5N－9

FPGAによる並列暗号解析装置の構成 (2)
－ASICとの比較－

高橋 勝己, 飯田 全広†, 水上雄介, 中島 克人, 宮田 裕行

三菱電機 (株), †三菱電機エンジニアリング (株)

1 はじめに

近年, インターネットの急速な広がりなどにより, 通信の安全性確保が注目されるようになってきた. 安全性確保では, 暗号化や復号, 及び, これらを用いた認証等の技術と同様, 暗号自体の解析技術も重要な技術の1つである.

1970年代前半に米国標準暗号として採択されたDES(Data Encryption Standard)は, これまで, 差分解読法や線形解読法などの統計的手法から全数探索まで様々な解析・検討の対象として用いられてきた. RSA社が行なった"DES Challenge I,II"においても, インターネット上の計算機を数千台規模で接続したチームやASIC(Application Specific Integrated Circuit)を使用した専用装置によって, 全数探索の手法による鍵探索に成功したという報告がなされている[1].

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[2][3]を用いてDES暗号の鍵探索を行なった場合の性能と他のASICをベースとした専用装置と比較し, RASHの暗号解析装置としての性能や拡張性について報告する.

2 暗号解析:DES全数探索

専用装置やWS(ワークステーション)/PCクラスタを用いてDESの全数探索を行なう装置の試算や実例について, 性能を比較したものが表1である. これらの装置は, その用途において絶対性能を求めるか, 適用範囲の自由度, 開発コスト等の条件に従って, "ASIC", "FPGA", "WS/PCクラスタ"の使い分けがなされる.

2.1 ASICベースの装置

ASICベースの装置は, 目的に特化したASICを使用している分, 絶対性能で勝る. このため, 用途は非常に限定されるが, 高い絶対性能を求める場合には, ASICをベースとした装置が適している.

2.2 FPGAベースの装置

FPGAベースの装置は, ASICベースの構成とほぼ同じ性質を持つが, FPGA内の回路情報の書き換えにより, その用途を変更できる点が大きく異なる. このため, 用途に自由度を残した上で, 高い絶対性能を求める場合には, FPGAをベースとした装置が適している.

Parallel Cryptanalysis Machine using FPGA(2)
-compare ASIC-
K. Takahashi, M. Iida, Y. Mizukami, K. Nakajima, H. Miyata
Mitsubishi Electric Corporation, †Mitsubishi Electric Engineering Co.,LTD.

2.3 WS/PCクラスタ

WS/PCクラスタは, システムの構築や様々なアルゴリズムの試用が容易であるという特徴を持っているが[1], プログラムによる鍵探索性能(暗号化性能)は, 数十～百数十Mbps程度であるため, 全数探索を行なうためには必要とする台数が数千台規模となり現実的ではない.

3 ASICとの比較

3.1 全数探索性能の比較

表1において当社ASIC版とある装置は, タイムメモリートレードオフ解読法(以下TMTO法と略す)を用いて鍵を探索する装置だが[7], この装置がもつ全数探索の機能に注目し, RASHを用いたDES暗号の全数探索と比較する. これは, 両者がボードや筐体単位のスケーラビリティを確保しており, ハードウェアの構成も非常に似通っているためである. この2つの仕様を比較したものが表2である.

表2: 当社ASIC版とRASHの比較(全数探索)

	当社ASIC版	RASH
使用チップ	ASIC	FPGA
回路規模	150KGate推定	92KGate相当
バス	VME	CompactPCI
基盤サイズ	233×160mm	233×160mm
F関数実現方式	パイプライン	16段ループ
動作周波数	33MHz	40MHz
暗号回路性能	2,112Mbps	160Mbps
暗号回路/チップ	2個	3個
チップ/ボード	4個	8個
ボード/筐体	13枚	6枚
装置性能	3.5Tbps(16筐体)	0.74Tbps(32筐体)
全数探索所要日数	15.2日	72.4日

両装置のDES回路の実装は, DESが持つ16段のF関数を単位として見た場合, ASIC版は2段を単位とした8直列のパイプライン, RASHは1段を16回ループさせるという違いを持っている. 従って, 暗号化1回路で比較した場合, RASHの暗号化スループット性能比は1:14だが, レンテンシ性能ではASIC版で241nsec, RASHで400nsとなり、その比は3:5程度になる.

なお, 装置性能の比較においては, RASHが当社ASIC版の基本構成とほぼ同じ体積となる構成を想定した. この比較では, 今回のRASHを用いた実装でも, ASIC版の5倍程度の時間(2カ月半)で全数探索を行なうことができる.

[1]DESの全数探索では, 探索問題の分割コストは非常に小さいため, WS/PCクラスタを用いた分散処理も容易に実現できる.

表 1: 各専用装置の鍵探索性能

		動作周波数	チップ内 DES 回路数	チップ 暗号化性能	全数探索 所要時間	想定装置構成・規模 (チップ単価)
ASIC	Eberle[4]	250MHz	1	1,000Mbps	16 日	100 万ドル規模 ($300.0)
	Wiener[5]	50MHz	1	3,200Mbps	3.5 時間	100 万ドル規模 ($10.5)
	EFF DES Cracker[6]	2.5MHz	24	3,800Mbps	9 日	29 ボード,2 シャーシ
	当社 ASIC 版 [7]	33MHz	2	4,224Mbps	15 日	16 筐体
FPGA	RASH[8]	40MHz	3	480Mbps	72 日	32 筐体
PC/WS	Pentium[9]	300MHz	−	53Mbps	1,007 日	1000 台規模
	DEC α[10]	300MHz	−	137Mbps	390 日	1000 台規模

3.2 TMTO 法性能の比較

RASH は, CAM(Contents Addressable Memory)[2]を搭載したドータボードの付加, 及び, 回路情報の書き換えによって, 当社 ASIC 版と同様に TMTO 法による鍵探索装置として用いることができる. TMTO 法は, ある平文を想定して作成した大量の表を予め用意し, これを用いて鍵探索を行なう方法である. 表作成には時間を要するが, 鍵探索に要する時間は短くて済む[3].

表 3は, 当社 ASIC 版と同じパラメータで TMTO 法を実現した場合 [7] の両装置の性能を表 2と同じ基準で比較したものである. TMTO 法では, 表作成・鍵探索共に DES の暗号化に簡単な加工を付加した変形暗号化が動作の基本となる[4]. RASH において, ドーターボードを付加したボードはボード 2 枚分のスロットを必要とするため, 付加するボードは筐体毎に 1 枚のみとした. 従って, 鍵探索時には筐体毎に 1 枚, 全 32 枚を使用して鍵探索が行なわれる. また, FPGA 内にもドーターボードの制御回路が必要となるが, 鍵探索時のみ制御回路込みの回路情報に書き換えることで, 制御回路追加による表作成時の性能低下を防いでいる.

表 3: 当社 ASIC 版と RASH の比較 (TMTO 法)

	当社 ASIC 版	RASH
表作成所要期間	1 カ月	6 カ月
鍵探索所要時間	64 分	122 分

なお, ドーターボード付加を表作成終了後に行なう場合には, "6 枚 / 筐体" とできるため, 表作成期間を 5 カ月程度に短縮できる.

3.3 適用範囲の比較

ASIC を用いた専用装置では, 適用範囲を拡張する場合, 予めその拡張を想定し, 機能を付加させておく必要がある. 3 直列の DES である Triple-DES に対応する場合も, ASIC 版では DES 回路を接続するための機能を予め組み込んでおかなければならないが, FPGA 版では 3 つの独立した DES 回路を接続した回路情報に書き換えることで対応することができる. 3 直列以外の組合せも同様に実現できる. DES 以外にも, FEAL,RC5,Skipjack などの共通鍵暗号はもちろん, 楕円暗号等についても回路規模が大きくないものは ASIC と同様に実装することができる.

また, FPGA で構成できるゲート規模には ASIC 以上に制限があるが, RASH には隣接する FPGA 間でデータを送受信するための通信路が用意されているため, 複数 FPGA で 1 つの機能を実現することも可能である. このように, RASH は暗号解析装置として見た場合にも広い適用範囲を持っている.

4 おわりに

本稿では, FPGA ベース並列マシン RASH を DES の全数探索に用いた場合の性能について, 他の装置と比較した結果について述べた. 本装置は, 異なる暗号への対応はもちろん, TMTO 法のように処理が複数のフェーズに分かれており, 必要となる機能が異なる場合にも, 回路情報の書き換えによって対応することができる. 今後も, RASH の暗号解析装置としての適用範囲の検証を継続する予定である.

参考文献

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

[2] 中島他, "FPGA ベースの並列マシン RASH の概要," 情報処理学会第 58 回全国大会 1H-08, 1999

[3] 浅見他, "FPGA ベースの並列マシン 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

[4] H.Eberle, "High-speed DES implementation for network applications," Advances in Cryptology - Proceedings of CRYPTO'92, Lecture Notes in Computer Science, Vol.740, pp521-539, Springer-Verlag, 1993

[5] M.J.Wiener, "Efficient DES key search," Technical Report TR-244, School of Computer Science, Carleton University, Canada, May 1994, Presented at the Rump Session of CRYPTO'93.

[6] "Cracking DES: Secrets of Encryption Research, Wrietap Politics & Chip Design," Electronic Frontier Foundation.

[7] 飯田他, "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," 電子情報通信学会 1998 年暗号と情報セキュリティのシンポジウム, SCIS'98-6.2.C, 1998.

[8] 飯田他, "FPGA による並列暗号解析装置の構成 (1)–DES 暗号等の鍵探索 –," 情報処理学会第 58 回全国大会 5N-08, 1999

[9] B.Schneier and D.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.

[10] E.Biham, "A Fast New DES Implementation in Software," Proceedings of 4th International Workshop FSE97, Lecture Notes In Computer Science 1267, Springer Verlag pp.260 - pp.272, 1997.

[2]TMTO 法において, 鍵探索時の表の格納に用いる.

[3]ただし, 全数探索と異なり, 一部探索できない鍵の範囲が生じる.

[4]RASH では 17 段ループとすることで動作周波数を変えずに実現するものとしている.