5N－8

FPGAによる並列暗号解析装置の構成 (1)
–DES暗号等の鍵探索 –

飯田 全広†, 水上雄介‡, 高橋 勝己‡, 浅見 廣愛‡, 佐藤 裕幸‡
†三菱電機エンジニアリング (株), ‡三菱電機 (株)

1 はじめに

近年のコンピュータと通信の融合は，電子商取引 (EC: Electronic Commerce) に代表される流通機構の電子化をもたらした．通信媒体を通る情報の盗聴や偽造防止等の安全性の確保は暗号アルゴリズムに大きく依存する．したがって，強い暗号アルゴリズムの開発が重要である．

一方，現在の暗号技術は暗号アルゴリズムだけではなく，暗号解読技術も同様に発展している．とりわけ，計算機能力の増大によって，従来は不可能とされてきた共通鍵ブロック暗号の全数探索による解読を可能とした．1997年のRSA社が行なった“DES(Data Encryption Standard) Challenge”では56bit長のDESの暗号鍵が，インターネットを通じてリンクされた数千のコンピュータによって解かれた[1]．また，1998年の“DES Challenge II”では鍵探索が3日という記録を作った装置[2]についての報告がなされた．これらにより，全数探索による解読危険性がまた明らかにされたといえる．

以上から，強い暗号アルゴリズムの開発には，暗号解読法，暗号解析技術の研究が共に重要であることが判る．一般に暗号解析には膨大な暗号結果を収集する必要があり，これらを効率よく行うことが求められている．そこで我々は，並列処理技術を用い高速に暗号処理を行う暗号解析装置の研究・開発を行ってきた．

本稿では，我々が提案しているFPGA (Field Programmable Gate Array) ベース並列マシンRASH (Reconfigurable Architecture based on Scalable Hardware) [3][4]を鍵探索に適用した時の性能などについて報告する．

2 RASHの構成

2.1 鍵探索への適用可能性

RASHは以下の要件を満たす装置として開発された．

1. アルゴリズムを回路として実装する．
2. 回路化・並列化によって，ソフトウェアでの性能を大幅に上回ること．
3. 装置構成がスケーラブルであること．

これらの要件から，RASHが鍵探索用途に適した装置であると考えた．

Parallel Cryptanalysis Machine using FPGA(1)
–DES Key searching–
M.Iida†, Y.Mizukami‡, K.Takahashi‡, H.Asami‡, H.Sato‡
†Mitsubishi Electric Engineering Co.,LTD., ‡Mitsubishi Electric Corporation

2.2 装置構成

複数のアルゴリズムに対応するために，処理を行うデバイスとして，何度でも回路が書き換えられるSRAMタイプのFPGAを採用している．

演算ボード上には8個のFPGAが実装され，最大6枚の演算ボードを一つの筐体に搭載することが可能である．また，演算ボード単位または筐体単位で増減可能にすることでスケーラビリティが確保されている．

図1にRASHのハードウェア構成を示す．

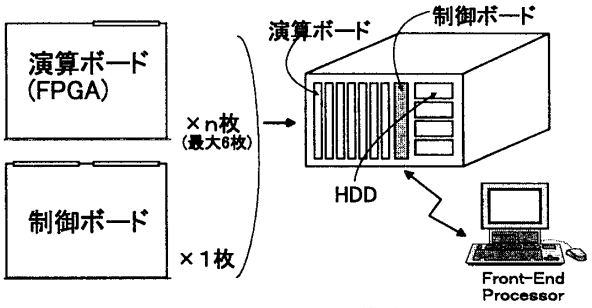

図 1: RASHの構成

Front-End Processor(以下, FEPと略す)は，ユーザインタフェース，FPGAの回路データの管理および筐体間をまたがるデータ転送の制御を行う．FPGAの回路データはFEPから筐体内の制御ボードに送られ，制御ボードから演算ボード上の各FPGAにダウンロードされる．

また，FEP-本体間のI/FはEthernetで接続され，本体内の各ボードはCompactPCIバスで接続されている．

2.3 演算ボードの構成

演算ボードの主な仕様を表1に示す．

表 1: 演算ボードの主な仕様

項目	仕様
基板サイズ	233mm × 160mm (6U)
外部バス	CompactPCI Bus(32bit 同期)
内部バス	32bit 非同期バス
搭載メモリ	2MB
FPGA	ALTERA社 FLEX10K100A
FPGAのゲート規模	62K ～ 158K ゲート相当
搭載FPGA個数	8個 /1 演算ボード
FPGA 間接続	メッシュ接続，内部バス
FPGA クロック	16種類から選択

演算ボード内で各FPGAは図2のようにバスと隣接FPGAの直接結線で接続され，それぞれ独立した

クロックで動作可能である．また，全 FPGA に共通クロックも供給されている．

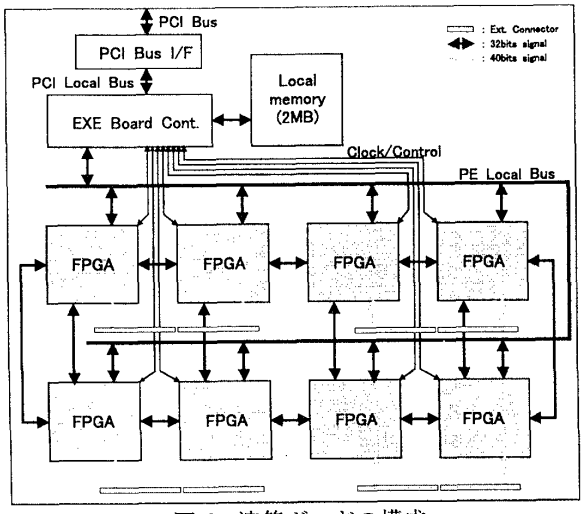

図 2: 演算ボードの構成

3 性能評価

3.1 DES 暗号の実装結果

図 3に FPGA 上に実装した DES 暗号の構成を示す．実装した回路は，3 個の並列動作可能な DES 暗号コア，DES コアの制御回路およびバスインタフェース回路からなる．DES 暗号コアは，F 関数 1 段を 16 回ループすることで 1 回の暗号結果を得るものである．

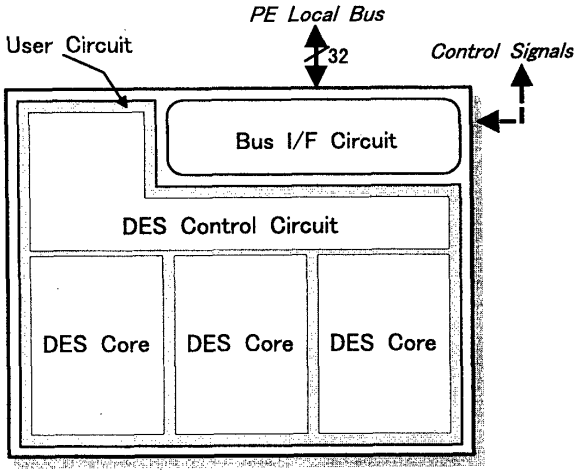

図 3: DES 回路の FPGA への実装

DES の暗号回路とバスなどの共通回路を合わせた回路規模，暗号化性能を表 2に示す．

表 2: DES 暗号の実装結果

項目	内容
DES 回路	F 関数 1 段の 16 回ループ
DES 回路個数	3 個 /FPGA
動作周波数	40MHz
全数探索性能	480Mbps/FPGA

3.2 性能比較

DES 暗号専用 LSI や汎用マイクロプロセッサ上で DES の暗号化を行った場合と FPGA の単体性能比較を表 3に示す．

FPGA 単体の性能においては専用 LSI の性能には及ばないが，マイクロプロセッサの性能を大幅に上回っている．演算ボード単位の性能は FPGA 単体性能の 8 倍，すなわち 3.8Gbps であるので，専用 LSI に匹敵する性能が得られたことが判る．

表 3: DES 暗号の性能比較

対象	性能
Intel Pentium(300MHz)[5]	53Mbps
DEC α チップ (300MHz)[6]	137Mbps
FPGA(1 段,16loop,3 回路,40MHz)	480Mbps
DES 暗号 LSI(16 段,2 回路,33MHz)[7]	4.2Gbps

4 鍵探索以外の応用

今回の評価は DES の全数探索に用いた場合を示したが，鍵探索以外に暗号の入出力の統計データ収集用回路等を追加することで，高速なデータ収集が可能である．

また，新しい暗号アルゴリズムの事前評価にも使用可能である．

5 おわりに

本稿では，FPGA ベース並列マシン RASH を暗号解析に適用し，DES の全数探索で性能を評価した結果について述べた．RASH は FPGA を用いているため様々な暗号に対応でき，さらに暗号回路以外に情報収集用の回路を付加できる点から暗号解析に向いた装置といえる．また，性能的には専用の暗号 LSI には及ばないものの一般のプロセッサよりは大幅に高速処理できる．

今後は DES 以外の暗号の性能評価，暗号解析ツールとしての周辺ソフトウェアの整備等を行う予定である．

参考文献

[1] “RSA - DES Cracked!,” DES Challenge home page, RSA Data Security, Inc.
Available at http://www.rsa.com/des/

[2] “EFF DES Cracker Project,”
Available at http://www.eff.org/descracker/

[3] 中島, 森, 佐藤, 高橋, 浅見, 水上, 飯田, 新留, “FPGA ベース並列マシン RASH の概要,” 情報処理学会第 58 回全国大会 1H-08, 1999

[4] 浅見, 佐藤, 飯田, 森, 中島, “FPGA ベース並列マシン RASH のシステム機能と構成,” 情報処理学会第 58 回全国大会 1H-09, 1999

[5] Bruce Schneier, Doug Whiting, ”Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor” Proceedings of 4th International Workshop FSE97, Lecture Notes In Computer Science 1267, Springer Verlag pp.242 - pp.259 1997

[6] Eli Biham, “Fast Software Encryption”, 4th International Workshop, FSE’97 Proceedings, 1997

[7] 飯田, 高橋, 宮田, 松本, “タイム - メモリトレードオフ解読法による暗号強度評価 装置の実現性検討”, 1998 年暗号と情報セキュリティシンポジウム講演論文集, SCIS98-6.2C, 1998