C-024

FPGA 上での暗号処理の効率的な実装と性能比較
Efficient Implementation and Performance Comparison of Cryptographic Processing on FPGA

森田 慧一† 八槇 博史†
Keiichi Morita Hirofumi Yamaki

1. 緒言

FPGA（Field-Programmable Gate Array）は、アクセラレータとして電力効率に優れている。本研究では、Data Encryption Standard（DES）を例にして、暗号処理の実装の効率化と他アクセラレータとの性能比較を行う。

近年のセキュリティ要件の高度化に伴い、暗号処理の効率化は益々重要となっている。特に環境要件を満たすためには、消費電力あたりの処理効率を向上させることが肝要である。そこで FPGA は、低消費電力アクセラレータとして注目されている。

本研究では、DES の鍵探索を題材として性能比較を行った。DES は歴史的に重要な暗号であることに加え、すでに使用が推奨されないものではありながら、依然随所で用いられている暗号アルゴリズムでもある。本研究では、DES の鍵探索を題材として性能比較を行った。

本論文の構成を述べる。第２章では、DES アルゴリズムと FPGA の基礎について述べる。第３章では、提案する効率的な実装手法について詳細に説明する。第４章では、実験結果と他アクセラレータとの性能比較を示す。最後に第５章で結論と今後の課題を述べる。

2. FPGA による暗号解読

2.1 FPGA

FPGA は再構成可能プロセッサである。FPGA 上に処理をフルパイプラインで実装した場合、単位時間あたりの処理性能はクロック周波数と並列処理数の積となる。FPGA の動作クロック周波数は、回路構成によって制限され、並列処理数は１処理あたりの使用リソース数によって制限される。

2.2 DES

DES は 1977 年に NIST によって標準化された共通鍵暗号方式である[1]。鍵長は 56bit であり、これは 2^{56} 通りの鍵を総当りで探索を行えば必ず解読できることを意味する。このことから DES は既に危殆化しているが、未だに IoT デバイスなどでの使用が続いている。総当たり探索処理は独立に処理できデータの授受も無いため並列化に向いている。

2.3 ハードウェアによる DES の鍵探索

FPGA を用いた DES の鍵探索実装に関する既存研究を挙げる。そして他アクセラレータによる実装も紹介する。

2.3.1 COPACOBANA

COPACOBANA は 2006 年に開発された並列計算機である[2]。120 基の Xilinx Spartan-3 XC3S1000 が用いられている。

2.3.2 crack.sh

crack.sh は 2012 年に公開されたオンラインクラッキングサービスである[3]。40 台の Xilinx Virtex-6 LX240T が用いられている。56 ビットの DES 鍵空間を 26 時間で全探索することができる。

2.3.3 Deep Crack

Deep Crack は電子フロンティア財団が 1998 年に構築した ASIC マシンである。1,856 個のカスタムチップで構成されている。

2.3.4 hashcat

hashcat はオープンソースのパスワードクラッキングソフトウェアである。汎用 GPU を用いて種々のハッシュを解析することができる。

本研究では、この hashcat による解析と、FPGA による解析とを比較することで、暗号解析分野における FPGA の適用可能性を検証する。

3. 実装

3.1 実験機材

実験機材として、FPGA ボード Kria KV260 Vision AI Starter Kit[5]と、デザインツール Vivado Design Suite 2024.2 を使用した。

3.2 実験方法

実験では HDL（Hardware Description Language）で DES を記述し、論理合成を行った。記述には文献[4]の面積最適化実装を使用した。

図 1 に DES のアルゴリズムを示す。

3.3 実験結果

DES の鍵探索処理をクロック周波数 625MHz において 50 並列で動作させることができた。これ以上のクロック周波数では論理合成が失敗し、これ以上の並列数は定格消費電流を超過した。

4. 性能比較

各実装の性能を比較する。まず、DES の FPGA 実装について表１に示す。デバイスファミリの進化に伴いクロック周波数が向上している。また、並列処理数についてはロジックセル数に比例している。

次に DES 実装の各アクセラレータにおいての消費電力を表２に示す。消費電力あたりの処理性能（MOPS/W）に

†東京電機大学　システムデザイン工学研究科　情報システム工学専攻
Department of Information System Engineering, School of System Design and Technology, Tokyo Denki University

注目されたい。GPU による実装と比較して、FPGA による実装は、7 倍程度の処理性能を示していることがわかる。このことから、暗号解読のアプリケーションでは、FPGA による実装が、一定の効果をもつことが示唆された。

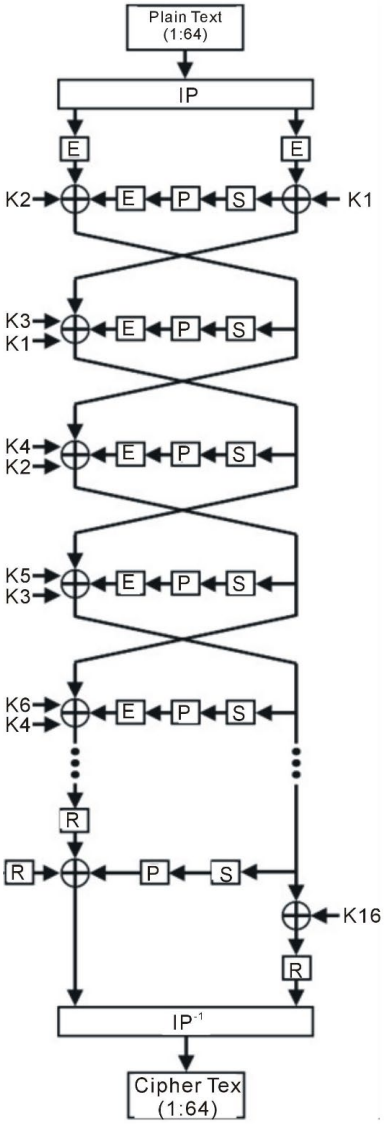

図 1　最適化された DES 実装

表 1　DES の FPGA 実装の比較

	COPACOBANA[2]	crack.sh[3]	本研究
クロック周波数(MHz)	136	400	625
並列処理数	4	40	50
ファミリ	Spartan-3	Virtex-6	Zynq UltraScale+ MPSoC
ロジックセル数(k)	17	241	256

表 2　DES 実装の消費電力の比較

	hashcat	本研究
デバイス	RTX4090	KV260
処理性能(GOPS)	137	31
消費電力(W)	450	15
消費電力あたりの処理性能(MOPS/W)	304	2067

5. 結言

本研究では DES の鍵探索処理を最新の FPGA 環境で実装した。その結果 FPGA デバイスの進化に伴い性能が向上していることがわかった。また、汎用アクセラレータを使用する場合に比べ消費電力あたりの処理性能が高いことを示した。

FPGA を用いたハードウェア計算は、生成 AI での適用可能性などの指摘も多い。今後、様々な応用について、その性能を検討していく予定である。

参考文献

[1] NIST, “The official document describing the DES standard”, 1999, https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf
[2] https://www.sciengines.com/copacobana/
[3] https://crack.sh/
[4] Bani-Hani R., Harb S., Mhaidat K. and Taqieddin E., ”High-Throughput and Area-Efficient FPGA Implementations of Data Encryption Standard (DES)”, 2014, Circuits and Systems, DOI: 10.4236/cs.2014.53007
[5] AMD, “Kria KV260 Vision AI Starter Kit”, 2024, https://www.amd.com/ja/products/system-on-modules/kria/k26/kv260-vision-starter-kit.html