A survey of Latin squares, orthogonal arrays and their applications to cryptography

Luca Mariot[1,2]

[1] Dipartimento di Informatica, Sistemistica e Comunicazione (DISCo)
Università degli Studi Milano - Bicocca

[2] Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis (I3S)
Université Nice Sophia Antipolis

luca.mariot@disco.unimib.it

Insalate di Matematica – June 28, 2016

Part 1: Introduction to Latin squares and orthogonal arrays

Latin Squares

Definition

A *Latin square* of order N is a $N \times N$ matrix L such that every row and every column are permutations of $[N] = \{1, \cdots, N\}$

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

Latin Squares: Existence and Construction

- Question: Does there exist a Latin square for all orders $N \in \mathbb{N}$?
- Yes: just set the first row to $1, 2, \cdots, N$ and build the next ones by cyclic shifts:

$$\sigma(x_1, x_2, \cdots, x_{N-1}, x_N) = (x_2, x_3, \cdots, x_N, x_1)$$

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Orthogonal Latin Squares

Definition

Two Latin squares L_1 and L_2 of order N are *orthogonal* if their superposition yields all the pairs $(x, y) \in [N] \times [N]$.

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

(a) L_1

1	4	2	3
3	2	4	1
4	1	3	2
2	3	4	1

(b) L_2

1,1	3,4	4,2	2,3
4,3	2,2	1,4	3,1
2,4	4,1	3,3	1,2
3,2	1,3	2,1	4,4

(c) (L_1, L_2)

Orthogonal Latin Squares: Existence

- Question: Are there orthogonal Latin squares for all $N \in \mathbb{N}$?
- No: for $N = 2$ we have only two Latin squares, and they are not orthogonal:

1	2
2	1

2	1
1	2

1,2	2,1
2,1	1,2

- What about other orders?

Euler's 36 Officers Problem (1/2)

« *A very curious question, which has exercised for some time the ingenuity of many people, has involved me in the following studies, which seem to open a new field of analysis, in particular the study of combinations. The question revolves around arranging 36 officers to be drawn from 6 different ranks and also from 6 different regiments so that they are ranged in a square so that in each line (both horizontal and vertical) there are 6 officers of different ranks and different regiments.* »

L. Euler, *Sur une nouvelle espèce de quarrés magiques*, 1782

Euler's 36 Officers Problem (2/2)

Euler did not find any solution, and set forth the following:

Conjecture

Let $N = 4k + 2$, for $k \in \mathbb{N}$. Then, there are no orthogonal Latin squares of order N.

In 1900, Gaston Tarry proved (by exhaustive search!) Euler's conjecture for $k = 1$, showing the unsolvability of the 36 officers problem

Disproof of Euler's Conjecture

In 1960, Bose, Shrikhande and Parker found counterexamples to Euler's conjecture for all $k \geq 2$

Major Mathematical Conjecture Propounded 177 Years Ago Is Disproved

The New York Times

Discussing their solution to problem, from left: Dr. E. T. Parker, Prof. S. S. Shrikhande and Prof. R. C. Bose

By JOHN A. OSMUNDSEN

Another major mathematical problem—this one 177 years old—has been solved. Its solution was reported at the 557th meeting of the American Mathematical Association, which ended at the New Yorker Hotel yesterday. It was the second such achievement to come out of the meeting, something attending mathematicians called "extremely rare." The solution to the first problem, known as Frobenius' conjecture, was reported by Prof. John G. Thompson, a 26-year-old mathematician from De-Paul University in Chicago. It dealt with so-called "group theory" and had puzzled mathematicians for more than fifty years. The second problem had resisted attempts at solution ever since Leonhard Euler (pronounced "oiler") stated it in a memoir in 1782. It became famous as Euler's conjecture. The three mathematicians who finally cracked the problem are now known among their colleagues as

Continued on Page 42, Column 1

Existence of Orthogonal Latin Squares

- In 1922, MacNeish gave a construction for all $N \not\equiv 2 \mod 4$
- The existence question of orthogonal Latin squares can be summarised as:

Theorem

Let $N \neq 2, 6$. Then, there exist orthogonal Latin squares of order N

Mutually Orthogonal Latin Squares (MOLS)

- A set of s pairwise orthogonal Latin squares is denoted as s-MOLS
- For all $N \in \mathbb{N}$, we have that $s \leq N-1$.

Theorem

Let $N = q = p^e$, where p is prime and $e \in \mathbb{N}$. Then, there exist $(N-1)$-MOLS

Construction. For all $\alpha \in \mathbb{F}_q \setminus \{0\}$, define the Latin square L_α as:

$$L_\alpha(i,j) = i + \alpha j, \text{ for all } i,j \in \mathbb{F}_q$$

- **Open problem**: What is the maximum number of MOLS for non-prime powers orders?

Orthogonal Arrays

Definition

An orthogonal array $OA(k,N)$ is a $N^2 \times k$ matrix where each entry is an element from $[N] = \{1, \cdots, N\}$, and such that by fixing any two columns $1 \leq i,j \leq k$, one gets all the possible pairs in $[N] \times [N]$

1	1	1	1
1	2	2	2
1	3	3	3
2	1	2	3
2	2	3	1
2	3	1	2
3	1	3	2
3	2	1	3
3	3	2	1

Equivalence between OA and MOLS

Theorem

A set of k-MOLS of order N is equivalent to an $OA(k+2, N)$

Construction ($\Rightarrow$). Given k-MOLS $L_1, \cdots L_k$, build a $N^2 \times k+2$ array as:

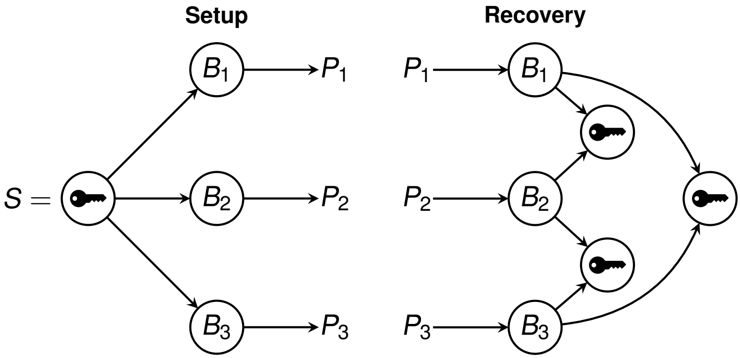
- Fill the first two columns with all pairs of $[N] \times [N]$ in lexicographic order
- For $1 \leq i \leq k$, fill column $i+2$ with L_i read from top left to bottom right

Part 2: Cryptographic applications of Latin squares and orthogonal arrays

Secret Sharing Schemes (SSS)

- Secret sharing scheme: a procedure enabling a dealer to share a secret S among a set $\mathcal{P}$ of n players
- (k, n) threshold schemes: at least k players out of n are required to recover S [Shamir79].

Example: $(2, 3)$–scheme



Applications of SSS

- Corporate digital signatures
- Key recovery systems
- Example: DNSSEC root key shared with a (5,7)–scheme

NewScientist

Home News In-Depth Articles Blogs Opinion TV Galleries Topic Guides Last Word Subscribe

SPACE TECH ENVIRONMENT HEALTH LIFE PHYSICS&MATH SCIENCE IN SOCIE

Short Sharp Science

Cutting-edge science, cut up

Not-so-secret seven hold keys to the internet

15:30 27 July 2010

Science In Society Technology

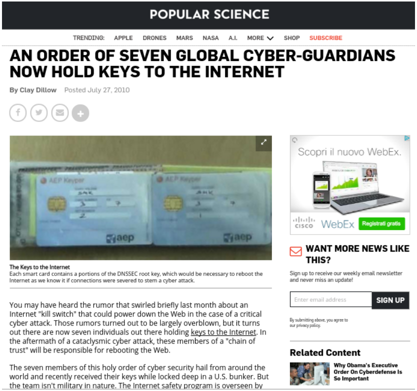
Gareth Morgan, technology editor

It's like something out of a Templar's mystical ritual: seven key holders are each assigned to guard a part of a key, and in times of great crisis, five of them must come together for the key's power to be unleashed and save the day. But this is no fantasy tale; it's the latest attempt to safeguard the internet.

The plan was drawn up by the internet domain name watchdog ICANN as a means to protect the internet in the event of a major attack on its infrastructure. The complete key can be used to reboot the systems at the heart of the internet which direct users to the genuine websites.

The BBC reports that UK-based business man Paul Kane is one of the key holders. He was given a smartcard which contains part of the root key needed to initiate the reboot, and plans to store that in a tamper-proof bag in a secure deposit box.

Other key holders include US-based security researcher Dan Kaminsky, who has previously uncovered flaws in the internet directory Domain Name System (DNS).



POPULAR SCIENCE

TRENDING: APPLE DRONES MARS NASA A.I. MORE SHOP SUBSCRIBE

AN ORDER OF SEVEN GLOBAL CYBER-GUARDIANS NOW HOLD KEYS TO THE INTERNET

By Clay Dillow Posted July 27, 2010

The Keys to the Internet
Each smart card contains a portions of the DNSSEC root key, which would be necessary to reboot the Internet as we know it if connections were severed to stem a cyber attack.

You may have heard the rumor that swirled briefly last month about an Internet "kill switch" that could power down the Web in the case of a critical cyber attack. Those rumors turned out to be largely overblown, but it turns out there are now seven individuals out there holding keys to the Internet. In the aftermath of a cataclysmic cyber attack, these members of a "chain of trust" will be responsible for rebooting the Web.

The seven members of this holy order of cyber security hail from around the world and recently received their keys while locked deep in a U.S. bunker. But the team isn't military in nature. The Internet safety program is overseen by

Related Content

Why Obama's Executive Order On Cyberdefense Is So Important

$(2, n)$-Schemes through n-MOLS

Setup Phase

1. The dealer D chooses a row $S \in \{1, \cdots, N\}$ as the secret

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

$(2, n)$-Schemes through n-MOLS

Setup Phase

1. The dealer D chooses a row $S \in \{1, \cdots, N\}$ as the secret

	1	2	3	4
	4	3	2	1
$\rightarrow$	2	1	4	3
	3	4	1	2

	1	2	3	4
	3	4	1	2
$\rightarrow$	4	3	2	1
	2	1	4	3

	1	2	3	4
	2	1	4	3
$\rightarrow$	3	4	1	2
	4	3	2	1

Example: $(2, 3)$-scheme, $S = 3$

Setup Phase

2. D randomly selects a column $j \in \{1, \cdots, N\}$

$$
\begin{array}{c|c|c|c|c|}
 & & \downarrow & & \\
\hline
 & 1 & 2 & 3 & 4 \\
\hline
 & 4 & 3 & 2 & 1 \\
\hline
\rightarrow & 2 & 1 & 4 & 3 \\
\hline
 & 3 & 4 & 1 & 2 \\
\hline
\end{array}
\quad
\begin{array}{c|c|c|c|c|}
 & & \downarrow & & \\
\hline
 & 1 & 2 & 3 & 4 \\
\hline
 & 3 & 4 & 1 & 2 \\
\hline
\rightarrow & 4 & 3 & 2 & 1 \\
\hline
 & 2 & 1 & 4 & 3 \\
\hline
\end{array}
\quad
\begin{array}{c|c|c|c|c|}
 & & \downarrow & & \\
\hline
 & 1 & 2 & 3 & 4 \\
\hline
 & 2 & 1 & 4 & 3 \\
\hline
\rightarrow & 3 & 4 & 1 & 2 \\
\hline
 & 4 & 3 & 2 & 1 \\
\hline
\end{array}
$$

Example: $S = 3$, $j \leftarrow 2$

$(2,n)$-Schemes through n-MOLS

Setup Phase

3. The value of $L_i(S,j)$ for $i \in [N]$ is the share of P_i

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2,3)$-scheme, $S = 3$, $j \leftarrow 2$, $B_1 = 1$, $B_2 = 3$, $B_3 = 4$

$(2, n)$-Schemes through n-MOLS

Recovery Phase

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2,3)$-scheme, $B_1 = 1$, $B_2 = 3 \Rightarrow (3,2)$

Recovery Phase

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

→

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

→

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2, 3)$-scheme, $B_2 = 3$, $B_3 = 4 \Rightarrow (3, 2)$

$(2, n)$-Schemes through n-MOLS

Recovery Phase

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2,3)$-scheme, $B_1 = 1$, $B_3 = 4 \Rightarrow (3,2)$

Security

5. Knowledge of a single B_i leaves S completely undetermined

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2, 3)$-scheme, $B_1 = 1$, $\Rightarrow$ $S =???$

$(2, n)$-Schemes through n-MOLS

Security

5. Knowledge of a single B_i leaves S completely undetermined

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2, 3)$-scheme, $B_2 = 3$, $\Rightarrow$ $S =$???

Security

5. Knowledge of a single B_i leaves S completely undetermined

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2, 3)$-scheme, $B_3 = 4$, $\Rightarrow$ $S =$???

Part 3: Orthogonal Latin squares through Cellular Automata

One-Dimensional Cellular Automata (CA)

Definition

One-dimensional CA: quadruple $\langle A, n, r, f \rangle$ where A is the finite set of states, $n \in \mathbb{N}$ is the number of cells on a one-dimensional array, $r \in \mathbb{N}$ is the radius and $f : A^{2r+1} \to A$ is the local rule.

Example: $A = \{0,1\}, n = 8$, $r = 1$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)

$$\cdots \boxed{0}\underbrace{\boxed{1}\boxed{1}\boxed{0}}\boxed{0} \cdots$$

$$\downarrow f(1,1,0) = 1 \oplus 1 \oplus 0$$

$$\boxed{0}$$

$$\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}$$

Parallel update $\Downarrow$ Global rule F

$$\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{0}$$

Remark: No boundary conditions $\Rightarrow$ The array "shrinks"

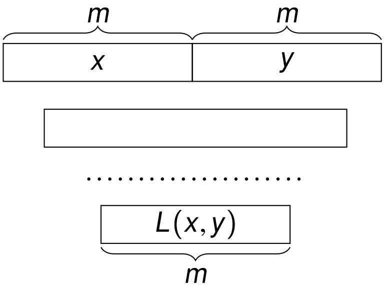
Latin Squares through Bipermutive CA (1/2)

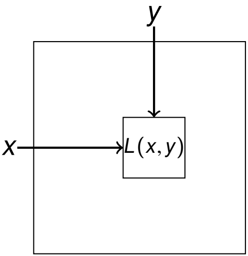
- Idea: determine which CA induce orthogonal Latin squares
- Bipermutive CA: local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ is defined as

$$f(x_1, \cdots, x_{2r+1}) = x_1 \oplus g(x_2, \cdots, x_{2r}) \oplus x_{2r+1}$$

Lemma

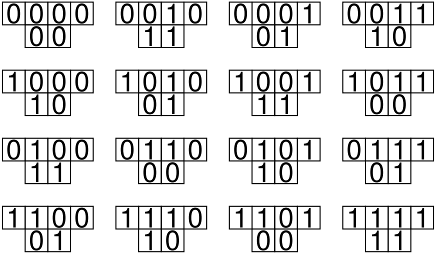
Let $\langle \mathbb{F}_q, 2m, r, f \rangle$ be a bipermutive CA with $2r | m$. Then, the CA generates a Latin square of order $N = 2^m$





Latin Squares through Bipermutive CA (2/2)

- Example: CA $\langle \mathbb{F}_2, 4, 1, f \rangle$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)
- Encoding: $00 \mapsto 1, 10 \mapsto 2, 01 \mapsto 3, 11 \mapsto 4$



(a) Rule 150 on 4 bits

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(b) Latin square L_{150}

Linear CA

- Local rule: linear combination of the neighborhood cells

$$f(x_1, \cdots, x_{2r+1}) = a_1 x_1 \oplus \cdots \oplus a_{2r+1} x_{2r+1} \quad , \; a_i \in \mathbb{F}_q$$

- Associated polynomial:

$$f \mapsto \varphi(X) = a_1 + a_2 X + \cdots + a_{2r+1} X^{2r}$$

- Global rule: $m \times (m+2r)$ $2r$-diagonal transition matrix

$$M_F = \begin{pmatrix} a_1 & \cdots & a_{2r+1} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_{2r+1} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_{2r+1} \end{pmatrix}$$

$$x = (x_1, \cdots, x_n) \mapsto M_F x^\top$$

Orthogonal Latin Squares by Linear CA

Theorem

Let $F = \langle \mathbb{F}_q, 2m, r, f \rangle$ and $G = \langle \mathbb{F}_q, 2m, r, g \rangle$, be linear CA. The Latin squares induced by F and G are orthogonal if and only if $P_f(X)$ and $P_g(X)$ are coprime

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(a) Rule 150

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

(b) Rule 90

1,1	4,2	3,3	2,4
2,2	3,1	4,4	1,3
4,3	1,4	2,1	3,2
3,4	2,3	1,2	4,1

(c) Superposition

Figure : $P_{150}(X) = 1 + X + X^2$, $P_{90}(X) = 1 + X^2$ (coprime)

Proof (idea)

The two Latin squares are orthogonal iff the following Sylvester matrix is invertible:

$$M = \begin{pmatrix} M_{\mathcal{F}} \\ M_{\mathcal{G}} \end{pmatrix} = \begin{pmatrix} a_1 & \cdots & a_{2r+1} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_{2r+1} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_{2r+1} \\ b_1 & \cdots & b_{2r+1} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & b_1 & \cdots & b_{2r+1} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_1 & \cdots & b_{2r+1} \end{pmatrix}$$

- Resultant of f, g: $Res(f,g) = det(M)$
- $Res(f,g) \neq 0 \Leftrightarrow gcd(f,g) = 1$

Open problems

Problem 1: Count (and build) pairs of coprime polynomials of degree n over $\mathbb{F}_q$:

- $(q-1)$-to-1 correspondence when $a_1 \in \mathbb{F}_q$ [Benjamin07], but for bipermutive CA we need $a_1 \neq 0$!
- Experiments on $q = 2$ relate to the OEIS A002450 sequence:

$$a(n) = 0, 1, 5, 21, 85, \ldots \Rightarrow a(n) = \frac{4^n - 1}{3}$$

Problem 2: Extend the construction to *orthogonal Latin hypercubes*

- First step: find under which conditions bipermutive CA generate Latin hypercubes

References

- [Benjamin07] Benjamin, A., Bennett, C.: The probability of relatively prime polynomials. AMS Mathematics Magazine 80(3):196–202 (2007)
- [Mariot14] Mariot, L., Leporati, A.: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Proceedings of ACRI 2014. LNCS vol. 8751, pp. 417–426. Springer (2014)
- [Shamir79] Shamir, A.: How to share a secret. Commun. ACM 22(11):612–613 (1979)
- [Stinson04] Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer (2004)