Vol.2021-EMB-58 No.6
2021/11/18

FPGA における加算器の電力解析攻撃耐性の評価

趙意琳[1]　張啓迪[1]　西川広記[1,2]　孔祥博[1]　冨山宏之[1]

概要：多くの IoT 機器は電力解析攻撃などのサイドチャネル攻撃の脅威にさらされている．加算器は電子回路の最も基本的なコンポーネントの 1 つである．本論文では，FPGA 上での電力解析攻撃に対する加算器の耐性を検証するために 3 種類の 32 ビット加算器の電力サイドチャネルリークを T 検定に基づいて分析する．実験の結果，キャリーチェーンを利用した桁上げ伝播加算器が電力や遅延，電力解析攻撃に対する耐性の面で最も有効である．

キーワード：サイドチャネル攻撃，T 検定，加算器，FPGA

1. はじめに

IoT デバイスは物理環境にさらされているため，サイドチャネル攻撃を受けやすい．サイドチャネルの中でも消費電力[1]は解析するための機器が高価ではないため，攻撃に適している．また，文献[2]によると電力解析攻撃は FPGA のセキュリティにとって深刻な脅威となっている．そのため，暗号技術は電力解析攻撃に対して安全に設計されなければならない．

この論文では，回路の最も基本的な構成要素の 1 つである加算器を対象に，3 種類の 32 ビット加算器の電力解析攻撃に対する耐性を評価する．評価には桁上げ伝播加算器（RCA），桁上げ先見加算器（CLA），およびキャリーチェーンを利用した RCA を用いる．そして，この 3 つの加算器を合成し，得られた消費電力から電力に基づくサイドチャネル情報がどの程度漏洩しているかを T 検定により統計的に評価する．

本論文の構成は以下の通りである．2 章では本研究で使用した 3 つの加算器について説明する．3 章では実験について説明する．4 章では本論文のまとめを示す．

2. FPGA 上の加算器

本章では FPGA 上の 3 つの加算器設計について説明する．本研究では Xilinx 社の 7 シリーズ FPGA を想定している．

2.1 桁上げ伝播加算器（RCA）

RCA は最も基本的な加算器として知られている．32 ビット RCA は 32 個の全加算器（FA）を順次連結して設計される．また，各 FA は次のように桁の和と次の FA へのキャリー信号を計算する．

$$S_i = A_i \oplus B_i \oplus C_i \tag{1}$$

$$C_{i+1} = A_i \cdot B_i + B_i \cdot C_i + C_i \cdot A_i \tag{2}$$

Xilinx の FPGA は 6 入力 LUT で構成されており，各 6 入力 LUT は 2 つの 5 入力 LUT として構成される．よって 1 つの FA は 6 入力 LUT にマッピングされ，32 ビット RCA は 32 個の LUT を使用する．LUT からのキャリーアウト信号は次の LUT の入力ポートに接続される．RCA の回路規模は小さいが，最悪の場合キャリーの伝播は 32 個の LUT すべてを経由するためクリティカルパスの遅延が長くなる．

2.2 桁上げ先見加算器（CLA）

CLA はキャリーを先読みすることで遅延を改善する回路である．CLA では各桁の位置に対して以下のようにキャリーの生成とキャリーの伝搬を計算する．

$$G_i = A_i \cdot B_i \tag{3}$$

$$P_i = A_i + B_i \tag{4}$$

そして，次の桁へのキャリーは次のように計算される．

$$C_{i+1} = G_i + P_i C_i \tag{5}$$

式(5)を再帰的に計算すると，次のようになる．

$$C_1 = G_0 + P_0 C_0 \tag{6}$$

$$C_2 = G_1 + P_1 C_1 = G_1 + P_1 G_0 + P_1 P_0 C_0 \tag{7}$$

$$C_3 = G_2 + P_2 C_2 = G_2 + P_2 G_1 + P_2 P_1 G_0 + P_2 P_1 P_0 C_0 \tag{8}$$

$$C_4 = G_3 + P_3 C_3 = G_3 + P_3 G_2 + P_3 P_2 G_1 + P_3 P_2 P_1 G_0 + P_3 P_2 P_1 P_0 C_0 \tag{9}$$

キャリー信号は並行して計算できるため，CLA は RCA よりも LUT 数が多いが，高速に計算できる．

2.3 キャリーチェーンを利用した桁上げ伝播加算器

Xilinx の FPGA には，キャリー信号を高速に伝播させるために Carry4 と名付けられた特別なハードウェアブロックがある．各 LUT の出力には，図 1 に示すように XOR ゲートと 2 入力マルチプレクサが配置され．マルチプレクサはチェーン化されている．キャリーチェーンを使うと，加算器は次のように計算できる．

$$P_i = A_i \oplus B_i \tag{10}$$

$$S_i = P_i \oplus C_{in} \tag{11}$$

$$C_{i+1} = G_i + P_i \cdot C_i = \overline{P_i} \cdot A_i + P_i \cdot C_i \tag{12}$$

1 立命館大学大学院理工学研究科
2 日本学術振興会特別研究員

Vol.2021-EMB-58 No.6
2021/11/18

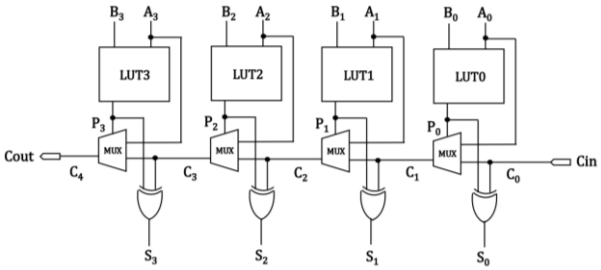

図 1　高速キャリーチェーン付き 4 ビット RCA

式(10)，(11)，(12)は，それぞれ LUT，XOR ゲート，マルチプレクサで計算される．この回路も 32 ビット RCA と同様に 32 個の LUT を使用する．ただし，RCA とは異なり，ある桁のキャリーアウト信号が次の桁の LUT に入ることはない．キャリー信号は内蔵された高速キャリーチェーンを介して伝播されるため，2.1 節で示した RCA よりもクリティカルパスの遅延が短くなる．

3. 電力解析攻撃耐性の評価

3.1 合成結果

ZCU106 FPGA デバイス用の Xilinx Vivado 2019.2 を用いて，3 つの 32 ビット加算器を合成する．ハードウェアの資源と遅延に関する結果を表 1 に示す．ハードウェアコストと性能の両方で，3 つの加算器の中では高速キャリーチェーンを持つ RCA が最も優れている．

表 1　加算器の資源と遅延

	RCA	CLA	キャリーチェーンを持つ RCA
LUT 数	32	148	32
遅延（ns）	6.408	3.470	2.907

3.2 電力解析

合成後のシミュレーションに基づいて 3 つの加算器の消費電力を解析する．解析には Vivado ツールキットと文献[4]で紹介されている電力解析ツールを使用した．その結果を図 2 に示す．32 ビットの加算器は FPGA の容量に比べて非常に小さいため，動的電力のみを評価した．また，各テストベンチには 200 個のテストベクターが含まれている．最初の 10 個のテストベンチでは，2 つのオペランドのうち 1 つが 0 に固定されている．そのため，最初の 10 個のテストベンチの電力が次の 10 個のテストベンチの電力よりも低くなっている．解析の結果，高速なキャリーチェーンを持つ RCA が最も低電力で動作することが判明した．

3.3 T 検定に基づく電力サイドチャネルのリーク解析

3.2 節で得られた電力に対して，サイドチャネルリークに対する耐性を評価するために T 検定[3]を行う．T 検定により求められた T 値が-4.5～4.5 の間であれば電力解析攻撃への耐性があると考えられる．

得られた T 値を図 3 に示す．T 検定の結果，CLA とキャリーチェーンを使用した RCA は，どのような場合でも T 値が-4.5～4.5 の間に収まっており，電力解析攻撃に対して安全であることが確認できる．特に高速キャリーチェーンを用いた RCA は高い耐性を示している．

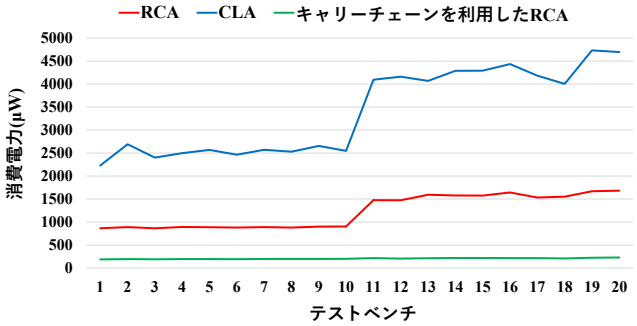

図 2　消費電力

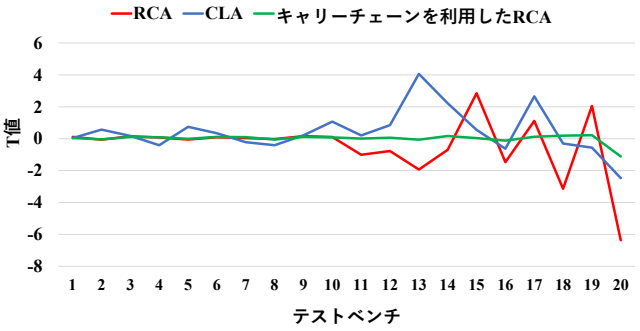

図 3　T 値

4. おわりに

本論文では電力サイドチャネル攻撃に対する異なる 3 つの加算器について耐性の評価を行った．その結果，キャリーチェーンを利用した RCA の優位性が明らかになった．今後は，回路の内部構造が電力解析攻撃への耐性にどのように影響するかについて，詳細な解析を行う予定である．

謝辞

本研究の一部は科研費 20H00590, 19H04081, 20J21208,および 21K19776 の支援による．

参考文献

[1] P. Kocher, J. Jaffe and B. Jun, “Differential power analysis,” *Annual International Conference Cryptology*, 1999.
[2] F.-X. Atandaert, L. van Oldenzeel, D. Samyde and J.-J. Quisquater, “Power analysis of FPGAs: How practical is the attack?,” *International Conference on Field Programmable Logic and Applications*, 2003.
[3] G. Goodwill, B. Jun, J. Jaffe and P. Rohatgi, “A testing methodology for side-channel resistance validation,” *NIST Non-invasive Attack Testing Workshop*, 2011.
[4] Q. Zhang, X. Kong and H. Tomiyama, “A toolkit for power behavior analysis of HLS-designed FPGA circuits,” *IEEE symposium on Low-Power and High-Speed Chips and Systems*, 2021.