Families of Block Ciphers from Combinatorial Designs

Dimitris E. Simos
(joint work with C. Koukouvinos, NTUA, Greece)

Project-Team SECRET
INRIA Paris-Rocquencourt

April 6, 2012
Cryptography and its Applications in the Armed Forces
Hellenic Military Academy "Evelpidon"
Vari, Attiki, Greece

Acknowledgements

- **Thanks** to Prof. Daras for the invitation and organization of the colloquium
- **Hellenic Military Academy "Evelpidon"** for the hospitality
- **INRIA** for financial support

Outline of the Talk

1. Private-Key Cryptosystems
   - Motivation
   - Cryptographic Algorithms
   - Encryption Schemes

Outline of the Talk

1. Private-Key Cryptosystems
   - Motivation
   - Cryptographic Algorithms
   - Encryption Schemes

2. Cryptanalysis
   - Brute-Force Attacks
   - Attack Models

Applications of Combinatorial Designs

1. Coding Theory where they give error-correcting codes that correct the maximum number of errors. A Hadamard code (equivalent to a first-order Reed Muller code) was used during the 1971 Mariner 9 mission to correct the error in picture transmission.
2. Telecommunications where they generate sequences used in digital communications.
3. Optics for the improvement of the quality and resolution of image scanners.
4. Cryptography for Military Science where they generate private-key cryptosystems resistent to most common cryptographic attacks. **(this talk)**

Motivation

- The algorithms for encryption and decryption (in Combinatorial Designs) are of reasonable length
- Exploit the mathematical structure of the designs to harvest cryptographic design principles

Motivation

- The algorithms for encryption and decryption (in Combinatorial Designs) are of reasonable length
- Exploit the mathematical structure of the designs to harvest cryptographic design principles

Similarities

- Hill cipher, i.e. using the incidence matrix of a combinatorial design for encryption and decryption
- Block ciphers, i.e. Blowfish, 3DES

Motivation

- The algorithms for encryption and decryption (in Combinatorial Designs) are of reasonable length
- Exploit the mathematical structure of the designs to harvest cryptographic design principles

Similarities

- Hill cipher, i.e. using the incidence matrix of a combinatorial design for encryption and decryption
- Block ciphers, i.e. Blowfish, 3DES

Design Goals

1. Require the key be shared only once
2. Use a relatively small key size
3. Computationally fast
4. Resistance to cryptographic attacks

Hadamard Matrices

Definition

A square $n \times n$ matrix H with elements ± 1 that satisfies $HH^T = nI_n$ is called a Hadamard matrix of order n

- Notation: H_n

Necessary Condition for the Existence of an H_n

The order of a Hadamard matrix is 1, 2, or $n \equiv (0 \mod 4)$

Hadamard Matrices

Definition

A square $n \times n$ matrix H with elements ± 1 that satisfies $HH^T = nI_n$ is called a Hadamard matrix of order n

- Notation: H_n

Necessary Condition for the Existence of an H_n

The order of a Hadamard matrix is 1, 2, or $n \equiv (0 \mod 4)$

Equivalence of Hadamard Matrices

Two Hadamard matrices are equivalent if one can be transformed into the other by a series of row or column:

- permutations
- negations

Plotkin arrays

Generalization of Hadamard matrices

Consider the entries of an H_n replaced with "symbolic" variables preserving the orthogonality property

Plotkin array of Order 8 and Type $(1,1,1,1,1,1,1,1)$

- $$P = \begin{pmatrix} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{pmatrix}$$
- $PP^T = fI_8$ whereas $f = A^2 + B^2 + \ldots + H^2$

Encryption Algorithm

Design of the Algorithm

1. Message: Assume a plaintext (msg) with n letters represented by a vector of length n (i.e. ASCII code)
2. Encryption Matrix: A of order $n \times n$, with entries $\{\pm 1\}$ where the matrix A satisfies $AA^T = kI_n$ for some constant $k \in \mathbb{N}$

Algorithm 1 Encryption Algorithm

function $\textsc{EncrAlg}(msg)$
Require: msg in ASCII code ▷ Encode a sample plaintext, msg
 $\textsc{Select}(A, d)$ ▷ Choose appropriate A and d
 $k \leftarrow (A, d)$ ▷ Form private key k
 $\textsc{Transmit}(k)$ ▷ Transmit securely the private key
 $\bar{m} \leftarrow \textsc{Convert}(msg)$ ▷ Convert original msg
 $\bar{c} \leftarrow \bar{m}A + d\bar{e}_n$ ▷ Encrypted msg is $\bar{c}$
 return $(\textsc{Transmit}(\bar{c}))$
end function

Decryption Algorithm

Theorem (Koukouvinos and Simos, 2011)

The encrypted message $\bar{c}$ which is transmitted with respect to the encryption algorithm is decrypted uniquely as $\bar{w} = 1/k(\bar{c} - d\bar{e}_n)A^T$ and $\bar{w} \equiv \bar{m}$.

Algorithm 2 Decryption Algorithm

---

function $\textsc{DecrAlg}(\bar{c})$
Require: given ciphertext $\bar{c}$ ▷ Decode a given ciphertext
  $\textsc{Receive}(A, d)$ ▷ Receive the securely transmitted private key
  $k \leftarrow (A, d)$ ▷ Set private key k
  $\bar{m} \leftarrow 1/k(\bar{c} - d\bar{e}_n)A^T$ ▷ Decrypt ciphertext $\bar{c}$
  $msg \leftarrow \textsc{Convert}(\bar{m})$ ▷ Original plaintext is msg
  return (msg)
end function

Encryption Scheme

Definition (Boyd and Mathuria, 2003)

An encryption scheme consists of three sets; a key set K, a message set M, and a ciphertext set C together with the following three algorithms.

1. A key generation algorithm
2. An encryption algorithm
3. A decryption function

Encryption Scheme

Definition (Boyd and Mathuria, 2003)

An encryption scheme consists of three sets; a key set K, a message set M, and a ciphertext set C together with the following three algorithms.

1. A key generation algorithm
2. An encryption algorithm
3. A decryption function

Private Key

- The pair (A, d)
- We can refer to the private key using only the encryption matrix A since d is of size $\mathcal{O}(1)$

Hadamard Cipher (Koukouvinos and Simos, 2011)

- Encryption matrix: The transpose of an Hadamard matrix of order n, H_n^T
- Key k: The Hadamard matrix, H_n, which consists of $n \times n$ bits
- Size of the key: $\mathcal{O}(n^2)$
- Encryption-Decryption: valid using the presented algorithms since $H_n H_n^T = nI_n$ (For any selection of two distinct row/columns of a Hadamard matrix the inner product of the row/columns is zero)

HADAMARD CIPHER (Koukouvinos and Simos, 2011)

- Encryption matrix: The transpose of an Hadamard matrix of order n, H_n^T
- Key k: The Hadamard matrix, H_n, which consists of $n \times n$ bits
- Size of the key: $\mathcal{O}(n^2)$
- Encryption-Decryption: valid using the presented algorithms since $H_n H_n^T = nI_n$ (For any selection of two distinct row/columns of a Hadamard matrix the inner product of the row/columns is zero)

Properties of the HADAMARD CIPHER

- Private-key (symmetric) block cipher
- The use of two inequivalent Hadamard matrices will result in two different ciphertexts

Hadamard matrices with one Circulant Core

1. A Hadamard matrix of order $n = p + 1$ which can be written as

$$\begin{array}{c|c} 1 & 1 \cdots 1 \\ \hline 1 & \\ \vdots & C \\ 1 & \end{array} \quad \text{or} \quad \begin{array}{c|c} 1 & \\ \vdots & C \\ 1 & \\ \hline 1 & -1 \cdots -1 \end{array}$$

   where $C = (c_{ij})$ is a circulant matrix of order p, is said to have one circulant core

2. Existence: Infinite families i.e. Paley, (1933) Stanton, Sprott and Whiteman, (1958, 1962) Marshall Hall Jr., (1956)

Hadamard Core Cipher

- Key k: The binary vector $A_c = [a_1, a_2, \ldots, a_p]$ which denotes the first row of the circulant matrix C and consist of of p bits
- Size of the key: $\mathcal{O}(n)$, since it consists of $p = n - 1$ bits
- Encryption-Decryption: as before using the Hadamard matrix $n = p + 1$ as an encryption matrix

Plotkin Cipher (Koukouvinos and Simos, AMIS, 2011)

- Encryption: Divide a message m of arbitrary length into blocks $m_1, \ldots, m_q$ of length 4 (padding the last block with zeros if necessary)
- Randomness: Random vectors $g_1, \ldots, g_q$ of length 4 are constructed using pseudorandom generators
- Encryption matrix: The Plotkin array of order 8 and type $(1, 1, 1, 1, 1, 1, 1, 1)$, denoted by P, where $PP^T = (A^2 + B^2 + \ldots + H^2)I_8$
- Encryption process: The matrix P is applied successively to $m_i \oplus g_i$
- Ciphertext: $c = P(m_1 \oplus g_1) \oplus \ldots \oplus P(m_q \oplus g_q)$
- Decryption: Divide c into blocks $c_1, \ldots, c_q$ of size 8 and compute $P^T c_i / f$
- Key k: The chosen entries $A, B, \ldots, H$ of P; (integer numbers)

Kronecker Hadamard Core Cipher

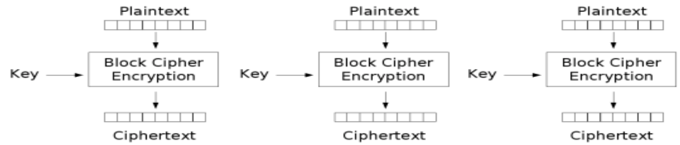
- Encryption matrix: The Kronecker product $\otimes_{i=1}^{k} H_i = H_1 \otimes H_2 \otimes \ldots \otimes H_k$ of H_i Hadamard matrices with one circulant core of orders n_i for $i = 1, \ldots, k$
- Key k: The concatenation $\oplus_{i=1}^{k} A_{c_i}$ of private keys $A_{c_i} = [a_{1_i}, a_{2_i}, \ldots, a_{p_i}]$, which consist of $\sum_{i=1}^{k} p_i$ bits
- Size of the encryption matrix: $\mathcal{O}(n^k)$, $n = \max_i\{n_i\}$, $\prod_{i=1}^{k} n_i \leq \prod_{i=1}^{k} n = n^k$
- Size of the key: $\mathcal{O}(n)$, $\sum_{i=1}^{k}(n_i - 1) \leq \sum_{i=1}^{k}(n) - k = k(n-1)$
- Approximation of a k-round Feistel cipher (DES, 3DES, Blowfish, FEAL, LOKI97)

Kronecker Plotkin Ciphers

- Analogue constructions
- The Kronecker product of orthogonal matrices is an orthogonal matrix

Electronic Codebook Mode (ECB)

- Repetition of the encryption process when the plaintext has more than n letters
- Disadvantage of ECB: If two plaintext blocks are the same, then the corresponding ciphertext blocks will be identical, and that is visible to the attacker
- Solution I: Choose A_i, $i = 1, \ldots, k$ to be $A_f \neq A_g$ for $i \leq f, g \leq k$ with $f \neq g$ for Kronecker based ciphers
- Solution II: Choose A_i encryption matrices of orders $\sum_{i=1}^{k} n_i = n$, where n is the size of the plaintext; Then the encryption process does not result in any repetition blocks



Electronic Codebook (ECB) mode encryption

Encryption with Hadamard Ciphers in Practice

Encrypting a Message with ECB Mode

1. C = ENCRYPT('HMAHMA',16) "Encrypt with H_{16}"
2. C = kaia?gcakaia?gca "Identical ciphertext blocks"
3. C = ENCRYPT('HMAHMA',24) "Encrypt with H_{24}"
4. C = ftaberhzia?wsteinbdarsfa "No repetition blocks"

Diffusion Principle in Block Ciphers

- If one bit of the plaintext is changed, then the ciphertext should change in 2 to 5 bits in an "unpredictable" manner
- Strict Avalanche Criterion (Webster and Tavares, 1985)

Diffusion in Hadamard Ciphers

1. C_1 = ENCRYPT('**1**000 0001',8) $\Rightarrow$ C_1 = 1**1**00 1**1**00
2. C_2 = ENCRYPT('**0**000 0001',8) $\Rightarrow$ C_2 = 1**0**00 1**0**00
3. HAMMINGDISTANCE(C_1, C_2) = 2

Frequency Analysis

- Simulation of a brute-force attack method
- Calculate frequency of occurences of every ASCII symbol

The Simulation Procedure

1. Used a sample plaintext of 23 characters
2. Encoded the plaintext by approximating the entry size for the Plotkin arrays and approximate size of the noise vector
3. Used Plotkin arrays of orders $4, 4, 8$ to compute the encryption matrix of order $128 (= 4 \cdot 4 \cdot 8)$ in Kronecker Plotkin cipher
4. Decoded the ciphertext using every key combination of key entry value equal to ± 1
5. Converted the decoded ciphertext to ASCII values and counted the frequency of each value that appears in the resulting combinations

Experimental Results (Koukouvinos and Simos, AMIS, 2011)

1. A brute force attack is not a feasible way of defeating the cipher
2. A brute force attack does not result in all possible plaintext messages (in contrast to OTP)
3. The size of the entries of the noise vector played a significant role in the decryption process

key size	noise size	ASCII $0-25$	values $26-50$	occurrences $51-75$	$\times$ $76-100$	10^5 $101-127$
10-14	128	25	5	5	7	8
10-14	1024	10	12	8	6	14
30-34	128	120	30	40	30	50
30-34	1024	65	90	45	50	40
50-54	128	310	50	70	30	40
50-54	1024	110	100	90	80	120

Key Length Recommendation

Kronecker Plotkin cipher is considered secure using a key of 128 bits

Known-Plaintext Attack

A known-plaintext attack is one where the adversary has a quantity of plaintext and corresponding ciphertext

(1) We need to recover the i-th column of the $n \times n$ encryption matrix $A = H_n$ or $A = P$, $A(i) = (a_{1,i},\ a_{2,i},\ \ldots,\ a_{n,i})$, without knowing the private key by solving the following n-linear systems, for $i = 1,\ \ldots,\ n$:

$$\begin{array}{rcl} m_1^1 a_{1,i} + m_2^1 a_{2,i} + \cdots + m_n^1 a_{n,i} & = & c_i^1 \\ m_1^2 a_{1,i} + m_2^2 a_{2,i} + \cdots + m_n^2 a_{n,i} & = & c_i^2 \\ \vdots & & \vdots \\ m_1^n a_{1,i} + m_2^n a_{2,i} + \cdots + m_n^n a_{n,i} & = & c_i^n \end{array}$$

(2) Denote the previous system as $MA(i) = C(i)$, where $C(i) = (c_i^1,\ c_i^2,\ \ldots,\ c_i^n)$

Result of the Cryptanalysis: Partial Secure

- Hadamard & Plotkin Ciphers are secure against known-plaintext attacks under the assumption that the adversary has knowledge of less than n messages of length n of the plaintext and the corresponding ciphertext
- One can find the encryption matrix A, if the matrix M is not singular

Chosen-Plaintext Attack

A chosen-plaintext attack is one where the adversary chooses plaintext and is then given the corresponding ciphertext

- Extra advantage of the adversary: knowledge of the encryption mechanism
- Breaking the system: solve n linear systems, $MA(i) = C(i)$ for $i = 1, \ldots, n$
- Outcome: No further information is revealed with respect to a known-plaintext attack

Chosen-Plaintext Attack

A chosen-plaintext attack is one where the adversary chooses plaintext and is then given the corresponding ciphertext

- Extra advantage of the adversary: knowledge of the encryption mechanism
- Breaking the system: solve n linear systems, $MA(i) = C(i)$ for $i = 1, \ldots, n$
- Outcome: No further information is revealed with respect to a known-plaintext attack

Result of the Cryptanalysis: Partial Secure

Hadamard and Plotkin ciphers are secure against chosen-plaintext attacks, since the ciphers are secure against known-plaintext attacks

How Secure is n in Practice?

- For a plaintext of $n = 64$ bits an attacker which can deduce $64 = 2^6$ messages of the same length can break the ciphers
- Totally impractical!

Solution

1. Kronecker Hadamard and Plotkin ciphers
2. Use 16 rounds of encryption; 16 Hadamard matrices or Plotkin arrays of order 16
3. Size of encryption matrix is $2^{4^{16}} = 2^{64}$; key is $16 \cdot 15 = 240$ bits

Comparison with the Security of DES

1. To break DES differential cryptanalysis requires 2^{47} chosen plaintexts (Bilham and Shamir, 1980)
2. Linear cryptanalysis needs 2^{43} known plaintexts to achieve similar results (Matsui, 1993)

Ciphertext-only Attack

A ciphertext-only attack is one where the adversary tries to deduce the decryption key or plaintext by only observing ciphertext

- Any value of the encrypted message is a function of n values of the plaintext and one column of the encryption matrix A
- Two or more same values of the encrypted message does not represent the same letter in the plaintext.
- No information is revealed by observation

Ciphertext-only Attack

A ciphertext-only attack is one where the adversary tries to deduce the decryption key or plaintext by only observing ciphertext

- Any value of the encrypted message is a function of n values of the plaintext and one column of the encryption matrix A
- Two or more same values of the encrypted message does not represent the same letter in the plaintext.
- No information is revealed by observation

Result of the Cryptanalysis: Secure

Hadamard and Plotkin ciphers are secure against ciphertext-only attacks

Security Comparison for Block Ciphers

Hadamard and Plotkin Ciphers

A chosen plaintext attack can break the ciphers; A key size of ≥ 128 bits provides security for brute-force attacks

3DES

A meet-in-the-middle attack provides security only for 112 bits, when using a key of 168 bits (three 56 bit DES keys)

Blowfish

Variable key size up to 448 bits

Sources

- Bruce Schneier, (1996, 2004)
- Declassified documents from National Security Agency (NSA)

Summary

Highlights

1. We constructed private-key block ciphers from combinatorial designs (Hadamard matrices and Plotkin arrays).
2. We presented a cryptanalysis for Hadamard and Plotkin ciphers which showed that the ciphers are secure against cryptographic attacks in most cases.
3. We conducted a simulation of brute-force attacks for Kronecker Plotkin ciphers, proving the security of these ciphers.

Summary

Highlights

1. We constructed private-key block ciphers from combinatorial designs (Hadamard matrices and Plotkin arrays).
2. We presented a cryptanalysis for Hadamard and Plotkin ciphers which showed that the ciphers are secure against cryptographic attacks in most cases.
3. We conducted a simulation of brute-force attacks for Kronecker Plotkin ciphers, proving the security of these ciphers.

Future Work

- Develop a public-key cryptosystem based on similar properties of combinatorial designs
- Consider more types of cryptographic attacks
- Implement the Hadamard and Plotkin ciphers for hardware-used cryptography purposes (i.e. Military, Intelligence Services)

References

- C.J. Colbourn, J.H. Dinitz and D.R. Stinson, "Applications of combinatorial designs to communications, cryptography, and networking," in Surveys in Combinatorics, J.D. Lamb and D.A. Preece (Eds.), Cambridge, Cambridge University Press, pp. 37–100, 1999.
- R. Harkins, E. Weber and and A. Westmeyer, "Encryption schemes using finite frames and Hadamard arrays," Experimental Mathematics, vol. 14, pp. 423–433, 2005.
- C. Koukouvinos, E. Lappas and D. E. Simos, "Encryption schemes using orthogonal arrays," J. Discrete Math. Sci. Cryptogr., vol. 12, pp. 615–628, 2009.
- C. Koukouvinos and D. E. Simos, "Encryption schemes using Plotkin arrays," Appl. Math. & Inf. Sci., vol. 5, pp. 500-510, 2011.
- C. Koukouvinos and D. E. Simos, "Encryption schemes from williamson matrices," to appear in J. Inf. Assur. Secur.
- B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, J. Wiley and Sons Inc., New York, 1996.

Thanks for your Attention!

Ευχαριστώ για την Προσοχή σας!