Non associative algebraic system in cryptology
Protection against "meet in the middle" attack

József Dénes
1122. Budapest, Csaba u. 10.

Tamás Dénes
1182. Budapest, Marosvásárhely u. 13/a.

1. Basic notions

In general the cryptology is based on fields which are commutative and associative. There is a method which studies the evolution of differences during encryption of pairs of plaintexts, and derives the most likely keys from a pool of many pairs. It is called differential cryptanalysis. Differential cryptanalysis can also be used to find collisions in "hash" functions. For DES (Data Encryption Standard) like cryptosystems the differences are usually in terms of exclusive or of the intermediate data in the pair. Differential cryptanalysis might apply "meet in the middle attack" (introduced in [2]).

Definition 1.1.

***Meet in the Middle Attack*: An attack in which the evolution of the data is studied from both directions: from the plaintext forwards towards an intermediate round and from the ciphertext backwards towards the same intermediate round. If the results at the intermediate round are not the same in both directions, then the tested value of the key is not the real value. If both results are the same in several encryptions, then the tested value of the key is the real value with high probability.**

Details in cryptography one can learn e.g. [14].
The latin squares are the tools for generalizations of finite field (see [6]).

Definition 1.2.

A finite set J on which two binary operations are defined (+) and (•) such J is a loop with respect to the operation (+) with identity element 0 say, J\0 is a group with respect to the operation (•) and for which the distributive laws a(b+c)=ab+ac and (b+c)a=ba+ca (a,b,c $\in$ J) hold, is called a *neofield*.

A neofield is not necessarily commutative or associative. Neofield can be applied in cryptology (see [6]). Neofields were first introduced by L.J.Paige in 1949. In [3] the applications of algebraic systems without associativity and commutativity has been predicted to apply in the future.
The number of latin squares without associativity and commutativity is much larger than group tables (see e.g. [1]).
The cryptosystems based on quasigroups are as follows:
equipment of hardware encryption (patent [8] theoretical construction [4],[7]), hash function (see [5]), transposition cipher (see [10]), Hamming distences (see [11]).
A cipher system based on neofield (see [6]).
In the remaining part of the this paper we shall mention an algorithm of zero knowledge proof based on latin squares.

2. Zero Knowledge Protocol

The classical method of authenticating a person by means of a machine is the use of a password (PIN number). There are many problems involved with the improper use of passwords. More sophisticated than simple passwords the challenge-and-response protocol.
It's hard to believe, but procedures exist that enable user A to convince user B that he knows a secret without giving B the faintest idea of what the secret is.
Such procedures are naturally enough called *zero knowledge protocols.*

Jean-Jacques Quisquater and Louis Guillou explain zero-knowledge with a story about a cave (see [13]). The cave, illustrated in Figure 1. has a secret.

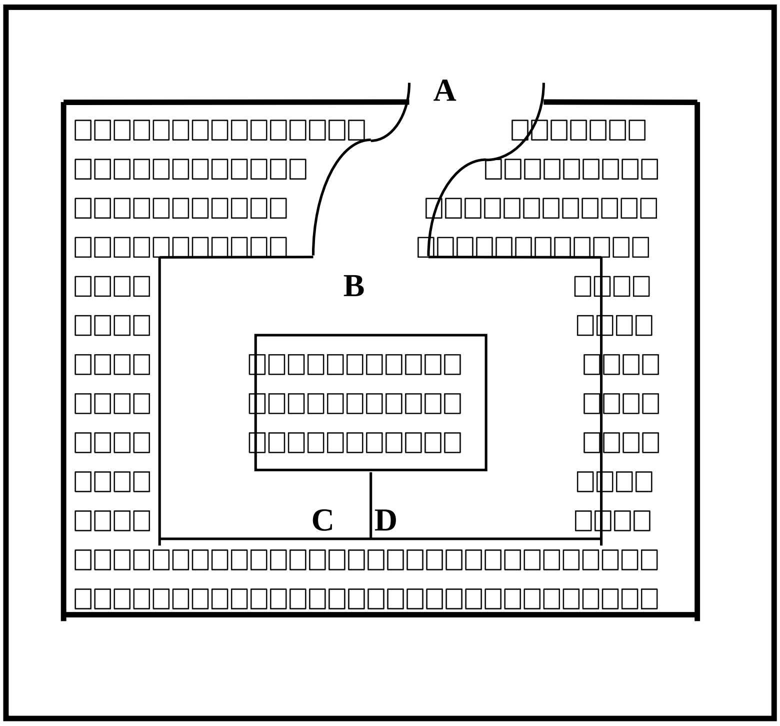


Figure 1.

Someone who knows the magic words can open the secret door between C and D. To everyone else, both passages lead to dead ends.
Peggy knows the secret of the cave. She wants to prove her knowledge to Victor, but she doesn't want to reveal the magic words. Here's how she convinces him:

(1) Victor stands at point A.
(2) Peggy walks all the way into the cave, either to point C or point D.
(3) After Peggy has disappeared into the cave, Victor walks to point B.
(4) Victor shouts to Peggy, asking her either to:
(a) come out of the left passage or
(b) come out of the right passage.
(5) Peggy complies, using the magic words to open the secret door if she has to.
(6) Peggy and Victor repeat steps (1) through (5) *n* times.

3. DD Algorithm

Assume the users $(u_1, u_2, ..., u_k)$ form a network.
u_i **has public-key $L_{u_i}, L^`_{u_i}$ (denote two isotopic latin squares at order *n*) and secret-key $I_{u_i}$ (denotes the isotopism of $L_{u_i}$ upon $L^`_{u_i}$).**
u_i **wants to proove identity for u_j but he doesn't want to reveal the secret-key (zero-knowledge proof).**

1. u_i **randomly permutes L_{u_i} to produce another latin square H.**
2. u_i **sends H to u_j.**
3. u_j **asks u_i either to:**
   a. prove that H and $L^`_{u_i}$ are isotopic,
   b. prove that H and L_{u_i} are isotopic.
4. u_i **complies. He either**
   a. prove that H and $L^`_{u_i}$ are isotopic,
   b. prove that H and L_{u_i} are isotopic.
5. u_i **and u_j repeat steps 1. through 4. *n* times.**

One of the present authors gave a lecture on DD Algorithm in 1996 at USC (Los Angeles), Prof L. Welch made a comment.
Prof L. Welch said that the security of the scheme varying on latin squares which used as a public-keys. Strongest so called pan-Hamiltonian latin squares. Pan-Hamiltonian latin squares are introduced by J. Wanless (see [15]).

Definition 3.1.

A latin square L at order *n* is a *pan-Hamiltonian* if every row cycle of L has length *n*.

Pan-Hamiltonian squares have applications besides the cryptography in the combinatorics. These squares have no proper subrectangles.
Pan-Hamiltonian latin squares has been called a C-type latin squares (see [7]). When *n* is not prime, a C-type nxn latin square cannot be a group table. For all $n \geq 7$, there exists a C-type latin square of order *n* that is not group table (see [7]).
Infinitely many values of *p* prime ($p \geq 11$ and $p \equiv 2 \bmod 3$) there exists a C-type latin square of order *p* which cannot based on a group (see [7]).

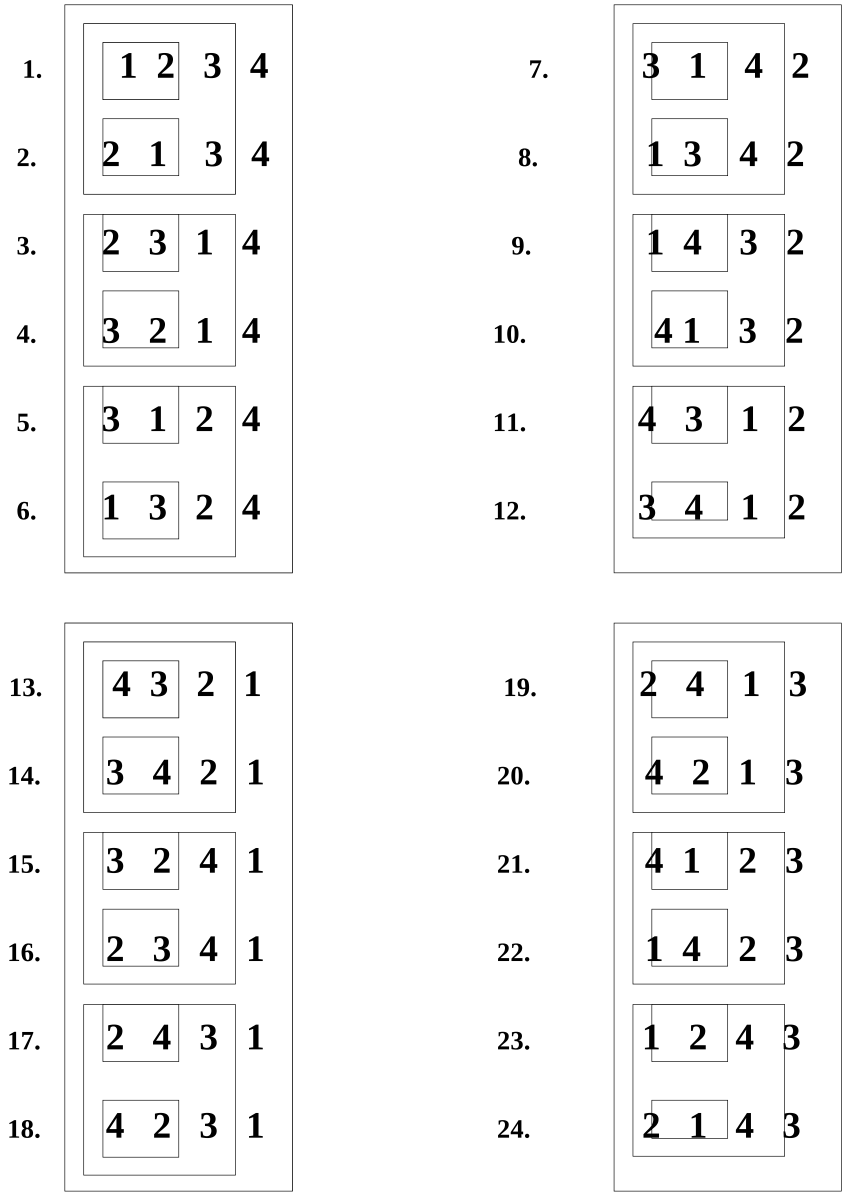
In [12] gave what is believed to be the first published example of a symmetric *11x11* latin square (see Figure 2.) which, although not cyclic, has the property that the permutation between any two rows is an 11-cycle. In [12] there was proved how this *11x11* latin square can be obtained by a general construction for *nxn* latin square where *n* is prime with $n \geq 11$**.**

$$
\mathbf{L=}\begin{array}{ccccccccccc}
0^{*} & 1^{*} & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\
1^{*} & 6^{*} & 3 & 5 & 9 & 10 & 0 & 2 & 8 & 4 & 7 \\
2 & 3 & 1 & 6 & 10 & 7 & 9 & 0 & 4 & 5 & 8 \\
4 & 5 & 6 & 2 & 1^{*} & 9 & 3 & 7 & 0^{*} & 8 & 10 \\
8 & 9 & 10 & 1 & 4 & 2 & 7 & 6 & 3 & 0 & 5 \\
5 & 10 & 7 & 9 & 2^{*} & 8 & 4 & 3 & 1^{*} & 6 & 0 \\
10 & 0 & 9 & 3 & 7 & 4 & 5 & 8 & 6 & 2 & 1 \\
9 & 2 & 0 & 7 & 6 & 3 & 8 & 10 & 5 & 1 & 4 \\
7 & 8 & 4 & 0 & 3 & 1 & 6 & 5 & 9 & 10 & 2 \\
3 & 4 & 5 & 8 & 0 & 6 & 2 & 1 & 10 & 7 & 9 \\
6 & 7 & 8 & 10 & 5 & 0 & 1 & 4 & 2 & 9 & 3
\end{array}
$$

Figure 2.

One of the present authors introduced an algorithm in [9]. (This algorithm has been called DT algorithm.) The DT algorithm lexicography listed all elements of the symmetric group of degree *n* (S_n**)** $(\pi_1, \pi_2, ..., \pi_{n!} \in S_n)$**.**

DT algorithm can be demonstrated (n=4) in Figure 3.



1. 1 2 3 4
2. 2 1 3 4
3. 2 3 1 4
4. 3 2 1 4
5. 3 1 2 4
6. 1 3 2 4
7. 3 1 4 2
8. 1 3 4 2
9. 1 4 3 2
10. 4 1 3 2
11. 4 3 1 2
12. 3 4 1 2
13. 4 3 2 1
14. 3 4 2 1
15. 3 2 4 1
16. 2 3 4 1
17. 2 4 3 1
18. 4 2 3 1
19. 2 4 1 3
20. 4 2 1 3
21. 4 1 2 3
22. 1 4 2 3
23. 1 2 4 3
24. 2 1 4 3

Figure 3.

The correspondence one to one the permutations of degree *n* and natural numbers *1* to *n!* . DT algorithm has the property for arbitrary natural number $1 \le m \le (n-1)!$ **there corresponds a single subset of** S_n **containing *n* permutations, which are the rows of a latin square of order *n* (see (1)). These latin squares (denote** $DL_m(n)$**) uniquely determines the row permutations as follows:**

(1) $$\mathrm{DL}_m(n) = \begin{bmatrix} \pi_m \\ \pi_{(n-1)!+m} \\ \pi_{2(n-1)!+m} \\ . \\ . \\ . \\ \pi_{(n-1)(n-1)!+m} \end{bmatrix} \qquad 1 \le m \le (n-1)! \qquad \pi_i \in S_n$$

A subset of latin squares of order *n* ($\mathrm{DL}_m(n)$) will defined by two parameters *(n,m)*. Consequently to store or transmission of the latin square is not neccesarily the original matrix. Simirarly to this property is really applicable to zero-knowledge-proof in the cryptography.

The Wilson theorem:
If *p* is prime number, then

(3) $(p-1)!+1 \equiv 0 \mod p$ **holds.**

Applying the Wilson theorem to the DT algorithm (see (9)), then we have the next theorem:

Theorem 1.

If *p* is prime number, then the $\mathrm{DL}_m(p)$ are pan-Hamiltonian squares.

Examples:

***n* is a prime: *n*=5 and *m*=1**

(4) $$\mathrm{DL}_1(5) = \begin{bmatrix} \pi_1 \\ \pi_{25} \\ \pi_{49} \\ \pi_{73} \\ \pi_{97} \end{bmatrix} = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \\ 4 & 5 & 2 & 3 & 1 \\ 5 & 3 & 4 & 1 & 2 \\ 3 & 1 & 5 & 2 & 4 \end{matrix}$$

***n*=5 but the latin square is not $\mathrm{DL}_m(n)$ type:**

$$\textbf{(5)} \qquad \mathrm{L}(5) = \begin{bmatrix} \pi_1 \\ \pi_{43} \\ \pi_{67} \\ \pi_{88} \\ \pi_{114} \end{bmatrix} = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \\ 5 & 3 & 4 & 2 & 1 \\ 3 & 4 & 1 & 5 & 2 \\ 2 & 1 & 5 & 3 & 4 \end{matrix}$$

$$\pi_{43} = \begin{pmatrix} 14 \\ 41 \end{pmatrix}\begin{pmatrix} 235 \\ 523 \end{pmatrix} \qquad \pi_{67} = \begin{pmatrix} 15 \\ 51 \end{pmatrix}\begin{pmatrix} 234 \\ 342 \end{pmatrix} \qquad \pi_{88} = \begin{pmatrix} 13 \\ 31 \end{pmatrix}\begin{pmatrix} 245 \\ 452 \end{pmatrix} \qquad \pi_{114} = \begin{pmatrix} 12 \\ 21 \end{pmatrix}\begin{pmatrix} 345 \\ 534 \end{pmatrix}$$

From the point of view of cryptology the $\mathrm{DL}_m(n)$ type latin squares have a further property that is stronger than the pan-Hamiltonian squares: Every pair of $\mathrm{DL}_m(n)$ rows (and columns, its number =$\begin{pmatrix} n \\ 2 \end{pmatrix}$) is a cycle of length *n* (see [9]).

References

**[1] R.E. Cawagas: Generation of NAFIL loops of small order
Quasigroups and Related Systems, 7 (2000) 1-5**

**[2] David Chaum, Jan-Hendrik Evertse: Cryptanalysis of DES with a reduced number of rounds, Sequences of linear factors in block ciphers
Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of CRYPTO'85, pp. 192-211, Springer 1985.**

[3] J. Dénes: Some thoughts on the decryption possibilities at encryption messages (in Hungarian), Híradástechnika 2001/7. 21-26

**[4] J. Dénes: On latin squares and digital encrypting communication system
To appear in P.U.M.A**

[5] J. Dénes, A.D. Keedwell: A new authentication scheme based on latin squares
Discrete Math., 106/107 (1992) 157-161.

[6] J. Dénes, A.D. Keedwell: Some applications of non associative algebraic system
in cryptology
To appear in P.U.M.A.

[7] J. Dénes, P.J. Owens: Some new latin power sets not based on groups
J.Comb. Theory, Ser. A.85 (1999) 69-82

[8] Dénes József, Petroczki Péter: Digitális titkosító kommunikációs rendszer
(A Digital Encrypting Communication System)
Hungarian patent No. 201437 A

[9] Dénes Tamás: Algorithm to the generation of all permutations of degree *n*
(in Hungarian), Információ Elektronika 1975/1-2.

[10] T. Dénes: Cardano and the Cryptography
Mathematics of the enciphering grill
(in Hungarian), Középiskolai Matematikai és Fizikai Lapok, 2001/6. 325-335

[11] A. Drapal: Hamming distances of groups and quasigroups
Discrete Math. 235 (2001) 189-197

[12] P.J. Owens, D.A. Preece: Some new non-cyclic latin squares that have cyclic and
Youden properties
Ars Combinatorica 44(1996) 137-148

[13] J.-J. Quisquater and L.C. Guillou, "De Procédés d'Authentification Basés sur une
Publication de Problémes Complexes et
Personnalisés dont les Solutions Maintenues
Secrétes Constituent autant d'Accréditations
Proceedings of SECURI-COM '89:
7th Worldwide Congress on Computer and
Communications Security and Protection,
Société d'Édition et d'Organisation d'Expositions
Professionnelles, 1989, pp. 149-158. (in French)

[14] G.J. Simmons (Ed.): Contemporary Cryptology
IEEE Press, New York, 1992.

[15] J. Wanless: Perfect factorisations of bipartite graphs and latin squares without
proper subrectangles.
The Electronic Journal of Combinatorics 6(1999)#R9