Markov Ciphers and Alternating Groups

G. Hornauer, W. Stephan,
R. Wernsdorf

SIT Gesellschaft für Systeme der Informationstechnik mbH
15537 Grünheide (Mark), Germany
Charlottenstraße 7

Abstract. This paper includes some relations between differential cryptanalysis and group theory. The main result is the following:
If the one-round functions of an r-round iterated cipher generate the alternating or the symmetric group, then for all corresponding Markov ciphers the chains of differences are irreducible and aperiodic.
As an application it will be shown that if the hypothesis of stochastic equivalence holds for any of these corresponding Markov ciphers, then the DES and the IDEA(32) are secure against a differential cryptanalysis attack after sufficiently many rounds for these Markov ciphers.
The section about IDEA(32) includes the result that the one-round functions of this algorithm generate the alternating group.

The theoretic foundations in group theory and Markov chains are described for instance in [Wie 64] and [Fel 58].

1 Properties of Markov Chains and Markov Ciphers

Let us recall some definitions and properties of Markov chains. The definitions follow the notations of [LMM 91]. In this section we will briefly review parts of this paper.

A sequence of discrete random variables $v_0, v_1, \ldots, v_r$ is a Markov chain if for $0 \le i < r$ (where $r = \infty$ is allowed):

$$P(v_{i+1} = \beta_{i+1} \mid v_i = \beta_i, v_{i-1} = \beta_{i-1}, \ldots, v_0 = \beta_0) = P(v_{i+1} = \beta_{i+1} \mid v_i = \beta_i).$$

A Markov chain is called homogeneous if $P(v_{i+1} = \beta \mid v_i = \alpha)$ is independent of i for all pairs (α,β).

Let $\Pi = \|p_{ij}\|$ denote the transition probability matrix of a finite homogeneous Markov chain with M states and p_{ij} the transition probabilities.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 453-460, 1994.

A finite Markov chain with the transition matrix Π is irreducible if for any (i, j) there is an r such that the (i, j) entry in the r-th transition matrix Π^r, $p_{ij}^{(r)} > 0$.

The chain is aperiodic if $\gcd\left(r_i = \min_r \left\{ p_{ii}^{(r)} > 0 \right\} ;\ 1 \le i \le M \right) = 1$.

Theorem 1 completes the probability theoretic background.

THEOREM 1 [Fel 58]:

If a finite, homogeneous, irreducible aperiodic Markov chain has a doubly stochastic transition matrix $\Pi = \left\| p_{ij} \right\|$, then in the limit all states become equally probable, i.e. $p_j^{\infty} = \frac{1}{M}$ (j=1, ... , M). (Doubly stochastic means, every row sum and every column sum of Π is 1.)

The encryption of a pair of plaintexts by an r-round iterated cipher is shown in the following scheme [LMM 91]:

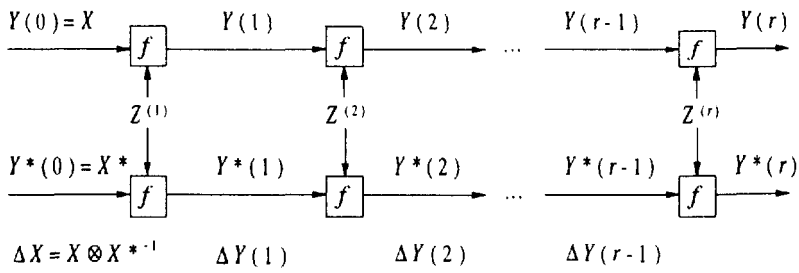

Figure 1

The *one-round function* $Y = f_Z(X)$ generates for every round subkey Z a one to one correspondence between X and Y.

Let the *"difference"* ΔX between two plaintexts (or two ciphertexts) X and X^* be defined as $\Delta X = X \otimes X^{*-1}$ where $\otimes$ denotes a specified group operation on the set of plaintexts (= set of ciphertexts) and X^{*-1} denotes the inverse of the element X^* in the group.

DEFINITION:

If there is a difference ΔX such that for all choices of α ($\alpha \neq e$) and β ($\beta \neq e$) $P(\Delta Y = \beta | \Delta X = \alpha, X = \gamma)$ is independent of γ when the subkey Z is uniformly random, then an iterated cipher with round function $Y = f_Z(X)$ is a *Markov cipher* in relation to the difference ΔX.

If there exists more than one difference ΔX which generates a Markov cipher, then all of these Markov ciphers are called *corresponding to the one-round function* f_Z.

THEOREM 2 [LMM 91]:

If an r-round iterated cipher is a Markov cipher and the r-round subkeys are independent and uniformly random, then the sequence of differences $\Delta X = \Delta Y(0), \Delta Y(1), \ldots, \Delta Y(r)$ is a homogeneous Markov chain.

THEOREM 3 [Lai 92]:

The transition matrix Π of a Markov cipher is doubly stochastic.

THEOREM 4 [Lai 92]:

For a Markov cipher the chain of differences is irreducible, if for every plaintext pair (X, X^*), $X \neq X^*$, and every ciphertext pair (Y, Y^*), $Y \neq Y^*$, there is an integer r_0 and a choice of subkeys for the first r_0 rounds such that, under the first r_0 rounds of the cipher with the chosen subkeys, X is encrypted to Y and X^* is encrypted to Y^*.

The cryptographic background needs the *Hypothesis of Stochastic Equivalence:*

For virtually all high probability (r-1)- round differentials (α, β),

$$P(\Delta Y(r-1) = \beta | \Delta X = \alpha)$$
$$= P(\Delta Y(r-1) = \beta | \Delta X = \alpha, Z^{(1)} = z_1, \ldots, Z^{(r-1)} = z_{r-1})$$

holds for a substantial fraction of the subkey values $(z_1, \ldots, z_{r-1})$.

In the following it is shown that if the one-round functions $Y = f_Z(X)$ fulfil special algebraic properties, then the conditions of Theorem 1 come true for the chain of differences of a Markov cipher.

2 Group Theoretic Conditions for the One-Round Function

In the following we consider an arbitrary r-round iterated cipher on a finite set X, which is a Markov cipher in relation to a given difference. We derive sufficient conditions for the corresponding Markov chain of differences to be irreducible and aperiodic. These conditions are independent of the given difference.

For some of the following notations we refer to standard books on group theory like [Wie 64] and [Rob 82].

Let $G := \langle \{ f_Z \mid Z \in \mathcal{Z} \} \rangle$ ($\mathcal{Z}$ - set of the round subkeys)

be the permutation group on X generated by the one-round functions f_Z and

$$\forall\, t \in \mathbb{N}: \quad H_t := \left\langle \left\{ f_{Z_1} \circ f_{Z_2} \circ \ldots \circ f_{Z_t} \mid (Z_1, Z_2, \ldots, Z_t) \in \mathcal{Z}^t \right\} \right\rangle$$

be the permutation group generated by the t-round functions.

LEMMA 1:

For every $t \in \mathbb{N}$ either $G = H_t$ or the group H_t is a proper normal subgroup of G.

LEMMA 2:

Let the Markov chain of differences be irreducible and periodic. Then there exists a $t \in \mathbb{N} \setminus \{1\}$ such that H_t is not doubly transitive.

From these two Lemmas we obtain

THEOREM 5:

Let $|X| \geq 3$ and every normal subgroup of G (except the identity group $\langle \{Id\} \rangle$) be doubly transitive. Then for all corresponding Markov ciphers the Markov chains of differences are irreducible and aperiodic.

Some special cases of G are considered in the following corollaries.

COROLLARY 1:

a) If G is a doubly transitive and simple group, then for all corresponding Markov ciphers the Markov chains of differences are irreducible and aperiodic.

b) If G is 4-transitive and $|X| \geq 5$, then for all corresponding Markov ciphers the Markov chains of differences are irreducible and aperiodic.

In the next two sections we will apply:

COROLLARY 2:

If G is the symmetric or the alternating group on X and $|X| \geq 5$, then for all corresponding Markov ciphers the Markov chains of differences are irreducible and aperiodic.

3 Application to the DES

The following scheme shows the one-round function f_Z of the DES [NBS 77]:

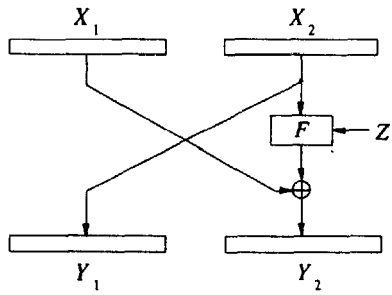

Figure 2

In [Wer 93] it is shown that the set $\{f_Z | Z \in \mathcal{Z}\}$ generates the alternating group, and therefore the following theorem is an immediate consequence of Corollary 2.

THEOREM 6:

If f_Z is the one-round function of the DES, then for all corresponding Markov ciphers the chain of differences is irreducible and aperiodic, i. e. after sufficiently many rounds all differences will be roughly equally probable.

CONCLUSION 1:

If the hypothesis of stochastic equivalence (see Section 1) holds for a part of the corresponding Markov ciphers, then the DES is secure against a differential cryptanalysis attack after sufficiently many rounds for all of these Markov ciphers.

The results hold for all r-round iterated ciphers, if the one-round functions are DES-like functions which generate the alternating group (see [EG 83]).

4 Application to the IDEA

In [Lai 92] the block cipher algorithm IDEA is defined (in [LMM 91] it is called "IPES"). A difference between plaintexts is given such that the IDEA is a Markov cipher. The considered one-round functions f_Z are demonstrated in the following figure:

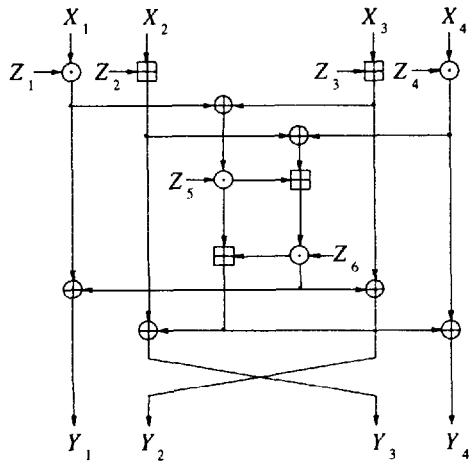

Figure 3

In order to treat several analytical approaches, the author of [Lai 92] introduced so called "mini" IDEA-ciphers IDEA(8), IDEA(16) and IDEA(32). These ciphers differ from IDEA = IDEA(64) only in their block lengths, which are 8, 16 and 32 respectively. Taking the analogous differences they are Markov ciphers too.

For the ciphers IDEA(8) and IDEA(16) it is proved that the Markov chains based on the given differences are irreducible and aperiodic [Lai 92]. That gives evidence to conjecture the same properties for IDEA(32) and IDEA(64). In [Lai 92] this remained an open question.

In the following, we will answer this question for IDEA(32).

The corresponding group G of the one-round functions (see Section 2) has the following properties:

LEMMA 3:

a) G is transitive.

b) G contains only even permutations.

For the arbitrary chosen permutation $f_Z \in G$ with the key parameters

$(Z_1, Z_2, \ldots, Z_6) = (218, 133, 79, 184, 97, 113)$

we computed a part of the cycle representation. The computations took nearly 30 hours on a SUN workstation.

Starting from the zero vector we found a cycle with a length of

$3\,639\,977\,669 = 211 \cdot 17\,251\,079.$

On the basis of this cycle length, of Theorem 13.10 in [Wie 64] and of the results of Lemma 3 we proved Theorem 7.

THEOREM 7:

For IDEA(32) we have $G = A_{2^{32}}$. ($A_{2^{32}}$ = Alternating group on $X := \{0,1\}^{32}$.)

The result of Theorem 7 provides the possibility to apply Corollary 2.

THEOREM 8:

If f_Z is the one-round function of the IDEA(32), then for all corresponding Markov ciphers the chain of differences is irreducible and aperiodic, i. e. after sufficiently many rounds all differences will be roughly equally probable.

CONCLUSION 2:

If the hypothesis of stochastic equivalence (see Section 1) holds for a part of the corresponding Markov ciphers, then IDEA(32) is secure against a differential cryptanalysis attack after sufficiently many rounds for all of these Markov ciphers.

5 Comments

- The result of Theorem 7 implies that several other imaginable cryptanalytic "short-cuts" of IDEA(32) can be excluded or restricted (see [Wer 93]). Though the results of Section 4 do not refer to the full IDEA(64), they may serve as arguments for the cryptographic strength of this algorithm.
- For an r-round iterated cipher for some special keys the one-round functions $(f_{Z_1},...,f_{Z_r})$ may generate only a subgroup $G' \subset G$ that is not doubly transitive. This provides that the hypothesis of stochastic equivalence does not always hold (see also [Lai 92]). Hence the DES and the IDEA(32) may not be secure for all differences which fulfil Theorem 6 and Theorem 8 respectively.
- The behaviour of differences which do not generate Markov chains is unknown. Its analysis is an open, interesting problem.

References

[EG 83] Even, S.; Goldreich, O.
DES-like Functions Can Generate the Alternating Group
IEEE Transactions on Information Theory, IT-29, Nr. 6, 1983, 863 - 865

[Fel 58] Feller, W.
An Introduction to Probability Theory and Its Applications
Volume I, Second Edition 1958
John Wiley & Sons, Inc., New York

[Lai 92] Lai, X.
On the Design and Security of Block Ciphers
ETH Series in Information Processing, v.1 (Dissertation)
Hartung-Gorre Verlag, Konstanz, 1992

[LMM 91] Lai, X.; Massey, J. L.; Murphy, S.
Markov Ciphers and Differential Cryptanalysis
Proc. EUROCRYPT '91, LNCS 547, 1991, 17 - 38

[NBS 77] Data Encryption Standard (DES)
US NBS, FIPS PUB 46, 1977, Washington

[Rob 82] Robinson, D. J. S.
A Course in the Theory of Groups
Graduate Texts in Mathematics, Springer, 1982, New York

[Wer 93] Wernsdorf, R.
The One-Round Functions of the DES Generate the Alternating Group
Proc. EUROCRYPT '92, LNCS 658, 1993, 99 - 112

[Wie 64] Wielandt, H.
Finite Permutation Groups
Academic Press, 1964, New York and London