Plaintext-dependant Repetition Codes Cryptanalysis of Block Ciphers - The AES Case

Eric Filiol*
ESAT/DEASR/SSI, B.P. 18, 35998 Rennes, FRANCE
eric.filiol@esat.terre.defense.gouv.fr

January 20, 2003

Abstract

This paper presents a new "operational" cryptanalysis of block ciphers based on the use of a well-known error-correcting code: the repetition codes. We demonstrate how to describe a block cipher with such a code before explaining how to design a new ciphertext only cryptanalysis of these cryptosystems on the assumption that plaintext belongs to a particular class. This new cryptanalysis may succeed for any block cipher and thus is likely to question the security of those cryptosystems for encryption. We then apply this cryptanalysis to the 128-bit key AES. Our results have been experimentallly confirmed with 100 **effective** cryptanalysis. Our attack enables to recover two information bits of the secret key with only 2^{31} ciphertext blocks and a complexity of $\mathcal{O}(2^{31})$ with a success probability of 0.68.

Keywords: AES, block cipher, cryptanalysis, coding theory, repetition codes.

1 Introduction

In October 2000, the NIST has selected Rijndaël as the *Advanced Encryption Standard* (AES) to replace the DES and extent it to a massive world-wide usage.

The growing dependence of the commercial community on AES -for its data security functions- make it desirable to keep under review the strength

*also INRIA, projet CODES, Domaine de Voluceau 78153 Le Chesnay Cédex, FRANCE *Eric.Filiol@inria.fr*

of this cryptographic standard. Although several interesting properties have been pointed out [7, 9, 13] and cryptanalysis proposed [4], none of them is thought to make it less secure than expected by its key size.

The evaluation of the AES, as well as for the other finalists [1], has been essentially based on the the former cryptanalysis or their variant forms: differential cryptanalysis [2], linear cryptanalysis [11], ... and no significative results were likely to question their strength. Finally we must admit that security consideration as a key point in the final choice was not so relevant as we could have imagined since all of the finalists offer a suitable high security. To quote Adi Shamir [15], "*any new real life cryptanalysis which may appear in the future will equally challenge the finalists*".

On the other hand, the future seems to favour block encryption, at least on the trade level. Few stream ciphers are known or proposed whereas meanwhile many block systems are proposed (17 block cipher systems for only 5 stream ciphers have been suggested for the *New European Schemes for Signature, Integrity and Encryption* (NESSIE) project [14]). As for the AES, only block ciphers were requested. Though we can strongly affirm that a very consequent theory for stream encryption exists, the block encryption theory does not provide more than a few cryptanalytic techniques and results on the constituent primitives at the round level. A rigorous and global description of formalization of a whole system, including a combinatorial approach in particular, is still to come. In other words, who can affirm that hiding a trap, for example, is totally impossible without being detected (this has still been more or less an open question for the DES; on the contrary, the answer is easy for the stream encryption); and what about the existence of particular global mask values on input and output which could drastically improve linear cryptanalysis techniques. The authors of AES acknowledge this second fact [5, Chap 7 and paragraph 2 of page 124], which moreover is also relevant for any cryptosystem.

Actually, most of cryptanalysis capacity depends on the ability of detecting these high correlations if there are some. In real-life cryptanalysis it is not so much the maximum average correlation potential that is relevant but the maximum correlation potential corresponding to the given key under attack [5]. Our experience in cryptanalysis shows us that very often it is more interesting and efficient to consider this potential when considering a particular class of plaintext. In case of block ciphers, this approach is particularly efficient since plaintext represents an active part in the production of the block cipher. This fact has recently been pointed out by the statistical analysis of the Algebraic Normal Form of Boolean functions modeling a block cipher [7].

In this paper we intend to introduce a new representation of block cipher cryptanalysis related to this approach. On the assumption that a given subset of plaintext space has been encrypted and that consequently, particular, higher correlation properties exist between only the resulting subset of ciphertexts and any key of the key space, we design an attack using repetition codes on ciphertext blocks only. This cryptanalysis is called *Plaintext-dependent Repetition Codes Cryptanalysis* (PDRC attack for short). It differs from a classical chosen-plaintext attack as we do not have to choose or even know any of the plaintext blocks. Moreover, a PDRC attack uses only ciphertext blocks. Thus the difficulty is to find suitable properties that leaks information about the key from the ciphertext. By using the combinatorial and statistical package *CoHS* (Combinatorics over Huge Sets) that we developped for the study of huge complex and discrete sets, we have managed to find such properties for several block ciphers and use them in a modified version of linear cryptanalysis. This paper presents the AES cryptanalysis. With the knowledge of only 2^{31} ciphertext blocks, we recovered two information bits on the key with a work factor of 2^{31} ciphertext-blocks readings and a probability of success of 0.68. Those results have been confirmed by 100 **effective** cryptanalysis we implemented. An additionnal set of 564 information bits is currently tested and should very likely allow to recover the complete key without requiring an exhaustive search step.

This paper is organized as follows. Section 2 presents theoretical preliminaries and notation. Then Section 3 details the formal model of the new cryptanalysis based on repetition codes. In particular we give a combinatorial resistance criterion against PDRC attack. Section 4 illustrates this approach by considering the AES. We give detailed experimental cryptanalysis results obtained with 100 cryptanalysis. Section 5 concludes while presenting open problems and future studies.

It is worth noticing and important to insist on the fact that this new AES cryptanalysis does not rely on a weakness or trap which could be declared as specific to it. We just use a "natural weakness" of block ciphers as explained in Section 3.1. Other block ciphers currently studied present the same weakness and are likely to succumb to this cryptanalysis. In fact, the suitability and the security of block ciphers for encryption must be questionned.

2 Background Theory and Notation

2.1 Repetition Codes

Let us consider a *Binary Symmetric Channel* (BSC) of parameter p used to transmit messages over a binary alphabet. Its transition probability matrix is the square matrix of order 2 whose coefficients are given by $a_{i,j} = q$ whenever $i \neq j$ and $a_{i,j} = q = 1 - p$ otherwise.

In other words, if an emitter sends bit b_t then $\hat{b}_t = b_t \oplus e_t$ will be effectively received with probability p (channel error probability). To recover from transmission errors one uses error-correcting codes and in particular linear codes. A binary linear code $[n, k, d]$ is a vector subspace of $\mathbb{F}_2^n$, of dimension k. Its *minimal distance* d is the minimum Hamming weight of all non zero codewords (that is to say the n-bit vectors). In other words $d = min_{x \in \mathbb{F}_2^n}\{wt(x)\}$ where $wt(x)$ denotes the number of non zero positions in $x = (x_1, \ldots, x_n)$. Then a well-known result [10] defines the number of errors on a codeword that can be corrected by a code of minimal distance d as $\frac{d-1}{2}$.

A n-repetition code, on a set of two symbols, is a $[n, 1, n]$ linear code and consists of two codewords, each one of them is made up of n identical symbols. Whenever $q > p$, maximum likelihood decoding (MLD) amounts to find out in the received vector which symbol is repeated most. The vector will be decoded as 0 if its Hamming distance to null vector is less than its distance to vector $(1, 1, 1, \ldots, 1)$, otherwise it is decoded as 1. Thus MLD reduces to majority decoding.

Example 1 *Let us consider the message* 01100 *and a 3-repetition code. Then the sequence* 000 111
111 000 000 *is transmitted. The sequence* 010111101110100 *is received and decoded as* 01110. *There is one residual error.*

These codes are the most easily decodable among codes ensuring a high protection. Moreover, repetition codes are the most efficient ones when dealing with high noise probability p [12].

Proposition 1 *[12] Let $n = 2s+1$. Then the n repetition code is correcting at most s errors and is a perfect code. Its bit error probability (residual decoding error) is given by*

$$P_{err} = \sum_{i=s+1}^{n} \binom{n}{i} p^i \cdot q^{n-i}. \tag{1}$$

The term *perfect* means that every words in the "ambient" space $\mathbb{F}_2^n$ is decodable for maximum likelihood as in a perfect block code. Finally the probability of successful decoding is given by

$$P_{succ} = 1 - P_{err}$$

It is worth noticing that if $p < \frac{1}{2}$ the $P_{err,2s+1}$ tends towards 0 as $s \to \infty$.

2.2 Block Ciphers and Linear Cryptanalysis

A block cipher working on m-bit plaintext blocks P_i with a n-bit secret key K ((m, n)-block cipher for short) is a mapping from $\mathbb{F}_2^m \times \mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Each time a given key K is chosen, the resulting mapping restriction is a permutation over $\mathbb{F}_2^m$. A block cipher is thus a set of 2^n permutations over $\mathbb{F}_2^m$. Note that it represents a very small subset of all these permutations ($(2^m)!$ in total).

Linear cryptanalysis [11] of block ciphers is a known plaintext attack in which a very large number of plaintext-ciphertext pairs are used to determine the value of a subset of key bits, thus greatly reducing the exhaustive search part.

A condition for applying linear cryptanalysis to such a block scheme is to find "effective", probabilistic linear expressions between any plaintext block P_i, any ciphertext block C_i and any key K of the form:

$$< P_i, u > \oplus < C_i, w > \stackrel{p}{\cong} < K, v > \tag{2}$$

where $< ., . >$ denotes the usual scalar product over $\mathbb{F}_2^m$. If this equation holds with a probability $p \neq \frac{1}{2}$ then by checking the left-hand side of Equation (2) for a large number N of plaintext-ciphertext pairs, the right-hand side of this equation may be guessed by a simple maximum likelihood decoding. A single information bit about the key is obtained. This cryptanalysis is effective if the deviation $|p - \frac{1}{2}|$ is large enough. In [11], it is shown that the probability of successful guessing is very small as soon as $N > |p - \frac{1}{2}|^{-2}$.

Generally the linear approximation described by Equation (2) is obtained by "chaining" single-round linear approximations obtained by considering statistical biases in the constituent primitives. This implies that other, possibly higher correlations that are depending on the global structure of the systems are out of analysis capabilities [5, Chap 7 and paragraph 2 of page 124].

3 Repetition Codes Cryptanalysis of Block Ciphers

3.1 Block Ciphers and Repetition Codes

Let us consider a given property $\mathcal{I}$ and let us denote $P_{\mathcal{E}}[\mathcal{I}]$ the probability of $\mathcal{I}$ to be satisfied on set $\mathcal{E}$. Then a block cipher can be broken if we have, for some $\mathcal{I}$, $P_{\mathbb{F}_2^{m+n}}[\mathcal{I}] \neq \frac{1}{2}$.

Each key K in the key space $\mathcal{K} = \mathbb{F}_2^n$ selects a corresponding permutation over $\mathbb{F}_2^m$. Thus K may be recover if $P_{\mathbb{F}_2^m}[\mathcal{I}_K] \neq \frac{1}{2}$ where $\mathcal{I}_K$ denotes the property $\mathcal{I}$ related to the key K. Then we may dispose of an attack if we can exhibit such a property verified for any $K \in \mathcal{K}$ (denoted $\mathcal{I}_{\mathcal{K}}$). For linear cryptanalysis, $\mathcal{I}_{\mathcal{K}}$ is a particular linear probabilistic equation.

Let us now consider the plaintext space $\mathcal{P} = \mathbb{F}_2^m$ and a partition $(\mathcal{P}_i)_{i<2^k}$ of $\mathcal{P}$ for some $k \in \mathbb{N}$. Without loss of generality we suppose that $|\mathcal{P}_i| = 2^{m-k}$ for all i. Now suppose there exists (possibly many) $\mathcal{P}_i$ such that $\mathcal{I}_{\mathcal{P}_i}[\mathcal{I}_{\mathcal{K}}] = p_i \neq \frac{1}{2}$. Since the encryption key $K \in \mathcal{K}$ remains the same for all the plaintext blocks, we may compare the encryption process as a Binary Symmetric Channel (BSC) with parameter p_i where the noise is produced by the plaintext blocks from $\mathcal{P}_i$ (see Figure 1). The BSC is directly and closely determined by $\mathcal{P}_i$. The noisy version $\widehat{\mathcal{I}_K}$ of $\mathcal{I}_K$ is a (possibly complex)

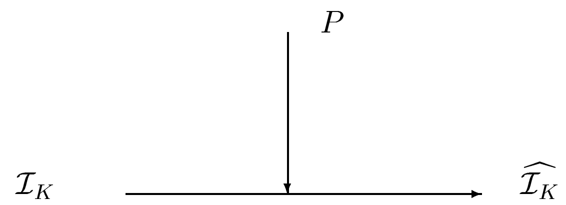

Figure 1: Block Cipher and Binary Symmetric Channel

function $f(C)$ of ciphertext blocks C. In other words encrypting N plaintext blocks $P \in \mathcal{P}_i$ may be equivalently defined as transmitting $\mathcal{I}_K$ by means of a N repetition code through a BSC of parameter p_i. From Figure 1, it means that over $\mathcal{C}_i$ we have $P[\mathcal{I}_K = \widehat{\mathcal{I}_K}] = 1 - p_i$.

The aim of the designer is to obtain a set of permutations over $\mathcal{C}$ such that no obvious properties $\mathcal{I}$ leaks information about the key. But the situation is likely to be very different when considering a restriction to a subset $\mathcal{C}_i \subsetneq \mathcal{C}$. If we have

$$P_{\mathcal{C}}[\mathcal{I}] = \sum_{i=0}^{2^k} P_{\mathcal{C}_i}[\mathcal{I}] \cdot P[\mathcal{C}_i] = \frac{1}{2}$$

we however may have many $P_{\mathcal{C}_i}[\mathcal{I}]$ different from $\frac{1}{2}$ (it suffices that $\sum_i \epsilon_i = \sum_i (p_i - \frac{1}{2}) = 0$). This fact seems to be partly explained by the fact that the actual number of permutations over $\mathcal{C}$ effectively represented by a block cipher is extraordinary negligible compared of the total number of permutations over the same plaintext space.

3.2 Description of the PDRC Attack

With the setting defined in the previous section, we now can describe the plaintext-dependent repetition code cryptanalysis, very simply. Note, once again, that local independance from the plaintext (due to the restriction to a particular subset $\mathcal{C}_i \subsetneq \mathcal{C}$) allows us to design a **ciphertext only attack**. We first present Algorithm A.1 which uses only one repetition code.

Input: *N (N odd) ciphertext blocks C_j encryted by key K from plaintext $P_j \in \mathcal{C}_i$ ($1 \leq j \leq N$) and a probabilistic information $\mathcal{I}_{\mathcal{K}}$ such that $\mathcal{I}_{\mathcal{K}} \overset{p_i}{\cong} f(C_j)$ for some g and for all j.*
Output: *Exact value $\mathcal{I}(K)$ for the actual key.*

1. *Initialize counter $ct \leftarrow 0$.*
2. *For each of the N ciphertext blocks C_j*
   (a) *Compute $f(C_i)$.*
   (b) *If $f(C_i) = 1$ then $ct++$.*
3. *end for*
4. *If $ct \geq \frac{N+1}{2}$ then $\mathcal{I}(K) = 1$ else $\mathcal{I}(K) = 0$.*

Complexity of algorithm A.1 is easy to evaluate. It performs only N evaluations of f. Thus complexity is $\mathcal{O}(N)$. Since N is the length of the repetition code, according to Section 2.1, it depends only on p_i and p_{succ}, the probability of successful guessing for $\mathcal{I}(K)$.

To the knowledge of the author there does not exist a general formula for N directly from parameters p_i and p_{succ}. We can only tabulate results for fixed values of them. It is a well-known fact that for a fixed p_i, p_{succ} increases with N.

Example 2 *Let us consider $p_i = 0.49999$. Then $p_{succ} = 0.501784$ for $N = 49999$ while $p_{succ} = 0.5025$ for $N = 99999$.*

In order to obtain a as high as possible probability of success, we designed a second algorithm A.2 which uses *concatenated repetition codes*. The concatenation codes have been in introduced by Forney in 1966 [8] and generalized by Zinov'ev in 1976 [16]. The principle is to use two codes as depicted in Figure 2. The combination of inner encoder, channel and outer decoder can

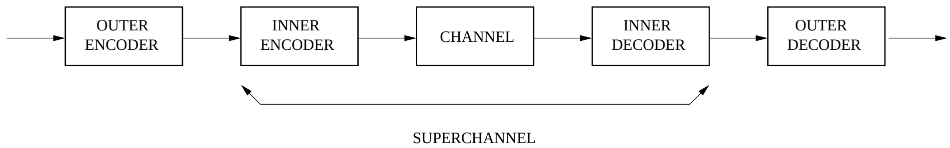

Figure 2: A Concatenated Code

be thought of as forming a new channel (called a *superchannel*). The aim is to improve the correcting capacity of the inner code by use of a second code. When transmitting over a very noisy channel, repetition codes are suitable outer codes in classical concatenated codes.

In our cryptanalytic case, the superchannel is a BSC with parameter $p' = 1 - P_{\text{succ}}$ produced by the inner decoding residual error. We then iterate the decoding process on this superchannel with an outer repetition code. Here is the algorithm A.2 whose complexity is in $\mathcal{O}(N_1 \cdot N_2)$:

Input: *$N_1 \cdot N_2$ (N_1, N_2 odd) ciphertext blocks C_j encryted by key K from plaintext $P_j \in \mathcal{C}_i$ ($1 \leq j \leq N$) and a probabilistic information $\mathcal{I}_\mathcal{K}$ such that $\mathcal{I}_\mathcal{K} \overset{p_i}{\cong} f(C_j)$ for some g and for all j.*
Output: *Exact value $\mathcal{I}(K)$ for the actual key.*

1. *Initialize counter $ct1 \leftarrow 0$.*
2. *For $1 \leq k \leq N_1$*
   (a) *Initialize counter $ct2 \leftarrow 0$.*
   (b) *For each of the N_2 ciphertext blocks C_j (k-th set)*
      i. *Compute $f(C_i)$.*
      ii. *If $f(C_i) = 1$ then $ct2 ++$.*
   (c) *end for*
   (d) *if $ct2 \geq \frac{N_2+1}{2}$ then $\mathcal{I}(K) = 1$ else $\mathcal{I}(K) = 0$.*
3. *If $\mathcal{I}(K) = 1$ then $ct1 ++$.*

4. *end for*
5. *If* $ct1 \geq \frac{N_1+1}{2}$ *then* $\mathcal{I}(K) = 1$ *else* $\mathcal{I}(K) = 0$.

While generally concatenated codes yield a better probability of success, it is not the case when the outer and inner codes are both repetition codes.

Proposition 2 *Let N an odd number of ciphertext blocks. Algorithm A.1 has a higher probability of success than Algorithm A.2.*

The proof is given in Appendix C. However the concatenated code approach allow us to compute a lower bound of A.1 success probability. The general Formula (1) cannot be computed directly as soon as N is too large.

3.3 Resistance Criterion against PDRC Attack

PDRC attack is possible if and only if there exists a subset $\mathcal{C}_i \subset \mathcal{C}$ such that $P_{\mathcal{C}_i}[\mathcal{I}_{\mathcal{K}}] \neq \frac{1}{2}$ for some property $\mathcal{I}$. This allow us to formulate the following resistance criterion against PDRC Attack.

Proposition 3 *Let S be a (m, n) block cipher and let us consider a property $\mathcal{I}$ about the key bits relatively to the ciphertext bits. S is immune against the PDRC attack relatively to property $\mathcal{I}$ if and only if $\forall j \in \mathbb{N}$ the partition $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_j)$ of $\mathcal{C}$ is such that*

$$\forall k \leq j, \quad P_{\mathcal{C}_k}[\mathcal{I}] = \frac{1}{2}.$$

The cryptanalyst's work is to find a exploitable property $\mathcal{I}$ and a particular subset of "meaningful" plaintext blocks in order to conduct PDRC attack on S. On cryptographer's side things may be far more difficult. This difficulty is summarized with the four open problems here following.

3.3.1 Open Problems

1. *PDRC immunity problem* .- Given a property $\mathcal{I}$, is it possible to design a system S which is PDRC-immune relatively to $\mathcal{I}$?
2. *Weak trap problem* .- Given $\mathcal{C}_i \subset \mathcal{C}$, is it possible to design a system S such that $P_{\mathcal{C}_i}[\mathcal{I}] \neq \frac{1}{2}$ for some interesting $\mathcal{I}$ (the trap) ?
3. *Strong trap problem* .- Given $\mathcal{I}$ a property, is it possible to design a system S such that for all $\mathcal{C}_i \subset \mathcal{C}$ we have $P_{\mathcal{C}_i}[\mathcal{I}] \neq \frac{1}{2}$?

4. <u>*PDRC feasibility*</u> .- Given S a system and $\mathcal{C}_i$ a plaintext subset, is it possible to find some property $\mathcal{I}$ suitable for PDRC attack of S.

Problems 2 and 3 mean that it would be possible to hide a trap $\mathcal{I}$ in the system S.

Conjecture 1 *There always exists a property $\mathcal{I}$ for which any block cipher system S is not PDRC-immune.*

If true, this means that block ciphers are insecure systems.

Problem 4 is clearly the most important to solve, from cryptanalyst's point of view. In order to try to solve it, we used the combinatorial, statistical package *CoHS*[1] (Combinatorics over Huge Sets) that we developped to find structural properties in complex sets of huge size. It is a non public package up to now being still under development. With *CoHS*, a (m, n) block cipher is seen as a family of 2^{m+n} m-bit blocks where each of the block is repeated 2^n times. For PDRC attack, it aims at finding particular structures between blocks for given subsets. Then identified structures may be eventually turned into statistical properties. The main advantage of this package is that it does not require to build the whole family but only a subset of a reasonable size. CoHS's theoretical aspects should be published in the near future as soon as its development is frozen and patenting process is completed.

4 The AES Cryptanalysis

We will not recall the structure of the AES since we do not exploit it. Interested reader will find a complete description as well as technical details in [5]. Once again, we point out that the AES is not weaker than other block ciphers for PDRC attack. Other systems are under current study and first results have exhibited the same weaknesses. We just choose the AES as a "fashion" block cipher to illustrate PDRC attack. The bit notation in AES encryption are given in Appendix A.

4.1 The Repetitition Codes for the AES

The main problem is then to find a suitable property $\mathcal{I}_{\mathcal{K}}$ presenting a bias for a subset $\mathcal{C}_i \subset \mathcal{C}$ of particular interest. The idea has been to tune *CoHS*

[1] In fact, *CoHS* is a subpackage of the cryptanalytic package *VAUBAN*, that has been developped for operational cryptanalysis purposes of symmetric cryptosystems and hash functions. *VAUBAN*'s status is up to now not fixed yet.

in order to work on a linear cryptanalysis basis. In this case, we need to have an approximation of the form:

$$< P, u > \oplus < C, w > \overset{q}{\cong} < K, v >$$

where u, v and w are masks used for bit selection. If we manage to find a subset $\mathcal{C}_i$ for which there exists $v', w' \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ such that

$$< C, w' > \overset{q'}{\cong} < K, v' > \tag{3}$$

with $q' \neq \frac{1}{2}$ then we get a property $\mathcal{I}_\mathcal{K}$ suitable to be used as a repetition code.

Let $(x_8, x_7, \ldots, x_1)$ denote an octet. We choose to work with plaintext in English language in ASCII coding that is to say when most significant bit x_8 of each 8-bit character is zero or when bit x_5 is zero. Thus we considered the two following plaintext subsets (all mask values are written in hexadecimal; the second set corresponds to a particular encoding of the English language):

$$\mathcal{C}_i = \{C_j \& 7F7F7F \ldots 7F7F7F7F7F7F7F7F7F7F | C_j \in \mathbb{F}_2^{128}\}$$

$$\mathcal{C}_i = \{C_j \& EFEFEF \ldots EFEFEFEFEFEFEFEFEFEF | C_j \in \mathbb{F}_2^{128}\}$$

Then we tried to find pairs of mask values (v', w') yielding equation of the form (3). *CoHS* package has been run during four months on four ATHLON XP2000+ PC with 512 Mo RAM and 80 Go HD. We tuned the parameter in order to obtain values w' of weight as low as possible (mainly to reduce the computing time and produce a few first results). Up to now two equations for mask $0xEFEFEFEF\ldots$ have been produced and confirmed as suitable with 100 cryptanalysis (in fact 27 equations have been produced each of them having a cryptanalysis probability of success ranging from 0.68 to 0.88. Only the mentionned one produced a joint probability large enough) but *CoHS* is still running and an additionnal set of 564 equations has been produced (mask values w' have higher weight; both for masks $7F7F7F\ldots$

and $0xEFEFEFE\ldots$) and are currently tested by 100 more cryptanalysis:

$$
\begin{aligned}
1 \oplus c_{71} \quad = \quad & k_2 \oplus k_3 \oplus k_4 \oplus k_6 \oplus k_7 \oplus k_8 \oplus k_9 \oplus k_{10} \oplus k_{12} \oplus k_{13} \\
& \oplus k_{15} \oplus k_{17} \oplus k_{20} \oplus k_{24} \oplus k_{25} \oplus k_{30} \oplus k_{33} \oplus k_{36} \oplus k_{43} \\
& \oplus k_{44} \oplus k_{45} \oplus k_{47} \oplus k_{48} \oplus k_{49} \oplus k_{50} \oplus k_{53} \oplus k_{54} \oplus k_{56} \\
& \oplus k_{60} \oplus k_{63} \oplus k_{66} \oplus k_{67} \oplus k_{68} \oplus k_{71} \oplus k_{72} \oplus k_{73} \oplus k_{74} \\
& \oplus k_{76} \oplus k_{78} \oplus k_{80} \oplus k_{81} \oplus k_{82} \oplus k_{83} \oplus k_{86} \oplus k_{87} \oplus k_{96} \\
& \oplus k_{97} \oplus k_{98} \oplus k_{99} \oplus k_{100} \oplus k_{101} \oplus k_{103} \oplus k_{104} \oplus k_{105} \oplus k_{106} \\
& \oplus k_{107} \oplus k_{109} \oplus k_{111} \oplus k_{112} \oplus k_{116} \oplus k_{117} \oplus k_{118} \oplus k_{122} \oplus k_{123} \\
& \oplus k_{126}
\end{aligned}
$$

which holds with probability $p = 1 - 0.499971 = 0.500029$ and

$$
\begin{aligned}
c_{19} \quad = \quad & k_0 \oplus k_4 \oplus k_{11} \oplus k_{13} \oplus k_{14} \oplus k_{16} \oplus k_{17} \oplus k_{18} \oplus k_{19} \oplus k_{20} \\
& \oplus k_{21} \oplus k_{23} \oplus k_{24} \oplus k_{25} \oplus k_{27} \oplus k_{31} \oplus k_{32} \oplus k_{33} \oplus k_{34} \\
& \oplus k_{35} \oplus k_{37} \oplus k_{38} \oplus k_{39} \oplus k_{40} \oplus k_{46} \oplus k_{47} \oplus k_{49} \oplus k_{50} \\
& \oplus k_{51} \oplus k_{53} \oplus k_{54} \oplus k_{55} \oplus k_{56} \oplus k_{58} \oplus k_{61} \oplus k_{63} \oplus k_{66} \\
& \oplus k_{67} \oplus k_{68} \oplus k_{69} \oplus k_{70} \oplus k_{71} \oplus k_{72} \oplus k_{74} \oplus k_{75} \oplus k_{81} \\
& \oplus k_{82} \oplus k_{83} \oplus k_{84} \oplus k_{85} \oplus k_{86} \oplus k_{87} \oplus k_{88} \oplus k_{89} \oplus k_{100} \\
& \oplus k_{103} \oplus k_{106} \oplus k_{109} \oplus k_{110} \oplus k_{111} \oplus k_{113} \oplus k_{115} \oplus k_{117} \oplus k_{119} \\
& \oplus k_{121} \oplus k_{123}
\end{aligned}
$$

which holds with probability $p = 1 - 0.499972 = 0.500028$.

As *CoHS* does not provide the exact probability of the resulting equation but only potential weak associate structures, we apply statistical tests to evaluate it, and to confirm *CoHS* hypothesis. Detailed statistical testing protocol is given in Appendix B. However it is important to keep in mind that equations have been first deterministically produced by *CoHS*) and only then statistically tested before implementing the final cryptanalysis. Only a subset of equations yielding the best joint probability has been kept but ALL equations produced by *CoHS* have presented effectively and individually high cryptanalysis probability of success (between 0.68 and 0.88). In order to be precise, we did not test equations produced by *CoHS* and keep only the best individual ones.

Now it is important to explain how equations of the form of Equation (3) may work. On the whole ciphertext space these equations are normally permutations and they hold with exact probability $\frac{1}{2}$ (since they are linear equations) when the considered block cipher is well designed (which is the case for most of them). This is verified for any key and thus for any permutation.

But at local level, that is to say when considering ciphertext blocks produced from a plaintext subset, this equation does not generally hold with exact probability $\frac{1}{2}$. This fact can be explained as follows. Any (m, n)-block cipher may be described as a Boolean function f_j over ${\mathbb{F}_2}^{m+n}$ relatively to each of its output bits $j, 0 \leq j < m$. Let now consider a given partition $(\mathcal{C}_i)_{1 \leq i \leq 2^k}$ of the whole plaintext space $\mathbb{F}_2^m$. We suppose that any $\mathcal{C}_i$ contains 2^{n-k} elements. On that whole space we have

$$P[< K, v >= f_j(K)] = \frac{1}{2}$$

thus for any $v \in \mathbb{F}_2^n$ and any j. But since we have

$$P[< K, v >= f_j(K)] = \sum_i \frac{1}{2^k} \cdot P[f_{j,\mathcal{C}_i}(K) =< K, v >]$$

where $f_{j,\mathcal{C}_i}$ is the restriction of f_j on $\mathcal{C}_i$, we may very likely have a few $\mathcal{C}_i$, if not all, such that $P[f_{j,\mathcal{C}_i}(K) =< K, v >] \neq \frac{1}{2}$. This fact has been implicitly ackowledged by the AES designers [5, Chap 7 and paragraph 2 of page 124]. A toy permutation is presented as an example in Appendix D to illustrate this local effect.

From a design point of view, this implies that chaining block cipher primitives (in Feistel ciphers or SP-networks) will likely result in uncontrollable, unsuspected structural biases in the whole structure of the system.

4.2 Simulation Results

From these probability and Formula (1) we obtain the suitable repetition parameter N and hence the number of required ciphertext blocks. The following parameter have been taken for our attack using Algorithm A.1 :

$$N = 2500100001 \cong 2^{31} \qquad P_{\text{succ}} \geq 0.7875.$$

The attack described in Algorithm A.1 has been implemented for 100 different, randomly chosen keys. The plaintext has been randomly generated too and bit selected according to mask value corresponding to English language in ASCII coding. Each experiment took 7 hours on four ATHLON XP 2000+ PC. Most of the time has been spent for plaintext generation.

The experimental probability of success over the 100 cryptanalysis for each of the two equations is 0.72 (while the 25 remaining equations provides high probability of success too). This is slightly lower that expected.

This probably comes from the difference between the empirical and exact approximation probabilites for the equations.

But the most noticeable result is that the actual probability of success for the two equations to hold is 0.68 (joint probability). On the assumption that these equations are independent we should observe a joint success probability of 0.5184 instead. This means that the two equations are not independant at all and somehow existence of structural biases is confirmed. Other sets of such equations offering such a high joint bias are under testing.

5 Future Work and Conclusion

In this paper we have presented a new cryptanalysis of block cipher by means of a N repetition code where N is precisely the number of ciphertext blocks we need. We experimentally confirmed the expected results with 100 **effective** cryptanalysis. The attack managed to recover two information bits with only 2^{31} ciphertext block and success probability of 0.68.

The search for other equations, in particular involving several ciphertext bits, is under way and will very likely allow to find additional information bits on the secret key with the same complexity (in other word the number of ciphertext blocks). An additionnal set of 564 information bits will very likely suppress the remaining exhaustive search step. First results are excellent and complete equations will be published as soon as 100 more **complete, effective** cryptanalysis are completed.

In parallel, this attack is currently applied to other block ciphers, in particular Serpent, Twofish and DFC. The first results seem to be very promising. Other block ciphers may likely succumb to this attack as well.

At last, a slightly modified version of *CoHS* should allow to greatly reduce the number N of ciphertext blocks we need for PDRC-attack and thus provide a far more operationnal extent while increasing the success probability.

The results presented in this paper should likely cast a shadow on block ciphers in the future and challenge their suitability for data encryption and more generally for cryptgraphic use.

Acknowledgement

I would like to thank Don Coppersmith who helped me very much to improve the technical quality of the paper. He detected some typos and above all

helped me to clarify some points that effectively needed to be explained. I am sure that much work still need to be done for that.

References

[1] http://www.nist.gov/aes

[2] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, *Journal of Cryptology*, Vol. 4, No 1, 1991, pp. 3-72.

[3] P. Camion, Majority Decoding of Large Repetition Codes for the R-ary Symmetric Channel. In: *Proceedings of the AAECC'88 Conference*, Lecture Notes in Computer Science 357, pp 458–466, Springer Verlag, 1989.

[4] N. Courtois, J. Pieprzyk, Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, *Advances in Cryptology - ASIACRYPT 2002*, Lecture Notes in Computer Science 2501, Springer Verlag, 2002.

[5] J. Daemen, V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer Verlag, 2002.

[6] W. Feller, *An Introduction to Probability Theory*, Wiley, 1966.

[7] E.Filiol, A New Statistical Testing for Symmetric Ciphers and Hash Functions, in *Proceedings of ICICS 2002*, Lecture Notes in Computer Sciences 2513, Springer, 2002.

[8] G.D. Forney, *Concatenated Codes*, M.I.T Press, Cambridge MA, 1966.

[9] J. Fuller, W. Millan, *On Linear Redundancy in the AES S-Box*, , IACR preprint 111, 2002. Available at *http://eprint.iacr.org/2002/111.ps.*

[10] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[11] M. Matsui, Linear Cryptanalysis Method for DES Cipher, in: *Advances in Cryptology - Eurocrypt'93*, Lecture Note in computer Science 765, pp 386–397, Springer Verlag, 1994.

[12] R. McEliece, *The Theory of Information and Coding*, Addison Wesley, 1977.

[13] S. Murphy and M.J.B. Robshaw, Essential Algebraic Structure within the AES. In: M. Yung, editor, *Advances in Cryptology - CRYPTO 2002*, Lecture Notes in Computer Science 2442, pp 1–16, Springer Verlag, 2002.

[14] *http://www.cryptonessie.org*

[15] Adi Shamir, *Third AES Conference*, New York, 2000.

[16] V.A. Zinov'ev, Generalized Concatenated Codes, *Problemy Peredachi Informatsii*, Vol. 12, No 1, pp. 5-15, 1976.

A Detailed Notation for the AES

We take the first test vector of the file *ecb_tbl.txt* provided by the AES designers, in order to precise the notation we use for the attack.

$$K = 00010203050607080A0B0C0D0F101112$$

Leftmost key bit is denoted k_0 and rightmost key bit is denoted k_{127}. Hence we have

$$K = (k_0, k_1, \ldots, k_{126}, k_{127})$$

In other words for the test key here given we have $k_0 = 0, k_{126} = 1, k_{127} = 0$.

The same bit ordering is considered for plaintext and ciphertext blocks.

$$P = 506812A45F08C889B97F5980038B8359$$

$$C = D8F532538289EF7D06B506A4FD5BE9C9$$

The particular set of plaintext we consider are then defined by

$$p_i = 0 \quad \forall 0 \leq i \leq 127 \text{ and } i \equiv 0 \bmod 8$$

B Optimized Evaluation of Correlation Probabilities

Let be a probabilistic equation $f(x) = b$ which holds with unknown probability p. We only know that $p \neq \frac{1}{2}$. Our aim is to guess an accurate enough value p_0 of p. How many random values x must be taken in order to compute p_0 such that $\frac{p_0}{p}$ is as close as possible to 1. Note that considering the ratio rather than the difference between p_0 and p is more significant.

Let us now consider the Bernouilli random variable X_i of parameter p corresponding to the equation evaluation result when taking value x_i:

$$X_i = \begin{cases} 1 & \text{if } f(x_i) = b \\ 0 & \text{otherwise} \end{cases}$$

Let us note $S_N = \sum_{i=1}^{N} X_i$. It is a known result that S_N has a Gaussian distribution $\mathcal{N}(N \cdot p, \sqrt{N \cdot p \cdot q})$ with $q = 1 - p$. Let us now note $\widehat{S_N} = S_N \times \frac{1}{N \cdot p}$. Its mena value is given by:

$$E[\widehat{S_N}] = E[S_N \times \frac{1}{N \cdot p}] = \frac{1}{N \cdot p} \times N \cdot p = 1$$

since $N \cdot p$ is an unknown but constant value. In the same way, we have for the variance:

$$V[\widehat{S_N}] = \frac{q}{N \cdot p}.$$

Evaluating p amounts to find α and N such that, for a fixed ϵ,

$$\alpha = P[1 - \epsilon \leq \widehat{S_N} \leq 1 + \epsilon] \text{ is maximal}$$

By using the following equality:

$$P[1 - \epsilon \leq \widehat{S_N} \leq 1 + \epsilon] = 2 \cdot \Phi^* \left(\frac{\epsilon}{\sqrt{\frac{q}{N \cdot p}}} \right) - 1$$

where $\Phi^*(.)$ denotes the Gaussian cumulative density function , we obtain N for fixed α and ϵ.

In order to evaluate the probability p of equations we considered, we fixed $\epsilon = 10^{-4}$ and $\alpha = 0.9999$. Then $N = 1,520,000,000$.

Each equation has been tested with N different keys on the assumption that plaintext was English in ASCII coding ($0xEFEFEF\ldots$ and $0x7F7F\ldots$ classes). It is important to note that the random generation of key *and* plaintext before applying either of the two possible maskin values has been done by means of a high quality random generator (not that of the C language which is very poor). Moreover SHA-1 has been applied to the random values before in order to prevent unsuspected biases (debiasing techniques). I hope that other people will reproduce these testing and confirmed the results.

C Proof of Proposition 2

Let us write $N = N_1 \cdot N_2$ where N_1 and N_2 are odd integers. Since Algorithm A.1 uses a $[N, 1, N]$ repetition code, its correcting capacity is given by $\frac{N-1}{2} = \frac{(N_1 \cdot N_2 - 1}{2}$.

Suppose now that in Algorithm A.2, the superchannel's code is a $[N_1, 1, N_1]$ repetition code. It can correct at most $\frac{N_1-1}{2}$ errors. The $[N_2, 1, N_2]$ outer repetition code will then correct at most $\frac{N_2-1}{2}$. Consequently the maximum number of errors that can be corrected by the resulting concatenated code is $\frac{(N_1-1)(N_2-1)}{4}$. It is easy to verify that

$$\frac{(N_1 \cdot N_2) - 1}{2} > \frac{(N_1 - 1)(N_2 - 1)}{4}$$

hence the result.

D Toy Permutation with Local Bias

Let f be the permutation over $\mathbb{F}_2^8$ given by

```
(215, 100, 200, 204, 233, 050, 085, 196,
 071, 141, 122, 160, 093, 131, 243, 234,
 162, 183, 036, 155, 004, 062, 035, 205,
 040, 102, 033, 027, 255, 055, 214, 156,
 075, 163, 134, 126, 249, 074, 197, 228,
 072, 090, 206, 235, 017, 022, 049, 169,
 227, 089, 016, 005, 117, 060, 248, 230,
 217, 068, 138, 096, 194, 170, 136, 010,
 112, 238, 184, 189, 176, 042, 225, 212,
 084, 058, 175, 244, 150, 168, 219, 236,
 101, 208, 123, 037, 164, 110, 158, 201,
 078, 114, 057, 048, 070, 142, 106, 043,
 232, 026, 032, 252, 239, 098, 191, 094,
 059, 149, 039, 187, 203, 190, 019, 013,
 133, 045, 061, 247, 023, 034, 020, 052,
 118, 209, 146, 193, 222, 018, 001, 152,
 046, 041, 091, 148, 115, 025, 135, 077,
 254, 147, 224, 161, 009, 213, 223, 250,
 231, 251, 127, 166, 063, 179, 081, 130,
 139, 028, 120, 151, 241, 086, 111, 000,
 088, 153, 172, 182, 159, 105, 178, 047,
```

```
051, 167, 065, 066, 092, 073, 198, 211,
245, 195, 031, 220, 140, 076, 221, 186,
154, 185, 056, 083, 038, 165, 109, 067,
124, 226, 132, 053, 229, 029, 012, 181,
121, 024, 207, 199, 177, 113, 030, 080,
003, 097, 188, 079, 216, 173, 008, 145,
087, 128, 180, 237, 240, 137, 125, 104,
015, 242, 119, 246, 103, 143, 095, 144,
002, 044, 069, 157, 192, 174, 014, 054,
218, 082, 064, 210, 011, 006, 129, 021,
116, 171, 099, 202, 007, 107, 253, 108)
```

and let us note the input $x = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$ and the output $f(x) = y = (y_7, y_6, y_5, y_4, y_3, y_2, y_1, y_0)$. Now let us consider the restriction of f when $(x_7, x_6, x_5, x_4) = (1, 1, 1, 0)$. The we have for this particular subset of inputs

$$P[x_0 \oplus x_3 = y_0] = \frac{5}{16} \neq \frac{1}{2}$$

and

$$P[x_0 \oplus x_3 = y_0 \oplus y_1] = \frac{5}{8} \neq \frac{1}{2}.$$