Stream Cipher based on Latin Cubes

Yukun Cheng, Yunqing Xu
Department of Mathematics, Ningbo University, Ningbo 315211, China
E-mail: xuyunqing@nbu.edu.cn

***Abstract*—Edon80 is a hardware binary additive synchronous stream cipher submitted to the last phase of the eSTREAM project. The period of keystream of Edon80 is relatively short and there is a key recovery attach on it. In this paper, by modifying the IVSetup mode and the Keystream mode of Edon80, and by introducing a new e-transformation based on Latin cubes, we design a binary additive synchronous stream cipher named CHAINS80 with a much larger keystream period and it can resist the key recovery attack given by Johansson and Hell.**

Keywords—stream cipher; Edon80; key recovery attack; quasigroup; Latin square

I. INTRODUCTION

Edon80, a hardware stream cipher, was submitted to the eSTREAM project and was designed by Gligoroski, Markovski, Kocarev, and Gusev. Its original description is given in [1].

In [2] Hong observed that there is a small probability, for the period of the keystream sequence to be quite short. This was further studied by the designers of Edon80 in [3, 4] and Xu in [5]. But this property could not be utilized in any kind of attack.

Johansson and Hell [6] use the analysis of the periods of the keystream of Edon80 in [4] to mount an attack that can recover the key with complexity around 2^{69}. This is the most advanced attack on Edon80, with a concrete setup that shows how to recover the secret key [7]. By adding just a few more e-transformations to the chain of 80 can not to resist the attack, but doubling the e-transformations to 160 times would be sufficient to counter the attack. However, such a modification would double the cost of the hardware and the number of the required gate[6].

In this paper, we will introduce a new e-transformation based on Latin cubes, and replace the four quasigroups employed in Edon80 by a Latin cube to design a new stream cipher named CHAIN80. The new stream cipher could remove the two weakness of Edon80 described as above. It can resist the key recover attack given by Johansson and Hell, and the average period of the key stream will be increased from 2^{102} to 2^{256}. The rest of this paper is organized as follows. In Section 2 we give a description of the mathematical definitions and theorems that CHAINS80 based on. Then we describe CHAINS80 from algorithmic point of view in Section 3. In Section 4 we discuss the security and the period of the keystream sequences of CHAINS80. Finally, we give the conclusion in Section 5.

II. PRELIMINARIES

A Latin square of order n is an $n\times n$ array on an n-set Q, such that each symbol in Q occurs exactly once in each 1-dimensional subarray. A Latin cube of order n is a 3-dimensional $n\times n\times n$ array on an n-set Q, such that each symbol in Q occurs exactly once in each 1-dimensional subarray. We shall call a 1-dimensional subarray where only the first coordinate changes a *fiber*, changing only the second coordinate gives us a *row*, and the third coordinate a *column*. It is easy to see that each fiber is a permutation of the set Q, and this also true for each row and each column. Keeping the first coordinate fixed gives us a layer. Fixing the second coordinate gives a slice and the third coordinate a floor. A layer thus contains rows and columns, a slice contains columns and fibers and a floor contains fibers and rows. It is easy to see that each layer is a Latin square on the set Q, and this also true for each slice and each floor.

Let L be a Latin cube on set Q with indices in Q, and denote $L(i,j,k)$ the element of L in position (i,j,k). Define a ternary operation β on Q:

$$\beta(x, y, z) = L(x, y, z), \qquad \forall x, y, z \in Q.$$

The pair (Q, β) is called a 3-quasigroup on set Q, and $|Q|$, the cardinal number of Q, is called the order of (Q, β).

A Latin cube defines a 3-quasigroup, and, it is easy to see, the multiplication table of a 3-quasigroup defines a Latin cube. Therefore the notions of a 3-quasigroup and a Latin cube will be freely interchanged in this paper.

Lemma 1. Let (Q, β) be a 3-quasigroup of order n, and x, y, z be variables. $\forall\ a, b, c \in Q$,

(1) each of the following equations, $\beta(x,a,b)=c$, $\beta(a,y,b)=c$ and $\beta(a,b,z)=c$, is uniquely resolvable in Q;

(2) each of the following equations, $\beta(x,y,a)=b$, $\beta(x,a,z)=b$ and $\beta(a,y,z)=b$ has n solutions in Q^2;

(3) the equation $\beta(x,y,z)=a$ has n^2 solutions $(x,y,z)\in Q^3$.

Proof: Statement (1) is true since each fiber, each row and each column is a permutation of Q.

For any given $x=x_0\in Q$, from (1) we know that the equation $\beta(x_0,y,a)=b$ has a unique solution in Q. So, $\beta(x,y,a)=b$ has $n=|Q|$ solutions in Q^2. Similarly, This is also true for the equations $\beta(x,a,z)=b$ and $\beta(a,y,z)=b$.

For any given $x=x_0\in Q$, from (ii) we know that the equation $\beta(x_0,y,z)=a$ has n solutions in Q^2, so, $\beta(x,y,z)=a$ has n^2 solutions in Q^3.

© 2015. The authors - Published by Atlantis Press

Definition 1. Let Q be a finite set and (Q, β) be a 3-quasigroup. Let Q^+ be the set of all nonempty words (i.e. finite strings) formed by the elements of Q. The elements of Q^+ will be denoted by $x_1x_2\ldots x_v$, where $x_i \in Q$ (i = 1, 2, …, v) and v is a positive integer. $\forall(\xi,\eta) \in Q^2$ be an ordered pair, we define a mapping $E_{\beta,(\xi,\eta)}$: $Q^+ \to Q^+$ as follows. $\forall\ x_1x_2\ldots x_v \in Q^+$,

$$E_{\beta,(\xi,\eta)}(x_1x_2\cdots x_v) = y_1y_2\cdots y_v,$$

where

$$\begin{cases} y_1 = \beta(\xi,\eta,x_1), \\ y_2 = \beta(\eta,y_1,x_2), \\ y_i = \beta(y_{i-2},y_{i-1},x_i), \quad i = 3,4,\cdots,v. \end{cases}$$

The mapping $E_{\beta,(\xi,\eta)}$ is called an e-transformation of Q^+ based the 3-quasigroup (Q, β) with leader pair (ξ,η).

III. Algorithmic Description of CHAINS80

A. Keystream Mode

CHAINS80 works in two modes: keysetup mode and keysteram mode. In order to better to present how CHAINS80 works, we will start the description of keysteram mode that is presented at the Table 1. In the first row of Table 1, we place a periodic (potentially infinite) string that has shape: 01230123…0123…. The next 80 rows in Table 1 describe 80 e-transformations of that string with leaders (ξ_i,η_i) $(0 \le i \le 79)$ obtained from IVSetup mode. The recurrence equations for these transformations are:

$$\begin{cases} a_{0,0} = \beta(\xi_0,\eta_0,0), \\ a_{0,1} = \beta(\eta_0,a_{0,0},1), \\ a_{0,j} = \beta(a_{0,j-2},a_{0,j-1},j(\bmod 4)), \ \ j \ge 2, \\ a_{i,0} = \beta(\xi_i,\eta_i,a_{i-1,0}), \qquad 1 \le i \le 79, \\ a_{i,1} = \beta(\eta_i,a_{i,0},a_{i-1,1}), \qquad 1 \le i \le 79, \\ a_{i,j} = \beta(a_{i,j-2},a_{i,j-1},a_{i-1,j}), \qquad 1 \le i \le 79,\ j \ge 2. \end{cases}$$

The output of the stream cipher is every second value of the last e-transformation i.e. the keystream can be described as:

$$\text{Keystream} = a_{79,1}a_{79,3}a_{79,5}\cdots a_{79,2k-1}, \quad k = 1,2,\cdots.$$

TABLE I. KEYSTREAM MODE OF CHAINS80

(ξ_i,η_i)	0	1	2	3	0	1	2	3	0	…
(ξ_0,η_0)	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$	$a_{0,8}$	…
(ξ_1,η_1)	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
(ξ_{79},η_{79})	$a_{79,0}$	$\boxed{a_{79,1}}$	$a_{79,2}$	$\boxed{a_{79,3}}$	$a_{79,4}$	$\boxed{a_{79,5}}$	$a_{79,6}$	$\boxed{a_{79,7}}$	$a_{79,8}$	…

B. IVSetup Mode

In this mode, Key as a vector of 80 bits is represented as a concatenation of 40 2-bit variables K_i, i.e. Key= $K_0K_1\ldots K_{39}$. In order to offering the working quasigroup to perform the e-transformations in keystream mode and IVSetup mode, we make assignment of a 3-quasigroup of order 4. It is known that there are 55296 Latin cubes of order 4, but not each of them is suitable for our purposes. By our investigations, we take the 3-quasigroup as shown in the Fig. 1, where F_i means floor i.

F_0	0	1	2	3
0	1	2	3	0
1	0	3	2	1
2	2	1	0	3
3	3	0	1	2

F_1	0	1	2	3
0	2	0	1	3
1	3	1	0	2
2	0	3	2	1
3	1	2	3	0

F_2	0	1	2	3
0	3	1	0	2
1	2	0	1	3
2	1	2	3	0
3	0	3	2	1

F_3	0	1	2	3
0	0	3	2	1
1	1	2	3	0
2	3	0	1	2
3	2	1	0	3

Fig. 1: The Latin cube used in CHAINS80

The nature of IVSetup mode in fact is that using the values of initial vector IV to compute the initial values of the internal states (ξ_i,η_i) $(0 \le i \le 79)$ (which would be used in keystream mode. Padding the initial vector IV of length 64 bits by 16 constant bits 1110010000011011 (represented as the string 32100123 of 2-bits), we will obtain a concatenation of 40 2-bit variables IV= $v_0v_1\ldots v_{31}32100123 = v_0v_1\ldots v_{39}$. We perform 80 e-transformations on IV as described in the following recurrence equations:

$$\begin{cases} t_{0,0} = \beta(K_0,v_0,K_0), \\ t_{0,1} = \beta(v_{39},t_{0,0},K_1), \\ t_{0,j} = \beta(t_{0,j-2},t_{0,j-1},K_{j(\bmod 40)}), \quad 2 \le j \le 39 \text{ or } 120 \le j \le 159, \\ t_{0,j} = \beta(t_{0,j-2},t_{0,j-1},v_{j(\bmod 40)}), \quad 40 \le j \le 119, \\ t_{i,0} = \beta(K_i,v_{39-i},t_{i-1,0}), \qquad 1 \le i \le 39, \\ t_{i,0} = \beta(K_{i(\bmod 40)},K_{79-i},t_{i-1,0}), \quad 40 \le i \le 79, \\ t_{i,1} = \beta(v_{39-i},t_{i,0},t_{i-1,1}), \qquad 1 \le i \le 39, \\ t_{i,1} = \beta(K_{79-i},t_{i,0},t_{i-1,1}), \qquad 40 \le i \le 79, \\ t_{i,j} = \beta(t_{i,j-2},t_{i,j-1},t_{i-1,j}), \qquad 1 \le j \le 79,\ 2 \le j \le 159. \end{cases}$$

After all 80 e-transformations are performed, the values of $(\xi_i,\eta_i) = (t_{79,i}, t_{79,i+80})$ $(0 \le i \le 79)$.

IV. Security of CHAINS80

The internal states (ξ_i,η_i) of CHAINS80 have a space of $4^{80}\times4^{80}=2^{320}$. However we know that the exhaustive search attack on the key=$K_0K_1\ldots K_{39}$ is 2^{80}. Thus the attack by searching the state space is obviously more worse than the exhaustive search attack. We will show that an exhaustive search attack on the key is the best attack on CHAINS80.

A. Security of IVSetup Mode

We consider that the attacker would jeopardize the security of the system, if the attacker can gain some knowledge about

the internal states of the cipher by knowing the initialization vector IV. According to the designation of CHAINS80, it is easy to see that the internal states are loaded into the registers (ξ_i, η_i) $(0 \le i \le 79)$ from the corresponding values of $t_{79,j}$ $(0 \le j \le 159)$ which depend on the 40 unknown variables $K_0K_1\ldots K_{39}$ in a highly nonlinear way., If the IV, i.e., $v_0v_1\ldots v_{39}$ were known to the attacker. However, there is not known methodology to solve such huge and complex system of equations based on 3-quasigroup, except the simple combinatorial approach by examining all the possibilities. There are $4^{40}=2^{80}$ possible choices of the key, and $4^{80}\times4^{80}=2^{320}$ possible assignments of the internal states (ξ_i, η_i) $(0 \le i \le 79)$. Therefore the best choice for an attacker is to guess the key.

From algebraic point of view, given the key $K_0K_1\ldots K_{39}$, IVSetup mode maps $(v_0,v_1,\ldots,v_{39})$ into $(\xi_0, \xi_1,\ldots, \xi_{79}, \eta_0, \eta_1,\ldots, \eta_{79})$. Thus IVSetup mode can be regarded as a function that maps $\{0,1\}^{64} \to \{0,1\}^{320}$. In addition, IVSetup mode acts as a one-way function, since it is computationally infeasible to find the value $(v_0,v_1,\ldots,v_{39})$ by given $(\xi_0, \xi_1,\ldots, \xi_{79}, \eta_0, \eta_1,\ldots, \eta_{79})$. So, the attacker cannot apply a chosen initial vector attack.

B. Security on Related Key Attack

Related key attack try to find two different keys which can produce the same keystream. CHAINS80 initializes (ξ_i, η_i) by the values of $(t_{79,i}, t_{79,i+80})$ $(0 \le i \le 79)$ obtained in the IVSetup mode where each bit of the Key is involved in a highly correlated and nonlinear way. In addition, since computation of the initial values for (ξ_i, η_i) $(0 \le i \le 79)$ are done by involvement of 64 bit vector of IV, the search for keys which produce a same keystream (related or unrelated) should be done in a space of $2^{80}\times2^{64}=2^{144}$ possibilities. By birthday paradox, finding a combination of the key and IV which could give the same keystream would take 2^{72} attempts. However, this kind of attack would only be possible when the collisions exist and they are easy to be find. Besides, IVSetup mode acts as a one-way and collision resistant function. So, CHAINS80 can resist the related key attack.

C. Security on Guess-and-Verify Attack

In this attack, after guessing some parts of the internal states of the CHAINS80, the intruder will try to predict the next bits outputted.

The essence of the design of CHAINS80 is that the output string from the $(i-1)$-th e-transformation determines which floor of the Latin cube to operate in the i-th e-transformation in order. In addition, the performance of the e-transformations is also related with the leader pairs (ξ_i, η_i) $(0 \le i \le 79)$. Thus, in order to try to predict the cipher outputted, the intruder has to at least know the string outputted from 79-th e-transformation, so, what is needed is having the assumption about the leader pair (ξ_{79}, η_{79}). The total number of guessing this situation is only 16, not very big. Similarly, for predicting the string outflowing from 79-th e-transformation $E_{\beta,(\xi_{79},\eta_{79})}$, the intruder has to at least know the input coming from 78-th e-transformation $E_{\beta,(\xi_{78},\eta_{78})}$. Therefore, in order to have a better prediction, the intruder has to be aware of the actual value of (ξ_{78}, η_{78}). This implies additional 16 guesses have to be made. And by this analogy, the total number of guesses that we have to make to achieve success of the guesses is rapidly increasing to a value of $16^{80} = 2^{320}$. So, the key exhaustive search attack is better than this attack.

D. Expected value of the period of CHAINS80

Let $Q=\{0,1,2,\ldots,n-1\}$, L be a Latin cube on Q and (Q, β) be the 3-quasigroup corresponding to L. For a fixed $z_0 \in Q$, define a mapping σ_{z_0} on Q^2 as follows:

$$\sigma_{z_0}(ij) = j\beta(i, j, z_0), \forall ij \in Q^2,$$

here we denote (i, j) by ij for short. From Lemma 1 we know that for fixed z_0 and j, $\beta(i, j, z_0)$ is uniquely determined by i. So, σ_{z_0} is a permutation on Q^2. We call σ_{z_0} a chain permutation of floor z_0 of L (or (Q, β)).

Example 1. Fig. 1 is a Latin cube on set $Q = \{0, 1, 2, 3\}$. Suppose (Q, β) is the 3-quasigroup defined by L. Then we have

$$\sigma_0 = \begin{pmatrix} 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 & 30 & 31 & 32 & 33 \\ 01 & 12 & 23 & 30 & 00 & 13 & 22 & 31 & 02 & 11 & 20 & 33 & 03 & 10 & 21 & 32 \end{pmatrix}$$

Every permutation can be written as disjoint cycles. A cycle of a chain permutation of layer z_0 of a 3-quasigroup (Q, β) can be written in a special shape $(i,j,\beta(i,j,z_0),\beta(j,\beta(i,j,z_0),z_0),\ldots)$, where $i, j \in Q$. e.g., the chain permutations of of layers 0, 1, 2, 3 of (Q, β) corresponding to the Latin cube in Fig. 1, denoted by σ_0, σ_1, σ_2 and σ_3, respectively, can be written as:

σ_0 = (00122023321131)(03),
σ_1 = (002132312)(01033)(1)(2),
σ_2 = (003223)(01102)(12)(133),
σ_3 = (0)(0130221)(0311232)(3),

where a cycle of length 1 (ii) is denoted by (i) for short.

Let R_i $(i=0,1,\ldots,79)$ denote the factor by which e-transformer $E_{\beta,(\xi_i,\eta_i)}$ increases the period in Table 1. Then R_i is random variable. Let $E^{(m)} = E_{\beta,(\xi_{m-1},\eta_{m-1})} \cdots E_{\beta,(\xi_1,\eta_1)} E_{\beta,(\xi_0,\eta_0)}$ We give 1000 performing of e-transformation $E^{(9)}$ with initial sequence 01230123… and have found the numerical values for the distributions of the random variables R_i, i = 0, 1,…, 9 and the expected values $E(R_i)$ shown in Table 2, and R_i converges a distribution shown in the following:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{8} & 0 \end{pmatrix}$$

TABLE II. THE DISTRIBUTION OF THE FIRST 10 RANDOM VARIABLES

i	The distribution of R_i																$E(R_i)$
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
0	$\frac{504}{1000}$	$\frac{496}{1000}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.496
1	$\frac{61}{1000}$	$\frac{319}{1000}$	$\frac{35}{1000}$	$\frac{255}{1000}$	0	$\frac{100}{1000}$	0	$\frac{147}{1000}$	0	0	$\frac{83}{1000}$	0	0	0	0	0	4.513
2	$\frac{67}{1000}$	$\frac{77}{1000}$	$\frac{47}{1000}$	$\frac{174}{1000}$	$\frac{21}{1000}$	$\frac{43}{1000}$	$\frac{45}{1000}$	$\frac{100}{1000}$	$\frac{16}{1000}$	$\frac{11}{1000}$	$\frac{6}{1000}$	$\frac{46}{1000}$	$\frac{123}{1000}$	$\frac{69}{1000}$	$\frac{155}{1000}$	0	8.298
3	$\frac{82}{1000}$	$\frac{58}{1000}$	$\frac{44}{1000}$	$\frac{43}{1000}$	$\frac{48}{1000}$	$\frac{94}{1000}$	$\frac{52}{1000}$	$\frac{92}{1000}$	$\frac{61}{1000}$	$\frac{41}{1000}$	$\frac{56}{1000}$	$\frac{49}{1000}$	$\frac{54}{1000}$	$\frac{60}{1000}$	$\frac{166}{1000}$	0	8.601
4	$\frac{78}{1000}$	$\frac{104}{1000}$	$\frac{58}{1000}$	$\frac{101}{1000}$	$\frac{49}{1000}$	$\frac{63}{1000}$	$\frac{47}{1000}$	$\frac{44}{1000}$	$\frac{66}{1000}$	$\frac{48}{1000}$	$\frac{47}{1000}$	$\frac{72}{1000}$	$\frac{23}{1000}$	$\frac{71}{1000}$	$\frac{129}{1000}$	0	7.851
5	$\frac{77}{1000}$	$\frac{62}{1000}$	$\frac{54}{1000}$	$\frac{71}{1000}$	$\frac{64}{1000}$	$\frac{35}{1000}$	$\frac{70}{1000}$	$\frac{49}{1000}$	$\frac{80}{1000}$	$\frac{61}{1000}$	$\frac{73}{1000}$	$\frac{60}{1000}$	$\frac{42}{1000}$	$\frac{42}{1000}$	$\frac{160}{1000}$	0	8.446
6	$\frac{67}{1000}$	$\frac{75}{1000}$	$\frac{63}{1000}$	$\frac{60}{1000}$	$\frac{73}{1000}$	$\frac{59}{1000}$	$\frac{65}{1000}$	$\frac{75}{1000}$	$\frac{47}{1000}$	$\frac{41}{1000}$	$\frac{61}{1000}$	$\frac{51}{1000}$	$\frac{74}{1000}$	$\frac{52}{1000}$	$\frac{137}{1000}$	0	8.281
7	$\frac{70}{1000}$	$\frac{63}{1000}$	$\frac{64}{1000}$	$\frac{56}{1000}$	$\frac{61}{1000}$	$\frac{60}{1000}$	$\frac{50}{1000}$	$\frac{63}{1000}$	$\frac{49}{1000}$	$\frac{61}{1000}$	$\frac{81}{1000}$	$\frac{55}{1000}$	$\frac{66}{1000}$	$\frac{81}{1000}$	$\frac{120}{1000}$	0	8.298
8	$\frac{67}{1000}$	$\frac{77}{1000}$	$\frac{47}{1000}$	$\frac{174}{1000}$	$\frac{21}{1000}$	$\frac{43}{1000}$	$\frac{45}{1000}$	$\frac{100}{1000}$	$\frac{16}{1000}$	$\frac{11}{1000}$	$\frac{6}{1000}$	$\frac{46}{1000}$	$\frac{123}{1000}$	$\frac{69}{1000}$	$\frac{155}{1000}$	0	8.525
9	$\frac{64}{1000}$	$\frac{51}{1000}$	$\frac{58}{1000}$	$\frac{61}{1000}$	$\frac{68}{1000}$	$\frac{66}{1000}$	$\frac{58}{1000}$	$\frac{61}{1000}$	$\frac{62}{1000}$	$\frac{62}{1000}$	$\frac{74}{1000}$	$\frac{70}{1000}$	$\frac{58}{1000}$	$\frac{55}{1000}$	$\frac{129}{1000}$	0	8.505

Denote $R^{(80)} = \prod_0^{79} R_i$ be the factor that $E^{(80)}$ increase the period of the initial sequence 01230123…, then the period of the keystream $4R^{(80)}$. Apply ln on $R^{(80)}$ we have

$$\ln R^{(80)} = \sum_0^{79} \ln R_i.$$

We assume that all R_i ($0 \le i \le 79$) has the same distribution, then the mean $\mu = E(\ln R_i) \approx 1.91296$ and the variance $\sigma^2 = Var(\ln R_i) \approx 0.577191$. Form Central Limit Theorem we know that $R^{(80)}$ converges in distribution to a Log-normal $N(80\times1.91296, 80\times0.577191)$:

$$f(x) = \frac{1}{x\sqrt{0.577191\times80\times2\pi}} \exp\left(-\frac{(\ln x - 1.91296\times80)^2}{2\times0.577191\times80}\right)$$

Tthe expected value of $R^{(80)}$ is

$$E(R^{(80)}) = \int_0^{\infty} xf(x) \approx 2^{254}$$

and the expected value of the period of the keystream is $4E(R^{(80)}) = 2^{256}$.

E. Security on the Key Recovery Attack

Johansson and Hell [6] use the analysis of the periods of the keystream sequences of Edon80 in [4] to mount an attack that can recover the key with complexity around 2^{72}. If we consider the restriction put by the designers, i.e., only 2^{48} keystream bits can be produced by each key/IV pair, then the total complexity is around 2^{69}. This is the most advanced attack on Edon80.

In this attack, we assume a known plaintext scenario, i.e. the adversary had obtained the keystream sequence. When suffering the key recovery attack, CHAINS80, compared with Edon80, has the advantages as follows: (1) In Edon80, the quasigroups used in the e-transformations are directly determined by the key K_0, K_1,…, K_{79}, i.e., if knowing which quasigroup is used in the i-th e-transformation, the adversary also knows K_i. However, as shown in Table 1, quasigroups (i.e., the 4 floors in the Latin cube) applied in each e-transformer of CHAINS80 changes over time. The quasigroup used in the i-th e-transformation is determined by the string coming from the (i-1)-th e-transformation, not by the i-th key. (2) Each e-transformer of Edon80 will increase the period of the input string by a factor of 1,2,3 or 4, and the prime factors of the period of the keystream are only 2 and 3. Thus, the period of the keystream is easy to guess. However, in CHAINS80, the period of the input string by a factor of 1 to 15, the period of the keystream is much larger and and the prime factors are 2,3,5,7,11 and 13. This makes it is difficult to guess the period of the keystream in the key recovery attack. Thus, CHAINS80 can be sufficient to resist the key recovery attack.

From the above discussion, the variety of quasigroups applied in the new e-transformations and the long-period of the keystream makes CHAINS80 can resist the key recovery attack given by Johansson and Hell in [6].

V. Conclusion

In this paper, by modifying IVSetup mode and keystream mode of Edon80, we introduced a new e-transformation based on Latin cubes, and replace the four quasigroups employed in Edon80 by a Latin cube to design a new stream cipher named CHAIN80. Compared with Edon80, the new stream cipher could remove the known weakness of Edon80. It can resist the key recover attack given by Johansson and Hell, and the average period of the key stream will be increased from 2^{102} to 2^{256}.

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. Gligoroski, S. Markovski, L. Kocarev, M. Gusev. Edon80, eSTREAM, ECRYPT Stream Cipher Project, Report 2005/007 (2005), http://www.ecrypt.eu.org/stream/papers.html.

[2] J. Hong. Period of streamcipher Edon80. In: Maitra, S., Madhavan, C.E.V., Venkatesan, R. (eds.) INDOCRYPT 2005. LNCS, vol. 3797, pp. 23–34. Springer, Heidelberg, 2005.

[3] D. Gligoroski, S. Markovski, L. Kocarev, M. Gusev. Understanding periods in edon80.eSTREAM, ECRYPT Stream Cipher Project, Report 2005/054 (2005), http://www.ecrypt.eu.org/stream.

[4] D. Gligoroski, S. Markovski, S.J. Knapskog. On periods of Edon-(2*m*, 2*k*) family of stream ciphers. The State of the Art of Stream Ciphers, Workshop Record, SASC 2006, Leuven, Belgium.

[5] Y. Xu. On the Key-stream Periods Probability of Edon80. Inscrypt 2013, LNCS 8567, pp. 56–69. Springer-Verlag, Berlin Heidelberg (2014).

[6] T. Johansson, M. Hell. A Key Recovery Attack on Edon80. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 568–581. Springer, Heidelberg, 2007.

[7] D. Gligoroski, S. Markovski, S.J. Knapskong. The Stream Cipher Edon80.In: Robshaw, M. and Billet, O. (Eds.): New Stream Cipher Designs, LNCS 4986, pp. 152–169. Springer-Verlag, Berlin Heidelberg (2008).