Some Mathematical Topics in Symmetric Ciphers

La De Cifris incontra Milano

Università degli Studi di Milano - Bicocca
11 Settembre 2018

Symmetric Cryptography; private key

Abstract Definition of a cipher: a set of transformations E_k (**round functions**) of one space M (the set of possible messages) into a second space C (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular **key**. The transformations are supposed reversible so that unique deciphering is possible when the **key** is known.

1. In a *block cypher* the space of the messages M and the space of the cryptograms C coincide. Moreover,

$$M = C = \{0,1\}^n = V(n,2)$$

n is the length of the code.

2. for any fixed key k, the *encryption function* E_k is a permutation of V

Iterated ciphers: obtained by the composition of a finite number l of rounds. The *encryption function* is given by the composition of some permutations, called round functions: if k is a key, E_k is given by the composition of l rounds $\rho_{k,i}$:

$$E_k = \rho_{k,1} \circ \rho_{k,2} \circ \cdots \circ \rho_{k,l}$$

Included: some common ciphers (AES , SERPENT, PRESENT),

MATHEMATICS in particular: **groups**

Back to DES: Kaliski, Rivest and Sherman (1988) considered the question

Is DES (that is, the set of transformations it defines) a group?

Why?

Triple DES was being suggested as an improvement to DES:

Let T_a be a DES transformation, corresponding to the key a. The T_a are permutations of the message space, that is, elements of $Sym(2^n)$ acting on the elements of the vector space $\{0, 1\}^n$.

- Suppose $\{T_a,: a \in V\}$ is a group, that is, for all keys a, b there is a key c such that $T_a T_b = T_c$. Then Triple DES would make no sense;

- They gave some evidence that DES is not a group and K. W. Campbell and M. J. Wiener, in 1993 proved that DES is not a group

- Kaliski et al. showed that if the group generated by the transformations of a cipher is too small, then the cipher is exposed to certain cryptanalytic attacks.

- In 1993 Wernsdorf proved that the the round functions of DES generate the alternating group.

The Group of round functions, we call $\Gamma_\infty(C)$, is not the group of the Cipher C, $\Gamma(C)$.

$$\Gamma_\infty(C) =< \rho_{k,i}, k \in K >; \quad \Gamma(C) =< E_k, k \in K >$$

,

BUT: for a large class of ciphers, we were able to obtain informations for $\Gamma_\infty(C)$, **not** for $\Gamma(C)$.

Some properties of the group $\Gamma(C)$:

The group must be primitive: In 1999, Paterson showed that if $\Gamma(C)$ is an imprimitive group, then it is possible to embed a trapdoor in the cipher. However, the primitivity of $\Gamma_\infty(C)$ does not guarantee the absence of trap-doors.

A trapdoor is a hidden structure of the cipher, whose knowledge allows an attacker to obtain information on the key or to decrypt certain ciphertexts)

Primitive group If $\Omega = \{1, \ldots, n\}$ a transitive permutation group $H \leq Sym(\Omega)$ is primitive if it does not admit a non trivial block-system.

$$\{\Delta_1, \ldots, \Delta_t\}$$

is a block- system, if it is a partition of Ω, permuted by G.

A subgroup of an imprimitive group is imprimitive.

It makes sense to check if $\Gamma_\infty(C)$ is primitive.

Our cipher C:

$$V = V_1 \oplus \cdots \oplus V_s,$$

$s > 1$, where each V_i has the same dimension m over $GF(2)$, that is $n = ms$. For $v \in V$, we will write $v = v_1 + \cdots + v_s$, $v_i \in V_i$. Also, we consider the projections $\pi_i : V \to V_i$, which map $v \mapsto v_i$. For $\gamma \in Sym(n)$, we have

$$v\gamma = v_1\gamma_1 \oplus \cdots \oplus v_s\gamma_s,$$

for some $\gamma_i \in Sym(V_i)$, is a bricklayer transformation and any γ_i is a brick. maps γ_i are traditionally called S-boxes and map γ is called a parallel S-box.

A linear map $\lambda : V \to V$ is called a **proper mixing layer** if no sum of some of the V_i (except 0 and V) is invariant under λ.

In AES $V = M = \{0,1\}^{128}$, $m = 8$, $s = 16$. the S-boxes are all equal, and consist of inversion in the field $GF(2^8) = V_i$ with 2^8 elements, followed by an affine transformation: a linear transformation + translation. λ is the composition of so called **MixColumns** and another linear map called **ShiftRows** round functions: $\gamma\lambda\tau_k$, with τ_k translation given by the key k.

In this case, it is easy to answer to Paterson's question here:

an imprimitivity system consists indeed of the cosets of a subspace U of the message space V. I.e.

$$\{v + U : v \in V\}$$

where $v + U = \{v + u : u \in U\}$.

There are no such trapdoors in AES/Rijndael.

O'Nan-Scott Theorem about classification of primitive groups $\longrightarrow$ $\Gamma_\infty(C) = Alt(2^n)$ or $\Gamma_\infty(C) = Sym(2^n)$. As the rounds are even-So $\Gamma_\infty(C) = Alt(2^n)$

SOME REFERENCES

1. R. J. Anderson, E. Biham, and L.R. Knudsen, *SERPENT: A new block cipher proposal*, Fast Software Encryption, LNCS, vol. 1372, Springer, 1998, pp. 222-238.

2. R.Aragona; M. Calderini; A. Tortora; M.Tota, *Primitivity of PRESENT and other lightweight ciphers* JOURNAL OF ALGEBRA AND ITS APPLICATIONS. Pag.1-18

3. A. Caranti, F. Dalla Volta, and M. Sala, *On some block ciphers and imprimitive groups*, AAECC 20 (2009), no. 5-6, 229-350.

4. A.Caranti,F.DallaVolta,andM.Sala, An application of the O?Nan-Scott theorem to the group generated by the round functions of an AES-like cipher, Des. Codes Cryptogr. 52 (2009), no. 3, 293-301.

5. D. Coppersmith and E. Grossman, Generators for certain alternating groups with applications to cryptography, SIAM J. Appl. Math. 29 (1975), no. 4, 624-627.

6. J. Daemen and V. Rijmen, *AES proposal: Rijndael*, Tech. report, NIST, 1998, http://www.nist.gov/aes.

7. C. Fontanari, V. Pulice, A. Rimoldi, and M. Sala, *On weakly apn functions and 4-bit s-boxes*, Finite Fields and Their Applications 18 (2012), no. 3, 522?528.

8. B. S. Kaliski, Jr., R. L. Rivest, and A. T. Sherman, *Is the data encryption standard a group?* (Results of cycling experiments on DES), J. Cryptology 1 (1988), no. 1, 3?36.

9. K.G. Paterson, *Imprimitive permutation groups and trapdoors in interated block ciphers, Fast software encryption*, LNCS, vol. 1636, Springer, Berlin, 1999, pp. 201-214.

10. R. Sparr and R. Wernsdorf, *Group theoretic properties of Rijndael-like ciphers*, Discrete Appl. Math. 156 (2008), no. 16, 3139-3149