2A-05

軽量ストリーム暗号のハードウェア実装

岡部　忠†

地方独立行政法人東京都立産業技術研究センター†

1.はじめに

昨今 Internet of Things（IoT）向けのデバイスや人工知能技術が盛んに開発され、市販されている。ここ数年で IoT 向けのデバイスが流通してきたことにより、ネットワーク化された産業機器や民生機器が広く普及している。そして、IoT 向けのエッジデバイスやフォグデバイスは限定的な演算能力をもった小型なマイコンや FPGA といったプログラマブルデバイスを使用することが多い。来たるべき高度にネットワーク化された IoT 社会では、センシングした有意な情報を他者に対して秘匿するセキュアな情報伝達が必須であり、エッジデバイスやフォグデバイスといえども高いセキュリティ要件が課される。膨大な数のエッジデバイスから、フォグそしてクラウドへとデータが集約されていくに従い伝送されるデータ量は非常に膨大となり、高いセキュリティを保ちながら大容量のデータを転送する際には、ストリーム暗号が用いられる。

このような軽量なデバイス向けのストリーム暗号について国際的な標準化が行われ、2012 年に Trivium[1]と Enocoro[2]の 2 つの規格が国際標準として ISO/IEC29192-3 の軽量ストリーム暗号規格に選定された［3］。これらの 2 規格が標準化されて以降も軽量デバイス向けのストリーム暗号は盛んに開発され、提案されているが先行研究でこれらの規格に対するハードウェアの実装性能が報告されているものは少ない。そこで、本稿では ISO/IEC29192-3 以後に提案された軽量ストリーム暗号規格、Espresso［4］と Lizard［5］に対して 90nm や 65nm といったプロセスで製造された FPGA を実装対象とした場合の実装性能を評価した結果について報告する。

2.ISO/IEC29192-3 以降のストリーム暗号

2.1　Espresso

Espresso は鍵長 128bit、初期ベクトル 96bit のストリーム暗号であり、256bit の内部状態保持用の非線形フィードバックシフトレジスタと排他的論理和で構成されている。所定長ビットの秘密鍵と初期ベクトルが初期値として読み込まれ、259 サイクル経過後から有効な鍵系列が 1bit 単位で出力される。この鍵系列は 2^{256}-1 周期の鍵系列である。Espresso の擬似乱数ストリーム生成処理のブロック図を図 1 に図示する。

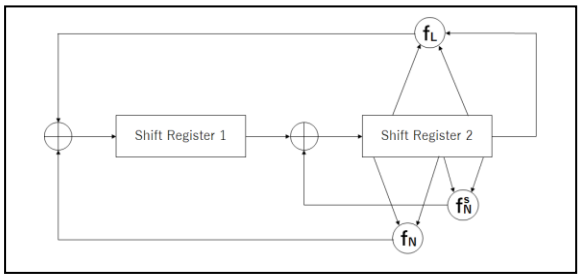

図 1 Espresso のブロック図

図 1 にあるように、2 種類の非線形フィードバックシフトレジスタと数種類の非線形論理演算や排他的論理和から構成されており、入力された暗号化鍵と初期ベクトルから初期化を行った後、毎サイクル 1bit の擬似乱数列が出力される。

2.2　Lizard

Lizard は鍵長 120bit、初期ベクトル 64bit のストリーム暗号であり、31bit と 90bit の 2 種の非線形フィードバックシフトレジスタと排他的論理和や非線形論理演算で構成されている。

図 2 にあるように、2 種類の非線形フィードバックシフトレジスタと数種類の非線形論理演算や排他的論理和から構成されており、入力された暗号化鍵と初期ベクトルから初期化を行った後、毎サイクル 1bit の擬似乱数列が出力される。

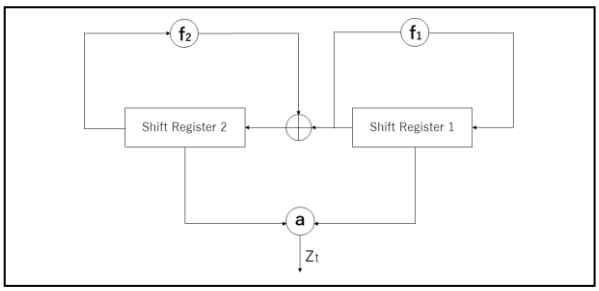

図 2　Lizard のブロック図

3.実装性能

前節で簡潔に述べた 2 種の軽量ストリーム暗

Hardware Implementation of Lightweight Stream Ciphers after International Standard, ISO/IEC 29192-3

Tadashi Okabe†
Tokyo Metropolitan Industrial Technology Research Institute†

号の FPGA 向けの実装性能を評価するとき、これらをどういった回路アーキテクチャで設計開発するかにより実装性能が大きく異なる。Espresso と Lizard は共に回路を構成する要素ブロックが比較的プリミティブなものであるため、アーキテクチャの検討を然程行わずにそれぞれ図 1 と図 2 の構造の通りに設計開発を行った。

実装対象デバイスを FPGA としたときの軽量ストリーム暗号 Espresso と Lizard の実装性能を表 1 に示す。参考として先行研究による軽量ストリーム暗号 Trivium [6]と Enocoro [7]の実装性能も合わせて付記した。実装性能を評価するに際して、ハードウェア開発言語として Verilog HDL を使った。本稿では、設計開発環境として Xilinx 社の統合開発環境 ISE14.7 を使用した。また、本稿では実装対照デバイスとして 90nm プロセスで製造された Xilinx 製 Spartan3 xc3s400-5fg320 と 65nm プロセスで製造された Xilinx 製 Spartan6 XC6SLX16-3CSG324 を用いた。

実装性能における性能指標として、消費する論理素子数である LUT 数、回路の専有面積として Xilinx 製 FPGA で使用される単位のスライス（slice）数、それぞれのストリーム暗号から出力される疑似乱数ストリーム生成のスループット（単位：Mbps）、スループットを占有面積で割った処理効率（単位：Mbps/slice）、シミュレーションによる消費電力（単位：mW）、および消費電力を占有面積で割った電力効率（単位：mW/slice）を記している。消費電力のシミュレーションではリファレンスクロックの動作周波数を 100MHz としてシミュレーションを行った結果を記載している。

実装性能の比較として、Trivium、Espresso や Lizard が毎サイクル 1bit ずつ擬似乱数ストリームを出力されるのに対し、Enocoro では毎サイクル 1Byte ずつ擬似乱数ストリームが出力されるためスループットや処理性能の点では優れていることがわかる。けれども、軽量かつ低電力という点では Espresso や Lizard の方が優れているといえる。

4.まとめ

本稿では、ISO/IEC29192-3 以降に提案された 2 種の軽量ストリーム暗号規格、Espresso と Lizard に対して、FPGA を実装対象デバイスとした場合の実装性能の評価を行った。今後は、本稿で評価に使用したストリーム暗号規格以外の規格との性能比較などを行う必要がある。

5.参考文献

[1] C.De Cannière, et al., “Trivium specifications”, 2006-10-09.

[2] D. Watanabe et al., “Enocoro-80: A Hardware Oriented Stream Cipher,” Second International Workshop on Advances in Information Security, 2008.

[3] “ISO/IEC 29192-3, Information technology - Security techniques - Lightweight cryptography, Part3 Stream ciphers”, 2012-10-01.

[4] E. Dubrova et al., “Espresso: A stream cipher for 5G wireless communication systems”, Cryptography and Communications 9, 273-289, 2017.

[5] A. Kusyanti et al., “Lizard Cipher for IoT Security on Constrained Devices”, IJACSA, Volume 10, Issue 11, 2019.

[6] D. Hwang et al., “Comparison of FPGA-targeted hardware implementations of eSTREAM stream cipher candidates,” State of the Art of Stream Ciphers Workshop (SASC2008), pp.151-162 (2008).

[7] 岡部, “IoT デバイスセキュリティ：ISO/IEC29192-3 軽量ストリーム暗号のハードウェア実装性能評価”, 31th KWS, 324-326, WIP-21.

表 1 FPGA への実装性能

	Device	LUT	Slice	Throughput [Mbps]	Efficiency [Mbps/slice]	Power [mW]	Power-Efficiency [mW/slice]
Trivium [6]	Sp3	—	50	240	4.8	—	—
	Sp3	—	344	13504	39.26	—	—
Trivium [7]	Sp3	294	149	210.4	1.41	4.46	0.030
	Sp6	149	38	270.0	7.11	3.27	0.086
Enocoro [7]	Sp3	267	237	892.8	3.77	16.11	0.068
	Sp6	267	76	1286.4	16.93	9.90	0.130
Espresso	Sp3	77	88	288.8	3.28	0.30	0.003
	Sp6	85	33	464.5	14.1	1.22	0.037
Lizard	Sp3	177	142	110.1	0.71	1.71	0.012
	Sp6	113	68	101.0	1.62	2.11	0.031