Decorrelated Fast Cipher

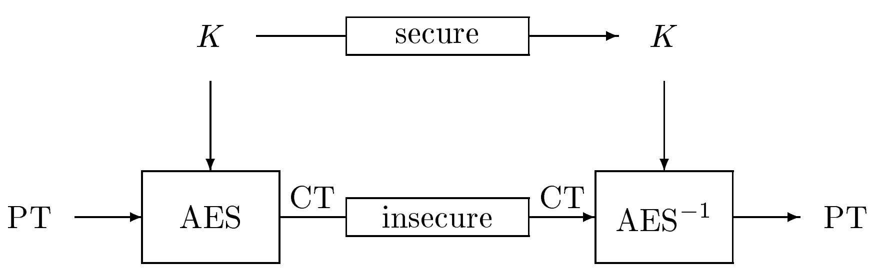
Serge Vaudenay

Ecole Normale Supérieure – CNRS

August 1998

First Advanced Encryption Standard Conference

Private Communications

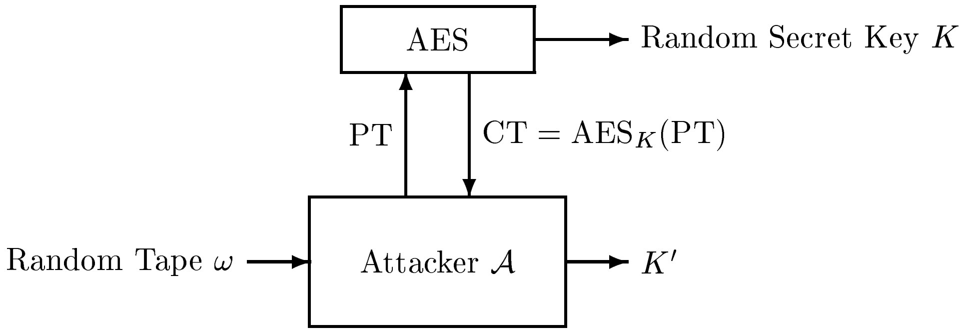


message space: $\mathcal{M} = \{0,1\}^{128}$

message block: $\mathrm{PT} \in \mathcal{M}$

encryption function: AES_K (permutation over $\mathcal{M}$)

Security of Block Ciphers



→ (secret) random permutation with a given (public) distribution

→ we study the attack "on average" on the key

Definition. AES *is* ϵ*-secure against a class* CL *of attack if*

$$\forall \mathcal{A} \in \mathrm{CL} \quad \Pr_{\omega,K}\left[\mathcal{A}^{\mathrm{AES}_K} = K\right] \le \epsilon$$

Previous Work on Provable Security

[Shannon 49]: notion of perfect secrecy, impossibility of achieving it

[Wegman-Carter 81]: provably secure MAC with universal hashing

[Luby-Rackoff 88]: the Feistel scheme with random round function is "almost" a random permutation

[Biham-Shamir 90]: notion of differential cryptanalysis

[Lai-Massey-Murphy 91]: notion of Markov cipher

[Matsui 93]: notion of linear cryptanalysis

[Nyberg-Knudsen 92]: construction of cipher which is provably resistant against differential cryptanalysis

[Matsui 96]: construction of MISTY which is provably resistant against differential and linear cryptanalysis

Perfect Decorrelation

To the order 1:

$$\forall \mathrm{PT} \quad \mathrm{AES}_K(\mathrm{PT}) \text{ has a uniform distribution}$$

To the order 2:

$$\forall \mathrm{PT} \neq \mathrm{PT}' \quad (\mathrm{AES}_K(\mathrm{PT}), \mathrm{AES}_K(\mathrm{PT}')) \text{ has a uniform distribution}$$

(among all $(\mathrm{CT}, \mathrm{CT}')$ such that $\mathrm{CT} \neq \mathrm{CT}'$)

To the order d:

$$\forall (\mathrm{PT}_i \neq \mathrm{PT}_j) \quad (\mathrm{AES}_K(\mathrm{PT}_1), \ldots, \mathrm{AES}_K(\mathrm{PT}_d)) \text{ uniform}$$

(among all $(\mathrm{CT}_1, \ldots, \mathrm{CT}_d)$ such that $\mathrm{CT}_i \neq \mathrm{CT}_j$)

Resistance Against Differential Cryptanalysis

If AES has a perfect decorrelation to the order 2, then for all $a \neq 0$ and $b \neq 0$, we have

$$\Pr_{K,\mathrm{PT}}[\mathrm{AES}_K(\mathrm{PT} \oplus a) = \mathrm{AES}_K(\mathrm{PT}) \oplus b] = \frac{1}{2^{128} - 1}.$$

$\rightarrow$ AES resists "on average" against any differential attack with a fixed characteristic.

Basic Examples

The Vernam Cipher (One-time pad) [Vernam 26]

$$\mathrm{AES}_K(\mathrm{PT}) = \mathrm{PT} \oplus K \quad \text{with} \quad K \in_U \{0,1\}^{128}$$

$\rightarrow$ perfect decorrelation to the order 1

Basic COCONUT Cipher

$$\mathrm{AES}_{A,B}(\mathrm{PT}) = (A \times \mathrm{PT}) \oplus B \;\; \text{with} \;\; (A,B) \in_U \mathrm{GF}(2^{128})^* \times \mathrm{GF}(2^{128})$$

$\rightarrow$ perfect decorrelation to the order 2

Design Strategy

- we do not need "perfect" decorrelation: we tolerate imperfect decorrelation as long as we can quantify it
- we do not want $\mathrm{GF}(2^m)$ multiplication: we want fast software implementations

  $\rightarrow$ use the integer multiplication
- we do not want *ad hoc* construction: we want to get decorrelation on arbitrary cipher by adding a few "decorrelation modules"

  $\rightarrow$ we add the

  $$F_{A,B}(x) = (A \times x + B) \bmod p \bmod 2^m$$

  decorrelation module with $(A,B) \in_U \{0,\ldots,2^m-1\}^2$.

Decorrelation Distance

To each random mapping F from $\mathcal{A}$ to $\mathcal{B}$ we associate the $\mathcal{A}^2 \times \mathcal{B}^2$-matrix $[F]^2$: the **pairwise distribution matrix**.

Given $x = (x_1, x_2) \in \mathcal{A}^2$ and $y = (y_1, y_2) \in \mathcal{B}^2$, we have

$$[F]^2_{x,y} = \Pr[F(x_1) = y_1, F(x_2) = y_2].$$

Definition. *Given two random functions F and G from $\mathcal{A}$ to $\mathcal{B}$, the pairwise decorrelation distance between F and G is*

$$||[F]^2 - [G]^2|| = \max_{x_1,x_2} \sum_{y_1,y_2} \left| \Pr\begin{bmatrix} F(x_1) = y_1 \\ F(x_2) = y_2 \end{bmatrix} - \Pr\begin{bmatrix} G(x_1) = y_1 \\ G(x_2) = y_2 \end{bmatrix} \right|$$

Theoretical Results

If

$$F_{A,B}(x) = (Ax + B) \bmod (2^{64} + 13) \bmod 2^{64}$$

for $(A, B) \in_U \{0,1\}^{128}$ and F^* is a random function on $\{0,1\}^{64}$ with a uniform distribution then

$$||[F]^2 - [F^*]^2|| \approx 2^{-58}.$$

If $\mathrm{DFC}_{A_1,B_1,\ldots,A_6,B_6}$ is a 6-round Feistel cipher in which each round function can be written

$$\mathrm{RF}_i(x) = \mathrm{CP}((A_i x + B_i) \bmod (2^{64} + 13) \bmod 2^{64})$$

for $(A_1, B_1, \ldots, A_6, B_6) \in_U \{0,1\}^{768}$ and C^* is a random permutation on $\{0,1\}^{128}$ with a uniform distribution then

$$||[\mathrm{DFC}]^2 - [C^*]^2|| \approx 2^{-113}.$$

Security Results

Let $\epsilon = ||[\mathrm{DFC}]^2 - [C^*]^2||$.

For any differential or linear distinguisher, if the complexity is far less than ϵ^{-1}, then the success probability is negligible.

$\rightarrow$ no such attacks possible if a key is used less than 2^{92} times.

For any iterated attack of order 1, if the complexity is far less than $\epsilon^{-\frac{1}{2}}$, then the success probability is negligible.

$\rightarrow$ no such attack possible if a key is used less than 2^{48} times.

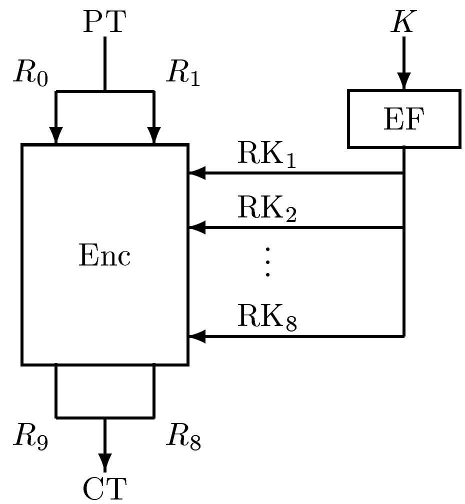
Iterated Attack of Order 1

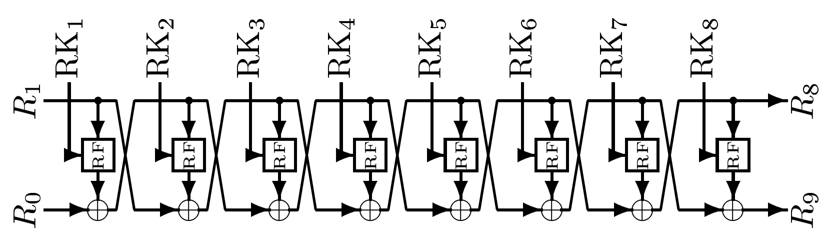
Input: a cipher AES, a complexity n, a test $\mathcal{T}$, an acceptance set A

1. for i from 1 to n do
   (a) get a new (X, Y) pair with $Y = \mathrm{AES}(X)$ pair
   (b) set $T_i = 0$ or 1 with an expected value $\mathcal{T}(X, Y)$
2. if $(T_1, \ldots, T_n) \in A$ accept otherwise reject

The attack is successful if AES is likely to be accepted and a random permutation is likely to be rejected.

One Encryption



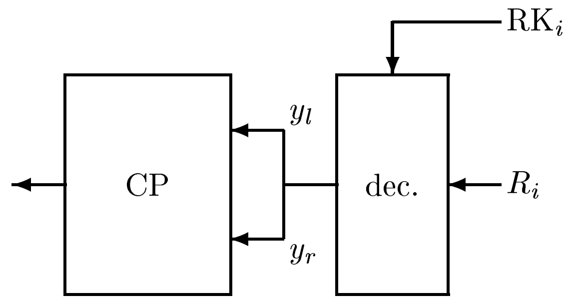


The Round Function

We let $\mathrm{RK}_i = (\mathrm{ARK}_i, \mathrm{BRK}_i)$.

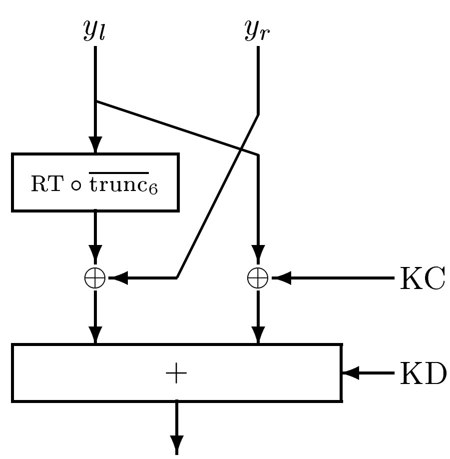
The output of the decorrelation module is

$$(\mathrm{ARK}_i \times R_i + \mathrm{BRK}_i) \bmod (2^{64} + 13) \bmod 2^{64}$$



The Confusion Permutation

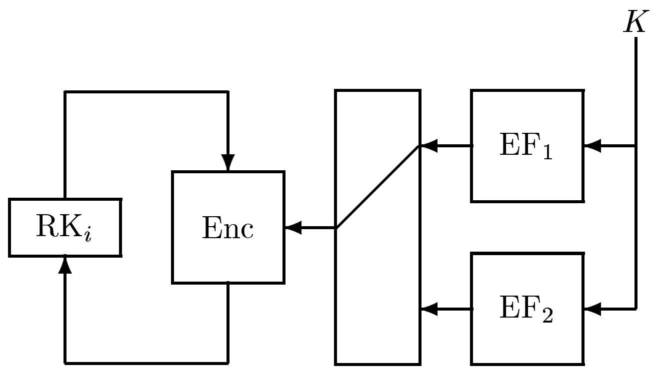
We use a Round Table $\mathrm{RT}(0), \ldots, \mathrm{RT}(63)$.



The Expansion Function

We use two linear functions EF_1 and EF_2 and let $\mathrm{RK}_0 = 0$.

$\mathrm{EF}_1(K)$ and $\mathrm{EF}_2(K)$ are used exactly 4 times.



Implementations

microprocessor	cycles-per-bit	clock-frequency	bits-per-second
AXP	4.36	600MHz	137.6Mbps
Pentium	5.89	200MHz	34.0Mbps
SPARC	6.27	170MHz	27.1Mbps

Motorola 6805 (smart cards): one encryption within 9.80ms.

Security

Assumption:

$\mathrm{Enc}_{\mathrm{EF}_1}$ indistinguishable from a random permutation within 4 calls

- no differential or iterated attack of order 1 on 6 rounds
- weak keys for $\mathrm{ARK}_2 = \mathrm{ARK}_4 = \mathrm{ARK}_6 = 0$ (one out of 2^{192})
- exhaustive search on 80 keys within 22 years for 2^{56}bps possible
- no timing attacks (with constant-time implementations)
- no photofinishing attack (no bitslice)
- weak when reduced downto 4 rounds

Errata

Last lines of EES in the extended abstract (p. 9):

`78d56ced 94640d6e f0d3d37b e67008e1` <u>`86d1bf27 5b9b241d`</u>$_{\mathrm{x}}$
<u>`eb64749a`</u>$_{\mathrm{x}}$

Eq. (26) in the extended abstract (p. 8) and Eq. (22) in the full report (p. 9):

$$\mathrm{EES} = \mathrm{RT}(0)|\mathrm{RT}(1)|\ldots|\mathrm{RT}(63)|\underline{\mathrm{KD}|\mathrm{KC}}$$