数理解析研究所講究録
第1554巻 2007年 32-39

三部符号及び三部符号形式によるRSA暗号系

岡山大学 大学院 自然科学研究科 丁 峰 神保 秀司 橋口 攻三郎
Graduate School of Natural Science and Technology, Okayama University
Feng Ding, Shuji Jimbo, Kosaburo Hashiguchi

1 序論

符号理論は2つの部分, 即ち, 単チャンネル符号理論と多チャンネル符号理論に区分される. 単チャンネル符号理論はとても深いし, 大きいし, 特に, 形式言語理論の分枝として, とても深く発展してきた. その一方, 多チャンネル符号理論は一般にエントロピー, 伝送速度, 雑音, チャンネル容量, 歪曲速度などのような情報理論の概念と関係している. 前の論文において, 我々は双符号と呼ばれる符号の新しい族を紹介する. Σ とは空集合でない有限アルファベットである. Σ^* とは Σ により生成される自由単位半群である. 双符号とは, 任意の $p,q\geq 1, 1\leq i_1,i_2,\ldots,i_p,j_1,j_2,\ldots,j_q\leq n$ に対して, $x_{i_1}x_{i_2}\ldots x_{i_p}y_{i_p}\ldots y_{i_1}=x_{j_1}x_{j_2}\ldots x_{j_q}y_{j_q}\ldots y_{j_1}$ ならば, 全ての $1\leq k\leq p$ に対して, $p=q$ かつ $i_k=j_k$ が成り立つような語の対の有限系列 $Z=((x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n))(n\geq 1, x_i,y_i\in\Sigma^*)$ である. 任意の双符号 Z は2チャンネル符号として使われる. 1番目のチャンネルで $x_{i_1}\ldots x_{i_p}$ を送り, 同時に2番目のチャンネルで $y_{i_1}^R\ldots y_{i_p}^R$ を送ってよい. もしくは, $x_{i_1}\ldots x_{i_p}$ が $y_{i_1}^R\ldots y_{i_p}^R$ より短いなら, 1番目のチャンネルで $x_{i_1}\ldots x_{i_p}y_{i_p}\ldots y_{i_j}$ を送ると同時に, 2番目のチャンネルで $y_{i_1}^R\ldots y_{i_{j-1}}^R$ を送ることが可能である. このとき $x_{i_1}\ldots x_{i_p}y_{i_p}\ldots y_{i_j}$ と $y_{i_j}^R\ldots y_{i_{j-1}}^R$ の長さはほとんど同じようにする.

この論文において, 我々は三部符号及び三部符号形式によるRSA暗号系を紹介する. 三部符号は以上のような語の対の有限系列 $Z=((x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n))$ である. どんな暗号化されたメッセージ w でも, w の左の部分, w の右の部分, および w の中央の部分の同時発生の組み合わせである. 例えば, $p=5$ に対して, w は $w=x_{i_1}x_{i_3}x_{i_5}x_{i_4}x_{i_2}y_{i_2}y_{i_4}y_{i_5}y_{i_3}y_{i_1}$ である. $p=6$ に対して, w は $w=x_{i_1}x_{i_3}x_{i_5}x_{i_6}x_{i_4}x_{i_2}y_{i_2}y_{i_4}y_{i_6}y_{i_5}y_{i_3}y_{i_1}$ である. 我々は三部符号のいくつかの性質を研究して, 三部符号判定問題は非可解であることを明らかにする. 1977年にRivest, Shamir と AdlemanはRSA暗号系を提案した. 第5節では, 我々は暗号化と復号化がRSA暗号系に依存して, 送る形式が三部符号の形となる公開鍵暗号系の1つの族を提案する. (文献 [5] において, 6個の暗号系が提案されている).

2 双符号

Σ とは空集合でない有限アルファベット (記号の集合) である. Σ^* とは Σ により生成される自由単位半群である. 長さ0の語は空語と呼ばれ λ で表す. Σ^+ は空でない語 (Σ 上の) の集合であ

る．任意の $x, y, z \in \Sigma^*$ に対し x は xy の接頭語で，z は yz の接尾語であり，y は xyz の因子である．$w \in \Sigma$ に対して，w の長さが $|w|$ で表される．空集合は ϕ で表される．

定義 2.1

$seq(\Sigma^*)$ は Σ 上の有限長である (空でない) 語系列の集合とする．任意の $X = (x_1, \ldots, x_n) \in seq(\Sigma^*)$ に関し，$n \geq 1$ とすべての $1 \leq i \leq n$ に対し $x_i \in \Sigma^*$ を満たす．n は X の長さで $|X|$ で表される．

定義 2.2

符号は有限長の (空でない) 語系列，$X = (x_1, \ldots, x_n) \in seq(\Sigma^*)$ である．つまり任意の $p, q \geq 1$ かつ $i_1, \ldots, i_p, j_1, \ldots, j_q (1 \leq i_k, j_l \leq n)$ に対し，$x_{i_1} \ldots x_{i_p} = x_{j_1} \ldots x_{j_q}$ なら，$p = q$ かつすべての $1 \leq k \leq p$ に対し $i_k = j_k$ が成り立つ．この時各 x_i は (X の) 符号語と呼ばれる．

次の定理はよく知られている．

定理 2.1

任意の与えられた語の有限語列，$X = (x_1, \ldots, x_n) \in seq(\Sigma^*)$ に対し，X が符号か決定できるアルゴリズムが存在する．

命題 2.1

任意の $Z \in seq(\Sigma^* \times \Sigma^*)$ に対し，$Z^{(+)}$ は線形文脈自由言語である．

定義 2.3

任意の有限語順序対列 $Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$ が与えられたとき，Z が双符号であるかどうかを決定する問題を双符号判定問題と呼ぶ．

定理 2.2

双符号判定問題は非可解である．

3 三部符号

この節では三部符号の概念を導入し，三部符号のいくつかの性質を明らかにする．

定義 3.1

$Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$ とする．
任意の $w \in Z^{(+)}$ に対して，w の双符号 Z 分解の集合 $DB(Z, w)$ を次の式により定義する．
$DB(Z, w) = \{(i_1, i_2, \cdots, i_p) \mid p \geq 1, 1 \leq k \leq n$ かつ $w = x_{i_1} \cdots x_{i_p} y_{i_p} \cdots y_{i_1}\}$

次の命題は定義より明らかである．

命題 3.1

任意の $Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$ に対して，次の (1) と (2) は等価である．

(1) Z は双符号である．

(2) 任意の $w \in Z^{(+)}$ に対して, $|DB(Z,w)| = 1$ である.

定義 3.2

語の対の有限系列 $Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$ に対して, Z により三部的に生成される語の集合 $Z^{(+,3)}$ を帰納的に次のように定義する.

(1) 任意の $1 \leq i \leq n$ に対して, $x_i y_i \in Z^{(+,3)}$ であり, (x_i, λ, y_i) を $x_i y_i$ の三部分解という. また, (x_i, λ, y_i) のサイズを 1 とする. $x_i y_i$ の三部分解の集合を $TD(Z, x_i y_i)$ により表す. (i) を $x_i y_i$ の分解系列と呼び, $x_i y_i$ の分解系列の集合を $DT(Z, x_i y_i)$ で表す.

(2) 帰納的に $z \in Z^{(+,3)}$ とし, $(u,v,w) \in TD(Z,z)$ とし, p を (u,v,w) のサイズとする.

(a) p が奇数のとき, 任意の $1 \leq i \leq n$ に対して, $ux_i v y_i w \in Z^{(+,3)}$ であり, $(u, x_i v y_i, w)$ は $ux_i v y_i w$ の三部分解である. また, $(u, x_i v y_i, w)$ のサイズは $p+1$ である. z の分解系列が $(j_1, j_2, \cdots, j_p)$ のとき, $ux_i v y_i w$ の分解系列は $(j_1, j_2, \cdots, j_p, i)$ である. $ux_i v y_i w$ の分解系列の集合を $DT(Z, ux_i v y_i w)$ で表す.

(b) p が偶数のとき, 任意の $1 \leq i \leq n$ に対して, $ux_i v y_i w \in Z^{(+,3)}$ であり, $(ux_i, v, y_i w)$ は $ux_i v y_i w$ の三部分解である. また, $(ux_i, v, y_i w)$ のサイズは $p+1$ である. z の分解系列が $(j_1, j_2, \cdots, j_p)$ のとき, $ux_i v y_i w$ の分解系列は $(j_1, j_2, \cdots, j_p, i)$ である. $ux_i v y_i w$ の分解系列の集合を $DT(Z, ux_i v y_i w)$ で表す.

定義 3.3

任意の $Z \in seq(\Sigma^* \times \Sigma^*)$ は, 任意の $w \in Z^{(+,3)}$ に対して, w の分解が一意的, すなわち, $|DT(Z,w)| = 1$ のとき, 三部符号である.

命題 3.2

任意の語の対の有限系列 $Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$ に対して, 次の (1) と (2) が成立する.

(1) 任意の $w \in Z^{(+,3)}$ に対して, $p \geq 1, 1 \leq i_1, i_2, \cdots, i_p \leq n$ が存在し, $w = x_{i_1} x_{i_2} \cdots x_{i_p} y_{i_p} \cdots y_{i_1}$ が成立する.

(2) 任意の $p \geq 1, 1 \leq i_1, i_2, \cdots, i_p \leq n$ に対して, $x_{i_1} x_{i_2} \cdots x_{i_p} y_{i_p} \cdots y_{i_1} \in Z^{(+,3)}$ である.

系 3.1

任意の $Z \in seq(\Sigma^* \times \Sigma^*)$ に対して, $Z^{(+)} = Z^{(+,3)}$.

系 3.2

任意の $Z \in seq(\Sigma^* \times \Sigma^*)$ と $w \in Z^{(+,3)}$ に対して, 次式が成立する.

$$|DT(Z,w)| = |DB(Z,w)|$$

系 3.3

任意の $Z \in seq(\Sigma^* \times \Sigma^*)$ に対して, 次の (1) と (2) は等価である.

(1) Z は双符号である.

(2) Z は三部符号である.

定義 3.4
任意の有限語順序対列 $Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$ が与えられたとき, Z が三部符号であるかどうかを決定する問題を三部符号判定問題と呼ぶ.

定理 3.1
三部符号判定問題は非可解である.

4 RSA暗号系

この節では, RSA 暗号系の基礎部分を概観する. まず, RSA 暗号系に対して必要な代数の基本原理を述べる. この論文において, 自然数は正整数のことである.

自然数 n に対して, $(Z_n, +, \times)$ は $(\mathrm{mod}\ n)$ と $Z_n = \{0, 1, \cdots, n-1\}$ 上で定義された演算の環を表す. Z_n でこの環を簡単に示す. Z_n^* は集合 $\{a \in Z_n \mid a$ と n は互いに素である $\}$ を示す. オイラー関数 ϕ は任意の $n \geq 1$ に対して, $\phi(n) = |Z_n^*|$ として定義される. 定義より下記を容易に理解できる.

Fact 1　p と q を二つの異なる素数とする.

(1) $\phi(p) = p - 1$

(2) e に対して, $\phi(p^e) = p^{e-1}(p-1)$

(3) $\phi(p-q) = (p-1)(q-1)$

下記の定理 (オイラーの定理) と系はよく知られている.

定理 4.1
任意の互いに素な二つの正整数 n と a に対して, $a^{\phi(n)} \equiv 1 \pmod{n}$ である.

系 4.1
素数 p と, p に対して素である正整数 a に対して, $a^{p-1} \equiv 1 \pmod{p}$ である.

RSA 暗号系の構成方法を概観する.

定義 4.1
RSA 暗号系のユニットは下記を満足する五個の部分 $\langle p, q, e, d, n \rangle$ から構成される.

(1) p と q は二つの異なる素数である.

(2) e と d は $e \cdot d \equiv 1 \pmod{lcm(p-1, q-1)}$ を満足する二つの異なる正整数である.

(3) $n = p \cdot q$

定義 4.2

一般にRSA暗号系は$k \geq 1$個のユニットから成り立つ, 即ち, $U_i = \langle p_i, q_i, e_i, d_i, n_i \rangle$ $(1 \leq i \leq k)$である. 各々のユニット$U_i = \langle p_i, q_i, e_i, d_i, n_i \rangle$は上記の条件を満足する.

以下において, 2進アルファベット$\Sigma = \{0, 1\}$上の暗号系を考える. (p, q, e, d, n)は定義4.1のようなRSA暗号系のユニットとする. 平文wは長さ$\lceil \log_2 n \rceil$のいくつかのブロックから成り立つ記号列$w = a_1 a_2 \cdots a_r$ $(r \geq 1, a_i \in \Sigma)$である. $w = b_1 b_2 \cdots b_s$, $b_i \in \Sigma^{\lceil \log_2 n \rceil}$ $(1 \leq i \leq s)$である. wの任意のブロックMを考える, CはMの暗号化された語とする. 下記が成立する.

暗号鍵 : (e, n)と暗号化 : $C \equiv M^e \pmod{n}$

復号鍵 : (d, n)と復号化 : $M \equiv C^d \pmod{n}$

定理 4.2

三つの部分から成る正整数(e, d, n)は定義4.1の中の条件を満足すれば, 下記が成立する.

$$(M^e)^d \equiv M \pmod{n}$$

上記の定理の中に, MとCは二つの役割を演じる: (i) 2進系列である, (ii) 2進系列が表す整数を示す.

記法 4.1

一般にRSA暗号系は$k \geq 1$個のユニットから成り立つ, $U_i = \langle p_i, q_i, e_i, d_i, n_i \rangle$ $(1 \leq i \leq k)$である. 各々のユニット$U_i = \langle p_i, q_i, e_i, d_i, n_i \rangle$は上記の条件を満足する. 以下において, 各々のユニット$U_i = \langle p_i, q_i, e_i, d_i, n_i \rangle$において, 以下の (1) と (2) の記法を用いる.

(1) 任意の$M (0 \leq M < n_i)$に対して, $e_i(M)$は暗号化されたメッセージCを表示する : $e_i(M) = C \equiv M^{e_i} \pmod{n_i}$

(2) 任意の暗号化されたメッセージ$C (0 \leq C < n_i)$に対して, $d_i(C)$は最初のメッセージMを表示する : $d_i(C) = M \equiv C^{d_i} \pmod{n_i}$

5 三部符号を用いたRSA暗号系の提案

この節では, 暗号化と復号化がRSA暗号系に依存して, 送る形式が三部符号の形となる公開鍵暗号系の1つの族を提案する.(文献 [5] において, 6個の暗号系が提案されている).

注意 5.1

以下において, 各々の暗号系の中に, RSA暗号系のいくつかのユニットを使用する, 即ち, $1 \leq i \leq m$に対して, $(p_1, q_1, n_1, e_1, d_1), (p_2, q_2, n_2, e_2, d_2), \cdots, (p_m, q_m, n_m, e_m, d_m)$ $(m \geq 2)$であり, $(p_i, q_i, n_i, e_i, d_i)$は定理4.2と記法4.1のようなRSA暗号系のユニットである.

以下において, 全ての$1 \leq i, j \leq n$に対して, (i)$|x_i| = |x_j|$と (ii)$|y_i| = |y_j|$が成立する任意の三部符号$Z = ((x_1, y_1), \cdots, (x_n, y_n)) \in seq(\Sigma^* \times \Sigma^*)$に対して, ZのX-長は$|x_1|$であるという.

この暗号系では, 鍵オートマトンの概念を必要とするので最初に有限オートマトンの定義を与え, 次に鍵オートマトンの定義を与える.

定義 5.1

有限オートマトンとは5つ組 $M=(\Sigma,Q,\delta,q_0,F)$ のことをいう. ここに Q は空でない有限集合で, その要素は状態 (state) と呼ばれる. Σ はアルファベットで, δ は $Q\times\Sigma$ から Q への関数で遷移関数 (transition function) と呼ばれる. また, $q_0\in Q$ は初期状態 (initial state), $F\subseteq Q$ であり, その要素は最終状態 (final state) と呼ばれる.

遷移関数 δ を

(1) $\delta(q,\varepsilon)=q$ $(q\in Q)$

(2) $\delta(q,ax)=\delta(\delta(q,a),x)$ $(q\in Q,a\in\Sigma,x\in\Sigma^*)$

によって, $Q\times\Sigma^*$ から Q への関数に拡張する.

M によって受理される語の全体を $L(M)$ と書く. すなわち,

$$L(M)=\{w\in\Sigma^*\mid\delta(q_0,w)\in F\}$$

である. これを有限オートマトン M によって受理される言語という.

定義 5.2

鍵オートマトン $\mathcal{A}$ は7組 $\mathcal{A}=\langle\Sigma,Q,\delta,\{q_0\},Q,\mathcal{K},f\rangle$ であり, 次の (1)-(4) が成立する.

(1) $\Sigma=\{0,1\}$

(2) $\langle\Sigma,Q,\delta,\{q_0\},Q\rangle$ は有限オートマトンである.

(3) $\mathcal{K}$ は各要素がある公開鍵暗号系の1つのユニットであり, 有限集合である.

(4) f は写像 $f:Q\to\mathcal{K}$ である.

定義 5.3

鍵オートマトン $\mathcal{A}=\langle\Sigma,Q,\delta,\{q_0\},Q,\mathcal{K},f\rangle$ は $\mathcal{K}$ の各要素が RSA 暗号系の1つのユニットであるとき, RSA-鍵オートマトンと呼ばれる.

暗号系 5.1 は次の項目により成立する.

(1) x (≥ 2) の人, $A_1,\ldots,A_x$ の作る集合.

(2) 各 $1\leq i\leq x$ に対し, A_i は定義 5.2, 5.3 を満たす RSA-鍵オートマトン $\mathcal{A}_i=\langle\Sigma_i,Q_i,\delta_i,\{q_{0_i}\},Q_i,\mathcal{K}_i,f_i\rangle$ をもつ. $\mathcal{A}_i$ について, $\mathcal{K}_i$ の各要素 $(p_{ij},q_{ij},n_{ij},e_{ij},d_{ij})$ $(1\leq j\leq m_i)$ に対して, (p_{ij},q_{ij},d_{ij}) は非公開とするが, その他は公開とする. またその他に RSA 暗号系の2つのユニット $(p_{0ij},q_{0ij},n_{0ij},e_{0ij},d_{0ij})$ $(j=1,2)$ をもち, (n_{0ij},e_{0ij}) $(j=1,2)$ を公開する.

(3) ある平文 M を A_i に送る場合, 下記の暗号化復号化法 5.1 を用いて暗号文 C を送信する.

(4) 送信文を受信した A_i は, 暗号文 C に暗号化復号化法 5.1 を用いることにより平文 M を得る.

以下に, 暗号化復号化法 5.1 について形式的に記す.

5.0.1 暗号化復号化法 5.1

暗号化復号化法 5.1 は RSA-鍵オートマトン $\mathcal{A} = \langle \Sigma, Q, \delta, \{q_0\}, Q, \mathcal{K}, f \rangle$ と RSA 暗号系の 2 つのユニット $(p_{0j}, q_{0j}, n_{0j}, d_{0j}, e_{0j})$ $(j = 1, 2)$ に基づいて実行される．ここで，$\mathcal{K} = \{(p_i, q_i, n_i, e_i, d_i) \mid 1 \leq i \leq h\}$ $(h \geq 1)$ とする．

アルファベット $\Sigma = \{0, 1\}$ 上のブロック符号 $U = (u_1, \ldots, u_m)$ に対して，暗号化復号化を次のように行う．ここで，$u_i \in \Sigma^+$, $|u_i| \leq \min\{\lceil \log_2 n_j \rceil \mid 1 \leq j \leq h\}$ $(1 \leq i \leq m)$ が成立しているとする．

(1) まず $1 \leq l < \min\{\lceil \log_2 n_{01} \rceil, \lceil \log_2 n_{02} \rceil, \lceil \log_2 n_j \rceil \mid 1 \leq j \leq h\}$ である正整数 l を送信者が選ぶ．

(2) 送信者は鍵 e_{01} で $w_1 = e_{01}(l)$ を求める．ここで，w_1 は長さ $\lceil \log_2 n_{01} \rceil$ の 2 進系列である．$w_1 = x_{01}y_{01}$ とおく．$x_{01} = hp(w_1)$, $y_{01} = hs(w_1)$ とする．

(3) 送信者が通信文 $u_{i_1}u_{i_2}\cdots u_{i_s}$ $(s \geq 1, 1 \leq i_j \leq m)$ を送信したいとする．$t \geq 1$ に対して，s は $s = 2 \cdot t$ とする．(ここで，s は偶数である．奇数の場合も同様に扱える．)

(4) 送信者は長さ s の 2 進系列 $\gamma = a_1 \cdots a_s$ をランダムに生成する．ここで，$a_i \in \{0, 1\}$ $(1 \leq i \leq s)$ である．各 $1 \leq j \leq s$ に対して，$q_j = \delta(q_0, a_1a_2\cdots a_j)$ とおく．そして，$f(q_j) = (p_{k_j}, q_{k_j}, n_{k_j}, e_{k_j}, d_{k_j})$ $(1 \leq k_j \leq h)$ とする．

(5) 送信者は，γ を長さ $\lceil \log_2 n_{02} \rceil$ のブロックに分割する．つまり，$\gamma = b_1b_2\cdots b_g$ $(1 \leq g \leq s)$ とする．ただし，$1 \leq i \leq g$ に対して，$b_i \in \{0, 1\}^+$, $|b_i| = \lceil \log_2 n_{02} \rceil$ であり，必要なら，(4) の γ の右にいくつかの 0 を並べて $|\gamma| = g \times \lceil \log_2 n_{02} \rceil$ となる新しい γ を作る．ここで，$0 \leq b_i < n_{02}$ $(1 \leq i \leq g)$ が成立する．

(6) 送信者は各 $1 \leq i \leq g$ に対して，鍵 e_{02} で $w_{2i} = e_{02}(b_i)$ を求める．ここで，w_{2i} は長さ $\lceil \log_2 n_{02} \rceil$ の 2 進系列である．$w_{2i} = x_{02i}y_{02i}$ とおく．$|x_{02i}| = l$, $|y_{02i}| = \lceil \log_2 n_{02} \rceil - l$ とする．

(7) 三部符号 $Z(U, l, \gamma)$ を次のように定義する

$$\begin{aligned} Z(U, l, \gamma) \quad = \quad & ((x_{01}, y_{01}), (x_{021}, y_{021}), (x_{022}, y_{022}), \cdots, \\ & (x_{02g}, y_{02g}), (x_1, y_1), (x_2, y_2), \cdots, (x_s, y_s)) \end{aligned}$$

ここで，各 $1 \leq j \leq s$ に対し，以下が成り立つ．

x_jy_j は長さ $\lceil \log_2 n_{k_j} \rceil$ $(1 \leq k_j \leq h)$ の $e_{k_j}(u_{i_j})$ を示す 2 進系列であり，$|x_j| = l$, $|y_j| = \lceil \log_2 n_{k_j} \rceil - l$ が成立する．

(8) 通信文 $u_{i_1}u_{i_2}\cdots u_{i_s}$ のかわりに次の 2 進系列を送信する

$$x_{01}x_{021}\cdots x_{02g}x_1x_3\cdots x_{s-1}x_sx_{s-2}\cdots x_4x_2y_2y_4\cdots y_{s-2}y_sy_{s-1}\cdots y_3y_1y_{02g}\cdots y_{021}y_{01}$$

受信者は以下のように復号化を行う．

(1) 受信者は鍵 d_{01} を用いて，$x_{01}y_{01}$ から l を得る．

(2) 受信者は鍵 d_{02} を用いて, l と $((x_{021}, y_{021}), (x_{022}, y_{022}), \cdots, (x_{02g}, y_{02g}))$ から, $\gamma = a_1 \cdots a_s$ を得る.

(4) 受信者は l と γ と RSA-鍵オートマトン $\mathcal{A}$ を用いて, $x_1x_3 \cdots x_{s-1}x_sx_{s-2} \cdots x_4x_2y_2y_4 \cdots y_{s-2}y_sy_{s-1} \cdots y_3y_1$ を復号して, 復号した語を並べかえて通信文 $u_{i_1}u_{i_2} \cdots u_{i_s}$ を得る.

参考文献

[1] F.L.Bauer, Decrypted Secrets : Methods and Maxims of Cryptology, Springer, 1997

[2] J.Berstel and D.Perrin, Theory of Codes, Academic Press, 1985

[3] M.A, Harrison, Introduction to Formal Language Theory, Addison-Wesley, 1978

[4] K. Hashiguchi, F. Ding and S. Jimbo, Modified simplified Curve Integrated Encryption Schemes and modified ElGamal Cryptosystems over bicodes, submitted to Theoret. Comput. Sci.

[5] K. Hashiguchi, F. Ding and S. Jimbo, Tricodes and modified RSA cryptosystems, submitted to Theoret. Comput. Sci.

[6] K.Hashiguch, K.Hashimoto and S.Jimbo, Modified RSA cryptosystems over bicodes, Advances in Algeebra (Proceedings of ICM Satellite Conference in Algebra and Related Topics) (2002, Hong Kong), K.P.Shum, Z.X.Wan and J.P.Zhang eds, World Scientifis, 2003, pp.377-389

[7] K.Hashiguchi, T.Mizoguchi, K.Hashimoto and S.Jimbo, Bicodes and modified RSA cryptosystems, submitted to Theoret. Comput. Sci.

[8] K.Hashiguchi and T.Mizoguchi, Introduction to bicodes, Algebraic Engineering(Proceedings of The International Workshop on Formal Languages and Computer Systems, Kyoto, Japan 18-21 March 1997 and The First International Conference on Semigroups and Algebraic Engineering, Aizu, Japan 24-28 March 1997), C.L. Nehaniv and M. Ito eds, World Scientific, 1999, pp.219〜229

[9] D.R.Stinson, CRYPTGRAPHY Theory and Practice, Second Edition, CRC Press, Inc, 2002