並列計算機を用いたタイムメモリトレードオフ法の実現

4 F − 4

高橋 勝己, 飯田 全広†, 宮田 裕行, 松本勉‡

三菱電機 (株), †三菱電機エンジニアリング (株), ‡横浜国立大学

1 はじめに

近年のコンピュータと通信の進歩は、暗号の役割を大きく拡大することになった。あらゆる情報がコンピュータに記憶され、インターネットなどでその情報が伝達される状況が生じ、その際、企業の秘密やプライバシーを守るために、暗号の技術が必要とされるようになってきた。しかし、近年の技術の進展は、従来不可能と見られてきた共通鍵ブロック暗号の全数探索による解読可能性を確実に高めている。1997 年 6 月には、RSA が行なっていた "DES(Data Encryption Standard) Challenge" にあった 56bit の DES の鍵が、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というニュースが流れた。これにより、全数探索による解読危険性がまた明らかにされた。しかし、同時に数千 / 数万台の計算機を用いて数カ月の時間を要するという解読の困難さをも示すこととなった。

タイムメモリトレードオフ法 [1][2] は、全数探索の 1 種であるテーブルルックアップ法を改良したものである。我々は、現在最も広く用いられていると考えられている 56bit の DES を対象として、本方式を並列計算機に適用する方法について検討した。本方式の採用により、並列計算機における効率的な鍵の検索が見込めることになった。以下、タイムメモリトレードオフ法、本計算機構成、処理内容について述べる。

2 タイムメモリトレードオフ法

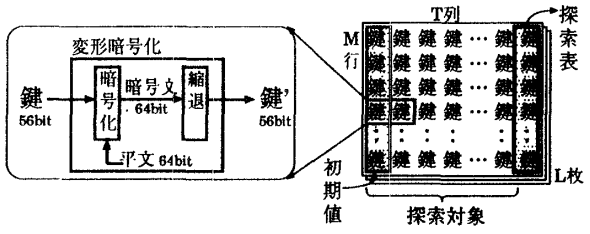

図 1: 変形暗号化と探索表

本手法は、テーブルルックアップ法の問題点であった表のサイズを大幅に縮小すると同時に、一度表を作成しておけば、全数探索よりも遥かに少ない計算量で処理できる手法である。

本手法では、図 1に示す変形暗号化を用いて、事前に L 枚の探索表を作成する。この探索表は、M 個の初期値をそれぞれ T 回変形暗号化を繰り返すことで作成される。選択平文に対応する暗号文を入手した後は、暗号文を縮退し、探索表との比較を行なう。探索表の中に一致するものがなければ、その値に変形暗号化を施し比較することを繰り返す。これにより、図の探索対象と示されている範囲に現れる全ての鍵を検証することができる。この比較によって一致したとして検出されるのは、真の鍵ばかりではないため、その後、暗号文の作成に用いられた鍵であるかどうかの検証を行なう。

この時、探索によって発見できるのは、探索対象となっている鍵のみである。この鍵の生成は DES の暗号化を元に行なっているが、その中には重複するものも少なくない。このため、鍵の探索に成功する確率を 80% 以上にするためには、LMT の積を鍵が持つ範囲の倍程度 (56bit 鍵の場合:$LMT \approx 2^{57}$) にする必要がある[1]。

3 本計算機構成

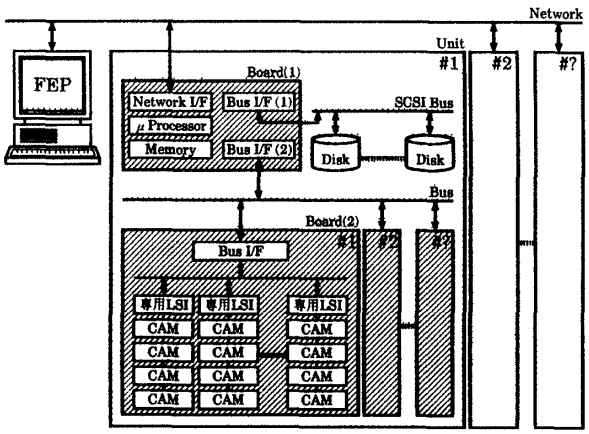

図 2: ハードウェア構成

本計算機では、本手法の表作成に 1 カ月、比較に 1 時間要するとして構成を考える。

図 2は、本並列計算機のハードウェア構成を示したものであり、以下の構成要素からなる。

FEP(Front-End Processor): ユーザとの I/F を司

Implementation of Time-Memory Trade-Off using a parallel machine

K. Takahashi, M. Iida, H. Miyata, T. Matsumoto

Mitsubishi Electric Corporation, †Mitsubishi Electric Engineering, ‡Yokohama National University

[1]本機では、L,T を数メガ、M を数キロのオーダとなる。

り、また、処理結果はもちろん、装置の処理状況などの表示も行なう。

ユニット: タイムメモリトレードオフ解読方法に基づき、独立に処理を行なう[2]。

ボード(1): 複数のI/Fを持ち、ユニット内の処理全体を制御する。各ユニットには、このボードが1枚挿入されている。

ボード(2): 専用LSIとCAMの組を複数持ち、解読法に基づく処理を行なう。鍵探索時には、1組で1枚の探索表との比較を担当する。各ユニットには、このボードが複数枚挿入されている。

- 専用LSI: 変形暗号化(DESの暗号化)を高速に行なうLSI。縮退の種類は処理時に選択できる[3]。
- CAM(連想記憶メモリ): 探索表を格納し、暗号文を変形させたものと高速に比較する。

ディスク: 探索表を格納するディスク。ユニット毎に数十ギガバイト、装置全体では数百ギガバイトの容量を必要とする。

本計算機では、各ユニットは独立に動作させることができ、ユニット間で情報を交換する必要はない。ユニット間接続もネットワークで実現しているため、ユニット単位であれば、システムの拡張等も自由である。

4 処理内容

本解読法は、表作成も鍵の探索も探索表単位で独立な処理である。このため、この探索表を均等に各ユニットへ割り当てることで、負荷分散を行なう[4]。なお、平文と暗号文はユーザーが与えるものとする。

4.1 表作成まで

FEPは各ユニットに探索表を割り当てる。ユニット内のプロセッサは、これを含む各種パラメータをFEPから受けとり処理を開始する。この時のユニット内の処理の流れは、次のようになる。

1. プロセッサは、各専用LSIに初期値や平文、縮退の種類を与えT回の変形暗号化を実施させる。
2. プロセッサは、各専用LSIから結果を収集し、次の初期値を与える。
3. 探索表の全ての要素が揃ったら、ディスクに表を格納する。
4. 割り当てられた表の作成を終えるまで1番の処理から繰り返す。
5. 表の作成が終了したら、FEPに対して終了報告を行ない処理を終了する。

FEPは全てのユニットの終了報告を受けとったら、表の作成が終了したとみなし、その旨を表示する。

4.2 表作成後

FEPは各ユニットに暗号文を渡し、処理が終了するのを待つ。この時のユニット内の処理の流れは、次のようになる。

1. ディスクから探索表を複数枚メモリへ取り込む。この作業は他の処理と並行して行なわれる。
2. プロセッサは、探索表をLSIを介してCAMに転送し、暗号文を与え鍵の探索を開始させる。これをユニット内の全CAMに対して行なう。
3. LSIとCAMの組は、探索表と暗号文を変形させつつ比較をT回繰り返す。一致するものがあった場合、その情報をプロセッサに報告し、その後、続きを実行する。比較が終了したら、プロセッサに対し終了を報告する。
4. プロセッサは、処理の終了を受けとったら、次の探索表を割り当てる。
5. プロセッサは、報告のあった鍵を生成し、実際にその鍵で暗号化を行ない、暗号文と比較する。一致した場合には、鍵を発見したとしてFEPに報告する。
6. 解である鍵を発見できるか、全ての探索表との比較を終えるまで1番の処理から繰り返す。
7. 全ての表との比較が終了したら、FEPに対して終了報告を行ない処理を終了する。

FEPは解である鍵の報告を受けたら、それを画面に表示し、他のユニットに対し、処理の終了を指示する。一方、全てのユニットの終了報告を受けとったら、鍵の探索に失敗したとみなし、その旨を表示する。

5 おわりに

これまでの検討において、本計算機は十分実現可能なレベルにあることが分かった。今後は、細部の検討を進めていく予定である。

参考文献

[1] M.E.Hellman, "A Cryptanalytic Time-Memory Trade-Off", IEEE Transactionson Infomation Theory, Vol.IT-26, No. 4, JULY 1980

[2] 狩野, 松本, "タイム - メモリトレードオフ解読法の効率を改善する一方法", 1996年暗号と情報セキュリティシンポジウム講演論文集, SCIS96-4B, 1996

[2] CompactPCI / VME 6U の基板８枚程度とディスク数個から構成される。

[3] 縮退の方法は制限されるが、それでも数百万以上のバリエーションを用意する。

[4] 鍵探索時は、ユニット内の表との探索を行なうため、別途負荷分散を行なう必要はない。