Vol.2021-EMB-58 No.7
2021/11/18

高位合成における最適化のサイドチャネル攻撃耐性への影響

水野拓己[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 デバイスはサイドチャネル攻撃の危険にさらされている．サイドチャネル攻撃の中でも，ターゲットとなるデバイスの電力を解析することで回路の秘密鍵を特定する電力解析攻撃が有名である．本論文では，暗号回路における性能と，サイドチャネル攻撃耐性との相関を調査する．C 言語で記述された AES 回路を高位合成した後，電力解析し，T 検定によってサイドチャネル攻撃耐性を評価する．

キーワード：AES，高位合成，最適化，T 検定

1. はじめに

近年 IoT デバイスのようなサイバーフィジカルシステムが広く普及している．IoT デバイスは様々な分野で活用され，生活を豊かにする一方で，機器自体がサイドチャネル攻撃などの物理的な攻撃の危険にさらされている[1]．サイドチャネル攻撃にはいくつかの種類があり，電力解析攻撃が最も効果的な攻撃手段の一つとして知られている．文献[2]では，電力解析攻撃に着目し，AES 回路の脆弱性を評価している．一方，最近では，C/C++などの高級プログラミング言語から RTL 回路を自動的に生成可能な高位合成技術が普及している．高位合成によって設計者は迅速に回路を生成することができるが，生成される回路は最適化の方法によって変化するため，その設計空間や性能は多様である．文献[3]では，S ボックスを最適化した AES 回路の電力解析攻撃耐性が調査されている．本研究では，AES 回路の性能とサイドチャネル攻撃耐性の相関を評価している．高位合成ツールの最適化オプションによって性能を向上させ高位合成した AES 回路と，最適化オプションを使用せずに合成した AES 回路の二つの回路を生成する．その後，二つの回路を比較し，T 検定によってサイドチャネル攻撃耐性の評価を行う．本研究の貢献は，性能とサイドチャネル攻撃耐性の評価を行うことである．

本論文の構成は以下の通りである．2 章では，AES 回路への最適化手法とその結果について述べる．3 章では，T 検定手法とその結果について述べる．4 章では，本論文の結論を述べる．

2. AES 回路の最適化

AES 回路を高位合成するために，Vivado HLS を使用する．Vivado HLS は様々な最適化の特徴を持っており，これらを組み合わせることで，回路の性能を高めることができる[4]．対象の FPGA として，Zynq 7000 を採用する．また，本研究で使用したプログラムは CHStone ベンチマークの AES プログラムである [5]．

表 1 は AES 回路の資源数を示す．シミュレーションの周期は 10ns である．デフォルトとは，Vivado HLS のデフォルトの設定で合成された AES 回路で，性能優先とは，パイプライン化とインライン展開の最適化オプションを使用して性能を向上させて合成された AES 回路である．この結果で着目したいのが，二つの回路の資源数に大きな変化がないことである．デフォルト性能の AES 回路が 1705 個の LUT を使用しているのに対し，性能優先の AES 回路は 2261 個の LUT を使用している．その一方で，性能優先の AES 回路のクロックサイクルは 1797 であり，デフォルト性能の AES 回路と比較してかなり短い．言い換えるならば，性能優先の AES 回路はデフォルト性能の AES 回路より約 2.5 倍高性能である．

表 1：AES 回路の資源数

	デフォルト	性能優先
LUTs	1705	2261
LUTRAMs	12	33
FFs	1748	1487
BRAMs	3	2.5
クリティカルパス遅延（ns）	3.509	7.905
クロックサイクル数	4545	1797
実行時間（ns）	16900	7220

3. T 検定

サイドチャネル攻撃耐性を評価するために，T 検定を使用する[6]．T 検定はセキュリティに関する最も一般的な評価の一つである．T 検定の基本的な考え方は，二つのデータセットの平均と分散が同一であるかどうかを調査することである．文献[6]に示されているように，サイドチャネル攻撃耐性の評価では，求められる T 値の絶対値が 4.5 以下であることが理想である．

本研究では，Vivado 2020.1 を用いて AES 回路を電力解析する．T 値の評価には，文献[7]で開発された解析ツール

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

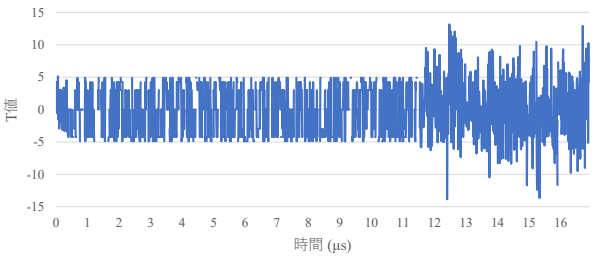
を使用して，128 ビットのランダム平文から 20 個，128 ビットの固定平文から 10 個の電力トレースを取得する．128 ビットの暗号鍵は固定する．ランダム平文の暗号化では，2 回目以降は前回の出力が次の入力になる．本実験では，このランダム平文と固定平文を用いて電力トレースを取得し，求められた T 値からサイドチャネル攻撃耐性を評価する．図 1 の(a)および(b)は、デフォルト性能で合成された AES 回路と，性能優先で合成された AES 回路についての T 検定の結果を示す．図 1 (a)では，T 値が±4.5 を超えた回数が 340 回であるのに対し，図 1 (b)では，195 回である．しかし，図 1 (b)の性能優先の AES 回路は，デフォルトの AES 回路よりも実行時間が短く，AES 回路のセキュリティ基準である±4.5 を超えた回数を単純に比較することはできない．

図 2 は，二つの AES 回路の T 値の絶対値の累積相対度数を示す．デフォルトの AES 回路では，T 値の 80%が±4.5 以下である．この結果は，性能優先の AES 回路に比べて，デフォルトの AES 回路のほうがサイドチャネル攻撃に強いことを示す．つまり，高性能な AES 回路は，サイドチャネル攻撃によって情報が漏洩しやすいため，AES 回路の性能とサイドチャネル攻撃耐性はトレードオフの関係にあることが示唆される．

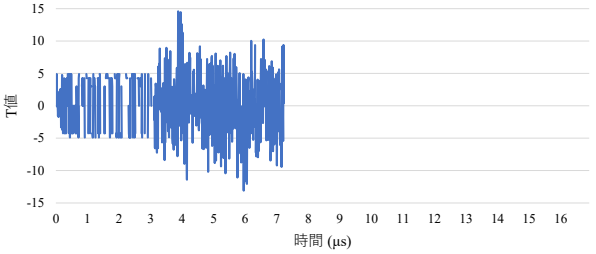
4. おわりに

本研究では，高位合成によって生成された AES 回路のサイドチャネル攻撃耐性を考察し，AES 回路の性能とサイドチャネル攻撃耐性のトレードオフを示した．我々の行った実験では，AES 回路をパイプライン化とインライン展開によって最適化しているが，回路の資源数はデフォルトで合成されたものとほぼ同じであった．今後は，資源数に大きな差がある場合の AES 回路のサイドチャネル攻撃耐性を評価する予定である．また，本研究では AES 回路を対象としていたが，他の暗号化回路でも同様の実験を行いたい．

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



(a) デフォルト性能の AES 回路の T 値



(b) 性能優先の AES 回路の T 値

図 1 性能の異なる AES 回路の T 検定結果

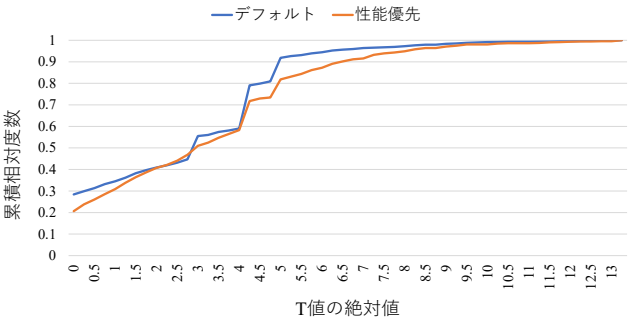


図 2 AES 回路の累積相対度数

参考文献

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[2] S. B. Örs, F. Gürkaynak, E. Oswald, and B. Preneel, “Power-analysis attack on an asic aes implementation,” *Information Technology: Coding and Computing (ITCC)*, vol. 2, pp. 546-552, 2004.

[3] L. Zhang, W. Hu and A. Ardeshiricham, Y. Tai, J. Blackstone, D. Mu, and R. Kastner, “Examining the consequences of high-level synthesis optimizations on power side-channel,” *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1167-1170, 2018.

[4] G. Martin and C. Smith, “High-level synthesis: Past, present, and future,” *IEEE Design & Test of Computers*, vol. 26, pp. 18-25, 2009.

[5] Y. Hara, H. Tomiyama, S. Honda and H. Takada, “Proposal and quantitative analysis of the CHStone benchmark program suite for practical C-based high-level synthesis,” *Journal of Information Processing*, vol. 17, pp. 242-254, 2009.

[6] G. Goodwill, B. Jun, J. Jaffe and P. Rohatgi, “A testing methodology for side-channel resistance validation,” *NIST Non-Invasive Attack Testing Workshop*, vol. 7, pp. 115-136, 2011.

[7] 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 (COOL Chips)*, 2021.