Elastic Block Ciphers

Dott. Emanuele Bellini[1]
Dott. Guglielmo Morgari Dott. Marco Coppola[2]

1 - Università degli Studi di Trento, Lab di Matematica Industriale e Crittografia

2 - Telsy S.p.a.

12 Settembre 2011

Problem

How to encrypt data of varying length, such as database fields or rows, or network packets, etc.?

Solutions:

- Padding ⇒ Overhead of encryption
- A-doc cipher ⇒ Analize security
- Modes of Encryption ⇒ Loss of security
- Stream Cipher ⇒ Less secure than block ciphers ??
- Elastic Cipher!

What is an Elastic Cipher?

Definition

Let $m, n \in \mathbb{N}$, $n \geq 1$. Let $\{0,1\}^{\geq n}$ denote the set of all binary strings with length at least n. A *message space* $\mathcal{M}$ is a nonempty subset of $\{0,1\}^{\geq n}$ for which $M \in \mathcal{M}$ implies that $M' \in \mathcal{M}$ for all M' of the same length of M.

The *key space* is $\mathcal{K} = \{0,1\}^m$.

An *elastic cipher* is a family of pseudo-random-permutations

$$F : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$$

.

When $\mathcal{M}$ is restricted to a set of messages of the same length we talk about a *fixed length block cipher* or simply a *block cipher*.

Bellare-Rogaway Elastic Cipher - Idea

The idea is to use an existing block cipher and to use it as a *black box*, which it is assumed to be secure.
This black box is then inserted inside a circuit allowing only certain primitives, such as bitwise addition, padding, or hash functions.

Bellare-Rogaway Elastic Cipher - How to prove security

Bellare-Rogaway criterion for the security of a block cipher:

- show that the block cipher is indistinguishible from a pseudorandom permutation

Bellare-Rogaway criterion for the security of an elastic cipher:

- show that the elastic cipher is indistinguishible from a pseudorandom permutation if the underlying block cipher has this property

Bellare-Rogaway Elastic Cipher - Adversary Advantage

Let F_0 and F_1 be two function families that have both identical domains and ranges.

Definition

The *adversary advantage* of A in distinguishing F_0 from F_1 is:

$$Adv_A(F_0, F_1) = Pr(f \overset{R}{\leftarrow} F_0 : A^f = 1) - Pr(g \overset{R}{\leftarrow} F_1 : A^g = 1)$$

where the probabilities are taken over the choice of f and A's internal coin tosses.

Bellare-Rogaway Elastic Cipher - Proof of security

Theorem

A cipher C will be considered secure against any attack which uses time t, q queries and memory m, if

$$Adv_C^{PRP}(t,q,m) = |\max_{\forall A t,q,m-adversary}\{Adv_A(C,PRP)\}| \leq \epsilon$$

Let E be the elastic version of C. Then Bellare and Rogaway show that Adv_E^{PRP} is bounded by Adv_C^{PRP} plus a term q^2, which means the security of E depends on the security of C and degrades with the number of queries allowed.

Bellare-Rogaway Elastic Cipher - Problems

1. Low efficiency. The underlying block cipher is applied at least twice even if the message length is only one bit more than the block cipher length.
2. Hard to prove security. It is hard (maybe impossible) to prove that there is no $(t, q, m) - distinguisher$ for a certain cipher.
3. Security guaranteed for only one model. In the oracle model proofs of security are based on indistinguishability from pseudo-random permutations, which means the elastic cipher is secure only against chosen plaintext attacks.

Cook's Elastic Cipher and our work

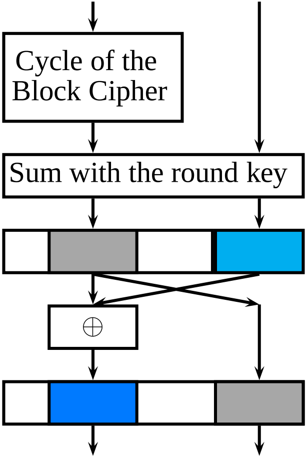
Given a block cipher of length L Cook's elastic cipher allows to encrypt messages of variable length from L to $2L$. Given some conditions on the key schedule, Cook's elastic cipher is secure against any key recovery attack if the underlying block cipher is, and it achieves complete diffusion in at most $q+1$ rounds if the underlying block cipher achieves it in q rounds. We extend Cook's construction inductively, obtaining an elastic cipher for any message length greater than L with the same properties of security as Cook's elastic cipher.

Cook's Elastic Cipher - How to prove security

Cook's critera for the security of an elastic cipher:

- achieve complete diffusion
- resist against key recovery attacks if the underlying BC does
- produce output bit strings which look like random bit sequences

One round of Cook's Elastic Cipher



Definition

The *cycle of a block cipher* is a Boolean function made of the least, over any key, number of consecutive rounds such that each bit of the cycle output is a function of at least two input bits. [a]

[a] E.g., AES cycle coincides with its round; DES cycle is the composition of two consecutive round.

More informally, a cycle of a BC is the minimum sequence of steps in which all input bits are processed by the round function.

Key schedule requirements

1. the key schedule should be a stand-alone algorithm that is usable to any BC;
2. the expanded-key bits should be (or as close to) pseudorandom (as practical);
3. the expanded-key rate for elastic block cipher should be a small multiple of the key expansion rate of a standard BC.

This three requirements can be satisfied if we use a pseudorandom generator (e.g. RC4).

Extension of Cook's Elastic Cipher - Idea

Our idea is to expand the elastic extension as it was a fixed length block cipher.
We call E_0 the underlying BC of length L, E_1 Cook's extension of E_0, E_2 Cook's extension of E_1 taken with fixed length between L and $2L$, and so on...
Our proofs rely the security of any extension E_n to that of E_0, and allow to increase the number of computations linearly with the input length.

Extension of Cook's Elastic Cipher - Scheme of E_2

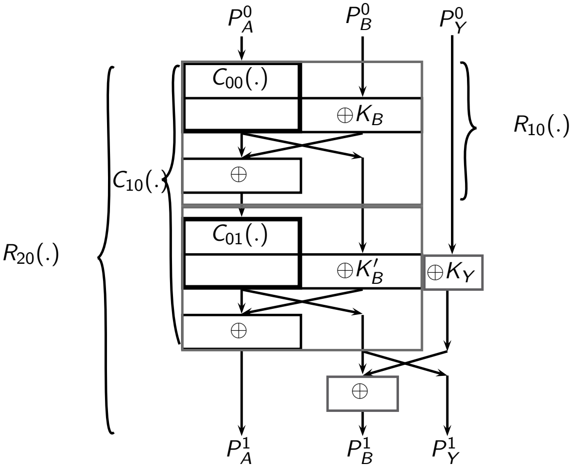
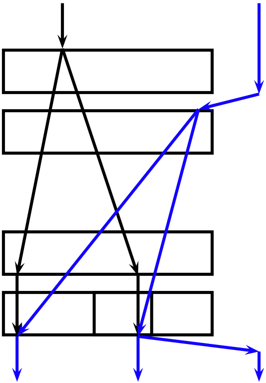


Figura: Details of the first round of E_2.

Proof of security - Diffusion



Theorem (Complete/Ideal Diffusion)

If complete/ideal diffusion occurs after q cycles in E_{n-1} (an elastic cipher working with length message $2^{n-1}L$), then it occurs after at most $q+1$ rounds in E_n(the elastic version of E_{n-1}).

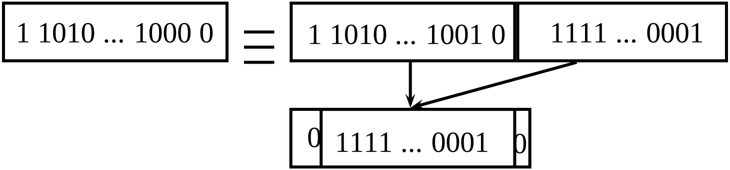
Proof of security - key recovery

Theorem (Security Against Key Recovery)

Given an elastic cipher, E_{n-1} of level $n-1$ (without initial and final whitening and key-dependent permutation), working on $2^{n-1}L$-bit blocks and its elastic version, E_n, that works on $(2^{n-1}L+y)$-bit blocks, where $0 \leq y \leq 2^{n-1}L$, if there exists an attack, $\mathcal{A}_n$, on E_n that allows the round keys to be determined for r consecutive rounds of E_n using $t_{\mathcal{A}_n}$ operation, then there exists an attack $\mathcal{A}_{n-1}$ on E_{n-1} with r cycles that finds the expanded key for E_{n-1} and that uses $t_{\mathcal{A}_{n-1}} < O(sr^2 + rt_{\mathcal{A}_n})$, assuming there are no message-dependent expanded key, meaning any expanded-key bits utilized in E_{n-1} depend only on the key and do not vary across plaintext or ciphertext inputs. In particular, if $\mathcal{A}_n$ is polynomial then $\mathcal{A}_{n-1}$ is polynomial.

Idea of the proof

In the picture it is shown how to convert a round key of E_n to a cycle key of E_{n-1}:



Grazie per l'attenzione!