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

高橋勝己[†] 飯田全広[††] 水上雄介[†]
山崎弘巳[†] 宮田裕行[†]
中島克人[†] 松本勉[†††]

タイムメモリトレードオフ解読法をDES（Data Encryption Standard）暗号に適用した場合の装置構成と，その装置の実現可能性や規模について示す．本手法を用いた装置は，要求仕様によってその規模が大きく変化するが，本稿では，“表作成に1カ月，鍵探索に1時間，鍵探索成功確率80%”という条件を設定し，提案装置の実現可能性を検討した．その結果，専用LSIを4石とCAM（Contents Addressable Memory）を8石搭載したボード13枚と制御用のボード1枚，および，32 GByteのディスクを組み込んだVMEシステムラック16箱で実現可能であることが分かった．

Feasibility Study of a Machine Configuration for Time-Memory Trade-Off Cryptanalysis

Katsumi Takahashi,[†] Masahiro Iida,[††] Yusuke Mizukami,[†]
Hiromi Yamazaki,[†] Hiroyuki Miyata,[†] Katsuto Nakajima[†]
and Tsutomu Matsumoto[†††]

We propose a massively parallel machine which is dedicated to evaluating the strength of Data Encryption Standard (DES) based on time-memory trade-off (TMTO) cryptanalysis. We set up our target performance as one month precomputation and at most one hour key search for DES under the condition of 80% key success probability. We made a rough design on the machine architecture. Our target performance can be achieved by a machine with 16 VME system racks, each of which contains 32 GBytes disk, 13 cryptanalysis borads and a control processor board. Eight CAM chips and four of specially designed LSIs are mounted on each cryptanalysis board.

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．たとえば，電子商取引に代表される流通機構の電子化においては，取り扱われる情報に対する盗聴や偽造がただちに社会不安につながることから，通信の安全性確保が最重要課題の1つになっている．安全性確保では，暗号化や復号，および，これらを用いた認証などの技術と同様，暗号の強度評価技術[1]も重要な技術の1つである．

図1は，送信者と受信者があらかじめ暗号化鍵と呼ばれる数値を共有する共通鍵暗号方式によって公開された通信路を介して通信する例である．送信者は，平文（受信者に渡す情報）を暗号化鍵によって暗号化した暗号文を通信路を介して送り，受信者は，通信路を介して受け取った暗号文を暗号化鍵によって復号することで平文を入手する．このとき，第三者は，通信路上の暗号文を入手することはできるが，暗号化鍵を持っていないため復号できず，平文を入手することはできない．仮に，暗号文を平文に戻せるものが暗号化鍵のみであり，第三者が通信路上の複数の暗号文の中の1つについて，その文の暗号化前の平文を入手，もしくは予測できる場合，全数探索によって暗号化鍵を求めることができる．しかし，N bitの暗号化鍵を全数探索で求めるには，2^N 回の暗号化と比較が必要で

† 三菱電機株式会社
Mitsubishi Electric Corporation
†† 三菱電機エンジニアリング株式会社
Mitsubishi Electric Engineering Co., Ltd.
††† 横浜国立大学
Yokohama National University

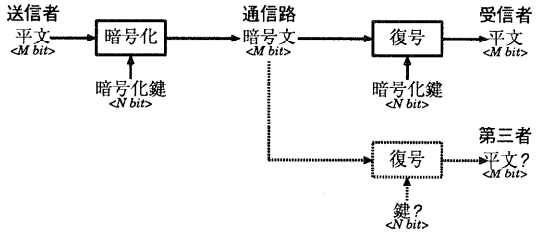


図1 共通鍵暗号方式おける通信
Fig. 1 Cryptosystem (common key).

あり，演算量の面から従来は実質的に不可能とされてきた．しかし，近年の計算機性能の向上によって，全数探索による鍵探索の実現性も高まり，注目を集めている．

たとえば，鍵長 56 bit の米国標準暗号 DES（Data Encryption Standard）を対象として 1997 年に RSA 社が行ったコンテスト “DES Challenge” において，鍵の探索に成功したという報告がなされている[2]．さらに，翌 1998 年，探索時間に制限が加えられた “DES Challenge II” においても同様の報告がなされており，ネットワークで接続された 5 万台の計算機を使用して，39 日で鍵の探索に成功したことは有名である[3]．同年 7 月には，EFF（Electronic Frontier Foundation）が，1800 個の専用 LSI を使用し，毎秒 880 億個以上の鍵を探索できる専用装置を用いて，56 時間で鍵の探索に成功した．この装置を用いれば，全数探索も 10 日未満で実行できる計算になる．さらに，Wiener は，DES 暗号を対象として 3.5 時間で全数探索を実行する装置が 100 万ドルの費用で実現できると提案している[4]．しかし，Wiener の提案した装置は，6.4 Gbps の暗号化性能を持つ専用チップが 10 ドルで入手でき，このチップを 57,600 個使用することを前提としているため，現状では現実的でない．

特定のソフトウェアを用いて作成した文書が通信路に流れる場合，文書の先頭にはソフトウェア固有のヘッダが挿入されていることが多いため，このソフトウェアが使用されることを想定することで，暗号文入手前に平文を予測することができる．この場合，あらかじめこれを暗号化して得られるすべての暗号文にソートやハッシュを施したうえで，テーブルに格納しておき，通信路から暗号文を入手した後はテーブル検索のみで鍵を探索するテーブルルックアップ法（Table Lookup，以下 TL 法と略す）がある．TL 法の利点は，テーブルを生成するのに要する時間は全数探索と同じであるものの，1 度作成した後は，複数の暗号文それぞれに対応する鍵を短時間で求めることができる点にある．しかし，テーブルとして 2^N 個の暗号文と鍵の対応を格納する記憶領域が要求されるという欠点がある．

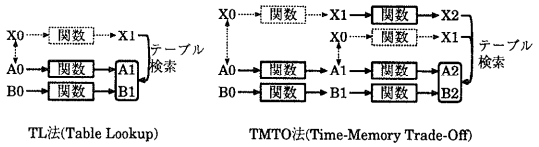


図2 TL 法と TMTO 法
Fig. 2 Table Lookup and Time-Memory Trade-Off.

想定平文に対応する暗号文を複数入手し，それぞれに対応する鍵を求める場合，全数探索では膨大な時間を，TL 法では膨大な記憶領域を，それぞれ必要とする．両者のそれぞれの問題を緩和する手法として提案されたのが，タイムメモリトレードオフ解読法（Time-Memory Trade-Off Cryptanalysis，以下 TMTO 法と略す）[5]である．TMTO 法は，全数探索より短い時間で，また，TL 法より少ない記憶容量で，鍵の探索を行うことができるため，TMTO 法を実現するための各種アルゴリズムが提案されている[6)~9)]．しかしながら，これまで TMTO 法を実現する装置の具体的な構成に関する報告はない．

本稿では，現在広く用いられている暗号である DES を対象として，想定平文があらかじめ得られる場合に短時間で鍵探索を実施できる TMTO 法を採用した強度評価装置の構成について提案し，“事前に 1 カ月かけて表を作成すれば，8 割の確率で 1 時間以内に暗号化鍵を発見できる装置” が現実的なハードウェア規模，即ち，14 枚のボードと 32 GByte のディスクを組み込んだ VME システムラック 16 箱で実現可能であることを示す．

2. TMTO 法：Hellman 方式

図 2 は，1 対 1 の写像を持つ関数の出力値 $X1$ から関数の入力値 $X0$ を求める際の TL 法と TMTO 法の違いを示したものである．TL 法は初期値を入力としたときの関数の出力値を，TMTO 法はその値をさらに入力として用いたときの関数の出力値を用いて表（テーブル）を作成する．TL 法では，$A0$，$B0$ のいずれかと $X0$ が等しいとき，$X1$ による表検索から $X0$ を求めることができ，TMTO 法では，$A0$，$A1$，$B0$，$B1$ のいずれかと $X0$ が等しいとき，$X1$ もしくは $X2$（$X1$ を入力としたときの関数の出力値）による表検索から，$X0$ を求めることができる．このように，TMTO 法では，関数を複数回経た値を表に用いることによって，表検索や関数演算が増えるものの，同じサイズの表からより広い範囲を探索することができる．

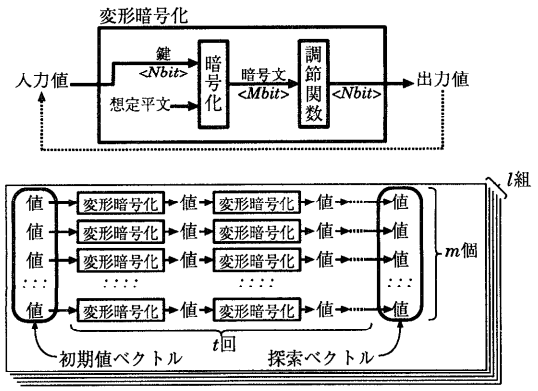


図3 Hellman 方式
Fig. 3 Hellman's Method.

TMTO 法で用いる関数は，出力値を入力値として再帰的に用いるため，Hellman は，想定平文と称する 1 ブロック（DES の場合は 64 bit $(=M)$）の平文を入力として固定し，暗号化の後段に調節関数を加えた“変形暗号化”を関数として定義した[5]（図 3）．調節関数は，ビット長の調整（$M \geq N$ とする．DES の場合は鍵長 N=56 bit）と出力値への擾乱を加える関数であり，たとえば，上位ビットの削除と特定の値との排他的論理和で実現できる[9]．これにより，変形暗号化の出力を入力として再帰的に用いることができるようになる．

Hellman は，この変形暗号化を用いて，初期値と調節関数がそれぞれ異なる l 組の「m 個の異なる初期値（初期値ベクトル）とその個々の値に変形暗号化を t 回施して得られる値（探索ベクトル）」のペアを記憶するとき，暗号化鍵が探索ベクトルの作成時に変形暗号化の入力に使用された値（のべ lmt 個）のいずれかと一致すれば，「変形暗号化と m 要素との値比較」を基本単位として，$O(lt)$ の演算量で暗号化鍵を求めることができることを示した．

3. TMTO 法：提案方式

3.1 変形暗号化の変更

Hellman が示した変形暗号化は調節関数を暗号化の後に配置したものであったが，本稿で提案する TMTO 法ではこの 2 つを逆転させた変形暗号化を用いる（図 4）．この逆配置により後述の鍵探索における作業を減らすことができる．

また，調節関数には，上位ビットの削除と $0, m, 2m, \cdots, (l-1)m$ との排他的論理和をとる関数を採用する．この関数の採用と初期値ベクトルの初期値を $0, 1, 2, \cdots, m-1$ とすることにより，初期値ベクトル

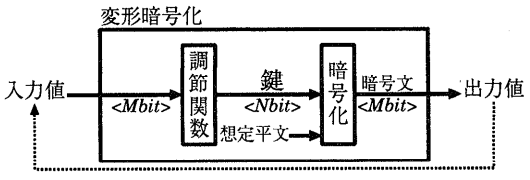


図4 新変形暗号化の構造
Fig. 4 New construction of modified enciphering.

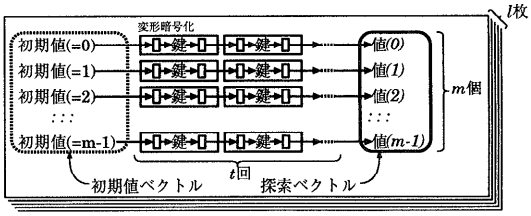


図5 表作成
Fig. 5 Table making.

を入力とした変形暗号化において，暗号化の入力値として同じ値が使用されることを防ぐことができる．また，初期値ベクトルの内容が固定であるため，Hellman の方式における l 組の初期値ベクトルの記憶も不要になる．さらに，排他的論理和をとる値を 0 とすることにより，通常の暗号化回路としても利用できる．

3.2 表 作 成

表作成では，初期値ベクトルに対して変形暗号化を t 回実行して得られる探索ベクトル（m 要素の表）を l 枚作成し，記憶する（図 5）．

この探索ベクトルの生成手順を次に示す．

(1) 初期値ベクトルの個々の初期値を入力として変形暗号化を t 回実行する（2 回目以降の入力には前回の変形暗号化の出力値を用いる）．
(2) 探索ベクトルと称する t 回目の変形暗号化の出力値 m 個を格納する．
(3) 調節関数を変えて (1)~(2) 操作を探索ベクトルが l 枚になるまで繰り返す．

以上の手順で表作成は終了する．探索ベクトルの格納に必要な記憶容量は，探索ベクトルの各要素が 1 word で表現されるとして，lm word である．表作成の演算量は，変形暗号化の回数に支配され，$O(lmt)$ となる．

3.3 鍵 探 索

鍵探索では，入手暗号文と探索ベクトルを用いて暗号化鍵を探索する（図 6）．

入力暗号文が探索ベクトルのある要素と一致すれば，その要素を得るために表作成時に行った最後の変形暗号化の内部で使用された鍵が求める暗号化鍵であると

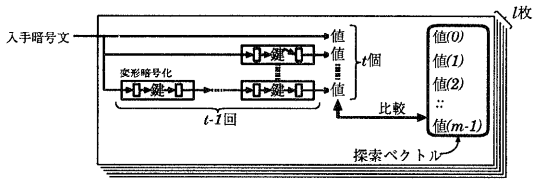


図6 鍵探索
Fig. 6 Key searching.

断定できる．この値を求めるには，対応する初期値に $t-1$ 回の変形暗号化と 1 回の調節関数を施せばよい．

入力暗号文が探索ベクトルのどの要素とも一致しなければ，入力暗号文に変形暗号化を施し，再度探索ベクトルと比較する．一致した要素がある場合，対応する初期値に $t-2$ 回の変形暗号化と 1 回の調節関数を施したものが求める暗号化鍵である可能性が高い．今回暗号化鍵であると断定できないのは，調節関数が行うビット長調整において異なる入力値が同じ出力値となる可能性があるためである．暗号化鍵であると断定するためには，初期値に $t-1$ 回の変形暗号化を施した値が入力暗号文と一致するのを確認する必要がある．この一致確認処理を虚報判定，一致しなかった場合を虚報と称する．

なお，入力暗号文を $t-1$ 回変形暗号化しても探索ベクトルの要素と一致しなければ，他の探索ベクトルを用いて同様の処理を繰り返す．

以下に鍵探索および虚報判定の手順を示す．

- 鍵探索の手順
  (1) 探索ベクトルを 1 つ取り出し，変形暗号化の調節関数を探索ベクトル作成に用いられたものに合わせる．
  (2) 入手暗号文と探索ベクトルの各要素を比較する．探索ベクトルの中に一致する値があれば，虚報判定を行う．
  (3) 探索ベクトルと比較した値を入力として変形暗号化を実施し，変形暗号化の出力値を再度探索ベクトルの各要素を比較する．探索ベクトルの中に一致する値があれば，虚報判定を行う．
  (4) (3) を $t-1$ 回繰り返す．
  (5) 格納しているすべての探索ベクトル（l 枚）に対して，(1)〜(4) の一連の操作を繰り返す．
- 虚報判定の手順
  (1) 暗号文と一致した探索ベクトルの値に対応する初期値を求める．
  (2) 鍵探索において暗号文に対して行った変形暗号化回数を n として，初期値を入力とした変形暗号化を $t-n$ 回実行する（2 回目以降の入力には前回の変形暗号化の出力値を用いる）．
  (3) (2) において得られた値と入手した暗号文を比較する．一致した場合には $t-n$ 回目の変形暗号化の内部で使用された鍵（最後の変形暗号化の入力値に調節関数を施したもの）が暗号化鍵であるとして，鍵探索を終了する．一致しない場合には虚報判定を終了し，鍵探索に戻る．

以上の手順で鍵探索は終了する．すべての探索ベクトルとの比較が終了しても暗号化鍵が発見できない場合，TMTO 法による鍵探索は失敗したとして終了する．この TMTO 法において探索できる鍵は，図 5 において “鍵” と示されている部分に現れた数値のみである．したがって，暗号化鍵が図の “鍵” の部分に現れなかった値である場合，暗号化鍵を見つけることはできない．

暗号文と m 要素の探索ベクトルの比較は，m エントリのハッシュや CAM（Contents Addressable Memory：連想記憶メモリ）を用いることでほぼ定数オーダの手間と見なすことができるため，虚報判定を除けば，鍵探索の演算量オーダは，変形暗号化と探索ベクトルの要素との比較を合わせた処理の回数に支配され，$O(lt)$ となる．

3.4 TMTO 法の性質

TMTO 法を実現する装置に要求される演算量と記憶容量は，以下のようになる．

- 表作成の演算量：……$O(lmt)$
- 鍵探索の演算量：……$O(lt)$
- 記憶容量：……$O(lm)$

したがって，演算量と記憶容量の面から見れば，l, m, t の各値は小さいほどよい．しかし，TMTO 法は，探索ベクトル作成時の変形暗号化において一度も出現しなかった鍵については発見できないという性質を持っている．鍵の探索に成功する確率の下限値（P_L）は，上記 3 つの変数 l, m, t と鍵ビット長 N を用いて次式のように表すことができる[6]．

$$P_L \simeq 1-\exp(-kg(u)) \tag{1}$$

$$k=\frac{lmt}{2^N},\ u=\frac{mt^2}{2^N},\ g(u)=\frac{1}{u}\int_0^u \frac{1-e^{-x}}{x}dx \tag{2}$$

式 (1) をグラフにしたのが**図 7** である．

式 (1) と図 7 が示すように，鍵探索成功確率下限値 P_L は，k と $g(u)$ が大きいほど高くなる．言い換え

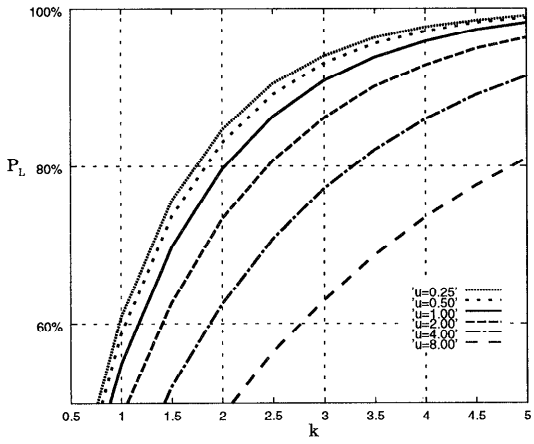


図7 k, u と鍵探索成功確率下限値 P_L との関係
Fig. 7 The relation of lower bound of success probability and k, u.

れば，l，m，t の積が大きいほど，l，m，t の積が一定の場合には mt^2 の値が小さいほど，高くなる．しかし，これら l，m，t の増減は，演算量と使用記憶容量に大きな影響を及ぼす．

また，鍵探索において発生する虚報判定で実施する変形暗号化の実行回数の期待値 E は，次式で表すことができる[6]．

$$0 \leq E \leq \frac{u}{6}lt \tag{3}$$

楠田らの文献で示されているこれら式 (1)～(3) の性質は，Hellman の方式に対するものであるが，本稿で示した変形暗号化を用いても同じ性質を持っているものと見なせる．これは，暗号化と調節関数が同じであるとして，本稿の初期値ベクトルを調節関数によって変形したものを Hellman の方式での初期値ベクトルに用いると，両方式において鍵の探索に成功する値の種類が一致するためである．

4. 目標性能と装置構成

4.1 目標性能の設定

本章では，現在広く用いられているブロック長 64 bit (=1 word)，鍵長 56 bit の暗号である DES を対象として，現実的な装置を構成する場合の構成案について提案し[12)~14)]，その動作や規模について述べる．装置構成は目標とする性能によって大きく変化するため，我々は**表 1** の性能を条件として設定した．

鍵探索成功確率は，k の増加によって理論上 100%に近付けることができることが分かっている．$k=1$ の場合でも u が十分小さければ，約 60%の成功確率が得られる．今回我々は「鍵探索成功確率がある程度高い」と納得が得られるであろうケース，すなわち，鍵探索成功確率が 80%となる "$u=1$, $k=2$" のケースを選択して以後の装置構成を検討した．

表 1 目標性能（対象暗号：DES）
Table 1 Target performance for DES.

項目	目標値
鍵探索成功確率	約 80%
探索ベクトル作成時間	約 1 カ月
鍵探索時間	約 1 時間

4.2 l, m, t のパラメータ設定

高速な変形暗号化と，探索ベクトルとの高速な比較を実現するため，変形暗号化には専用 LSI を，比較には CAM を用いることを想定する．高速な比較の実現方法としては，プロセッサとメモリを使用したハッシュ法による表検索[10),11)]もあるが，高速なプロセッサや繁雑な衝突制御が必要となる．それに対し CAM は，必要とする制御用回路の規模が小さく，変形暗号化を行う専用 LSI に組み込むことが容易であると考えたからである．

本装置では，現実性の観点から

- 鍵探索において使用する CAM は最新のもの（64 bit × 8 k エントリ）
- 探索ベクトル格納のために使用するシステム全体の総ディスク容量を 512 GByte

とし，"$u=1$, $k=2$"，および，式 (1)，(2) を前提として l，m，t を以下のように決定した．

$$\begin{aligned} l = 2^{22} &= 4\,\text{M 枚} \\ m = 2^{14} &= 16\,\text{K 個} \\ t = 2^{21} &= 2\,\text{M 回} \end{aligned}$$

4.3 装置への要求性能

表作成において，表 1 の目標性能を満たすために必要となる変形暗号化の性能 V_t（スループット）は，

$$\begin{aligned} V_t &= \frac{lmt}{31\,(\text{day}) \times 24\,(\text{hour}) \times 3600\,(\text{sec})} \\ &\simeq 53.8\,(\text{Gword/s}) \end{aligned} \tag{4}$$

である（1 word=64 bit）．次に，鍵探索において，変形暗号化と探索ベクトルとの比較を合わせた性能 V_k（ターンアラウンド）は，

$$V_k = \frac{lt}{3600\,(\text{sec})} \simeq 2.44\,(\text{Gword/s}) \tag{5}$$

である．また，探索ベクトルの記憶に必要な容量は，初めに設定した 512 GByte である．

本装置に要求されている性能をまとめると**表 2** のようになる．

表2 要求仕様
Table 2 Performance request.

項目	要求値
変形暗号化性能	約 53.8 Gword/s
鍵探索性能	約 2.44 Gword/s
記憶容量	512 GByte

4.4 装置全体の構成

前節の議論をふまえて，実際のハードウェア構成は以下の3方針で検討を進めた．

(1) 市販品をできる限り利用する．
(2) 処理の並列度を活かせる構成にする．
(3) 装置規模をスケーラブルにする．

この方針は，現実的なシステムを想定しつつ，低コストでの高性能を目指した結果に基づいている．最終的には**図8**に示したハードウェア構成を採用する．なお，図8の中の個数に関する根拠は，5章で述べる．

本装置の利用者は，FEP（Front-End Processor）上ですべての指示を行う．FEPは，利用者の要求に応じ，表作成や鍵探索の操作を各UNITに指示する．各UNITは指示に従い，UNIT内の資源を利用して表作成や鍵探索を実施する．各部の機能と概略動作は以下のとおりである．

FEP（Front-End Processor）： 利用者と本装置のインタフェースをとる計算機．市販のPC（Personal Computer）またはWS（Work Station）を利用する．利用者はこの計算機を通して本装置全体を制御する．

Network： FEPと各ユニットの間の情報交換に用いる．通信量はきわめて小さいため，ユニットの増減を簡単に行えるイーサネットを使用する．

UNIT： 装置の規模を変更する際の単位．規模の変更を容易に行うために，装置は複数の独立なUNITによって構成される．このUNITは，汎用のフレームに電源，後述のDISK，CNTボード，EXEボード複数枚を組み込んだものとなる．TMTO法に基づく処理では，UNIT間でのデータ転送はなく，UNITに対する制御はFEPからNetworkを介して行われる．また，FEPに対する最終結果の報告も，UNITからNetworkを介して行われる．

DISK： 探索ベクトルを格納するハードディスク．数十GByteを各UNITに用意し，装置全体で512 GByteとする．表作成では，1カ月かけて生成された探索ベクトルが順次書き込まれる．また，鍵探索では，1時間で全探索ベクトルの読み出しが行われる．

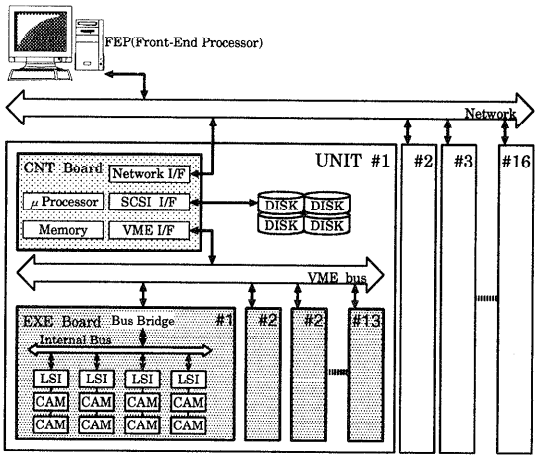


図8 ハードウェア構成
Fig. 8 Design of the machine.

CNTボード： UNIT制御を行う汎用CPUボード．インタフェースとしては，広く使用されているVME（対EXEボード）とSCSI（対DISK），イーサネット（対FEP）を採用する．CNTボードは，表作成では各EXEボードで生成された探索ベクトルを集め，UNIT内のDISKに格納する．また，鍵探索ではDISKから探索ベクトルを読み出して各EXEボード内のCAMにロードし，探索ベクトルと入手暗号文との比較をEXEボードに行わせる．したがって，探索ベクトルはUNITを跨いでデータ転送されることはない．

EXEボード： 後述の変形暗号化LSIとCAMを搭載するボード．表作成では変形暗号化LSIを用いて探索ベクトルを作成し，鍵探索では，CAMに探索ベクトルをロードし，変形暗号化LSIによって入手暗号文を変換しながら探索ベクトルとの比較を行う．

LSI： 変形暗号化（調節関数とDESの暗号化）とCAMの制御を行う専用のLSI（変形暗号化LSIと称する）．1つの変形暗号化LSIは，変形暗号化を行う回路2つとCAMを制御する回路1つを内蔵する．表作成では変形暗号化を行う回路を2つとも探索ベクトルの作成に用い，鍵探索では1つを入手暗号文の変換と探索ベクトルとの比較に，もう1つをその際に発生する虚報判定に用いる．構成の詳細については次節で述べる．

CAM： 探索ベクトルをロードし，変形暗号化LSIから入力された値と比較を行い，一致した場合はそのアドレス，すなわち，m 要素中の要素位置を出力する．なお，CAMは鍵探索でのみ用い，表作成では使用しない．

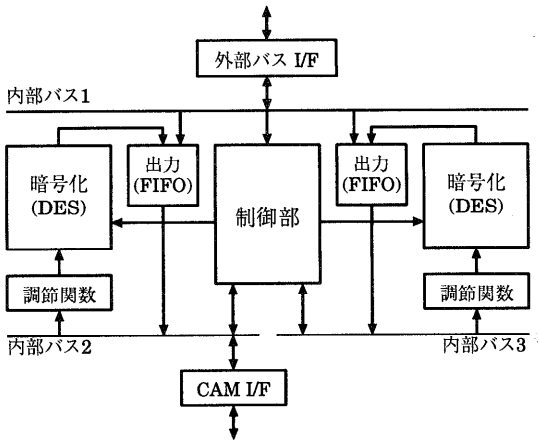


図9 変形暗号化 LSI 内部構成
Fig. 9 Construction of modified enciphering LSI.

4.5 変形暗号化 LSI の構成と動作

本節では装置の根幹をなす部品である変形暗号化 LSI の構成について述べる．

図 9 は変形暗号化 LSI の内部構成を示したものである．図に示すように，LSI 内には変形暗号化を行う“調節関数”と DES の“暗号化”のペア（変形暗号化回路と称する）が 2 組搭載されており，各々には“出力 FIFO”が付随している．これらは，独立して変形暗号化を繰り返し実行できるように，“内部バス 2，3”も独立なものとしている．これら 2 組の制御を行う“制御部”や，入出力の制御を行う“外部バス I/F”は，共通リソースとして搭載する．また，“CAM I/F”は，LSI 内の変形暗号化回路も，LSI が制御する CAM も 2 つあるため，この点から見れば 2 組用意することもできるが，LSI の使用ピン数を抑えるために 1 組とした．また，調節関数は，探索ベクトルごとに異なる変換を行わなければならないが，LSI の構成上単純な回路で実現可能であることが望ましい．そこで，初期値ベクトルとして与える値を $0 \sim m-1$ とし，探索ベクトルに通し番号を付け，通し番号を $\log m$ ビット左シフトした値と入力値の排他的論理和をとり，その値の下位 56 ビットをとるという調節関数を採用した．

表作成では，変形暗号化 LSI の 2 つの変形暗号化回路を使って探索ベクトルを作成する．作成手順は次のとおりである．

(1) CNT ボードが変形暗号化 LSI 内部の両変形暗号化回路に初期値をセットする．
(2) 両変形暗号化回路は，t 回の変形暗号化（調節関数+暗号化）を繰り返し実行し，その結果を出力 FIFO に移す．
(3) CNT ボードが出力 FIFO の値を読み出す．
(4) (1)～(3) を全探索ベクトルの作成が終了するまで繰り返す．

次に，鍵探索では，変形暗号化 LSI の 2 つの変形暗号化回路を別の用途に用いて鍵を探索する．探索手順は次のとおりである．

(1) CNT ボードが探索ベクトルを CAM にロードする．
(2) CAM I/F を持つ側の変形暗号化回路は，入手暗号文を変換しながら，CAM I/F を介して CAM に格納されている探索ベクトルと比較を t 回繰り返す．比較において一致するものがあった場合は，CAM が報告したアドレスから対応する初期値を求め，その初期値を用いて残るもう 1 つの変形暗号化回路が虚報判定を行う．
(3) (1)～(2) の作業を全探索ベクトルに対して繰り返す．

変形暗号化 LSI は，TMTO 法において以上のように動作する．また，TMTO 法では鍵の探索成功確率は 100%に達しないため，鍵探索に失敗した場合に備え，変形暗号化 LSI には，全数探索の機能も用意した．すなわち，制御部に鍵の自動生成回路と，暗号化結果と入手暗号文との比較回路を設けた．後者の比較回路は，TMTO 法における虚報判定のための比較回路と共用である．

5. 評　　価

本装置の全体構成は前章で述べたが，本章ではその構成要素である変形暗号化 LSI の使用個数，回路規模などを含めて，装置全体の規模について報告する．

5.1 変形暗号化 LSI

変形暗号化 LSI には，現時点でコストパフォーマンスの高い 0.3 μm プロセスのゲートアレイを想定し，電源電圧を 3.3 V として，次の環境を用いて設計・評価を行った．

- HDL（Hardware Description Languagc）設計：DesignBook ver.2.1
- 論理検証（RTL: Register Transfer Level）：verilog-XL ver.2.5 (97a)
- 論理合成：DesignCompiler ver.9701
- 論理検証（Gate Level），消費電力計算：サインオフシステム．各社のプロセスに依存したライブラリを使用．

以上のツールによる変形暗号化回路部分の設計・評価結果は次のようになった．

- 動作周波数：33 MHz
- 回路規模：約 30 K ゲート

- 消費電力：約 1.4 W

5.2 鍵探索用 CAM

今回，対象として検討・調査した大容量・高速 CAM は，米国 MUSIC Semiconductors 社の LANCAM 1st Family[15] の MU9C8481L である．この CAM の仕様は次のとおり．

- 構成：64 bit × 8 K 要素
- 比較時間：100 ns (16 bit) ～330 ns (64 bit) 程度
- 入出力ポート：16 bit
- パッケージ：44 pin PLCC
- 電源電圧：3.3 V

比較時間に示されているように，CAM 単体では 3 Mword/s (=1/330 ns) の性能を持つ．これを，変形暗号化 LSI は，12 cycle かけて制御する（動作周波数 33 MHz）．したがって，その比較速度は 2.75 Mword/s (=33 MHz/12 cycle) と見積れる．

5.3 装置規模と性能

変形暗号化 LSI には，2 つの変形暗号化回路が搭載できるため，1 つの変形暗号化 LSI で，毎秒 66M 個の変形暗号化を実行できる．したがって，表作成の式 (4) の変形暗号化性能を満たすために必要となる個数は，815 個 ((53.8 Gword/s)/(66 Mword/s)) である．一方，鍵探索の式 (5) の鍵探索性能を満たすために必要となる個数は，1 個の変形暗号化 LSI と 2 個の CAM 1 組が実行できる探索ベクトルとの比較回数が毎秒 2.75 M 個であることから，変形暗号化 LSI が 887 個 ((2.44 Gword/s)/(2.75 Mword/s)) と CAM が 1774 個（LSI の倍）となる．

UNIT 内の基幹バスには，現在広く組込み用システムに使用されている VME バスを選定し，搭載する基板のサイズは，32 ビットバスのダブルハイト（6U）基板（233.35 mm × 160 mm）とした．この基板には少なくとも 4 個の変形暗号化 LSI と 8 個の CAM が搭載できる．UNIT 数は，バスのバンド幅や UNIT 内に搭載できるボード枚数で不都合が生じた場合には後で修正を加えるものとして，初めに 16 個と定めた．バスで転送されるデータの総量は，表検索・鍵探索とも UNIT 内の探索ベクトルの総量と等しく，UNIT 数 16 個の場合には各 UNIT で 32 GByte となる．鍵探索では 1 時間ですべての探索ベクトルを DISK からロードできるだけのバンド幅が必要となるが，VME はこの速度である 8.9 MByte/s を満たしているのでバスのバンド幅については問題ない．最後に，ユニット内の基板枚数は，前述の LSI 数と基板への搭載数から 13 枚とした．

以上から本装置の規模を簡単にまとめると**表 3** のようになる．

表 3 装置規模と性能
Table 3 Scale and performance of machine.

項目	値
LSI 動作周波数	33 M (Hz)
変形暗号化回路規模	30 K (Gate)
LSI 内変形暗号化回路数	2 (個)
LSI 全体回路規模（推定）	150 K (Gate)
EXE ボード内 LSI 数	4 (個)
EXE ボード内 CAM 数	8 (個)
UNIT 数	16 (台)
UNIT 内 DISK 容量	32 G (Byte)
UNIT 内 EXE ボード数	13 (枚)
LSI 総数	832 (個)
CAM 総数	1,664 (個)
全 DISK 容量	512 GByte
LSI 消費電力（推定）	3～5 (W)
UNIT 消費電力（推定）	200～280 (W)
全消費電力（推定）	3,200～4,480 (W)
探索成功確率	80%
表作成時間	約 1 カ月 (30.4 日)
鍵探索時間	約 1 時間 (64 分)
全数探索時間	約半月 (15.2 日)

5.4 装置外形

本装置の 1 UNIT は，表 3 に示すように VME ボード 14 枚（CNT ボート 1 枚と EXE ボード 13 枚），および DISK（18 GByte × 2 本，または 9 GByte × 4 本）で構成される．したがって，これを収納するラックは 20 スロットの VME システムラック（VME ボードを 20 枚搭載可能）程度となる．

6. 考　　察

前章では，要求仕様を満たす装置の規模などについて述べた．本章では，本装置における要求仕様や構成，規模について考察を行う．

6.1 要求仕様に関する考察

今回の装置構成は，表 1 で示した表作成と鍵探索の実行時間，および，鍵探索成功確率の設定に基づいて行ったものである．しかし，装置に要求される演算性能や記憶容量は，要求仕様によって変わる．たとえば，鍵探索の演算量，および，探索ベクトルの総容量を変えずに，表作成の演算量を変えることで，鍵探索成功確率を上げることも可能である[16]．このように，要求仕様によって装置に要求される性能が異なり，それにともない装置構成も変化するため，運用において，今回の要求仕様が妥当であるかどうかの検討は，今後の課題である．

6.2 装置容量に関する考察

本装置の基本単位である UNIT は，32 GByte の DISK を内蔵する．この UNIT は，市販されている

ワークステーションと同程度の大きさであり，装置全体でもUNITが16台であるので，装置規模として無理のある大きさではない．

6.3 並列度に関する考察

今回の構成は，表作成の各変形暗号化処理の高い独立性を利用して，並列処理を行っている．TMTO法の2つの作業における並列度は，理論的に表作成で$ml\,(64\times 2^{30})$，鍵探索で$l\,(4\times 2^{20})$である．このうち装置で利用した並列度は表作成で1664，鍵探索で832であるため，装置の並列度はまだ増やすことができる．

6.4 スケーラビリティに関する考察

装置の規模を上げる場合，探索ベクトルの枚数lを増やす方法が最も容易な方法である．lの変更は，表作成の演算量（$O(lmt)$），鍵探索の演算量（$O(lt)$），必要な記憶容量（$O(lm)$）に同比率で影響を及ぼすため，装置全体が定倍することで対応できる．本装置はUNIT単位で増減可能なことから，このlの変更によるスケーラビリティは十分あると考える．このlの変更によって，鍵探索成功確率下限値は図7の$k=l/2^{21}(=lmt/2^{56})$，$u=1$のように変動する．

6.5 l，m，tの変更容易性に関する考察

l，m，tのうち，いずれか1つの値のみを変更する（装置規模の変更を含む）場合の変更容易性について考える．

探索ベクトルの枚数lの変更容易性については，前節のスケーラビリティの項で述べたように十分ある．

探索ベクトルの要素数mの変更は，表作成の演算量（$O(lmt)$）と必要な記憶容量（$O(lm)$）に影響を及ぼすが，本装置の構成では，鍵探索において使用するCAMへの影響が最も大きい．mを減らす変更の場合，本装置では，EXEボードの構成を変更しなければならない．逆に，mを整数倍にする変更であれば，1枚の探索ベクトルを用いた鍵の探索を複数の変形暗号化LSIとCAMのペアで分割実行することで対応することができる．したがって，装置としてはlを整数倍するのと等価である．

探索ベクトル作成時の変形暗号化繰返し回数tの変更は，表作成の演算量（$O(lmt)$）と鍵探索の演算量（$O(lt)$）に影響を及ぼすが，表作成でも鍵探索でも変形暗号化を実行する回数を格納する制御部のレジスタの値を変更することで対応でき，装置構成自体を変える必要はない．

l，m，tは以上のような変更容易性を持つ．

7. 今後の課題

7.1 他暗号への適用に関する課題

暗号強度評価装置の構成としては，“性能を重視し，柔軟性をある程度犠牲にする構成”と，“柔軟性を重視し，性能をある程度犠牲にする構成”の2つの選択肢がある．

本装置では前者を選択し，変形暗号化を行う手段として専用LSIを採用した．したがって，本装置では，対象の暗号をDES以外に変える場合，対象暗号専用のLSI開発，および，LSI交換というコストがかかる．一方，柔軟性を重視する構成をとり，専用LSIの代わりに回路情報の変更が可能なPLD（Programmable Logic Device）を使用した場合，絶対性能は落ちるものの回路情報を書き換えることで対象暗号を変更できる．

FPGA（Field Programmable Gate Array）やCPLD（Complex PLD）のようなPLDは，ALTERA社やXilinx社のロードマップを見る限り，変形暗号化を行う回路（変形暗号化LSIのDESの暗号化部分で約30Kゲート）を2つ以上内蔵できるゲート容量を近い将来期待することができる．変形暗号化部分と制御部分を分離し，変形暗号化部分だけPLDで作成すれば，実装後でも暗号化部分のみを随時入替え可能である．また，容量が許せば前後に暗号化以外の付加回路を追加することもできる．PLDによる実装が実現できれば，種々の暗号アルゴリズムへの対応とTMTO法以外の探索方法への適応が可能になり，柔軟かつ高性能なシステムの実現性が高まるといえる．

したがって，今後は性能重視の専用LSIを使用する構成のほかに，近年，急速な進歩をとげているこのようなFPGA/CPLDなどのデバイスを使用した装置構成の検討も課題といえる．

7.2 鍵長と装置規模に関する課題

今回対象としたDESは，鍵長が56ビットである．しかし，最近の暗号は，安全性の向上から鍵サイズは長大化傾向にあり，**表4**に示す各暗号もほとんどが64ビット以上の鍵を採用している．

TMTO法も，全数探索と同じく鍵のビット長の増減によって，演算量が大きく変動する．仮に，ΔNビット鍵長が増加すると，鍵の探索範囲は$2^{\Delta N}$倍となり，同じ鍵探索成功確率を維持する場合には装置規模も$2^{\Delta N}$倍になる．

一方，同じ鍵探索成功確率を維持するとともに，装置規模も変えない場合には，表作成時間は$2^{\Delta N}$倍，鍵探索時間は$2^{2\Delta N}$倍となる．これは，鍵探索成功確

表4 代表的な共通鍵暗号アルゴリズム
Table 4 Well-known common key ciphers.

名称	鍵長	開発者/開発元
DES	56	NSA, NIST (米国)
FEAL	64/128	NTT
T-DES	112/168	(ANSI X9.17 (Revised))
Multi2	64	日立
IDEA	128	Lai, X. ら (スイス)
LOKI	64	Brown, L. ら (オーストラリア)
RC5	任意	RSADSI (米国)
Skipjack	80	NSA, NIST (米国)
MISTY	128	三菱電機

率下限値を示す式(1), (2)において同じ k, u を選択した場合の例である. lmt と mt^2 は $2^{\Delta N}$ 倍, 装置の記憶容量の制限から lm は一定となり, l, m, t の各値は,「l は $2^{\Delta N}$ 倍, m は $1/2^{\Delta N}$ 倍, t は $2^{\Delta N}$ 倍」となるからである.

本装置はUNIT単位で増設可能なことから, ある程度のスケーラビリティを持っている. しかし, 鍵が長い暗号に適用し同じ鍵探索成功確率を得るためには, 装置規模を増やす必要があり, また, 装置規模を増やさない場合でも, CAMのサイズ変更や処理時間の増大が発生するため, 別途評価が必要である.

7.3 装置コストに関する課題

今回は実現性を装置規模, 具体的な構成の2点に絞って検討を進め, その結果から実現可能であることを示した. また, 実際に製造しようとした場合, その開発費や製造コストが一番の問題となることが多いため, 市販品の利用やコストパフォーマンスの良いゲートアレイの採用など, コスト低減対策も同時に行った. しかし, 装置規模と性能の関係は前述のように複雑であり, 設定条件によって変化するため, 装置規模とコストとの関係などはさらに整理が必要であろう.

8. おわりに

本稿では, DES暗号を対象としてTMTO法に基づく暗号強度評価装置の構成とその規模を示した. 本装置は, 動作速度33 MHz程度で変形暗号化の回路を2個内蔵した専用LSIが832個, CAMが1664個, 総ディスク容量が512 GByte程度の規模であり, 装置容積もVMEシステムラック16箱に収めることができる. 個々の項目については, 評価・検討の詳細化を必要とするものもあるが, 表作成1カ月, 鍵探索1時間, 鍵探索成功確率80%とした本稿の提案装置は, 十分実現が可能なものであると考える.

参考文献

1) Kusuda, K. and Matsumoto, T.: A strength evaluation of the Data Encryption Standard, *IMES Discussion Paper E-Series*, No.97-E-5, The Bank of Japan Institute for Monetary and Economic Studies (Aug. 1997). Available at http://www.imes.boj.or.jp/english/edps_index.html
2) RSA: DES Cracked!, DES Challenge home page, RSA Data Security, Inc. Available at http://www.rsa.com/des/
3) RSA Laboratories: DES Challenge II, DES Challenge II home page, RSA Data Security, Inc. Available at http://www.rsa.com/rsalabs/des2/
4) Wiener, M.J.: Efficient DES key search, Presented at the Rump Session of CRYPTO'93, (1993).
5) Hellman, M.E.: A Cryptanalytic time-memory trade-off, *IEEE Trans. Infomation Theory*, Vol.IT-26, No.4, pp.401–406 (1980).
6) 楠田浩二, 松本 勉: タイム・メモリ・トレードオフ解読法の最適化とブロック暗号への適用, 1995年暗号と情報セキュリティシンポジウム講演集, SCIS95-A3.2 (1995).
7) 狩野卓司, 松本 勉: 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).
8) Kusuda, K. and Matsumoto, T.: Optimization of time-memory trade-off cryptanalysis and its application to DES, FEEL-32, and Skipjack, *IEICE Trans. Fundamentals*, Vol.E79-A, No.1, pp.35–48 (1996).
9) 松本 勉, 金 逸俊, 原 崇: タイム・メモリ・トレードオフ暗号強度評価法における探索時間と記憶容量の削減, 電子情報通信学会技術報告, ISEC97-10 (May 1997).
10) 松本 勉, 原 崇: 完全ハッシュ関数を用いたタイム・メモリ・トレードオフ暗号強度評価法について, 電子情報通信学会1997年基礎・境界ソサイティ大会講演論文集, A-7-9, p.134 (Sep. 1997).
11) 松本 勉, 原 崇, 金 逸俊: タイム・メモリ・トレードオフ暗号強度評価法の能力, 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.B (1998).
12) 高橋勝己, 飯田全広, 宮田裕行, 松本 勉: 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, 第55回情報処理学会全国大会論文集, 4F-04 (1997).
13) 高橋勝己, 飯田全広, 宮田裕行, 松本 勉: タイムメモリトレードオフ解読法を用いた暗号強度評価装置, 信学技報, ISEC97-39 (1997).

14) 飯田全広，高橋勝己，宮田裕行，松本　勉：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).
15) MUSIC Semiconductors: LANCAM 1st Family: Preliminary Data Sheet, Rev.1 (Nov. 1997). Available at http://www.music.com/
16) Matsumoto, T. and Kim, I.: Achieving higher success probability in time-memory trade-off cryptanalysis without increasing memory size, *1997 Korea-Japan Joint Workshop on Infomation Security and Cryptology* (Oct. 1997).

(平成 10 年 10 月 23 日受付)
(平成 11 年 5 月 7 日採録)

高橋　勝己（正会員）

1967 年生．1988 年仙台電波工業高等専門学校情報工学科卒業．同年三菱電機（株）に入社し，第五世代コンピュータ・プロジェクトの並列推論マシンや，レーダシステムの並列信号処理計算機の開発等に従事．

飯田　全広（正会員）

1964 年生．1988 年東京電機大学電子工学科卒業．同年三菱電機エンジニアリング（株）入社．オフィスサーバ，DB エンジン等の開発に従事．1995 年同社を休職し，九州工業大学大学院情報工学研究科に入学．1997 年博士前期課程修了．現在同社に復職．

水上　雄介

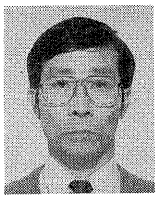
1966 年生．1988 年電気通信大学電気通信学部応用電子工学科卒業．同年三菱電機（株）に入社し，LSI 設計開発に従事．1990 年より中型汎用コンピュータの CPU 開発に従事．現在，同社情報技術総合研究所において，情報セキュリティ技術開発に従事．

山崎　弘巳（正会員）

1961 年生．1985 年東京工業大学大学院物理学専攻修士課程修了．同年三菱電機（株）に入社し，耐環境型特殊用途向け計算機・信号処理器の開発に従事．

宮田　裕行（正会員）

1957 年生．1980 年京都大学工学部情報工学科卒業，1982 年同大学院修士課程修了．同年三菱電機（株）に入社し，情報電子研究所において，通産省スーパーコンピュータ・プロジェクトに参画し，大規模並列プロセッサの開発に従事．1998 年に鎌倉製作所に異動．現在，同所において，宇宙・防衛関係の情報システム開発等に従事．並列アーキテクチャ，並列アルゴリズム等にも興味を持つ．工学博士．IEEE Computer Society 会員．



中島　克人（正会員）

1953 年生．1977 年京都大学工学部電気第二工学科卒業，1979 年同大学院修士課程修了．同年三菱電機（株）に入社し，汎用・専用計算機の開発に従事．1982 年より第五世代コンピュータ・プロジェクトに参画し，推論マシンのアーキテクチャ/言語処理系などの研究開発に従事．1993 年よりリアルワールド・コンピューティング（RWC）プロジェクトに参画．現在，同社情報技術総合研究所において，並列・分散処理向けアーキテクチャおよびミドルウェアの研究開発等に従事．最適設計・スケジューリング技術・可変構造型計算機等にも興味を持つ．工学博士．IEEE Computer Society 会員．

松本　勉（正会員）

1958 年生．1986 年 3 月東京大学大学院博士課程修了，工学博士．同年横浜国立大学工学部電子情報工学科講師，1989 年 11 月同助教授．1996 年 4 月同大学院工学研究科人工環境システム学専攻助教授．主として暗号と情報セキュリティの研究と教育に従事．電子情報通信学会情報セキュリティ研究専門委員会副委員長（平成 11 年度）．日本セキュリティマネジメント学会理事．1999 年 1 月 IACR（国際暗号研究学会）理事．