コンピュータセキュリティ 10−12
(2000. 7. 25)

秘密鍵を特定できない暗号

鈴木 秀一

東京電機大学

〒270-1382 千葉県印西市武西学園台 2-1200

ssuzuki@chiba.dendai.ac.jp

概 要

多重アファイン鍵暗号は、実質的に一変数アファイン関数で構成されていて、1 バイトあたり整数の掛け算を 0.5 回程度しか実行しない。パソコン (Pentium III 600MHZ, Delphi 5.0 のみで記述されたプログラム) 上で 573 MBits/Sec 以上の暗号化速度をソフトウェアのみで実現できる。一方、本暗号は新しい単純な安全性の仕組みを持っていて、平成 11 年 5 月に暗号理論の専門家たちに本暗号を公表して以来、解読の手がかりは見出されていない。この安全性のアイディアをさらに発展させ、「暗号の塔」を構成すると、秘密鍵を特定できない暗号を構成できる。弱鍵を使用しないことを仮定すると、この「暗号の塔」を解読することは非常に困難であることが導かれる。

キーワード

ストリーム暗号, 多重アファイン鍵システム, 暗号の塔.

1 多重アファイン鍵システム

まず多重アファイン鍵システムの定義を述べる。

1.1 アファイン鍵

アファイン鍵とは有限環の元や整数を成分とする次のような構造体 K である。

$$K = \{a,\ b,\ c,\ n\}$$

ここで、a, b はアファイン関数の係数、c はこの鍵が何回使用されたかをカウントするカウンタ、n はこのアファイン鍵を使用できる回数の上限、すなわちアファイン鍵の寿命である。n は

$$n \times (K \quad \text{によって出力される擬似乱数のビット数}) < (a,\ b\ \text{のビット数の和})$$

となるように設定する。通常は $n = 3$ である。

整数または有限環の元 x に対するアファイン鍵 K の作用を $K(x) = ax + b$ で定義する。

1.2 多重アファイン鍵システム

多重アファイン鍵システムとは、複数のアファイン鍵 $\{K[i]\}$ と、そのアファイン鍵同士の間の相互作用を定義する鍵書き換えのプロシージャ $w(i,j)$ の組

$$\mathcal{K} = \{\{K[i]\}, w(i,j)\}$$

である。ここで、$w(i,j)$ は $K[i]$ を $K[j]$ で書き換えることを意味する。これはどのようなものであってもよいので無数の多重アファイン鍵システムを構成できる。ここでは最も安全であると考えられる以下のモデルを考える。

1.3 多重アファイン鍵暗号のアルゴリズム

以下では、32 ビットの符号無し整数を用いた多重アファイン鍵システム $\{\{K[i]\}, w(i,j)\}$ と初期値 x_0 を用いて、平文 $\{m_k\}$ を暗号化し暗号文 $\{c_k\}$ を得るものとする。ここでは仮に 32 個のアファイン鍵を扱うものとする。

ここでは整数のアファイン演算 $ax+b$ を以下のようなような意味で計算する。この演算を**安定化演算** (**stable multiplication**) ということにする。

```
a*x+b=((a*x+b shr 16)) xor (a*x+b)
```

鍵の書き換えのとき、アファイン鍵の係数がともに偶数であると、この鍵は偶数のみ出力するので、次第に鍵や生成される乱数の最下位ビットが 0 になる確率が高くなる。この効果が累積されて、鍵が下のほうから次第に 0 になっていく傾向がある。生成される乱数の上位半分は 0 になり難い。これを下半分に排他的論理和してこの傾向を拡散させるわけである。この演算を用いて鍵書き換えのプロシージャ $w(i,j)$ を以下のように記す。

```
procedure w(i,j:integer):integer;
begin
   K[i].a:=(K[i].a*K[j].a+K[j].b) or 2;
   j:=(j+1) and 31;
   K[i].b:=(K[i].b*K[j].a+K[j].b) or 1;
end;
```

このようなプロシージャを用いて以下のアルゴリズムで多重アファイン鍵暗号を定義する。

1. `i=0, k=1, vkey=0`
2. `x0=K[i](x0) , K[i].c=K[i].c+1`
3. `c[k]=m[k] xor (x0 and 65535)` (encription)
4. `j=(x0 shr 16) and 31`
5. `if K[i].c` $\geq$ `K[i].n then`
   `vkey=(vkey+1) and 31, j=(j+vkey) and 31, w(i,j) , K[i].c=0`
6. `i=j, k=k+1 goto 2.`

このようにすると、弱鍵でない通常状態では `vkey` の影響はほとんど無い。しかし、少数の鍵のみを使用する弱鍵に近い疑わしい状況になると、強制的に全体の鍵を使うように仕向けられる。多数のアファイン鍵が同時に弱鍵になる確率は極めて小さい。このタイプの擬似乱数生成に対する弱鍵 (短い周期の擬似乱数を生成する多重アファイン鍵) は一例も見出されていない。なお、ここで使用された `vkey` を鍵回転パラメータということにする。

2 多重アファイン鍵暗号の速度

多重アファイン鍵暗号は度重なるアルゴリズムの改変を実施し、その度に実行速度と安全性が増してきている。最近、富士ソフト ABC 株式会社の井関氏から、「実行速度の計測で 10MBytes の大きなファイルを使用しているが、小さいファイルを使用した場合より遅い結果が出るのではないか」、また「鍵書き換えの計算もイ

ンライン展開したほうが有利である」という指摘を頂いた。実際、他の暗号アルゴリズムの実行速度もそのように計測されていると考えられるので、本暗号でも次の2点を変更してみた。

- 小さいファイルを多数回、暗号化を繰り返して実行速度を計測した。
- 鍵書き換え、擬似乱数生成の過程もすべてプログラムの中にインライン展開してみた。

従来、実行速度は Pentium III (600MHZ) の環境で 280MBits/sec 程度あったが、このような変更を施してみると、573MBits/sec 程度の速度で暗号化が行われていることが計測できた。高級言語のみで記述された暗号の中では最も高速な結果であろうと考えられる。

3 多重アファイン鍵システムが生成する擬似乱数の周期

本節では、前節で扱った形式の多重アファイン鍵システムが生成する擬似乱数の周期を計測してみる。もとより、多重アファイン鍵システムによって生成される擬似乱数の周期は非常に長いので、鍵の個数は4個程度、鍵の係数も4〜12ビット程度のミニチュア版を用いて計測してみた。この表の鍵の成分の最初の値は乱数生成の初期値である。

鍵の個数 n	鍵の長さ L bits	鍵の成分	周期 p	$p^{1/nL}$
3	4	9,8,14,4,12,7,3	13165	2.2
4	4	14,11,10,7,4,3,13,11,4	56693	1.98
3	4	7,7,3,12,11,3,9	12971	2.2
2	10	725,998,779,252,152	2251617	2.08
5	4	12,13,6,12,8,13,6,6,12,11,9	359431	1.9
2	12	2420,3316,2463,284,1109	131994432	2.18
4	6	16,51,50,29,55,48,14,37,1	51487411	2.1
4	6	8,59,62,42,31,24,48,21,18	11512780	1.97
3	8	251,42,183,236,7,40,119	152418175	2.19
2	8	126,65,143,8,142	268091	2.18

表 1:

表中の $p^{1/nL}$ の値はかなり安定した値をとる。多数の周期の可能性があることと、多重アファイン鍵の個数と係数の長さは生成される擬似乱数の周期に指数的に影響することが読み取れる。このことから、実用的な鍵のサイズとしてアファイン鍵の個数32個、係数は32ビットの符号無し整数を用いた場合、生成される擬似乱数の周期 p は $p > 2^{32\times 32} = 1.798 \times 10^{308}$ となると予想できる。これは暗号用の擬似乱数としては十分な長さである。M系列の乱数のように長周期の擬似乱数生成法も知られている。しかし多重アファイン鍵システムによる擬似乱数の生成法はランダムな鍵を用いても、安定して長周期の擬似乱数を生成する点に特徴がある。このような性質は、暗号用の擬似乱数として望ましいと考えられる。

4 多重アファイン鍵システムが生成する擬似乱数の検定

多重アファイン鍵システムで生成される擬似乱数に対して、各種の検定を実施してみた。結論から言うと、実施したすべての検定で真正乱数と区別できる事実は見出せなかった。ここで行われた検定は [1] で実行可能なプログラムを公開しているので再確認できる。

4.1 01頻度検定

32個のアファイン鍵で32ビット符号無し整数による多重アファイン鍵システムを用いて、1Mbytes の擬似乱数を生成し、16ビットの擬似乱数5000個のデータをとって0, 1頻度検定を行い、これを866例計算してみた。ほぼ正確に正規分布し、0の出現する頻度の平均は49.99%、分散は0.0313となった。最大値は50.569, 最小値は49.439であった。

4.2 線形複雑度

多重アファイン鍵システムから生成される擬似乱数をビット列と見て、これを離散フーリエ変換しパワースペクトルを求めると、最小のものでも 10^{-10} 程度であった。同じビット列を複数回繰り返してパワースペクトルを求めてみると 10^{-30} 程度のものが周期的に現れた。すなわち本システムの生成する擬似乱数は非線型であり、数万程度の少数の線形フイードバックシフトレジスタによっては実現できないことがわかった。

4.3 χ^2 検定

多重アファイン鍵システムによって、1GBytesの32ビットの擬似乱数を生成し、3000個の擬似乱数をサンプリングし、自由度30の χ^2 検定量を1133例計算した。これはほぼ正確に χ^2 分布し、平均が30.013、分散が61.571となった。また同様のサンプリングで、自由度20の χ^2 検定量を620例計算した。これもほぼ正確に χ^2 分布し、平均が19.803、分散が41.649となった。一様乱数であるという仮説は棄却できないと考えられる。

5 暗号の塔

多重アファイン鍵システムの秘密鍵は、外部から観察できない擬似乱数を用いて、ランダムに書き換えられるので、そこから生成された擬似乱数から秘密鍵を特定することは困難である。ここでは、実際に秘密鍵を特定できない暗号を構成する。

暗号の塔

$$\mathcal{T} = \oplus_{i=1}^{\infty} \mathcal{K}_i, \qquad \mathcal{K}_i = \{K_i^0, \cdots, K_i^{M-1}, k_i, v_i, w_i(a,b)\}$$

は多重アファイン鍵システムの無限列である。ここで k_i は各層におけるカレントキー番号、v_i は各層の鍵回転パラメータである。暗号の塔のアルゴリズムは2種類ある。$\mathcal{K}_i$ が $\mathcal{K}_{i+1}$ を直接書き換える形式と各 $\mathcal{K}_i$ が独立な多重アファイン鍵システムとして擬似乱数を生成し、$\mathcal{K}_{i+1}$ が生成する擬似乱数で $\mathcal{K}_i$ を書き換える方式である。ここでは後者について説明する。暗号化は最下位の層 $\mathcal{K}_1$ のみで実行される。

各階層の多重アファイン鍵はそれぞれ本文で述べたアルゴリズムで擬似乱数を生成、または鍵書き換えを実行し、その結果を用いてカレントキー番号を定める。鍵の寿命は原則として3である。ただし第3層から第 $2+s$ $(s \geq 0)$ 層までは鍵の寿命を2とする。$s=0$ のときは全ての鍵の寿命が3である。

ここでは仮に1 WORDのビット数を16 (8, 32, 64でもよい) とする。各鍵は2WORDの長さを持つ。まずこの暗号の概略を述べる。

- $\mathcal{K}_1$ は2WORDの長さの擬似乱数を生成し、そのうちの下位1WORDの擬似乱数を暗号などのために出力する。
- 各 i について、$\mathcal{K}_i$ は2WORDの擬似乱数を生成する。この擬似乱数は下位層の鍵書き換えに使用される。常時鍵回転のパラメータ v_i を使用する。
- 各 i について、K_i^j の寿命が尽きたとき、$\mathcal{K}_{i+1}$ は2個の2WORDの擬似乱数 r, r' を生成する。

$$K_i^j.a = r \text{ or } 2, \quad K_i^j.b = r' \text{ or } 1$$

によって鍵書き換えを実行する。例えば次のようなプロシージャを用いる。

```
function maff(i:LONGWORD) LONGWORD;
begin
  z:=K[i][ck[i]].a * x[i] + K[i][ck[i]].b;
  x[i]:=z xor (z shr 16);inc(K[i][ck[i]].c);
  maff:=x[i];
  if K[i][ck[i]].c>=K[i][ck[i]].n then
  begin
     K[i][ck[i]].c:=0;r1:=maff(i+1);r2:=maff(i+1);
     K[i][ck[i]].a:=r1 or 2;K[i][ck[i]].b:=r2 or 1;
  end;
  v[i]:=(v[i]+1) and 3i;ck[i]:=(v[i]+(x[i] shr 16)) and 31;
end;
```

- 各層の鍵も使用された回数がカウントされ、鍵の寿命に達すると上層の鍵で書き換えられる。

6 秘密鍵を特定する試み

暗号の塔の秘密鍵は3回使用されると上層の鍵を2回使用して書き換えられるので、無限に高い暗号の塔では必ず使用されない秘密鍵が存在し、秘密鍵を特定できないことは自明である。さらに短い期間、低い層の鍵が特定できる可能性もほとんどないことを説明する。

6.1 塔の一階のセキュリティ

それぞれのアファイン鍵は4WORD以上の長さを持つ。$\mathcal{K}_1$ の各鍵は3WORDの擬似乱数を出力すると、$\mathcal{K}_1$ とは無関係な $\mathcal{K}_2$ で書き換えられてしまうのでまったく特定できない。本暗号を解読できるためには $\mathcal{K}_2$ を特定しなければならない。

6.2 塔の二階のセキュリティ

詳細な、しかし初等的な事実を入念に調べると、$\mathcal{K}_2$ も鍵の寿命を3に設定すると特定できないことが分かる。$\mathcal{K}_2$ を特定するためには $\mathcal{K}_3$ を特定しなければならない。状況は $\mathcal{K}_1$ より少し悪くなっているが、$\mathcal{K}_1$ で生成された擬似乱数の2WORDのうち1WORDのみ出力することが効いていて、$\mathcal{K}_2$ を特定できない。

6.3 塔の三階のセキュリティと鍵が特定できる確率

$\mathcal{K}_3$ のアファイン鍵も寿命が2のときは特定できない。$s=0$ のとき、すなわち $\mathcal{K}_3$ の鍵の寿命が3の場合、第3層の秘密鍵が特定できる確率を評価する。$\mathcal{K}_1, \mathcal{K}_2$ を特定する手段がないので、第1、2層の鍵の順番はまったく不確定である。ここで最悪の場合に、$\mathcal{K}_3$ の係数に関する方程式が偶然、正しいものになる確率を p とする。各層のアファイン鍵の個数を M とする。$\mathcal{K}_1$ の鍵が6回使用されたとき $\mathcal{K}_2$ の鍵は4回使用され、$\mathcal{K}_3$ の鍵は2回使用される。この回数より少ない回数で解読できる方程式を導くことはできないので、$p < M^{-12}$ である。寿命2の層が s 個あるとき

$$p < M^{-2s-12}$$

となる。$M = 64$, $s = 0$ のとき、この値は $p < 2.118 \times 10^{-22}$ となる。特に 64 個のアファイン鍵のうち偶然 20 個が特定できる確率は 3.287×10^{-434} より小さい。$s = 10$ 程度にすると、このシステムから何らかの意味のある情報を取り出すことは非常に困難である。

7 暗号の実装

暗号の塔は無限の高さを持つと仮定したが、実は有限の高さでも事実上は問題ない。$s = 0$ のとき、塔の高さを 128 とした場合、最上層の鍵が使用されるまでに出力される擬似乱数のバイト数は $3^{127} = 7.86 \times 10^{60}$ 以上であり、事実上最上層の鍵は使用されない。

このシステムから生成される擬似乱数は事実上無限大の周期を持つとしてよい。また、本システムを何らかの多項式で表現して擬似乱数を予測することもできない。弱鍵を使用しない仮定の元に、本暗号を実際に塔の高さを 128 として実装してみると、Pentium III 600MHZ の環境で 43MBits/sec 程度の実行速度で暗号化できた (直接上位層で下位層を書き換える方式では 52MBits/sec 程度)。このシステムでは、260 バイトの秘密鍵から多重アファイン鍵システムとして擬似乱数を生成し、128 層の鍵を設定する方式をとった。

[6],[7] では、本暗号の特殊な場合に弱鍵の存在が指摘されているが、この事実は筆者が平成 11 年 5 月の TAO の研究会で最初から指摘していたことである。[3] には、この欠点を排除するモデルも提案されている。[2] で提案されているモデル以後は弱鍵は非常に少なくなっている。[6],[7] の「致命的な欠陥」という記述は事実ではない。

参考文献

[1] Suzuki, Shuichi: `http://www.aa.alles.or.jp/~suzuki/`.

[2] Suzuki, Shuichi: The hash function using the multi-affine key system , JWISC 2000, Okinawa,2000.

[3] Suzuki, Shuichi: The cryptography using the multi-affine key system (In Japanese.), technical report of IEICE, ISEC 1999-32, Yamagata University 1999.

[4] Stinson, Douglas: Cryptography:Theory and practice, CRC press, inc, USA, 1995.

[5] 辻井重男, 笠原正雄: 暗号と情報セキュリティ, 昭晃堂, 1990.

[6] 盛合、宮野、下山: 「多重アファイン鍵暗号について」, SCIS2000 技術報告集 (沖縄), 2000.

[7] 盛合、宮野、下山: 「多重アファイン鍵暗号について」, 電子情報通信学会春季大会、技術報告集 (広島大学), 2000.