2S-08　FPGA ベース並列マシン RASH における TMTO 法暗号解析の実装 (2) ～性能評価～

飯田全広† 浅見廣愛‡ 中島克人‡ 森伯郎‡

†三菱電機エンジニアリング（株） ‡三菱電機（株）

1 はじめに

近年の計算機性能の向上から，全数検索法による鍵探索が実現可能になり注目を集めているが，この手法は暗号化に要する計算量が多く，暗号文を入手してから解読するまでの時間が極めて長い．一方，テーブルルックアップ法は，鍵探索時の計算量は少ないがテーブルサイズが膨大になるという欠点があった．そこでこれらの問題を緩和する手法として，鍵探索時の計算量が全数探索より少なく，記憶量がテーブルルックアップ法より少ない TMTO 法 (Time-Memory Trade-Off Cryptanalysis)[1] が提案されている．我々も専用 LSI を用いた TMTO 法による暗号解析装置の提案 [2] を行っているが，TMTO 法では事前計算フェーズと鍵探索フェーズで異なるロジックが要求されるため，それぞれの機能を包含する LSI を構成する必要があった．

一方，FPGA(Field Programmable Gate Array) は，集積度と速度の向上が著しく，ASIC(Application Specific IC) 等の適用領域を侵食しつつある．また，FPGA は回路を変更できると言う ASIC にはない特徴を持つことから，フェーズ毎に回路機能を変更したい TMTO 法に適した LSI と言える．

我々は FPGA の再構成性を活かした柔軟で拡張性の高い並列マシン RASH (Reconfigurable Architecture based on Scalable Hardware)[3] を開発し，DES 暗号の全数探索 [4] や CAM(Contents Addressable Memory) を用いた TMTO 法による鍵探索 [5] に適用してきた．本稿では，CAM の代わりに汎用性の高い SDRAM 拡張メモリモジュールを搭載した RASH 上で，TMTO 法による鍵探索を実現した結果について報告する．

2 TMTO 法向け RASH の構成

2.1 装置構成

図 1 に RASH のハードウェア構成を示す．

一つの筐体内には，8FPGA が実装された演算ボードを 6 枚搭載し，その内の 1 枚の演算ボードにはドータメモリカードを実装している．ドータメモリカードは 1FPGA 当たり 64MB の外部メモリを提供している．

2.2 演算ボードの構成

演算ボードの主な仕様を表 1 に示す．

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．さらに，拡張コネクタには各 FPGA から 40 ビットの信号が直接出ており，この拡張コネクタに拡張カード (ドータカード) を搭載可能である．

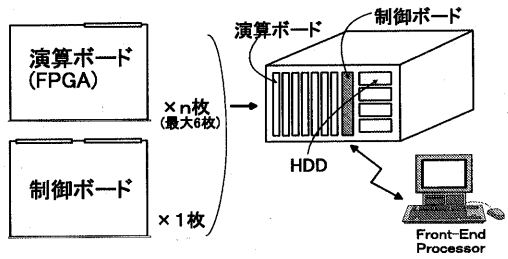

図 1: RASH の構成

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	SRAM 2MB
FPGA	ALTERA 社 FLEX10K100A-1
搭載 FPGA 個数	1 演算ボードあたり 8 個
FPGA 間接続	メッシュ接続，内部バス
FPGA クロック	16 種類 (4.9MHz～60MHz) から 1 つを選択
拡張コネクタ	各 FPGA から 40 ビット

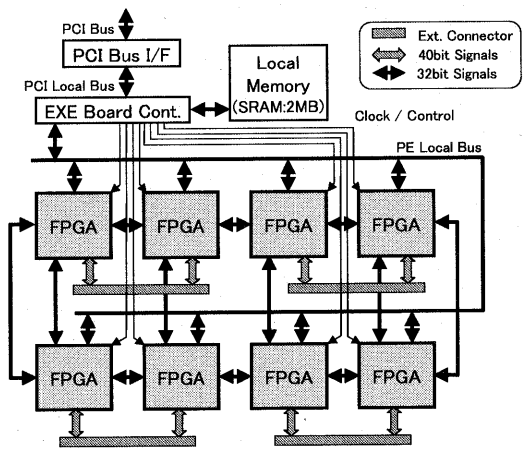

図 2: 演算ボードの構成

2.3 ドータメモリカードの構成と機能

図 3 にドータメモリカードの構成を示す．実際のドータメモリカードはこの構成 2 つを同一基板上に実装している．演算ボード上の FPGA から 40bit の信号が拡張コネクタを通して SDRAM コントローラに接続され，ドータメモリカードは 2 つの SDRAM モジュール (S.O.DIMM) をそれぞれ 2 つづつの FPGA で共有する．

図 4 に示したように，SDRAM コントローラは通常の SDRAM モジュールのアクセス制御のほかに，TMTO 法のヒットマップ検索機能を付加している．この機能は

Implemantaion TMTO Cryptanalysis on an FPGA based Parallel Machine RASH(2) – Efficiency Evaluation –
M.Iida, H.Asami, K.Nakajima, H.Mori
†Mitsubishi Electric Engineering Co.,LTD., ‡Mitsubishi Electric Corporation

演算ボード上のFPGAから出力されるアドレスのデータに1が立っている場合にFPGAへ割込みを発生させる機能である．この機能を用いてFPGAはヒットマップ検索をドータメモリカードと協調して実行する．ヒットマップ検索機能をメモリカード側で処理することで，FPGAの回路規模を削減するできるだけではなく，データの受け渡しがないことからヒット判定の時間を早くすることもできる．データのリード後にFPGA側で判定する場合，判定までに10クロック程度かかるところが，DESの暗号化サイクル(DESコアを2個搭載しているため8クロック)内にヒット判定が完了する．これによって，ヒット判定のためにFPGAの動作を止めることなく処理することができる．

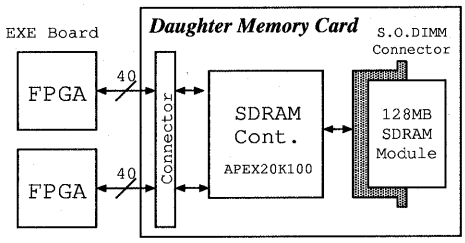

図 3: ドータメモリカードの構成

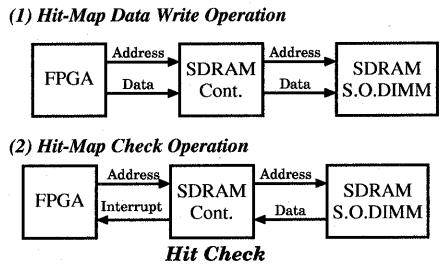

図 4: 鍵探索動作

3 性能評価

3.1 DES暗号の実装結果

図5にFPGA上に実装した事前計算用DES回路と鍵探索用DES回路の構成を示す．事前計算用DES回路は8段パイプライン構成のDESコアとローカルバス・インタフェース，制御回路からなり，鍵探索用DES回路は1段構成のDESコアとメモリカード・インタフェース，ローカルバス・インタフェース，および制御回路からなる．また，各フェーズのDES回路の実装結果を表2に示す．

表 2: DES暗号の実装結果

項目	事前計算用 DES 回路	鍵探索用 DES 回路
DES 回路構成	F 関数 8 段 2 回ループ	F 関数 1 段 16 回ループ
DES コア回路個数	1 個	2 個
論理規模	4173 LEs	3373 LEs
動作周波数	45MHz	42MHz

3.2 性能評価

TMTO法に基づくDES暗号の鍵探索の目標を2時間程度とした場合において，前述のRASHの構成で必要な台数を見積もる．

鍵探索回路の性能は，TMTO法のパラメータ$T = 2^{21}$から$42M/(16 \times 2^{21}) = 1.252$(探索表/秒)となり，2時間で鍵探索を完了するための回路数は，

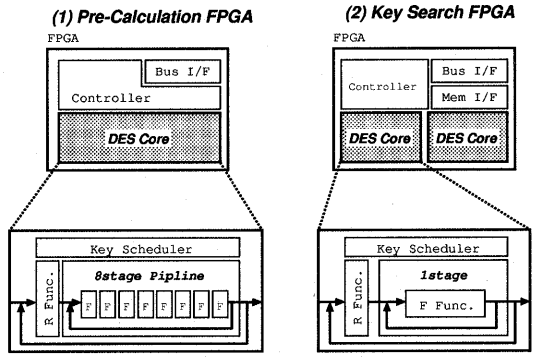

図 5: 事前計算用DES回路と鍵探索用DES回路の構成

$$2^{22}/(1.252 \times 3600 \times 2) = 466 \text{ 回路}$$

となる．これは演算ボード30枚に相当し，前述のRASHの構成では1筐体にドータメモリを搭載した演算ボードが1枚であることから，装置30台で実現可能である．

次に装置を30台とした場合の事前計算時間を見積もる．事前計算で作成する探索表の総エントリ数は，TMTO法のパラメータL (2^{22}) とM(2^{14}) の積であることから，64Gエントリとなる．一方，事前計算回路の性能は1FPGA当たり$45M/(2 \times T)$(エントリ／秒)となり，TMTO法のパラメータ$T = 2^{21}$を代入すると，約10.73(エントリ/秒)である．また，装置30台に搭載される回路数は30台$\times$6ボード$\times 8FPGA = 1440$回路である．以上から，事前計算を行うと，

$$64G/(1440 \text{ 回路} \times 10.73 \times 3600 \times 24) = 51.5 \text{ 日}$$

となり，約52日で計算が完了することになる．

4 おわりに

本稿では，FPGAベース並列マシンRASHをTMTO法による暗号解析に適用した結果について述べた．DES暗号を対象に鍵探索の目標を2時間程度とした場合，最大構成のRASH装置30台で実現でき(事前計算は約52日)，これは専用LSIを用いた場合[2]の倍程度の規模である．RASHはFPGAの回路を変更でき様々な暗号方式に対応できることから，専用LSIより高い柔軟性を持つ暗号解析ツールとして有効といえる．

参考文献

[1] M.E.Hellman, "A cryptanalystic time-memory trade-off," IEEE Transaction on Information Theory, Vol.IT-26, No.4, pp-401-406, 1980.

[2] 高橋, 飯田, 水上, 山崎, 宮田, 中島, 松本, "タイムメモリトレードオフ解読法に基づく暗号強度評価装置の実現性について," 情報処理学会論文誌, Vol.40, No.8, pp-3318-3328,1999-8.

[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, 飯田, 中島, 森, "FPGAベース並列マシンRASHでのDES暗号解析処理の改良," 情報処理学会論文誌：ハイパフォーマンスコンピューティングシステム, Vol.41, No.SIG 5(HPS 1), pp-50-57,2000-8.

[5] 高橋, 飯田, 中島, "FPGAベース並列マシンRASHのタイムメモリトレードオフ解読法の適用," 情報処理学会第60回全国大会 2J-01, 2000.