵と平文を送信した後, AES モジュールが暗号化を行い, VITI センサーのメモリデータを PC へ送信する.

また AES モジュールは 6MHz で動作しており、VITI センサーは 48MHz で動作している。AES モジュールは全 10 ラウンドで 1 クロックにつき 1 ラウンド進むため, VITI センサーは AES の各ラウンドで 8 つの 4 bit のサンプル, 全 10 ラウンドで 80 サンプル 40byte のデータを一回の暗号化処理の間にメモリに格納する。

実際に VITI センサーで消費電力の測定を行うと同時に, オシロスコープでも消費電力の測定を行った際の結果が図 4 である. VITI センサーで消費電力の増減を検知出来た事が確認できる.

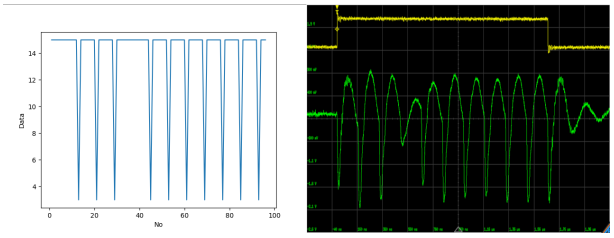

図 4　VITI センサーによる測定結果

今後の展望として, VITI センサーのより詳細な精度の評価と精度の改善方法の検討, そして AES モジュールのパワートレースを取得し, そのデータから CPA による鍵復元を試みる.

6　まとめ

クラウド上の FPGA へのサイドチャネル攻撃に用いる新たな電力センサーである VITI センサーは, 既存のセンサーと比べ多くの利点を持つ. 本研究では VITI センサーを再現し, 精度の計測や改善方法の検討を行う.

参考文献

[1] J. Gravellier, J. Dutertre, Y. Teglia, and P. Loubet-Moundi. “*High-speedring oscillator based sensors for remote side-channel attacks on FPGAs*”. In 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), pages 1–8, 2019.

[2] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori. “*An inside job: Remote power analysis attacks on FPGAs*”. In 2018 Design, Automation Test in Europe Conference Exhibition (DATE), pages 1111–1116, March 2018.

[3] Amazon Web Services. AWS EC2 FPGA HDK+SDK errata. https://github.com/aws/aws-fpga/blob/master/ERRATA.md, 2020

[4] T. Sugawara, K. Sakiyama, S. Nashimoto, D. Suzuki, and T. Nagatsuka. “*Oscillator without a combinatorial loop and its threat to FPGA in data centre*”. Electronics Letters, 55(11):640–642, 2019.

[5] B.Udugama, D.Jayasinghe, H.Saadat, A.Ignjatovic and S.Parameswara “*VITI: A Tiny Self-Calibrating Sensor for Power Variation Measurement in FPGAs*”, CR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925, Vol. 2022, No. 1, pp. 657–678.