FPGAベース並列マシンRASHによるパスワード解析

6K−7

佐藤裕幸[I]，浅見廣愛[I]，中島克人[II]，森伯郎[III]，
飯田全広[IV]，山田美和[V]，澤田一郎[V]，角田淳一[V]
I三菱電機（株）情報技術総合研究所，II三菱電機（株）本社開発業務部，III三菱電機（株）鎌倉製作所
IV三菱電機エンジニアリング（株），V警察大学校 警察通信研究センター

1 はじめに

パスワードの付与は、一般にシステム管理者等の監視を伴わないため、そのセキュリティは、個々人の意識に依存する。そのため、不正アクセスからの防御には、パスワードの脆弱性の検査が重要となる。我々は、この検査を効率的に行うための解析システムをFPGAベース並列マシンRASH上に開発したので、報告する。

2 FPGAベース並列マシンRASH

RASH[1]は、最新デバイス技術の適用による高速化および大集積化の進展が著しいFPGA（Field Programmable Gate Array）の柔軟性を最大限に活かし、かつ柔軟性の高い可変構造型並列計算機である。図1にRASHのハードウェアの構成を示す。RASHの基本構成（1ユニット）は最大6枚の演算ボードと、制御ボード、ディスク等から成る。演算ボードはCompactPCI基板上に8個のSRAMタイプのFPGA（10万ゲート相当）を搭載している。これらのFPGAは制御用のコントローラにローカルバスで接続されており、さらに32bitの信号線でメッシュ接続されている。また、演算ボード上には2MBのSRAMが搭載されている他、機能拡張のための拡張ボード用のコネクタが用意されている。用途に応じてメモリ等を搭載したドータボードを接続することにより、性能/機能を向上できるようになっている。

制御ボードはPentium MMX（233MHz）を搭載した市販のボードであり、演算ボードへのデータの分配等を行う。ユニット内の制御ボード、各演算ボード間はCompactPCIバスで接続され、複数ユニット間やFEP(Front End Processor)とはEthernetで接続が可能である。FEP及び制御ボード上には、複数ユニットをシングル・システムとして扱うための制御ソフトウェアが搭載されている。

このRASH上には、これまでDES（Data Encryption Standard）暗号鍵の全数探索[2]やTMTO（Time-Memory Trade-Off）法探索[3]の回路を実装し、高い探索性能を上げている。

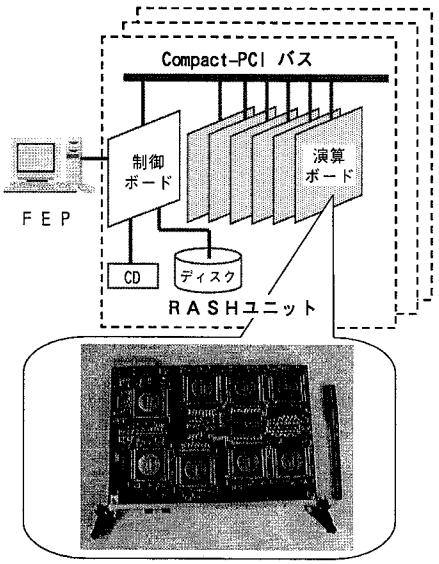

図1　RASHのハードウェア構成

3 パスワード解析機能

今回開発したパスワード解析機能は、平文と暗号文から対応する暗号鍵を探索する際に、全ての鍵をしらみつぶしに探索する全数探索ではなく、鍵を文字列と見なして一部の文字を限定して探索するものである。その処理は、GUIにより設定された探索条件に基づいて、ソフトウェアが探索文字列のワイルドカード部分の上位の展開を担当し、FPGA回路が下位の展開、暗号化及び暗号化結果と与えられた暗号文との照合を担当する。今回開発したFPGA回路は、ASCIIの可読文字（#20〜#7F）のみを探索対象とするDES暗号である。

探索条件の設定においては、対象となる暗号法や限定文字種を変更可能なように、FPGA回路を指定できる。また、探索文字列は、?が任意の一文字を*が0個以上の?を示すワイルドカード文字を含んだ文字列であり、ソフトウェアが担当するワイルドカード文字の取り得る値を指定することもできる。更に、探索文字列が暗号鍵の文字数に満たない場合に補完する文字及び左右どちらにそれを補完するかも指定できる。

探索の実行中は、図2に示すような画面により処理の進捗状況（探索速度、探索完了率、残り探索予想時間等）を定期的に更新表示する。

Password analysis on an FPGA-based parallel machine RASH

Hiroyuki Sato[I], Hiroai Asami[I], Katsuto Nakajima[I], Hakuro Mori[I], Masahiro IIDA[II], Miwa Yamada[III], Ichiro Sawada[III], Junichi Kakuta[III].
I:Mitsubishi Electric Corp., II:Mitsubishi Electric Engineering, III:National Police Academy.

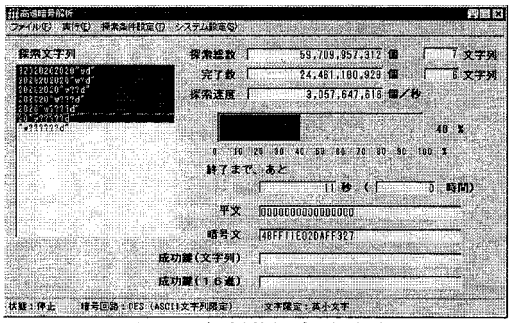

図２　解析状況表示画面

4 負荷分散方式

探索は、ソフトウェアが探索文字列の上位のワイルドカード部分を具体的な文字に置き換え、FPGAにそれを渡す。今回開発した FPGA 回路では、最大下位４文字のワイルドカードの展開を担当する。ソフトウェアから FPGA への探索文字列の分配(負荷分散) は、以下のように行っている（図３)。

- まず FEP は、上位のワイルドカードを展開して、１FPGA 当たり 10 個程度になる数の探索文字列を各ユニットに送る。
- 各ユニットの制御ボードは、FEP から送られた探索文字列を記憶し、各演算ボードのローカルメモリの各 FPGA の領域に探索文字列を１つずつ書き込む。なお、ローカルメモリは、予め FPGA 毎の領域を決めておく。
- 各 FPGA は、ローカルメモリの自領域より探索文字列を取り込み、その領域に取り込んだ旨を記録する。
- FEP は、定期的に各ユニットに進捗（探索完了数）を問い合わせ、ユニット内の未実行探索文字列が少なくなったら、探索文字列を供給する。
- 制御ボードは、FEP からの問い合せ時に、各演算ボードのローカルメモリを見て、探索文字列が取り込まれていたら自らが記憶している探索文字列を対応するローカルメモリに書き込む。

このように、ローカルメモリをバッファとして利用することにより、各 FPGA が遊休状態になることなく処理を進めることができる。そして、ソフトウェアが全体の制御や上位部分の展開を担当し、FPGA 回路が高速性を必要とする下位部分の展開や暗号化を担当しているので、柔軟な解析機能を持ちかつ FPGA 回路の性能を十分に引き出すことができるようになっている。

5 性能評価

今回開発した回路の 1FPGA 当たりの探索性能は、動作クロックから換算して、2,411 万鍵/秒である。我々が以前開発した全数探索版の FPGA 回路の性能が 3,375 万鍵/秒であったのに比較して、探索文字を限定しているため性能が若干劣っている。しかし、全数探索に比べて探索文字列を指定できるため探索範囲を限定できる効果は大きい。

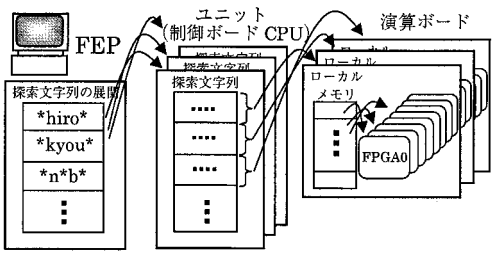

図３　負荷（探索文字列）の分配方法

これを評価するために、実際にパスワードの脆弱性の検査実験を行った。一般に、よくある禁止事項とされる「氏名」などの分かり易いパスワードを付与した場合においても、全数探索では RASH 32 ユニットを使用して 20 日を要していた。今回実現した機能では、付与した人の情報を明示的に示すことにより、特定文字列を優先的に探索を行う。そのため人間には推測しやすい、ichiro3, kyou.s, s.nobu.s, ken-ken, hide.tan, nob.lab のようなパスワードについては、演算ボード５枚構成の１ユニットで、どれも４分以内に該当文字列を検索できた。具体的には、パスワードが名前を構成する文字の並びを多く含むほど早く検索に至っており、脆弱性評価に関するひとつの方向性を示唆している。

また、ソフトウェアによる探索と比較すると、文献[4] から、Pentium-Ⅲ 1GHz 上の探索性能は 40 万鍵/秒となるので、演算ボード５枚構成の RASH １ユニットは、約 2,411 倍の性能となる。従って、上記の RASH での４分の探索は、Pentium-Ⅲ上では７日となる。

6 おわりに

以上、FPGA ベース並列マシン RASH 上のパスワード解析機能ついて報告した。今後は、探索範囲の重複除去や TMTO 法による暗号解析との組合せ等を行っていきたいと考えている。

参考文献

[1] 中島, 他: "ＦＰＧＡベース並列マシンＲＡＳＨの概要", 第 58 回情処全国大会, 1H-08, 1999.

[2] 浅見, 他: "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.

[3] 中島, 他: " FPGA ベース並列マシン上の TMTO 法暗号解析の実現", 2001 年暗号と情報セキュリティシンポジウム, Vol.1, pp.1-6, 2001.

[4] B.Schneier etc: "Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor", Proc. of FSE97, Lecture Notes In Computer Science 1267, Springer Verlag, 1997.