L-012

CryptMT の FPGA への実装

FPGA implementation of CryptMT

櫻井　敦規†　　岩井　啓祐†　　黒川　恭一†
Atsunori Sakurai　Keisuke Iwai　Takakazu Kurokawa

1．まえがき

近年の急速なネットワーク化により、通信内容の保全や第三者に対する情報の秘匿など、情報セキュリティに対して大きな関心が寄せられている。そのため、暗号の安全性の評価、標準化には世界各国が強い関心を持って取り組んでおり、そのひとつに次世代のストリーム暗号の選定を行うプロジェクト eSTRYM がある。このプロジェクトに応募された暗号に暗号長周期性、高次元均等分布を持つストリーム暗号 CryptMT がある。CryptMT は独自の新しい構造をしており、未だ十分に検証されていない暗号である[1]ため、本研究では、この暗号を FPGA にハードウェア実装し、その特性を検証することを目的とした。

2．CryptMT の構造

（1）CryptMT の概要

CryptMT は図 1 に示すような Mother generator と呼ばれる線形フィードバックレジスタ 128×156 bit（LFSR）による擬似乱数生成器と、Filter with memory と呼ばれるメモリ付きフィルタを結合したストリーム暗号である。また、Mother generator を初期化するための Booter と呼ばれる機構を持っている。理論的に 2^{19937}-1 の周期と、少なくとも 155 次元に均等分布することが保証されている。

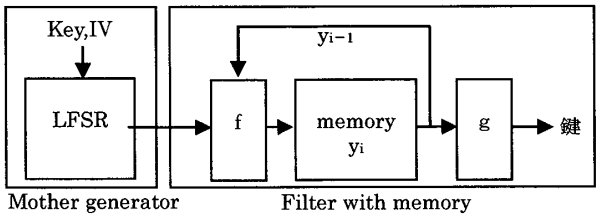

図 1 ：CryptMT

（2）Mother generator 部

CryptMT ver.3 においては Mother generator 部に図 2 に示すような SIMD-oriented Fast Mersenne Twister（SFMT）が用いられている。

（3）Filter with memory 部

SFMT で生成された乱数は、線形漸化式によっているため、予測可能である。そこで、図 3 に示す Filter with memory 部により非線形変換を行い、非線形擬似乱数を生成し、この出力と平文を XOR 演算することにより暗号化を行う。

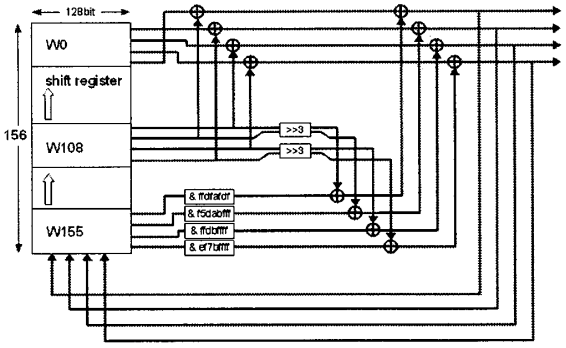

図 2 ：Mother generator 部

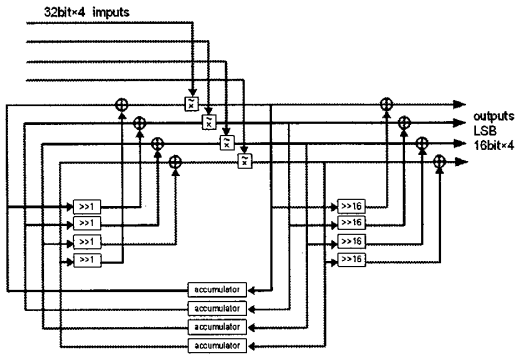

図 3 ：Filter with memory 部

（4）Booter 部

Booter 部は初期ベクトル及び鍵により Mother generator 部のシフトレジスタを図 4 に示す出力で初期化する。図中 H は鍵長 key、及び初期ベクトル IV により決定され、

$$H=(key+IV)\times 2/128$$

で求められる。

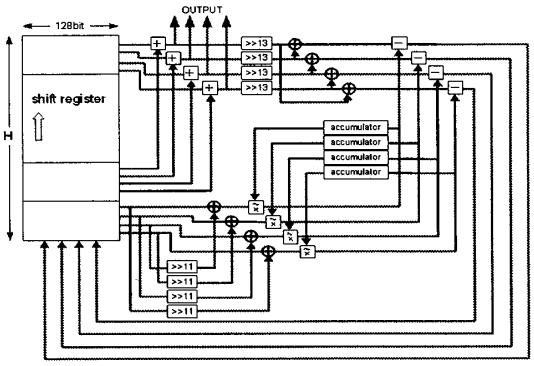

図 4 ：Booter 部

† 防衛大学校　情報工学科

3. CryptMT の実装

3.1 SCAPE へのハードウェア実装

（1）SCAPE の概要

SCAPE は、三菱電機（株）が開発したサイドチャネルアタック評価用プラットフォーム（SCAPE:Side Channel Attack Platform for Evalution）である。SCAPE には、図５に示すように Virtex-ⅡPRO（XC2VP70）が搭載されており、この FPGA に対象回路を搭載することになる。ストリーム暗号は、初期化する際に DPA が可能という研究[3]もあり、その評価を今後行うための基盤とするために、SCAPE を実装プラットフォームとして選択した。

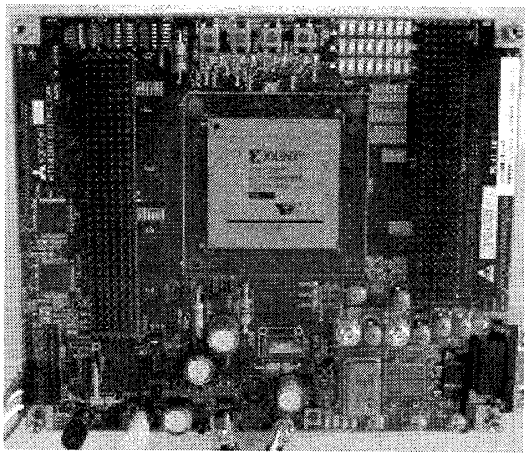

図５　SCAPE の外観

（2）実装環境

回路記述言語は Verilog-HDL を用い、Xilinx 社 ISE10.1.3 にて回路を作成した。

3.2 実装結果

鍵長、初期ベクトル長ともに 128bit の CryptMT を実装した結果を表１に示す。

表１　ハードウェア実装

使用 LUT 数	3524 （FF：1280）
最大周波数	61.733(MHz)
暗号化サイクル	0.125(ck/byte)

表１より、最大周波数と暗号化サイクル数より初期化サイクルを除いた暗号化のスループットが求められる。初期化を除いた暗号化のスループットは 3.951Gbps（理論値）となる。

4．考察

CryptMT の作者が公開しているソフトウェア実装との比較を表２に示す。

その結果、暗号化サイクル及びスループットともにソフトウェア実装したものと比較して、ハードウェア実装したもののほうが高速な動作が可能であることが確認できた。

表２　ソフトウェア実装との比較

	Pentium-M	Athlon64	H/W 実装
動作周波数	1.5GHz	3400＋	61.7MHz
暗号化サイクル (ck/byte)	10.21	7.67	0.125
スループット（理論値）	1.175Gbps	3.546Gbps	3.951Gbps

5　結論

本研究では CryptMT のハードウェア実装を行った。ソフトウェア実装よりも、ハードウェア実装のほうが、低い動作周波数にもかかわらず、高速な暗号化が可能であることを確認することができ、ハードウェア実装の有用性を確認することができた。

しかしながら、今回の実装においては、乗算器など ISE の基本モジュールを用いて実装を行っているため、回路の最適化を行う余地が残っているものと考える。よって、これらを最適化することにより、回路規模のコンパクト化及び高速化が期待できると考えられる。

また、シフトレジスタをブロック RAM に変更することにより、小型の FPGA にも回路を搭載可能になるものと考えられる。さらには、回路を専用 ASIC にすると更なる高速化が期待できるものと考える。

よって、今後の課題として、回路の最適化を行い、更なる高速化、小型化に向けた研究していく必要がある。また、今回はサイドチャネル攻撃の耐性についての評価を実施することができなかったが、サイドチャネル攻撃の耐性についても今後、評価していく必要があるものと考える。

参考文献

[1] “The eSTREAM portfolio”, http://www.ecrypt.eu.org/stream/portfolio.pdf

[2] Matsumoto, M., Saito, M., Nishimura, T. and Hagita, M : ”CryptMT3 Stream Cipher”, New Stream Chipher Designs , Lecture Notes in Computer Science(LNCS), vol. 4986, pp. 7 -19, 2008.

[3] 久門 亨，角尾 幸保，池永 剛，後藤 敏: “eSTREAM ストリーム暗号への差分電力解析”，電子情報通信学会論文誌 A,Vol.J91-A,No.11,pp.1036-1044,Nov.2008.