CAB 方式の暗号の公開鍵暗号部分の脆弱性

CAB 方式の暗号（以下 CAB 暗号）の公開鍵暗号部分が，行列を用いた ElGamal 暗号と同等である，すなわち，非可換行列の部分が意味をなさないことを，ケーリー・ハミルトンの定理を用いて示します。

セアラの暗号はケーリー・ハミルトンの定理により解読されます。私もセアラの暗号を改良して新しい暗号を作ろうとしましたが，結果的に脆弱性を克服できませんでした。このとき，私も CAB 暗号の公開暗号部分とまったく同じ暗号を考えていました。それから 1 か月もたたずに，CAB 暗号の特許公報を見てそれが同じ暗号であると知りました。以下に，私が考えた暗号が脆弱であることを示しますが，CAB 暗号とは独立して考えたものであるため，記法は CAB 暗号と異なっています。

まず，2×2 行列について示す。以下，素数による剰余類で考える。

ケーリー・ハミルトンの定理により $X^k = qX + rE$ （E は単位行列）と表せる。

また，$X^k A^m X^{-k}$ において，X^k の定数倍は無関係であるから，$X^k = X + rE$ としてもよい。

受信者の初期設定

$$Y = X + rE$$
$$B = YA^mY^{-1}$$ （r，m は乱数）

を計算する。ただし，Y と A は非可換であるとする。
Y, r, m が秘匿される。
A, B, X を公開する。

送信者の作業

$$Z = X + sE$$
$$C = ZA^nZ^{-1}$$
$$D = ZB^nZ^{-1}$$ （s，n は乱数）

を計算する。ただし，Z と A は非可換であるとする。
ここで

$$D = Z(YA^mY^{-1})^nZ^{-1} = Z(Y(A^m)^nY^{-1})Z^{-1}\ D = ZYA^{mn}Y^{-1}Z^{-1}$$

である。
D を鍵として，共通鍵暗号でメッセージ M を暗号化して M' を得る。
C と M' を受信者に送信する。
Z, D, s, n が秘匿される。

復号処理

Y と Z は交換可能であるから

$$YC^mY^{-1} = Y(ZA^nZ^{-1})^mY^{-1} = Y(Z(A^n)^mZ^{-1})Y^{-1} = YZA^{mn}Z^{-1}Y^{-1} = ZYA^{mn}Y^{-1}Z^{-1} = D$$

により，D を得る。
D を鍵として，M' を復号して M を得る。

この暗号の破り方

次のように，公開鍵 A, B, X から A^m が求められるので，行列を用いた ElGamal 暗号に対して複雑で計算時間がかかるだけであり，意味のない暗号方式と言える。

$B = YA^mY^{-1}$ より

$$BY = YA^m$$

ここで，ケーリー・ハミルトンの定理により

$$A^m = tA + uE$$

また　$Y = X + rE$

であるから

$$B(X + rE) = (X + rE)(tA + uE)$$

$$BX + rB = tXA + uX + rtA + ruE$$

これより r, t, u, rt, ru に関する 4 つの一次方程式が得られる。これらの一次方程式から，rt, ru を消去すれば t, u が r で表される。したがって，r に関する 2 次方程式が 2 つ得られ，r^2 を消去すれば r, t, u がただ 1 通りに定まる。

これにより $A^m = tA + uE$ が求まるので，この暗号は，行列を用いた ElGamal 暗号と同等である。

例

$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$，$X = \begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix}$，$r = 1, t = 1, u = 1$ とする。

$$Y = X + rE = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}, \quad Y^{-1} = (X + rE)^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$$

$$A^m = tA + uE = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$B = YA^mY^{-1} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 11 & 8 \end{pmatrix}\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} -11 & 5 \\ -31 & 14 \end{pmatrix}$$

逆に，これらを $BX + rB = tXA + uX + rtA + ruE$ に代入すると

$$\begin{pmatrix} -11 & 5 \\ -31 & 14 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix} + r\begin{pmatrix} -11 & 5 \\ -31 & 14 \end{pmatrix} = t\begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + u\begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix} + rt\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + ru\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 15 & -2 \\ 42 & -6 \end{pmatrix} + r\begin{pmatrix} -11 & 5 \\ -31 & 14 \end{pmatrix} = t\begin{pmatrix} 2 & 0 \\ 7 & 3 \end{pmatrix} + u\begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix} + rt\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + ru\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$15 - 11r = 2t + rt + ru$　　…①

$-2 + 5r = 2u + rt$　　…②

$42 - 31r = 7t + 3u + rt$　　…③

$-6 + 14r = 3t + 4u + ru$　　…④

②－③より

$$-44 + 36r = -7t - u \qquad \cdots⑤$$

①－②－④より

$$23-30r=-t-6u \qquad \cdots⑥$$

⑤，⑥より

$$t=-6r+7 \qquad \cdots⑦$$

$$u=6r-5 \qquad \cdots⑧$$

⑦，⑧を②に代入して

$$-2+5r=2(6r-5)+r(-6r+7)=0$$

$$6r^2-14r+8=0$$

$$3r^2-7r+4=0 \quad \cdots⑨$$

⑦，⑧を④に代入して

$$-6+14r=3(-6r+7)+4(6r-5)+r(6r-5)$$

$$6r^2-13r+7=0 \ \cdots⑩$$

2×⑨－⑩より

$$-r+1=0$$

よって　$r=1$

これを⑦，⑧に代入して $r=1,t=1,u=1$ となるから $A^m=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$ が得られる。

この解法において，連立一次方程式しか解いていないことに注意したい。

3×3 行列では

$$B(X^2+rX+sE)=(X^2+rX+sE)(tA^2+uA+vE)$$

となり，展開して $r,s,t,u,v,rt,ru,rv,st,su,sv$ についての 9 つの一次方程式が得られ，これらの一次方程式から，rt,ru,rv,st,su,sv を消去すれば t,u,v が r,s で表される。これにより r,s,r^2,s^2,rs についての一次方程式が 6 つ得られるから，r,s,t,u,v の値が一通りに定まる。

一般に k × k 行列では

k^2 個の一次方程式に対して，X についての係数が $k-1$ 個，A についての係数が k 個，係数の積が $k(k-1)=k^2-k$ 個ある。これより A についての係数が X についての係数の一次式で表される。したがって，方程式を X についての係数だけで表し，X についての係数の積を消去すれば，すべての係数がただ一通りに定まる。

補足

k×k 行列の縦（横）ベクトルのビット数を一定に保ちながら k を大きくすると，解読され難くなります。しかし，連立方程式を解くアルゴリズムは存在します。また，k が大きくなると暗号化，復号の計算量が増大しますし，鍵の大きさが大きくなります。計算量については，ケーリー・ハミルトンの公式を用いて次数下げを行えば，行列の積を計算することなく行列の累乗を計算でき，増大は防げますが，鍵の大きさは k に比例してしまいます。改良は難しいものと思われます。

CAB 方式の暗号の誤謬

次の CAB 暗号の特許の明細書から引用します。

http://jstore.jst.go.jp/detailPat.html?pat_id=31280&doc_num=%E7%89%B9%E9%96%8B2014-017556

この特許の明細書の公開鍵暗号についての主要部分は，次のようになります。

以下，ｄ×ｄの行列とし，mod　ｐ　で考える。

受信者の初期設定

$$M_A = S^{-k_A} Q^{n_A} S^{k_A}$$

を計算する。

n_A，k_Aを秘匿し，Ｑ，Ｓ，M_Aを公開する。

送信者の作業

$$M_B = S^{-k_B} Q^{n_B} S^{k_B}$$

$$M_{AB} = S^{-k_A} M_B^{n_A} S^{k_A}$$

を計算する。

M_{AB}を鍵として，共通鍵暗号でメッセージを暗号化する。

n_B，k_Bを秘匿し，M_Bと暗号化メッセージを受信者に送信する。

ここで,

$$M_{AB} = S^{-(k_A+k_B)} Q^{n_B n_A} S^{(k_A+k_B)}$$

である。

公開鍵暗号部分の強度の根拠として，以下のように述べています。

「共通秘密鍵への攻撃に対する強さについては，攻撃者は公開されている情報（ｐ，ｄ，Ｑ，Ｓ）と公開鍵M_A，M_Bから，次の問題を解き，秘密鍵n_A，k_A，（若しくはn_B，k_B）を得る必要がある。

[問題] 次を満たすn_A，k_Aを求めよ。　　$M_A = S^{-k_A} Q^{n_A} S^{k_A}$

これは，ＤＨ型（離散対数問題）よりはるかに難しい問題となる。仮にn_Aを得ることができても，それからk_Aを得るには，非線形問題を解かねばならない。このとき，不定方程式が出現し，数学的には解を得る確率は０となる。従って，生成される共有秘密鍵は，D-H より数学的に厳密に安全である。」

この主張には，重大な誤謬があります。それは，暗号を解読するにはk_Aを得なければならないと考えていることです。暗号を解読するには確かにn_Aを得なければなりませんが，k_Aを得る必要はあり

ません。n_Aと，S^{k_A}の 0 でない定数倍が得られれば十分です。

実際，n_Aと，c を 0 でない定数として $Y=cS^{k_A}$ が得られたとすると，

$$(M_B)^{n_A}=(S^{-k_B}Q^{n_B}S^{k_B})^{n_A}=S^{-k_B}Q^{n_Bn_A}S^{k_B}$$

であり

$$Y^{-1}(M_B)^{n_A}Y=c^{-1}S^{-k_A}S^{-k_B}Q^{n_Bn_A}S^{k_B}cS^{k_A}=S^{-(k_A+k_B)}Q^{n_Bn_A}S^{(k_A+k_B)}=M_{AB}$$

であるから，M_{AB}が得られます。

現実の暗号解読では，まず，ケーリー・ハミルトンの定理を用いて $M_A=S^{-k_A}Q^{n_A}S^{k_A}$ から$Y=cS^{k_A}$と $Z=Q^{n_A}$ を同時に求めます。

次に，離散対数問題 $Q^{n_A}=Z$ を解き，n_A を求めます。この離散対数問題は，ケーリー・ハミルトンの定理により，有限体上の離散対数問題（D-H）に帰着します。
したがって，「D-H より数学的に厳密に安全である」は間違いです。