複数の共通鍵暗号の同一 FPGA 上での比較

中島 裕介 † 小杉 敬和 ††　山本 和正 † 松浦 優彦 † 小柳 滋 ‡
† 立命館大学理工学研究科　†† 立命館大学情報理工学部

1 はじめに

インターネットの普及に伴い，個人がより広帯域の通信回線を利用し，大容量のマルチメディアデータのやり取りが頻繁に行われるようなり，映像配信や音楽配信などのサービスが一般的になってきている．情報漏洩が頻発する現在において，情報漏洩を防ぐ手段として暗号化技術の役割は大きなものとなっており，大規模な電子商取引システムやサービスでの暗号の利用も進んでいる．暗号化技術は数々のセキュリティ技術の中核をなすものの 1 つとして位置づけられており，安全性，暗号化速度，回路規模によって様々なアルゴリズムが要求されている．暗号は大きく分けて公開鍵暗号と共通鍵暗号に分けられ，公開鍵暗号はブロック暗号とストリーム暗号に分けられる．ブロック暗号に対してのストリーム暗号の優位点のひとつにはハードウェア実装時の処理速度の速さとその回路規模の小ささにあるといわれている．今までに様々な暗号アルゴリズムが提案されているが，同一 FPGA 上での検証は十分に行われていないため状況に応じたアルゴリズムの使い分けが難しいと言える．

そこで本論文では共通鍵暗号の中でもストリーム暗号である MUGI，VSC 暗号，またブロック暗号である Camellia に注目して同一 FPGA 上で実装することにより，それぞれの暗号アルゴリズムの特徴を検討することを目的とする．

2 暗号アルゴリズム

現在では暗号アルゴリズムにいくつかの標準化規格・推奨規格が選定されていることもあり，様々な暗号が登場している．一方 VSC は開発されてから比較的新しい暗号であり，どの規格にも選定されていないことから，VSC がどのような特徴を持った暗号かに重点をおいて実験を行う．

	米国政府標準暗号・推奨暗号	電子政府推奨暗号	欧州連合推奨暗号	ISO/ICE 国際標準暗号	インターネット標準暗号
128bit ブロック暗号	AES	AES Camellia	AES Camellia	AES Camellia SEED	AES Camellia SEED
64bit ブロック暗号		MISTY1	MISTY1	MISTY1	
ストリーム暗号		MUGI		MUGI	

図 1: 共通鍵暗号の標準化状況

2.1 VSC[4][5]

VSC(Vector Stream Cipher) は，独立行政法人情報通信研究機構が特許を保有するストリーム暗号方式の一種であり，独自暗号アルゴリズムのカオス理論に基いた多次元的ランダムベクトル列を生成するアルゴリズムである．処理速度の高速性や暗号強度，フレキシビリティに優れていることから動画や医療用画像，CAD といった大容量データのリアルタイムな暗号化・復号化を可能にすると言われている．

VSC128 では鍵長は 128 ビットで，「有限体上のパラメータ付き 2 次置換多項式の変形 Skew Product 変換の巡回的接続をコアとする非線形変換を 8 回繰り返すことによってストリームキーを生成する仕組みとなって」[4] いる．

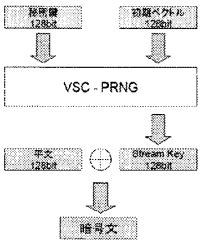

図 2: VSC128

2.2 MUGI

MUGI とは，内部構造に PANAMA と同様の構造を持ち,AES の持つ非線形性を加えた擬似乱数生成器である．ソフトウェア，ハードウェア両方のプラットフォームにおいて高速処理が可能であることを目標として 2003 年に日立製作所において開発された．

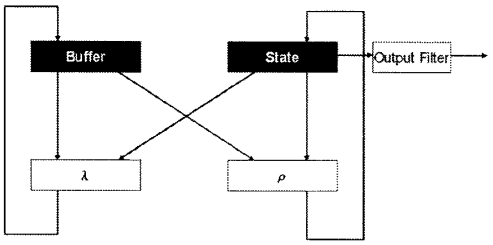

図 3: MUGI

2.3 Camellia[3]

Camelliaとは，NTTと三菱電機により2002年に共同開発されたブロック長128ビットのブロック暗号であり，Feistel構造を採用しているという特徴を持つ．鍵長はAESと同様に128ビット，192ビット，256ビットの3つを選択できる．また，CamelliaにはAESと同等の互換性があり，ハードウェアでの実装時に消費電力を抑えることができ，高速な暗号化・復号化に優れている．データ攪拌部では，鍵長が128ビットのときは18段のFeistel構造と6段ごとに全単射関数のFLとFL^{-1}から構成されている．[3]

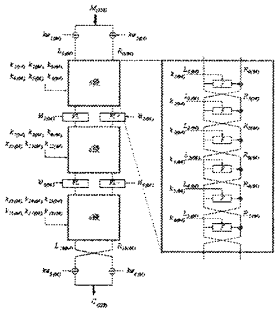

図 4: Camellia[3]

3 実験方法

本論文では，VSC，MUGI，Camelliaに焦点をあてて同一FPGA上で実装し，それぞれの回路規模，処理速度を示す．これら3つの暗号アルゴリズムは今までに同一FPGAでの比較が行われていないことから，それぞれのアルゴリズムの特徴を見出すために重要であると言える．実装にはXilinx社のISEを用いて実現する．また，FPGAにはVertex-5を用いる．

3.1 ISE

ISEとは，Xilinx社から提供されているロジックデザインに必要なすべてのツールを統合した開発環境で，FPGAおよびCPLD製品に対応している．HDL合成シミュレーション，インプリメンテーション，デバイスフィット，およびJTAGプログラミングが迅速かつ直観的に実行できるソフトウェアである．[7]

3.2 Vertex-5

Vertex-5 FPGAは，1.0Vトリプル酸化膜テクノロジを採用した，世界初の65nmプロセスFPGAである．選択するデバイスよって，最大330,000のロジックセル，1,200個のI/Oピン，48個の低消費電力トランシーバ，内蔵されたPowerPC 440，PCIeエンドポイント，およびイーサネットMACブロックを提供している．[7]

4 実験

VSC，MUGI，Camelliaを実験方法により実現した．ここに実験結果を示す．

表 1: 実験結果

	VSC128	MUGI	Camellia
Slice Registers	389	975	386
Slice LUTs	1126	1758	8111
Bit Slices	381	734	386
処理速度	1.90Gbps	17.56Gbps	3.02Gbps

この実験結果より，VSCは回路規模を小さく実装できるることが分かった．MUGIは他の2つの暗号より処理速度が速い結果となった．

5 おわりに

本実験結果をもとに3つの暗号についてさらに深い考察をしていきたい．また，現在推奨されている他の暗号アルゴリズムも同一FPGA上で実装し，回路規模，処理速度の比較を行い，それぞれのアルゴリズムの特徴を見出すことを目指す．

参考文献

[1] 株式会社日立製作所，疑似乱数生成器 MUGI 仕様書 Ver.1.3, http://cryptrec.nict.go.jp/ cryptrec_03_spec_cypherlist_files/PDF/10_02jspec.pdf, 2002

[2] 株式会社富士通研究所，暗号アルゴリズムの評価 PANAMA, http://www2.nict.go.jp/y/y213/ cryptrec_publicity/rep_ID0037.pdf, 2001

[3] 日本電信通話株式会社，三菱電機株式会社，128ビットブロック暗号 Camellia アルゴリズム仕様書, http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/06_01jspec.pdf, 2001

[4] 独立行政法人通信総合研究所カオス暗号チッププロジェクト，VSC128 仕様書，http://www.chaosware.com/vsc128.pdf, 2004

[5] ソフトバンク・テクノロジー株式会社，128 ビット VSC 暗号の安全性評価，http://www.tech.softbank.co.jp/release/2004/pdf/vsc040406.pdf, 2004

[6] 梅野健，スケーラブルなカオス暗号とハードウェア実装評価，http://ne.nikkeibp.co.jp/award/papers/2003co02.pdf, PP.1-4, 2003

[7] ザイリンクス株式会社，http://japan.xilinx.com/