一意復号可能な2次元ラビン型暗号

5H－3

林　彬　　清水　秀夫

金沢工業大学情報工学科

1　まえがき

Rabin 暗号 [1, 2] は解読の計算量と素因数分解のそれとの等価性が証明されている、という RSA 暗号 [3] にない特徴をもつ。

ラビン暗号の欠点としては、暗号文の復号が一意的でなく一般に 4 通りの可能な平文が存在すること、即ち暗号化関数が単射でないことが挙げられる [2]。その対策として、平文に意味のある付属情報を含める方法、文献 [4, 5, 6, 7] などの方法がある。

ところでラビン暗号の 2 次元版を小林 [8]、小山 [9] などが提案している。これらの暗号は 1 次元の場合と同様、一般に 16 個の平文 (対) が同一の暗号文 (対) に対応するという問題を抱えている。その一意復号化については、小山 [9] が論じている。2 次元暗号の有用な利用は現在のところ見当たらないが、将来使われるかも知れない。

本論文は著者らによる、一意復号可能なラビン暗号 [7] をまず紹介し、一意復号可能な 2 次元ラビン型暗号を提案する。

2　ラビン暗号

ラビン暗号においては $\{b, n\}$ を公開暗号鍵、$\{b, p, q\}$ を復号鍵とする。ここで p, q は秘密の大きな素数、$n = pq, 0 < b < n$ である。暗号化関数 E は平文空間 $\mathcal{M} = \mathbf{Z}_n = \{0, 1, ..., n-1\}$ から $\mathcal{M}$ への写像で、$E(M) = M(M + b)@n = C$ で定義される。C は暗号文であり、$a@b$ は a を b で割るときの余りを表す。復号は、暗号文 C を与えられて合同式

$$x^2 + bx - C \equiv 0 \pmod{n} \qquad (1)$$

を x について解き、平文を正しく復元することである。

正当な受信者は p, q を知っているので x を求めることができるが、一般にその解は 4 個ある。

Two-dimensional Rabin-type Cryptosystems with Unique-decipherability Property
Akira HAYASHI and Hideo SHIMIZU
Kanazawa Institute of Technology,
Nonoichi-machi,Ishikawa-ken 921 JAPAN.

3　一意復号可能なラビン暗号

著者らは次に述べる一意復号可能なラビン型暗号を提案した [7]。p, q は $p \equiv 3 \pmod 8, q \equiv 7 \pmod 8$ を満たす素数とする。以下簡単のため $b = 0$ とする。また平文集合を $\mathbf{Z}_n$ でなく、既約剰余系 $\mathbf{Z}_n^*$ とする。

＜暗号化＞　暗号文を $C = aM^2@n$ とする。ここで a は、$\mathcal{A} = \{1, -1, 2, -2\}$ に値をとり、平文 M の大きさ及びヤコビ記号 $J = (M/n)$[10] の値に応じて、次のように定められる。

$$\begin{aligned} M < n/2, J = 1 &\Rightarrow a = 1, \\ M < n/2, J = -1 &\Rightarrow a = -2, \\ M > n/2, J = 1 &\Rightarrow a = 2, \\ M > n/2, J = -1 &\Rightarrow a = -1. \end{aligned} \qquad (2)$$

＜復号＞　復号は合同式

$$x^2 \equiv C/a \pmod{n}$$

を解く。ここで$a \in \mathcal{A}$はルジャンドル記号対$L = ((C/p),(C/q))$の値により下記の表のように定める。複数個の解の中から正しい平文が満たす条件に合致するものを選ぶ。

L	a	条件
(1,1)	1	$0 < x < n/2, (x/n) = 1$
(1,-1)	-2	$0 < x < n/2, (x/n) = -1$
(-1,1)	2	$n/2 < x < n, (x/n) = 1$
(-1,-1)	-1	$n/2 < x < n, (x/n) = -1$

この暗号は一意復号可能である [7]。

4　一意復号可能な 2 次元ラビン型暗号

暗号化関数Eが平文空間$\mathcal{M}_2 = \mathcal{M} \times \mathcal{M}$から$\{(C_1, C_2)\} \subset \mathcal{M}_2$への写像で、

$$C_1 = aM_1M_2 @ n \quad (3)$$

$$C_2 = M_1M_2^{-1} @ n \quad (4)$$

で定義される暗号系を考える。ここでaは前節で述べた 1 次元ラビン暗号におけるaである。即ちM_1の大きさとヤコビ記号(M_1/n)の値により式 (2) でaを定める。これは小林 [8]、小山 [9] らのものとは異なるが、式 (3),(4) からM_2を消去すれば、M_1の 2 次合同式となるからラビン型暗号と称してもよかろう。

この暗号の復号は、先ず$C_1C_2 \equiv aM_1^2 \pmod{n}$から、$M_1$を一意的に復号する。そして$M_1$を式 (4) に代入すれば$M_2$を求めることができる。$M_2$の復号が一意的であることは明かであろう。

5　検討とむすび

本論文で提案した 2 次元ラビン型暗号は二つの平文の比が暗号文として与えられるが、これは大した難点ではあるまい。

参考文献

[1] M.O.Rabin: "Digital signatures and public-key functions as intractable as factorization", MIT/LCS/TR-212 Tech.memo,Massachusetts Institute of Technology(1979).

[2] 池野, 小山: 現代暗号理論, 第 7 章, 電子情報通信学会 (1986).

[3] R.Rivest,A.Shamir and L.Adleman: "A method for obtaining digital signatures and public-key cryptosystems", Comm.ACM,21(1978),pp.120-126.

[4] 黒沢, 伊東, 竹内: "素因数分解の困難さと同等の強さを有する逆数を利用した公開鍵暗号", 信学論 (A),J70-A,11,pp.1632-1636(1987).

[5] 鄭, 松本, 今井: "黒沢-伊東-竹内暗号系と Rabin 暗号系に関する考察", 第 9 回情報理論とその応用シンポジウム (1986),pp.667-672.

[6] 島田: "もう一つの実用的な公開鍵暗号について", 1992 年電子情報通信学会春季大会 A-336(1992).

[7] 林, 清水: "一意復号可能な Rabin 型暗号", 信学技報,**ISEC92**-4(1992).

[8] 小林, 田村, 根元: "2 次元の変形ラビン暗号", 信学論 (A),**J72-A**,5, pp.850-851(平 1-05).

[9] 小山: "2 次元公開鍵暗号": 信学論 (A),**J73-A**,11, pp.1872-1879(平 2-11).

[10] 高木: 初等整数論講義 (第 2 版), 共立出版 (1971).