Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

バレルシフタと加算器によるビット非独立なサイドチャネルリークの発生機序とその対策

Causality and Countermeasures of Bit-Interaction Side-Channel Leakage from Barrel Shifter and Adder

浅野　多聞 *　　菅原　健 *
Tamon Asano　　Takeshi Sugawara

キーワード サイドチャネル攻撃，マスキング，論理シミュレーション，バレルシフタ，加算器，RISC-V

あらまし

本稿は PROOFS2021 で発表済みの内容に基づく [1].

サイドチャネル攻撃への対策としてマスキングが広く用いられ，その構成や効率的な実装の研究が進められている．マスキングは，1 bit の情報をシェアと呼ばれる複数の bit で表現することで，消費電力等のサイドチャネル情報との相関をなくすことを目的としている．実装上のオーバーヘッドがマスキングの課題であり，効率的な実装方法が研究されている．特に Barthe らによって提案されたマスキングによる乗算アルゴリズム [2] のソフトウェア実装では，シェアの全要素を同一の汎用レジスタに詰めることで，CPU のビット演算の並列性を利用して効率的な処理を可能としている．

Gao らは，このシェアを同一の汎用レジスタに詰める手法をシェア・スライシングと呼び，ソフトウェア実装における Barthe の乗算アルゴリズムの安全性について研究を行った [3]．その結果，シェア・スライシングの安全性の前提条件である発生するリーケージのビット独立性が ARM プロセッサでは維持されず，一部のシフト命令でビット非独立なリークが発生することが実験により明らかになった．一部のシフト命令でビット非独立なリークが確認されたことからバレルシフタがビット非独立なリークの原因であると考察されているが，原因の特定には至っていなかった．

SCIS2021 で筆者らは，論理合成したオープンソースの RISC-V 実装を対象にした論理シミュレーションにより ALU 内部のビット非独立なリークについて評価を行った [4]．その結果，バレルシフタに起因するビット非独立なリークが存在することを示し，また加算器に起因するビット非独立なリークが存在することを示した．

そこで本稿では，バレルシフタと加算器によって生じるビット非独立なリークの詳細な発生機序を明らかにするため，論理シミュレーションによる検証を行う．その結果，バレルシフタによるビット非独立なリークが Gao らの仮説である選択信号の遅延に原因があることを示す．また，加算器によるビット非独立なリークが桁上がりによって生じることを示す．さらに，これらの結果から ALU 内のバレルシフタと加算器によるビット非独立なリークに対してハードウェアとソフトウェアによる対策を提案する．

参考文献

[1] Tamon Asano and Takeshi Sugawara. Simulation based evaluation of bit-interaction side-channel leakage on RISC-V processor. In *PROOFS2021, 10th International Workshop on Security Proofs for Embedded Systems*, 2021.

[2] Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub. Parallel implementations of masking schemes and the bounded moment leakage model. In *Advances in Cryptology - EUROCRYPT 2017, Proceedings, Part I*, Vol. 10210 of *Lecture Notes in Computer Science*, pp. 535–566, 2017.

[3] Si Gao, Ben Marshall, Dan Page, and Elisabeth Oswald. Share-slicing: Friend or foe? *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 152–174, 2020.

[4] 浅野多聞, 菅原健. ALU 内部のビット非独立なリーケージのシミュレーション評価. 暗号と情報セキュリティシンポジウム, 2021.

* 電気通信大学，東京都調布市調布ケ丘 1-5-1，The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan