Modification of Edon80 to Resist the Key Recovery Attack

Xiaomei Wang, 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 core of the cipher consists of quasigroup string e-transformations and it employs four quasigroups of order 4. The internal structure of Edon80 is highly pipelined, making it scalable from the speed of processing point of view. The best attack on Edon80 is the key recovery attack given by Johansson and Hell. In this paper, we give a modification to the Keystream Mode of Edon80 to resist the key recovery attack, and the modification keep the high parallelizability of Edon80.**

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

I. INTRODUCTION

Edon80 is a hardware stream cipher submitted to the last phase of the eSTREAM project. It was designed by Gligoroski, Markovski, Kocarev, and Gusev and its original description is given in [1]. Kasper et. al shown in [2] that the implementation of Edon80 requires only 2922 gates and it offers good scalability.

Hong indicated in [3] that the period of the keystream sequence could be quite small with some small probability. This was further studied by the designers of Edon80 in [4, 5] and Xu in [6]. But this property could not be utilized in any kind of attack.

Johansson and Hell [7] use the analysis of the periods of the keystream of Edon80 in [5] 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 [8]. 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[7].

In this paper, we will give a modification to Edon80 without adding any e-transformation to resist the key recover attack given by Johansson and Hell. The paper is organized as follows: In Section 2, we give a brief description of the key stream generation in Edon80, in Section 3, we give a detail description of the key recovery attack by Johansson and Hell, in Section 4, we give the modification of Edon80 to resist the key recovery attack. Finally, in Section 5, we give a conclusion for this paper.

II. DESCRIPTION OF EDON80

A quasigroup is an ordered pair $(Q,*)$, where Q is a set and $*$ is a binary operation on Q, such that the equations

$$a*x=b \quad \text{and} \quad y*a=b$$

have uniquely solvable for every pair of elements a, b in Q. 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 (e.g., see [9]) 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.

Definition 1 (e-transformation) Let Q be an alphabet (i.e. a finite set) and 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 $a_1a_2\ldots a_k$, where $a_i \in Q$ (i = 1, 2, …, k). Let $*$ be a quasigroup operation on set Q, i.e. $(Q, *)$ is a quasigroup. For each $a \in Q$, we define a map $e_{a,*}$: $Q^+ \to Q^+$ as follows. $\forall$ $a_1a_2\ldots a_k, \in Q^+$,

$$e_{a,*}(a_1a_2\ldots a_k) = b_1b_2\ldots b_k,$$

where

$$\begin{cases} b_1 = a * a_1, \\ b_i = b_{i-1} * a_i, \quad i = 2,3,\cdots,k. \end{cases}$$

The map $e_{a,*}$ is called an *e-transformation* of Q^+ based on the operation $*$ with leader a.

A. IVSetup Mode of Edon80

Let Q ={0,1,2,3} and $(Q,\bullet_i)$ (i=0,1,2,3) are four quasigroups shown in Fig. 1.

Let $Key = K_0K_1\ldots K_{39}$ and $IV = v_0v_1\ldots v\_{31}32100123 = v_0v_1\ldots v\_{39}$ be two vectors of 80 bits is represented as a concatenation of 40 2-bit variables. Let

$$(Q,*_i) = \begin{cases} \left(Q,\bullet_{K_i}\right), & 0 \le i \le 39, \\ \left(Q,\bullet_{K_{i-40}}\right), & 40 \le i \le 79. \end{cases} \tag{1}$$

Then we perform 80 e-transformations on IV as described in the Table I. All of those transformations can be described by the following recurrence equations:

$$\begin{cases} t_{0,0} = v_{39} *_0 K_0, & \\ t_{0,j} = t_{0,j-1} *_0 K_j, & 1 \le j \le 39, \\ t_{0,j} = t_{0,j-1} *_0 v_{j-40}, & 40 \le j \le 79, \\ t_{i,0} = v_{39-i} *_i t_{i-1,0}, & 1 \le j \le 39, \\ t_{i,0} = K_{79-i} *_i t_{i-1,0}, & 40 \le j \le 79, \\ t_{i,j} = t_{i,j-1} *_i t_{i-1,j}, & 1 \le i \le 79, 1 \le j \le 79. \end{cases}$$

After all 80 e-transformations are performed, let $a_i = t_{79,i}$ (i = 0, 1, …, 79) be the leaders used in the following *Keystream* mode.

$\bullet_0$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

$\bullet_1$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

$\bullet_2$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

$\bullet_3$	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	3	2	1
3	2	1	0	3

Fig. 1: Quasigroups employed in Edon80

TABLE I. E-TRANSFORMATIONS OF EDON80 DURING IVSETUP MODE

$*_i$		K_0	K_1	…	K_{39}	v_0	v_1	…	v_{39}
$*_0$	v_{39}	$t_{0,0}$	$t_{0,1}$	…	$t_{0,39}$	$t_{0,40}$	$t_{0,41}$	…	$t_{0,79}$
$*_1$	v_{38}	$t_{1,0}$	$t_{1,1}$	…	$t_{1,39}$	$t_{1,40}$	$t_{1,41}$	…	$t_{1,79}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$*_{38}$	v_1	$t_{38,0}$	$t_{38,1}$	…	$t_{38,39}$	$t_{38,40}$	$t_{38,41}$	…	$t_{38,79}$
$*_{39}$	v_0	$t_{39,0}$	$t_{39,1}$	…	$t_{39,39}$	$t_{39,40}$	$t_{39,41}$	…	$t_{39,79}$
$*_{40}$	K_{39}	$t_{40,0}$	$t_{40,1}$	…	$t_{40,39}$	$t_{40,40}$	$t_{40,41}$	…	$t_{40,79}$
$*_{41}$	K_{38}	$t_{41,0}$	$t_{41,1}$	…	$t_{41,39}$	$t_{41,40}$	$t_{41,41}$	…	$t_{41,79}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$*_{78}$	K_1	$t_{78,0}$	$t_{78,1}$	…	$t_{78,39}$	$t_{78,40}$	$t_{78,41}$	…	$t_{78,79}$
$*_{79}$	K_0	$t_{79,0}$	$t_{79,1}$	…	$t_{79,39}$	$t_{79,40}$	$t_{79,41}$	…	$t_{79,79}$

B. Keystream Mode of Edon80

Let $a_i = t_{79,i}$ (i = 0, 1, …, 79) from *IVSetup* mode be leaders. Take a periodic (potentially infinite) string 0 1 2 3 0 1 2 3 … 0 1 2 3 … as an initial stream. Let the value in $*_i$ at time t be denoted $a_{i,t}$. Then the values are updated as

$$\begin{cases} a_{0,0} = a_0 *_0 0, & \\ a_{0,j} = a_{0,j-1} *_0 (j \bmod 4), & 1 \le j, \\ a_{i,0} = a_i *_i a_{i-1,0}, & 1 \le j \le 79, \\ a_{i,j} = a_{i,j-1} *_i a_{i-1,j}, & 1 \le i \le 79, 1 \le j. \end{cases}$$

Then perform 80 e-transformations as described in Table II. The output of the last e-transformation is

$$z_0 z_1 z_2 \cdots z_n \cdots = a_{79,0} a_{79,1} a_{79,2} \cdots a_{79,n} \cdots.$$

Chose every second value of $z_0 z_1 z_2 \cdots z_n \cdots$ as the key stream, i.e. the *Keystream* can be described as:

$$\begin{aligned} Keystream &= z_1 z_3 z_5 \cdots z_{2k-1} \cdots \\ &= a_{79,1} a_{79,3} a_{79,5} \cdots a_{79,2k-1} \cdots. \end{aligned}$$

The quasigroup operations $*_i$, i = 0, 1, …, 79 in Table II are the same that in Table I.

TABLE II. E-TRANSFORMATIONS OF EDON80 DURING THE KEYSTREAM MODE

$*_i$		0	1	2	3	0	1	2	3	0	…
$*_0$	a_0	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$	$a_{0,8}$	…
$*_1$	a_1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$*_{79}$	a_{79}	$a_{79,0}$	$\boxed{a_{79,1}}$	$a_{79,2}$	$\boxed{a_{79,3}}$	$a_{79,4}$	$\boxed{a_{79,5}}$	$a_{79,6}$	$\boxed{a_{79,7}}$	$a_{79,8}$	…

III. DESCRIPTION OF THE KEY RECOVERY ATTACK

The key recovery attack given by Johansson and Hell [7] assume a known plaintext scenario i.e., the adversary had obtained the keystream sequence $z_1 z_3 z_5 \cdots$. The main ideas of the attack come from the following properties of Edon80,

- The quasigroup (Q, $\bullet_j$) ($0 \le j \le 3$) used in the ith e-transformer, $*_i$ ($0 \le i \le 79$), is directly determined by the key as shown in Formula (1). If the adversary knows which quasigroup is used in the ith e-transformer, he also knows K_i.
- The prime factors of the period of the keystream are only 2 and 3, and for small i, the period of the string produced by the ith transformer can be expected with large probability.

Fig. 2 is a visualization of the key recovery attack by dealing the matrix $(a_{i,j})_{80\times(u+v+1)}$ from Table 2 ($0 \le i \le 79$, $t \le j \le t + u + v$). The jth column corresponds to a specific time instance j, and the ith row corresponds to $*_i$, the ith e-transformer. A restriction to the first B rows simply corresponds to an Edon instance with only the first B e-transformers.

Each value $a_{i,j}$ in the matrix $M=(a_{i,j})_{80\times(u+v+1)}$ is computed from its neighbours on the left and above. That is, $a_{i,j}$ will depend on all values $a_{s,t}$ for $s < i$ and $t < j$.

To set up the attack, select the first B rows in matrix M as the upper part, and the remaining rows as the lower part. Let

$$X = (x_1, x_2, \ldots, x_v),$$

$$Y = (y_1, y_2, \ldots, y_u),$$

and $v=|X|$, $u = |Y|$ be the lengths of X and Y respectively, where x_i, $y_j \in \{0, 1, 2, 3\}$, i=1, 2, …, v; j=1, 2, …, u, with the

values located as shown in Fig. 2. It is easy to see that B=79–u. As can be seen, the vector X=(x_1, x_2, …, x_v) is simply v symbols come from the chain of the first B e-transformers starting with some predetermined time. The vector Y = (y_1, y_2, …, y_u) can be characterized as the values needed to compute the internal state of the lower part of the matrix M.

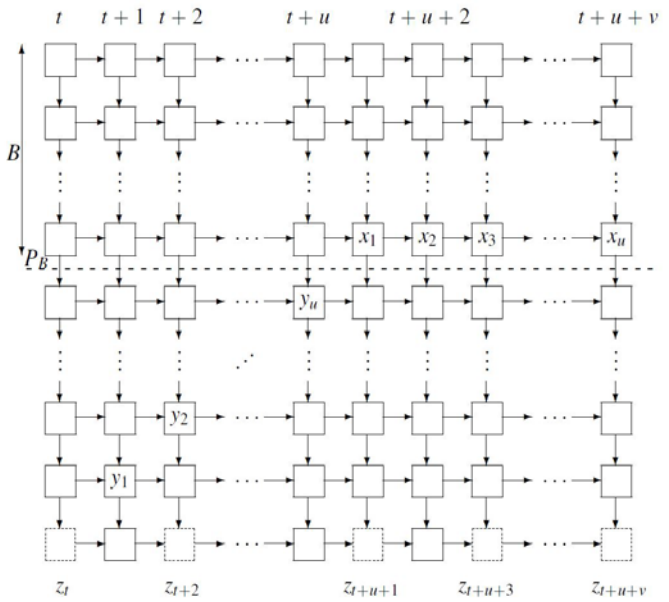

Fig. 2: Description of the ideas of the key recovery attack

Each quasigroup transformation will increase the period of the initial string by a factor of 1, 2, 3 or 4. Thus the period, denoted P_i, of the sequence produced by $*_i$ is given by

$$P_i = 2^{m_1} 3^{m_2}$$

for some positive integers m_1 and m_2. Then X = (x_1, x_2, …, x_v) is a segment in the Bth sequence with period P_B, and in the ith sequence produced by $*_i$ in Table II, the elements corresponding to time instance t and time instance $t + k\,P_B$, k = 0, 1, 2, … will have the same values for $i \le B$. Especially, which will be used in the following, the vector X = (x_1, x_2, …, x_v) will have the same value in every considered time instance t.

Suppose that for a moment the key bits used to determine the quasigroup operations in the lower part are known. Consider z_t, z_{t+2}, …, z_{t+u+1}, …, z_{t+u+v}, the (u+v)/2 key-stream symbols known to the adversary directly below X and Y in Fig.2, where u and v are odd positive integers. Using these known key-stream symbols, the number of possible combinations of X, Y will be reduced from 4(u+v) to approximately 2(u+v). Choose u and v such that $v > u$. This means not all X will be in the set of possible (X, Y) pairs. Then, the outcome of this part is a set Γ_k such that

$$\Gamma_k = \{X\text{: there exists } (X,Y) \text{ matching } z_{t+kP_B}, z_{t+kP_B+2}, \cdots, z_{t+kP_B+u+v}\}.$$

Combine this with the fact that the vector X=(x_1, x_2, …, x_v) at time instances t and $t + k\,P_B$ will be the same. This implies that X must occur in Γ_k for k = 0, 1, 2, … and hence in the intersection of them.

For each choice of Y = (y_1, y_2, …, y_u) used to define the key bits in the lower part, the sets Γ_k for k = 0, 1, 2, … are determined. Take $\Gamma = \cap \Gamma_k$ for Γ_k obtained so far, and continue until Γ is empty. If eventually $\Gamma = \emptyset$, the chosen value of the key bits is discarded. On the other hand, if at the end there is only one vector X in Γ, then we assume that we have found the correct key bits: $*_{79-u}$, $*_{79-u+1}$, …, $*_{79}$ can be determined by

$$(X, Y, z_{t+kP_B}, z_{t+kP_B+2}, \cdots, z_{t+kP_B+u+v}),$$

and K_{39-u}, K_{39-u+1}, …, K_{39} can be determined by $*_{79-u}$, $*_{79-u+1}$, …, $*_{79}$ and Formula (1) in Section 2.

The number of key bits that are guessed in this attack is 2u+2 and the complexity is about

$$2^{4u+d+3} \cdot \frac{u+d}{d},$$

where $d = v - u$.

There is a balance between the required length u+1 of the keystream and computational complexity. Consider a proper u and $\alpha_{P_B'}^{-1}$ times repeat of the attacks. The complexity of the computation

$$T = \alpha_{P_B'}^{-1} \cdot 2^{4u+d+3} \cdot \frac{u+d}{d} \tag{2}$$

where $\alpha_{P_B'}$ is the probability that $P_B \mid P_B'$, the reader can refer to [7] for detail.

After recovering 2(u+1) key bits we can either reconstruct the sequence after B e-transformers and apply the same attack again, now with much less complexity; or simply do an exhaustive key search on the remaining key bits.

The trade-off parameters in the attack are u and d. chose u = 13 and d = 4 gives about 2^{69} for both computational complexity and total amount of keystream. This concludes the key recover attack on Edon80.

IV. Modification of Edon80 to Resist the Key Recovery Attack

In this section, we described a modification to Edon80 to resist the above key recovery attack. The first property that the above key recovery attack based on is that the quasigroup (Q, $\bullet_j$) ($0 \le j \le 3$) used in e-transformer $*_i$ ($0 \le i \le 79$) is completely determined by the key. We will modify the Keystream Mode of Edon80 to remove this property.

Let Q ={0, 1, 2, 3}, (Q, $\bullet_i$) (i = 0, 1, 2, 3), Key = $K_0K_1\ldots K_{39}$ and IV = $v_0v_1\ldots v\_{31}32100123$ = $v_0v_1\ldots v\_{39}$. as shown in Section 2. (a_0, a_1, …, a_{79}) = ($t_{79,0}$, $t_{79,1}$, …, $t_{79,79}$) are get from Table I, the IVSetup Mode. We change the quasigroup operations in Table II, described in Formula (1), as follows

$$(Q, \otimes_i) = \begin{cases} (Q, \bullet_{K_i + a_{79-i} \bmod 4}), & 0 \le i \le 39, \\ (Q, \bullet_{K_{i-40} + a_{79-i} \bmod 4}), & 40 \le i \le 79. \end{cases} \tag{3}$$

i.e., modify the 80 e-transformations of Edon80 as described in Table III.

TABLE III. MODIFIED KEYSTREAM MODE OF EDON80

$\otimes_i$		0	1	2	3	0	1	2	3	0	…
$\otimes_0$	a_0	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$	$a_{0,8}$	…
$\otimes_1$	a_1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$\otimes_{79}$	a_{79}	$a_{79,0}$	$\boxed{a_{79,1}}$	$a_{79,2}$	$\boxed{a_{79,3}}$	$a_{79,4}$	$\boxed{a_{79,5}}$	$a_{79,6}$	$\boxed{a_{79,7}}$	$a_{79,8}$	…

On other parts of Edon80, the KeySetup Mode, *IV*Setup Mode, etc, keep unchanged.

From the description of the key recovery attack in Section 3 we know that the adversary can use the key recovery attack to get $K_{39-u}+a_u$, $K_{39-u+1}+a_{u-1}$, …, $K_{39}+a_0$ (mod 4) in Formula (3) with a computational complexity T in Formula (2). If $u \geq 30$ then $T > 2^{120}$. So, we suppose $u < 30$ in the key recovery attack.

To compute a piece of key, K_{39-u}, K_{39-u+1}, …, K_{39-u+k}, ($k \geq 0$), the adversary need to know a_u, a_{u-1}, …, a_{u-k}. By using a similar method as shown in Fig. 2 and the known $X = (x_1, x_2, \ldots, x_v)$, the adversary can get $X = (x_{2,v}, x_{3,v}, \ldots, x_{v,v})$ with a computational complexity 2^{2v-2} as shown in Fig. 3, where $x_{i,v}$ is in the string produced by $\otimes_{79-u+i}$ (i=2,3,…,v) in Table III. a_i (i=0,1,…,79) repeat at the end of each period of the string produced by $\otimes_i$, if

$$(x_{v-k,v}, x_{v-k+1,v}, \ldots, x_{v,v}) = (a_u, a_{u-1}, \ldots, a_{u-k})$$

happened, then the adversary got a piece of key: K_{39-u}, K_{39-u+1}, …, K_{39-u+k}. This implies that $u+v \geq 79-u+k$. The computational complexity of the key recovery attack, T in Formula (2), will be $2^{2(u+v)} = 2^{178-2u+2k} > 2^{118+2k}$.

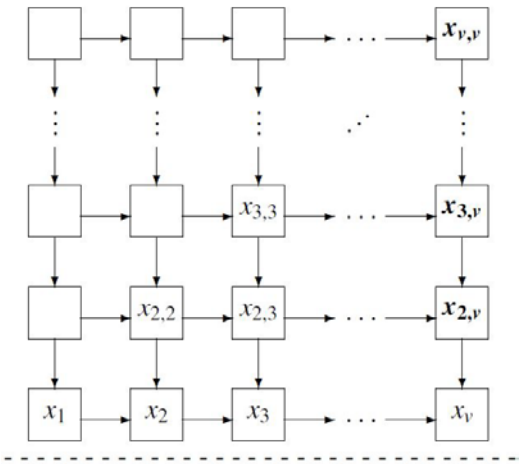

Fig. 3: Visualization of guessing (a_u, a_{u-1}, …, a_{u-k}).

The key space of Edon80 is $4^{40}=2^{80}$. An exhaustive key search need to compute the key and IV which consisting of 160 cycles, and then 80 cycles to get a_1, a_2, …, a_{79} in Table II. Each cycle need to compute 80 quasigroup operations. So an implementation of the software need $240 \cdot 80 \approx 2^{14}$ quasigroup operations to test one key. So, the computational complexity of exhaustive key search of Edon80 (and the modified Edon80) is about 2^{94}. The exhaustive key search would be much faster than the key recovery attack if we modify the Keystream Mode of Edon80 as shown in Formula (3) and Table III.

V. CONCLUSION

The key recovery attack can recover part of the key of Edon80 with computational complexity about 2^{69}. If we modify the Keystream Mode of Edon80 as shown in Section 4, the quasigroups $(Q, \bullet_j)$ ($0 \leq j \leq 3$) used in e-transformer $\otimes_i$ ($0 \leq i \leq 79$) will not be completely determined by the key, $K_0K_1\ldots K_{39}$, and then the computation of the key recovery attack will be more complex than exhaustive key search. So, the modification of the Keystream Mode of Edon80 can resist the key recovery attack given by Johansson and Hell [7].

Edon80 is highly parallelizable, making it scalable from the speed of processing point of view. The modification of the Keystream Mode in Section 4 does not cause any change to the parallelizability of Edon80.

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] M. Kasper, S. Kumar, K. Lemke-Rust, C. Paar. A compact implementation of Edon80. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/057 (2006), http://www.ecrypt.eu.org/stream.

[3] 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.

[4] 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.

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

[6] Y. Xu. On the Key-stream Periods Probability of Edon80. In: Liu, D., Xu, S., Yung, M. (Eds.): Information Security and Cryptology, Pre-Proceedings of The 9th International Confrence, pp. 50–64, Guangzhou, China, 2013.

[7] 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.

[8] 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).

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