Cryptographic classification of quasigroups of order 4

Guohao Liu, Yunqing Xu
Faculty of Science
Ningbo University
Ningbo 315211, China
xuyunqing@gmail.com

***Abstract*—Edon80 is a stream cipher design that had advanced to the third and last phase of the eSTREAM project. The core of the cipher consists quasigroup string e-transformations and it employs four quasigroups of order 4. The employed quasigroups have influence on the period of the key-stream. There are 576 quasigroups of order 4 in total which have the different period factors. In this paper, we discuss a cryptographic classification of quasigroups, and give a complete classification for the 576 quasigroups of order 4 according to the period factors.**

Keywords-Edon80; Latin square; period factor

I. INTRODUCTION

A quasigroup is an ordered pair $(Q,*)$, where Q is a set and $*$ is a binary operation on Q such that the equations $u*x=v$ *and* $y*u=v$ have uniquely solvable for every pair of elements u, v in Q. We will briefly mention the definition of Latin square in [1]. A Latin square on a set Q is an $|Q|\times|Q|$ array such that every symbol occurs in every row once, and also in every column once. It is fairly well known that the multiplication table of a quasigroup defines a Latin square; that is, a Latin square can be viewed as the multiplication table of a quasigroup with the headline and the sideline removed [2].

Consider an alphabet (i.e. a finite set) Q, and denote by Q^+ the set of all nonempty words (i.e. finite strings) formed by the elements of Q. The elements of Q^+ will be denoted by $x_1x_2\cdots x_m$, where $x_i\in Q$ (i=1, 2,$\cdots m$). Let $*$ be a quasigroup operation on set Q, i.e. consider a quasigroup $(Q,*)$. For each $\alpha\in Q$, we define a function $E_{\alpha,*}: Q^+\to Q^+$ as follows. $\forall X= x_1x_2\cdots x_m\in Q^+$,

$$E_{\alpha,*}(x_1x_2\cdots x_m)=y_1y_2\cdots y_m,$$

Where

$$\begin{cases} y_1=\alpha * x_1 \\ y_{i+1}=y_i * x_{i+1}, \quad i=1,2,\cdots m-1 \end{cases}$$

The function $E_{\alpha,*}$ is called an e-transformation of Q^+ based on the operation $*$ with leader α.

Edon80 was submitted to the eSTREAM project as a hardware stream cipher [3]. It has a unique design among known stream cipher designs: concatenates 80 basic building blocks derived form four small quasigroups of order 4. There are 576 quasigroups of order 4 for Edon80 designs, by Gligoroski's computer experiments, 384 of them are suitable, 64 of them are very suitable [4]. How to choose the right Latin squares is particularly important to a key-stream generater like that in Edon80. In this paper, we discuss the cryptography classification of Latin squares of order four based on mathematical theory.

The paper is organized as follows: in Section 2 we give the definition of period factors of a quasigroup and some results on the period factors. In Section 3 we give a classification to all of the quasigroups of order 4. We calculate the period factors of the quasigroups for every column conjugate class. Section 5 contains concluding remarks.

II. THE PERIOD FACTORS OF A QUASIGROUP

Let $X= x_1x_2\cdots x_m\in Q^+$. If there exist positive integers k and p such that $x_{i+p}= x_i$ when $i\geq k$, then we say that X is quasi periodic. If $k=0$, then we say that X is periodic. If p is the least number of such integers, the p is called the period of X.

Definition 2.1: Let Q be a n-set and σ be a permutation on Q. $\forall x\in Q$, the period of sequence $x\sigma(x)\sigma^2\cdots\sigma^i(x)\cdots$ is called the period factor of σ on x and denoted by $f_\sigma(x)$.

Lemma 2.2: [5] Suppose Q is a set and σ is a permutation on Q. If $x\in Q$ is in a cycle of σ of length k, then $f_\sigma(x)=k$.

It is obvious that $f_\sigma(x)$ is an integer and $1\leq f_\sigma(x)\leq n$. Then function $f_\sigma= f_\sigma(x)$ with domain Q is a random variable with sample space $N=\{1, 2,\cdots, n\}$.

Theorem 2.3: [5] Suppose Q is a set and σ is a permutation on Q. If the type of σ is $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$, i.e, σ *has* λ_i cycles of length i (i=1, 2 ,$\cdots$, n), and the probability distribution on Q is uniform : $\{P(x)=1/n : x\in Q\}$, then the probability distribution of f_σ

$$\begin{pmatrix} 1 & 2 & \dots & n \\ P(f_\sigma=1) & P(f_\sigma=2) & \dots & P(f_\sigma=n) \end{pmatrix}=\begin{pmatrix} 1 & 2 & \dots & n \\ \frac{\lambda_1}{n} & \frac{2\lambda_2}{n} & \dots & \frac{n\lambda_n}{n} \end{pmatrix}$$

Definition 2.4: Let $Q=\{1, 2,\cdots, n\}$, $(Q,*)$ be a quasigroup, $L=(l_{i,j})_{n\times n}$ be the Latin square of the multiplication table of $(Q,*)$. $\forall\ i\in Q$, the permutation

$$\sigma_i=\begin{pmatrix} 1 & 2 & \dots & n \\ l_{1i} & l_{2i} & \dots & l_{ni} \end{pmatrix}=\begin{pmatrix} 1 & 2 & \dots & n \\ 1*i & 2*i & \dots & n*i \end{pmatrix}$$

is called the ith column permutation of L (or $(Q,*)$).

Theorem 2.5: [5] Let $Q=\{1, 2,\cdots, n\}$, $(Q,*)$ be a quasigroup and σ_1, σ_2,$\cdots$ σ_n be the column permutations of $(Q,*)$. Suppose $X= x_1x_2\cdots x_m\in Q^+$ is periodic with period p. $E_{\alpha_0,*}$ is the e-transformation function of Q^+ based on the operation $*$ with leader $\alpha\in Q$ and

© 2013. The authors - Published by Atlantis Press

$$Y = y_1 y_2 \cdots y_m \cdots = E_{\alpha_0,*}(x_1 x_2 \cdots x_m \cdots).$$

If α_0 is in a cycle of length k of the permutation $\sigma = \sigma_{x_p} \sigma_{x_{p-1}} \cdots \sigma_{x_1}$, then Y is periodic and period of Y is $k \cdot p$.

Definition 2.6: Suppose Q is an n-set and $(Q,*)$ is a quasigroup, $\sigma_1, \sigma_2, \cdots \sigma_n$ are the column permutations of $(Q,*)$ and $S_*=\{\sigma_1, \sigma_2, \cdots \sigma_n\}$. For any positive integer p, let $S_*^p = \{\sigma_{i_p} \sigma_{i_{p-1}} \cdots \sigma_{i_1} : 1 \le i_1, i_2, \cdots i_p \le n\}$ be a multi-set.

$\forall (\sigma, x) \in S_*^p \times Q$, the period of sequence $x\sigma(x)\cdots \sigma^i(x)\cdots$ is called the period factor of $(Q,*)$ of degree p with σ and x and denoted by $f_*^p(\sigma, x)$. The function $f_*^p = f_*^p(\sigma, x)$ with domain $S_*^p \times Q$, is a random variable with sample space $N=\{1, 2, \cdots, n\}$. f_*^p is called the period factor of $(Q,*)$ of degree p.

Theorem 2.5: [5] Suppose Q is an n-set and $(Q,*)$ is a quasigroup and $S_* = \{\sigma_1, \sigma_2, \cdots \sigma_n\}$ is from *Definition 2.6*. Let $\{\tau_1, \tau_2, \cdots \tau_v\} = \langle S_* \rangle$ be the permutation group generated by S_* and suppose the type of τ_i is $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$ (i=1, 2, $\cdots$, n). Suppose the probability distribution on Q is uniform: $\{P(x) = 1/n : x \in Q\}$. For any positive integer p, if the multi-set $S_*^p = \{\sigma_{i_p} \sigma_{i_{p-1}} \cdots \sigma_{i_1} : 1 \le i_1, i_2, \cdots i_p \le n\} = \{n_1^{(p)} \cdot \tau_1, n_2^{(p)} \cdot \tau_2, \cdots, n_v^{(p)} \cdot \tau_v\}$, then the probability distribution of f_*^p is

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \frac{1}{n^{p+1}} \sum_{i=1}^{v} n_i^{(p)} \lambda_{i1} & \frac{2}{n^{p+1}} \sum_{i=1}^{v} n_i^{(p)} \lambda_{i2} & \cdots & \frac{n}{n^{p+1}} \sum_{i=1}^{v} n_i^{(p)} \lambda_{in} \end{pmatrix}.$$

III. A CLASSIFICATION OF QUASIGROUPS

Definition 3.1: Let $(Q,*)$ *and* $(Q,\bullet)$ be two quasigroups and τ is a permutation on Q, $(Q,\bullet)$ is called a column isomorphism of $(Q,*)$ and denoted by $\bullet = *^\tau$ *if* $\forall\ x, y \in Q$, $x \tau y = z$. Let L_1 and L_2 are the Latin squares corresponding to $(Q,*)$ and $(Q,\bullet)$, respectively. L_2 is called a column isomorphism of L_1 and denote by $L_2 = L_1^\tau$.

Let $\mathcal{L}_n$ be the set of all Latin squares on set Q. The orbits of column isomorphism are called the column isomorphism classes $\mathcal{L}_n$.

It is easy to see that two Latin squares have the same column permutation set if and only if they are in a same column isomorphism class. From Definition 2.6 we have the following lemma.

Lemma 3.2: If quasigroup $(Q,\bullet)$ is a column isomorphism of $(Q,*)$, and $f_*^{(p)}$ and $f_\bullet^{(p)}$ are the period factors of degree p of $(Q,*)$ and $(Q,\bullet)$, respectively. Then $f_*^{(p)} = f_\bullet^{(p)}$ for any positive integer p.

There are 576 quasigroups (Latin sqaures) of order 4 and they are lexicographically ordered. Denote L_i the ith Latin square of order four. The 576 quasigroups can be divided into 24 isomorphism classes I_i for $1 \le i \le 24$ in the following, where only the lexicographic numbers are given for simple.

I_1 = {1, 26, 51, 77, 100, 126, 147, 172, 197, 223, 246, 272, 305, 331, 354, 380, 405, 430, 451, 477, 500, 526, 551, 576}.
I_2 = {2, 25, 52, 78, 99, 125, 148, 171, 198, 224, 245, 271, 307, 333, 356, 382, 407, 432, 449, 475, 498, 524, 549, 574}.
I_3 = {3, 28, 53, 79, 102, 128, 145, 170, 195, 221, 244, 270, 306, 332, 353, 379, 406, 429, 452, 478, 499, 525, 552, 575}.
I_4 = {4, 27, 54, 80, 101, 127, 146, 169, 196, 222, 243, 269, 308, 334, 355, 381,408, 431,450, 476, 497, 523, 550, 573}.
I_5 = {5, 29, 55, 75, 97, 121, 154, 178, 208, 232, 250, 278, 309, 329, 359, 383, 401, 425, 433, 457, 481, 509, 535, 559}.
I_6 = {6, 30, 56, 76, 98, 122, 153, 177, 207, 231, 249, 277, 310, 330, 360, 384, 402, 426, 434, 458, 462, 510, 536, 560}.
I_7 = {7, 31, 49, 73, 103, 123, 161, 185, 209, 237, 263, 287, 290, 314, 340, 368, 392, 416, 454, 474, 504, 528, 546, 570}.
I_8 = {8, 32, 50, 74, 104, 124, 162, 186, 210, 238, 264, 288, 289, 313, 339, 367, 391, 415, 453, 473, 503, 527, 545, 569}.
I_9 = {9, 33, 63, 87, 107, 135, 150, 174, 200, 220, 242, 266, 311, 335, 357, 377, 403, 427, 442, 470, 490, 514, 544, 568}.
I_{10} = {10, 34, 64, 88, 108, 136, 149, 173, 199, 219, 241, 265, 312, 336, 358, 378, 404, 428, 441, 469, 489, 513, 543, 567}.
I_{11} = {11, 37, 57, 82, 110, 132, 163, 189, 212, 234, 259, 284, 293, 318, 343, 365, 388, 414, 445, 467, 495, 520, 540, 566}.
I_{12} = {12, 38, 58, 81, 109, 131, 165, 191, 214, 236, 261, 286, 294, 317, 344, 366, 387, 413, 443, 465, 493, 518, 538, 564}.
I_{13} = {13, 39, 59, 84, 112, 134, 164, 190, 211, 233, 260, 283, 291, 316, 341, 363, 386, 412, 446, 468, 496, 519, 539, 565}.
I_{14} = {14, 40, 60, 83, 111, 133, 166, 192, 213, 235, 262, 285, 292, 315, 342, 364, 385, 411, 444, 466, 494, 517, 537, 563}.
I_{15} = {15, 35, 61, 85, 105, 129, 167, 187, 215, 239, 257, 281, 298, 322, 352, 376, 394, 422, 436, 460, 488, 512, 530, 558}.
I_{16} = {16, 36, 62, 86, 106, 130, 168, 188, 216, 240, 258, 282, 297,321, 351, 375, 393, 421, 435, 459, 487, 511, 529, 557}.
I_{17} = {17, 41, 67, 95, 119, 143, 151, 175, 193, 217, 247, 267, 300, 328, 346, 370, 400, 424, 455, 479, 501, 521, 547, 571}.
I_{18} = {18, 42, 68, 96, 120, 144, 152, 176, 194, 218, 248, 268, 299, 327, 345, 369, 399, 423, 456, 480, 502, 522, 548, 572}.
I_{19} = {19, 47, 65, 89, 117, 141, 155, 183, 201, 225, 255, 279, 296, 320, 338,362, 390,410,448, 472, 492, 516, 542, 562}.
I_{20} = {20, 48, 66, 90, 118, 142, 156, 184, 202, 226, 256, 280, 295, 319, 337, 361, 389, 409, 447, 471, 491, 515, 541, 561}.
I_{21} = {21, 43, 70, 92, 113, 138, 157, 179, 203, 228, 252, 274, 303, 325, 349, 374, 398, 420, 439, 464, 485, 507, 534, 556}.
I_{22} = {22, 44, 69, 91, 114, 137, 159, 181, 205, 230, 254, 276, 301, 323, 347, 372, 396, 418, 440, 463, 486, 508, 533, 555}.
I_{23} = {23, 45, 72, 94, 115, 140, 158, 180, 204, 227, 251, 273, 304, 326, 350, 373, 397, 419, 437, 462, 483, 505, 532, 554}.
I_{24} = {24, 46, 71, 93, 116, 139, 160, 182, 206, 229, 253, 275, 302, 324, 348, 371, 395, 417, 438, 461, 484, 506, 531, 553}.

Definition 3.3: Let L_1 and L_2 be two Latin squares on set Q = {1, 2, $\cdots$, n} with column permutation sets $\{\sigma_1, \sigma_2, \cdots \sigma_n\}$ and $\{\tau_1, \tau_2, \cdots, \tau_n\}$, respectively. If there is a permutation γ on Q such that $\tau_i = \gamma \sigma_{j_i} \gamma^{-1}$ for i=1, 2, $\cdots$, n.

where $\{j_1, j_2, \cdots, j_n\}=\{1, 2, \cdots, n\}$, then L_2 is said to be a column conjugate of L_1, and denoted by $L_2 = \gamma L_1 \gamma^{-1}$.

Lemma 3.4: [6, Lemma 2.7] Let σ, τ and γ are permutations on a same set. If $\tau = \gamma\sigma\gamma^{-1}$, Then τ have the same cycle structure (type) as σ.

From Lemma II we have the following lemma.

Lemma 3.4: Suppose L_2 is a column conjugate of L_1. $(Q,*)$ *and* $(Q,\bullet)$ are the quasigroups correspond to L_1 and L_2, respectively. $f_*^{(p)}$ and $f_\bullet^{(p)}$ are the period factors of degree p of $(Q,*)$ *and* $(Q,\bullet)$, respectively. Then $f_*^{(p)} = f_\bullet^{(p)}$ for any positive integer p.

The orbits of column conjugate are called the column conjugate classes of $\mathcal{L}_n$. It is easy to see that a column conjugate class concludes several column isomorphism classes.

Let $Q = \{1, 2, \cdots, n\}$ and Ω_Q be the symmetric group of Q. We denote the elements of Ω_Q as show in Table I.

Since we have the conjugate relations in Table II, the 576 quasigroups of order 4 can be divided into 6 column conjugate classes:

TABLE I: ELEMENTS OF SYMMETRIC GROUP Ω_Q

τ_1=1	τ_7=(23)	τ_{13}=(032)	τ_{19}=(0123)
τ_2=(01)	τ_8=(012)	τ_{14}=(123)	τ_{20}=(0132)
τ_3=(02)	τ_9=(021)	τ_{15}=(132)	τ_{21}=(0213)
τ_4=(03)	τ_{10}=(013)	τ_{16}=(01)(23)	τ_{22}=(0231)
τ_5=(12)	τ_{11}=(031)	τ_{17}=(02)(13)	τ_{23}=(0312)
τ_6=(13)	τ_{12}=(023)	τ_{18}=(03)(12)	τ_{24}=(0321)

TABLE II
CONJUGATE RELATIONS OF THE LATIN SQUARES OF ORDER 4

$\tau_{23}L_{241}\tau_{23}^{-1} = L_{30}$	$\tau_4 L_{241}\tau_4^{-1} = L_{72}$	$\tau_2 L_{241}\tau_2^{-1} = L_{151}$
$\tau_{10}L_{241}\tau_{10}^{-1} = L_{468}$	$\tau_9 L_{241}\tau_9^{-1} = L_{38}$	$\tau_3 L_{241}\tau_3^{-1} = L_{85}$
$\tau_{20}L_{241}\tau_{20}^{-1} = L_{323}$	$\tau_6 L_{241}\tau_6^{-1} = L_{492}$	$\tau_{17}L_{241}\tau_{17}^{-1} = L_{50}$
$\tau_{12}L_{241}\tau_{12}^{-1} = L_{142}$	$\tau_{15}L_{241}\tau_{15}^{-1} = L_{351}$	$\tau_{10}L_{241}\tau_{10}^{-1} = L_{107}$
$\tau_{12}L_3\tau_{12}^{-1} = L_{327}$	$\tau_{10}L_4\tau_{10}^{-1} = L_{110}$	$\tau_{12}L_4\tau_{12}^{-1} = L_{302}$
$\tau_{10}L_5\tau_{10}^{-1} = L_{52}$	$\tau_{12}L_5\tau_{12}^{-1} = L_{73}$	$\tau_6 L_{14}\tau_6^{-1} = L_{138}$

$C_1=I_1$, $C_2= I_2 \cup I_5 \cup I_7$, $C_3= I_3 \cup I_9 \cup I_{18}$,
$C_4= I_4 \cup I_{11} \cup I_{24}$, $C_5= I_{14} \cup I_{21}$,
$C_6= I_6 \cup I_8 \cup I_{10} \cup I_{12} \cup I_{13} \cup I_{15} \cup I_{16} \cup I_{17} \cup I_{19} \cup I_{20} \cup I_{22} \cup I_{23}$.

Latin squares in each C_i (i = 1, 2, 3, 4, 5, 6) have the same period factor for each degree.

IV. CALCULATION OF PERIOD FACTORS FOR EACH CONJUGATE ISOMORPHISM CLASS

There are six column conjugate classes of quasigroups of order 4. Quasigroups in a same column conjugate class have the same period factor of any degree. Select one quasigroup from each column conjugate class, e.g., select $L_1 \in C_1$, $L_5 \in C_2$, $L_3 \in C_3$, $L_4 \in C_4$, $L_{14} \in C_5$, $L_{241} \in C_6$, as shown in Figure 1, and calculate the expected values of period factors of the six selected quasigroups.

FIG 1: SELECTED QUASIGROUPS OF ORDER 4

$$L_1 = \begin{matrix} 0&1&2&3\\ 1&0&3&2\\ 2&3&0&1\\ 3&2&1&0 \end{matrix} \quad L_3 = \begin{matrix} 0&1&2&3\\ 1&0&3&2\\ 3&2&0&1\\ 2&3&1&0 \end{matrix} \quad L_4 = \begin{matrix} 0&1&2&3\\ 1&0&3&2\\ 3&2&1&0\\ 2&3&0&1 \end{matrix}$$

$$L_5 = \begin{matrix} 0&1&2&3\\ 1&2&3&0\\ 2&3&0&1\\ 3&0&1&2 \end{matrix} \quad L_{14} = \begin{matrix} 0&1&2&3\\ 2&3&0&1\\ 3&2&1&1\\ 1&0&3&2 \end{matrix} \quad L_{241} = \begin{matrix} 1&3&0&2\\ 0&1&2&3\\ 2&0&3&1\\ 3&2&1&0 \end{matrix}$$

Firstly, we deal with $L_1 \in C_1$. The column permutations of L_1 are $\sigma_0=\tau_1$, $\sigma_1=\tau_{16}$, $\sigma_2=\tau_{17}$, $\sigma_3=\tau_{18}$. Let $S = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, and denote $S^P = \{\sigma_{i_p}\sigma_{i_{p-1}}\cdots\sigma_{i_1} : 0 \le i_1, i_2, \ldots, i_p \le 3\}$ be a multi-set. Table III is a multiplication table of permutations on $Q = \{0, 1, 2, 3\}$.

From Table III we have:

$$\begin{cases} S = \{\tau_1, \tau_{16}, \tau_{17}, \tau_{18}\} \\ S^2 = 4 \cdot \{\tau_1, \tau_{16}, \tau_{17}, \tau_{18}\} \\ S^3 = 16 \cdot \{\tau_1, \tau_{16}, \tau_{17}, \tau_{18}\} \end{cases} \quad (1)$$

TABLE III
A MULTIPLICATION TABLE OF PERMUTATIONS

·	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	τ_9	τ_{10}	τ_{11}	τ_{12}
σ_0	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	τ_9	τ_{10}	τ_{11}	τ_{12}
σ_1	τ_{16}	τ_7	τ_{19}	τ_{20}	τ_{22}	τ_{24}	τ_2	τ_{12}	τ_{14}	τ_{13}	τ_{15}	τ_8
σ_2	τ_{17}	τ_{21}	τ_6	τ_{22}	τ_{20}	τ_3	τ_{23}	τ_{15}	τ_{10}	τ_9	τ_{12}	τ_{11}
σ_3	τ_{18}	τ_{23}	τ_{24}	τ_5	τ_4	τ_{19}	τ_{21}	τ_{11}	τ_{13}	τ_{14}	τ_8	τ_{15}
·	τ_{13}	τ_{14}	τ_{15}	τ_{16}	τ_{17}	τ_{18}	τ_{19}	τ_{20}	τ_{21}	τ_{22}	τ_{23}	τ_{24}
σ_0	τ_{13}	τ_{14}	τ_{15}	τ_{16}	τ_{17}	τ_{18}	τ_{19}	τ_{20}	τ_{21}	τ_{22}	τ_{23}	τ_{24}
σ_1	τ_{10}	τ_9	τ_{11}	τ_1	τ_{18}	τ_{17}	τ_3	τ_4	τ_{23}	τ_5	τ_{21}	τ_6
σ_2	τ_{14}	τ_{13}	τ_8	τ_{18}	τ_1	τ_{16}	τ_{24}	τ_5	τ_2	τ_4	τ_7	τ_{19}
σ_3	τ_9	τ_{10}	τ_{12}	τ_{17}	τ_{16}	τ_1	τ_6	τ_{22}	τ_7	τ_{20}	τ_2	τ_3

For any positive integer p, denote

$$S^p = \{n_i^{(p)} \cdot \tau_i \mid i = 1,2,\cdots,24\}$$

Let $T_{11} = \{1, 16, 17, 18\}$, $T_{12} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 19, 20, 21, 22, 23, 24\}$, from Equations (1) we have

$$n_i^2 = \begin{cases} 4, i \in T_{11} \\ 0, i \in T_{12} \end{cases} \qquad n_i^3 = \begin{cases} 16, i \in T_{11} \\ 0, i \in T_{12} \end{cases}$$

Let

$$n_i^p = \begin{cases} m(p), i \in T_{11} \\ n(p), i \in T_{12} \end{cases}$$

Then we can get Equations (2) in the following.

From Equations (2) we obtain

$$n_i^{(p+1)} = \begin{cases} 4m(p), i \in T_{11}, \\ 0, \quad i \in T_{12}. \end{cases}$$

So, we have Equation (3).

$$\begin{cases} n_1^{(p+1)} = n_1^{(p)} + n_{16}^{(p)} + n_{17}^{(p)} + n_{18}^{(p)}, \\ n_2^{(p+1)} = n_2^{(p)} + n_7^{(p)} + n_{21}^{(p)} + {}_{23}^{(p)}, \\ n_3^{(p+1)} = n_3^{(p)} + n_{19}^{(p)} + n_6^{(p)} + n_{24}^{(p)}, \\ n_4^{(p+1)} = n_4^{(p)} + n_{20}^{(p)} + n_{22}^{(p)} + n_5^{(p)}, \\ n_5^{(p+1)} = n_5^{(p)} + n_{22}^{(p)} + n_{20}^{(p)} + n_4^{(p)}, \\ n_6^{(p+1)} = n_6^{(p)} + n_{24}^{(p)} + n_3^{(p)} + n_{19}^{(p)}, \\ n_7^{(p+1)} = n_7^{(p)} + n_2^{(p)} + n_{23}^{(p)} + n_{21}^{(p)}, \\ n_8^{(p+1)} = n_8^{(p)} + n_{12}^{(p)} + n_{15}^{(p)} + n_{11}^{(p)}, \\ n_9^{(p+1)} = n_9^{(p)} + n_{14}^{(p)} + n_{10}^{(p)} + n_{13}^{(p)}, \\ n_{10}^{(p+1)} = n_{10}^{(p)} + n_{13}^{(p)} + n_9^{(14)} + n_{14}^{(p)}, \\ n_{11}^{(p+1)} = n_{11}^{(p)} + n_{15}^{(p)} + n_{12}^{(p)} + n_8^{(p)}, \\ n_{12}^{(p+1)} = n_{12}^{(p)} + n_8^{(p)} + n_{11}^{(p)} + n_{15}^{(p)}, \\ n_{13}^{(p+1)} = n_{13}^{(p)} + n_{10}^{(p)} + n_{14}^{(p)} + n_9^{(p)}, \\ n_{14}^{(p+1)} = n_{14}^{(p)} + n_9^{(p)} + n_{13}^{(p)} + n_{10}^{(p)}, \\ n_{15}^{(p+1)} = n_{15}^{(p)} + n_{11}^{(p)} + n_8^{(p)} + n_{12}^{(p)}, \\ n_{16}^{(p+1)} = n_{16}^{(p)} + n_1^{(p)} + n_{17}^{(p)} + n_{18}^{(p)}, \\ n_{17}^{(p+1)} = n_{17}^{(p)} + n_{18}^{(p)} + n_1^{(p)} + n_{16}^{(p)}, \\ n_{18}^{(p+1)} = n_{18}^{(p)} + n_{17}^{(p)} + n_{16}^{(p)} + n_1^{(p)}, \\ n_{19}^{(p+1)} = n_{19}^{(p)} + n_3^{(p)} + n_{24}^{(p)} + n_6^{(p)}, \\ n_{20}^{(p+1)} = n_{20}^{(p)} + n_4^{(p)} + n_5^{(p)} + n_{22}^{(p)}, \\ n_{21}^{(p+1)} = n_{21}^{(p)} + n_{23}^{(p)} + n_7^{(p)} + n_2^{(p)}, \\ n_{22}^{(p+1)} = n_{22}^{(p)} + n_5^{(p)} + n_4^{(p)} + n_{20}^{(p)}, \\ n_{23}^{(p+1)} = n_{23}^{(p)} + n_{21}^{(p)} + n_2^{(p)} + n_7^{(p)}, \\ n_{24}^{(p+1)} = n_{24}^{(p)} + n_6^{(p)} + n_{19}^{(p)} + n_3^{(p)}. \end{cases} \quad (2)$$

$$\begin{cases} m(p+1) = 4m(p), \\ n(p+1) = n(p) = 0, \\ m(2) = 4, \\ m(3) = 16, \\ n(2) = n(3) = 0. \end{cases} \quad (3)$$

The solution of Equations (3) is

$$\begin{cases} m(p) = 4^{p-1}, \\ n(p) = 0. \end{cases}$$

Suppose the type of τ_i is $1^{\lambda_{i1}}2^{\lambda_{i2}}3^{\lambda_{i3}}4^{\lambda_{i4}}$ (i=1, 2, 3, 4), Applying Theorem 2.7, we have

$$P\left(f_{*_1}^{(p)} = 1\right) = \frac{1}{4^{p+1}}\sum_{i=1}^{24} n_i^p \lambda_{i1} = \frac{1}{4^{p+1}}(4^{p-1} \times 4) = \frac{1}{4},$$

$$P\left(f_{*_1}^{(p)} = 2\right) = \frac{2}{4^{p+1}}\sum_{i=1}^{24} n_i^p \lambda_{i2} = \frac{2}{4^{p+1}}(4^{p-1} \times 6) = \frac{3}{4},$$

$$P\left(f_{*_1}^{(p)} = 3\right) = \frac{3}{4^{p+1}}\sum_{i=1}^{24} n_i^p \lambda_{i3} = 0,$$

$$P\left(f_{*_1}^{(p)} = 4\right) = \frac{4}{4^{p+1}}\sum_{i=1}^{24} n_i^p \lambda_{i4} = 0.$$

So, the probability distribution of $f_{*_1}^{(p)}$ is

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \frac{1}{4} & \frac{3}{4} & 0 & 0 \end{pmatrix}.$$

The expected value $E(f_{*_1}^{(p)}) = 1\times 1/4 + 2\times 3/4 = 1.75$.

Use a similar way we obtain that for all positive integer p, the expected value of the period factor of $L_5 \in C_2$ is $E(f_{*_5}^{(p)}) = 2.75$.

For the expected value of the period factor of $L_3 \in C_3$, we have

$$E(f_{*_3}^{(p)}) = \begin{cases} 1.75, \text{when p is odd,} \\ 2.75, \text{when p is even.} \end{cases}$$

For the expected value of the period factor of $L_4 \in C_4$, we have

$$E(f_{*_4}^{(p)}) = \begin{cases} 2.75, \text{when p is odd,} \\ 1.75, \text{when p is even.} \end{cases}$$

For the expected value of the period factor of $L_{14} \in C_5$, we have

$$E(f_{*_{14}}^{(p)}) = \begin{cases} 2.5, \ p \equiv 1 (\text{mod} 3), \\ 2.5, \ p \equiv 2 (\text{mod} 3), \\ 1.75, \ p \equiv 0 (\text{mod} 3) \text{ and } p > 1. \end{cases}$$

For the expected value of the period factor of $L_{241} \in C_6$,

$$E(f_{*_{241}}^{(p)}) = \begin{cases} 2.5 - \frac{1}{2^{p+2}}, \text{when p is even,} \\ 2.5 + \frac{1}{2^{p+2}}, \text{when p is odd.} \end{cases}$$

V. CONCLUSIONS

The 576 quasigroups (Latin squares) are divided into 6 column conjugate classes and the quasigroups in each column conjugate class have the same period factors. From the point of view of the period of the key stream, it can be seen from Table IV that the 360 quasigroups in $C_2 \cup C_6$ are suitable, and the 72 quasigroups in C_2 are very suitable for key stream generators.

TABLE VI

column conjugate classes	the number of Latin squares of C_i	the expected value $E(f_*^{(p)})$
C_1	24	1.75
C_2	72	2.75
C_3	72	1.75 when p is odd, 2.75 when p is even.
C_4	72	2.75 when p is odd, 1.75 when p is even.
C_5	48	1.75, when $p \equiv 0$(mod3), p>1, 2.5, when $p \equiv 1$(mod3), 2.5, when $p \equiv 2$(mod3).
C_6	288	2.5–1/2^{p+2}, when p is even, 2.5+1/2^{p+2}, when p is odd.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of the National Natural Science Foundation of China under Grant No. 61373007 and Zhejiang Provincial Natural Science Foundation of China under Grant No. LY13F020039.

REFERENCES

[1] D.R. Stinson, Combinatrial Designs, Constructions and Analysis, Springer-Verlag New York, Inc, 2004, pp. 123--124.

[2] J. Dénes, and A.D. Keedwell, Latin squares and Their Applications. Academic Press, New York and London, 1974.

[3] D. Gligoroski, S. Markovski, L. Kocarev, M. Gusev, Edon80, eSTREAM, Report 2005/007 (2005).

[4] D. Gligoroski, S. Markovski, S.J. Knapskong, The Stream Cipher Edon80, Lecture Notes in Computer Science 4986, 2008: 152-169.

[5] Y. Xu, On the key-stream periods probability of Edon80 (preprint).

[6] J.J. Rotman, Advanced Modern Algebra, Prentice.