A New Linear Distinguisher for Four-Round AES

Tomer Ashur[1] and Erik Takke[2]

[1] Cryptomeria, Leuven, Belgium, tomer@cryptomeria.tech
[2] Eindhoven University of Technology, Eindhoven, The Netherlands, e.c.takke@tue.nl

Abstract. In SAC'14, Biham and Carmeli presented a novel attack on DES, involving a variation of Partitioning Cryptanalysis. This was further extended in ToSC'18 by Biham and Perle into the Conditional Linear Cryptanalysis in the context of Feistel ciphers. In this work, we formalize this cryptanalytic technique for block ciphers in general and derive several properties. This conditional approximation is then used to approximate the $\texttt{inv} : GF(2^8) \to GF(2^8) : x \mapsto x^{254}$ function which forms the only source of non-linearity in the AES. By extending the approximation to encompass the full AES round function, a linear distinguisher for four-round AES in the known-plaintext model is constructed; the existence of which is often understood to be impossible. We furthermore demonstrate a key-recovery attack capable of extracting 32 bits of information in 4-round AES using $2^{125.62}$ data and time. In addition to suggesting a new approach to advancing the cryptanalysis of the AES, this result moreover demonstrates a caveat in the standard interpretation of the Wide Trail Strategy — the design framework underlying many SPN-based ciphers published in recent years.

Keywords: Conditional Linear Cryptanalysis · AES · Statistical Distinguisher

1 Introduction

In 1992, Matsui and Yamagishi [MY92] presented a novel cryptanalytic method for block ciphers, which was later generalized by Matsui [Mat93] and named Linear Cryptanalysis. When used to analyze a block cipher, this method is concerned with discovering bits in the input and output of the cipher that are the same with high probability for almost all keys [Dae95, HN11, Mat93]. When such bits are found, one can launch an attack against the cipher, *e.g.* Matsui's Algorithm 1 and 2 key-recovery attacks.

This method has become a staple in the cryptanalysis of block ciphers and has influenced their design ever since. This includes the *Rijndael* cipher [DR20], which went on to become the *Advanced Encryption Standard* (AES) [DBN+01] in 2000. This cipher attempts to thwart standard linear cryptanalytic attacks by means of the *Wide Trail Strategy* (WTS) [DR01], the framework underlying its design. Following Rijndael's standardization as AES in 2000, the WTS has seen more widespread use, for example in the block ciphers Fides [BBK+13] and LED [GPPR11], and the hash-function Photon [GPP11]. It introduces non-linear behavior in a cipher by means of small non-linear s-boxes and forces any linear trail to activate many of those. By choosing the number of rounds for a cipher such that the correlation contribution of any trail is sufficiently small, the WTS argues that a cipher then becomes resistant to standard linear cryptanalytic attacks. Extending this argument to AES yield that four rounds can withstand these attacks.

However, Linear Cryptanalysis has been a field of close study, which has led to the inception of a large number of extensions. For this work, we highlight *conditional linear cryptanalysis* [BP18] and an unnamed predecessor presented in [BC14]. Both of these techniques partition the plaintext-ciphertext space and manage to increase the correlation

of a linear approximation by only considering the data from some parts of the partition; the techniques differ in their partition construction method. Note that these techniques should not be confused with *partitioning cryptanalysis* [HM97], which also constructs a partition, but attempts to extract information about the key using the *sizes* of the parts instead.

1.1 Organization and Our Contribution

Section 2 commences by stating the notation used throughout this work and necessary core concepts. We attempt to generalize conditional cryptanalysis for any block cipher and derive several properties in Section 3. By applying this technique to the AES s-box in Section 4, we demonstrate that it is capable of achieving a 2^{-1} correlation using only a quarter of the data, where the correlation magnitude of traditional linear approximations is known to be upper bounded by 2^{-3}. In Section 5, this approximation is then extended to the full AES round function, yielding a 2^{-16} correlation with all sixteen s-boxes active. When combined with a 3-round linear trail, this forms a novel statistical distinguisher for four-round AES. We furthermore demonstrate how in the known-plaintext model this distinguisher can be exploited to extract a minimum of 32 bits of the key using $2^{125.62}$ data. Since this complexity is beyond reach, our empirical validation breaks the approximation into smaller parts and verifies each of them separately. A discussion of the implications of these attacks for the WTS are then provided in Section 6 together with directions for future work and concluding words.

2 Preliminaries

2.1 Notation

Let $\mathbb{F}_{2^m}$ denote the finite field on 2^m elements. When $m = 1$, we use 0 and 1 to denote the elements in the group underlying $\mathbb{F}_2$ and refer to them as *bits*; elements in $\mathbb{F}_{2^8}$ are referred to as *bytes*. Bit-strings of length m are used to represent elements in $\mathbb{F}_{2^m}$. Hexadecimal notation is used to shorten the notation of these bit strings, *e.g.* we represent the element $\mathtt{10100111_b} \in \mathbb{F}_{2^8}$ as $\mathtt{A7_x}$. The binary operation $\oplus : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ represents addition on this field, which is commonly known as the *XOR* operation.

The n-dimensional vector space over $\mathbb{F}_{2^m}$ is denoted by $\mathbb{F}_{2^m}^n$. For a vector $v \in \mathbb{F}_{2^m}^n$, $v_i \in \mathbb{F}_{2^m}$ is used to indicate its ith coefficient, with $1 \leq i \leq n$. The binary operation $\oplus : \mathbb{F}_{2^m}^n \times \mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n : a, b \mapsto (a_1 \oplus b_1, \ldots, a_n \oplus b_n)$ denotes the addition of vectors. It will be clear from context whether $\oplus$ is used to denote addition on $\mathbb{F}_{2^m}$ or $\mathbb{F}_{2^m}^n$. Given that $\mathbb{F}_{2^n}$ is isomorphic to $\mathbb{F}_2^n$, we will primarily use $\mathbb{F}_2^n$ to denote the space on n-bit vectors; $\mathbb{F}_{2^n}$ is only used when this is more informative.

We call $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $n, m \in \mathbb{N}_+$ a *vectorial Boolean function*. When $n = m$ and F is invertible, F is called a *permutation*. In the special case that $m = 1$, the function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to be a *Boolean function*. Note that a vectorial Boolean function F can be viewed as a vector of Boolean functions $(f_1, \ldots, f_m)$ acting on the same input, with $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ for all $1 \leq i \leq m$. A Boolean function is *linear* if $f(x \oplus y) = f(x) \oplus f(y)$ for all $x, y \in \mathbb{F}_2^n$. Analogously, a vectorial Boolean function F is said to be linear when all Boolean functions $f_1, \ldots, f_m$ composing it are linear.

We use $a^\top x$ as shorthand notation for the inner product $\langle \cdot, \cdot \rangle : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2 : a, x \mapsto a_1 x_1 \oplus \ldots \oplus a_n x_n$. Observe that for fixed a, we can view $a^\top x$ as a Boolean function on x; we refer to a as the *mask* of x. The parity functions $a^\top x$ with $a \in \mathbb{F}_2^n \setminus \{0\}$ are the only linear Boolean functions. Consequently, any linear vectorial Boolean function F can be decomposed into a vector of functions $(a_1^\top x, \ldots, a_m^\top x)$. Note that this implies that

$F(x) = Mx$ for all $x \in \mathbb{F}_2^n$, when the ith row in $M \in \mathbb{F}_2^{m \times n}$ is equal to a_i for all $1 \leq i \leq m$. We will use M_F to denote this matrix for F.

The imbalance of a Boolean function is defined as

$$Imb(f) := \tfrac{1}{2}(|\{x \in \mathbb{F}_2^n \mid f(x) = 0\}| - |\{x \in \mathbb{F}_2^n \mid f(x) = 1\}|) \tag{1}$$

where $|\cdot|$ maps a set to its size. A function with imbalance 0 is said to be *balanced* [DR07]. For the parity functions it holds that $Imb(a^\top x) = \delta_{a,0} \cdot \frac{1}{2}|\mathbb{F}_2^n|$, with $\delta_{i,j}$ denoting the *Kronecker delta*.

2.2 Linear Cryptanalysis

When used to analyse an n-bit block cipher $E_k(x) = E(x,k) : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$, standard Linear Cryptanalysis is concerned with discovering masks $u, v \in \mathbb{F}_2^n$ such that the deviation of the probability $p_k := \mathbb{P}\big[u^\top x = v^\top E_k(x)\big]$ from $\frac{1}{2}$ is large for almost all keys $k \in \mathbb{F}_2^\kappa$ [Dae95, HN11, Mat93]. This deviation is denoted using ϵ_k and is referred to as the *bias* of the linear approximation (u, v). However, in this work, we make use of the concept of *correlation* as presented in [Dae95]. Here, the correlation of (u, v) with E_k is defined as

$$C_{v,u}^{E_k} := 2\epsilon_k = 2 \cdot \big(\mathbb{P}\big[u^\top x = v^\top E_k(x)\big] - \tfrac{1}{2}\big), \tag{2}$$

where one is consequently interested in discovering (u, v) for which the absolute value, or *magnitude*, of this correlation is large for almost all keys.

A common technique to discover such an approximation is through the construction of a *linear trail* [Bih95, HCN19, Mat93]. For an r-round key-alternating block cipher $E_k := \mathtt{A}_{k_r} \circ F \circ \mathtt{A}_{k_{r-1}} \circ \cdots \circ F \circ \mathtt{A}_{k_0}$ with $\mathtt{A}_k : \mathbb{F}_2^n \to \mathbb{F}_2^n : x \mapsto x \oplus k$ and $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ the round function, a trail is defined as $\tau := (\tau_0, \ldots, \tau_r) \in (\mathbb{F}_2^n)^{r+1}$. The *contribution* of this trail τ to the correlation of the linear *hull* (τ_0, τ_r) with E_k is computed as

$$C_\tau^{E_k} := \left(\prod_{i=0}^{r} C_{\tau_i,\tau_i}^{\mathtt{A}_{k_i}}\right) \cdot \left(\prod_{j=0}^{r-1} C_{\tau_{j+1},\tau_j}^{F}\right) = (-1)^{\bigoplus_{i=0}^{r} \tau_i^\top k_i} \cdot \prod_{j=0}^{r-1} C_{\tau_{j+1},\tau_j}^{F}, \tag{3}$$

where the second equality follows from [DR20, Equation 7.34]. When this trail is the dominant contributor [DGV95] to the correlation of (τ_0, τ_r) with E_k, we can approximate $C_{\tau_r,\tau_0}^{E_k} = C_\tau^{E_k}$.

2.3 The Wide Trail Strategy

The *Wide Trail Strategy* (WTS) was first introduced as a block cipher design philosophy by Daemen in 1995 [Dae95]. Throughout the design of the SHARK [RDP+96], SQUARE [DKR97], and BKSQ [DR00] ciphers, the concept was further developed into a broadly-applicable block cipher design framework [DR01], ultimately forming the basis of the Rijndael cipher.

The strategy attempts to avert linear approximations with large correlations from forming in a cipher by forcing the correlation contribution of all linear trails through the cipher to be small. To achieve this, the strategy advocates the use of key-alternating *Substitution-Permutation Networks* (SPN) with a specific format for the substitution function $\gamma : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and permutation function $\lambda : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Here, *bricklayer function* γ introduces non-linear behavior into the cipher by treating the n-bit block as the concatenation of m-bit bundles and applying a non-linear permutation to each bundle — these permutations are referred to as the *s-boxes* of γ. Meanwhile, the permutation function λ is a linear transformation aimed at spreading information between the bundles. This concept of information spreading is closely linked to that of *diffusion*, which was first introduced by Shannon [Sha49] to denote the quantitative spreading of information.

Computing the correlation contribution of a linear trail for such a cipher is rather straightforward. Following Equation 3, only the one-round approximations for the round-functions influence the correlation magnitude, while [DR20, Equation 7.36] demonstrates that a proper linear approximation for λ yields a correlation of amplitude 1. As such, only the approximations over the function γ need to be considered. According to [DR20, Equation 7.37], the correlation of an approximation (u, v) with a bricklayer function γ is computed as

$$C^{\gamma}_{v,u} = \prod_{i=0}^{n/m-1} C^{S_i}_{[v]_i,[u]_i}, \tag{4}$$

where S_i denotes the s-box γ applies to the ith m-bit bundle, and $[v]_i$ denotes the part of v that masks this bundle. It thus follows that the correlation of a trail is computed as the product of the approximation correlations for each of the s-boxes.

When γ applies the same s-box S for all bundles, this expression allows for the formulation of an upper bound on the correlation contribution of a trail. For any chosen permutation function λ it is possible to compute a lower bound n_r on the number of *active* s-boxes any r-round trail must contain. Here, an s-box is considered active in a trail when it is assigned a non-zero input mask, output mask, or both. When we furthermore observe that $C^{S}_{v,u} = 1$ if and only if $u = v = 0$, we can see that the absolute correlation contribution of an r-round linear trail is upper bounded by c^{n_r}, where c is an upper bound on the magnitude of the correlation of a linear approximation with S.

To account for the possibility that the correlation contributions of several linear trails amplify one another by means of the linear hull effect, the WTS requires the number of rounds r to be chosen such that the contribution of a linear trail is at most $\kappa^{-1} \cdot 2^{-n/2}$, where κ denotes the key size. It then argued that even in the unlikely scenario that a linear hull contains κ trails with such a contribution, it would only be detectable when all κ trails amplify one another simultaneously — an event that is expected to occur for an insignificant fraction of the key space. Although not proof of security, the authors argue that this shows the WTS to be a sound design strategy.

2.4 AES

The Advanced Encryption Standard (AES) [DBN+01] is the standardized version of the Rijndael cipher [DR20] that is best described as an r-round key-alternating substitution-permutation network. Its encryption function can be expressed as the composition

$$\texttt{AES}^r_k := \texttt{A}_{k_r} \circ \texttt{RF}' \circ \texttt{A}_{k_{r-1}} \circ \texttt{RF} \circ \cdots \circ \texttt{RF} \circ \texttt{A}_{k_1} \circ \texttt{RF} \circ \texttt{A}_{k_0}, \tag{5}$$

where $\texttt{A}_{k_i} : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128} : x \mapsto x \oplus k_i$ denotes the addition of round key k_i and $\texttt{RF}, \texttt{RF}' : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128}$ denote the round functions. In the first $r - 1$ rounds, the round function $\texttt{RF} := \texttt{MC} \circ \texttt{SR} \circ \texttt{SB}$ is used, while the last round applies $\texttt{RF}' := \texttt{SR} \circ \texttt{SB}$, with $\texttt{SB}, \texttt{SR}, \texttt{MC} : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128}$.

The standardized cipher specifies three AES variants — AES-128, AES-192, and AES-256 — differing in two aspects. First, the variants involve 10, 12, and 14 rounds respectively. Second, the lengths of the master key k used are 128, 192, and 256 bits. AES includes a specification for the key expansion algorithm used to generate the individual round keys k_i from k. In Section 5 we will use the fact that this algorithm reuses part of this master key as the initial round key k_0. Aside from this, it is assumed that the round keys generated by this algorithm are statistically independent [LMM91].

The AES state is most conveniently represented using a 4×4 byte matrix, an example of which is provided in Figure 1. This example demonstrates that the 128-bit state may additionally be viewed as a byte-vector $(p_0, \ldots, p_{15}) \in \mathbb{F}_{2^8}^{16}$ storing the byte entries of the matrix in column-major order.

p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

Figure 1: A convenient representation of the AES state.

The vectorial Boolean function `SB`, short for `SubBytes`, applies the s-box $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ to each of the sixteen bytes. This s-box is best described as the composition $\texttt{T} \circ \texttt{L} \circ \texttt{inv}$. Here, $\texttt{inv} : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8} : x \mapsto x^{254} \mod \texttt{11B}_\texttt{x}$ maps an element in $\mathbb{F}_{2^8} \setminus \{0\}$ to its multiplicative inverse modulo $\texttt{11B}_\texttt{x}$ and zero to itself. The function $\texttt{L} : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ is a linear permutation — its matrix representation is provided in Equation 6 — while $\texttt{T} : \mathbb{F}_2^8 \to \mathbb{F}_2^8 : x \mapsto x \oplus \texttt{63}_\texttt{x}$ is an affine translation.

$$M_{\texttt{L}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{6}$$

The `ShiftRows` (`SR`) operation is a linear function permuting the bytes in the state. Assuming zero-based indexing, this operation cyclically shifts the bytes in the ith row of the state i steps to the left. An illustration is provided in Figure 2.

`SR`:

p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

$\mapsto$

p_0	p_4	p_8	p_{12}
p_5	p_9	p_{13}	p_1
p_{10}	p_{14}	p_2	p_6
p_{15}	p_3	p_7	p_{11}

Figure 2: Illustration of the application of `ShiftRows` to the state.

The `MixColumns` (`MC`) function is best described as a linear transformation $\texttt{H} : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$ that is applied to each of the four 32-bit columns in the state. The matrix associated with `H` is included as supplementary material.

The `SubBytes` function forms the *substitution part* of this SPN and is the only non-linear component contained in the round function `RF`. As such, one of its purposes is to thwart linear cryptanalysis against the cipher. It is in particular the properties of the non-linear function `inv` that deter linear attacks. Because we will analyze the linear properties of the `inv` function, it may be more insightful to ignore the algebraic structure underlying this function and instead view it as a lookup table. For both `inv` and S, these tables are provided as supplementary material.

The `ShiftRows` and `MixColumns` functions form the *permutation* part of this substitution-permutation network. As illustrated in Section 2.3, the purpose of these functions is to

force any linear trail through the AES to have many active s-boxes, thus yielding a small contribution to the correlation of the hull containing it.

3 Conditional Approximation

In [BC14], Biham and Carmeli show that one can improve the data complexity of a linear attack by partitioning the data into classes and computing the correlation of the approximation for each class individually. The authors illustrate that for properly chosen partitions one will find that the magnitude of the approximation correlation for at least one of the classes is larger than one would observe when computing the correlation using all data. Where Biham and Carmeli only briefly review this technique, we will attempt to formalize it and its notation, and illustrate some of its properties. In this formalization, we restrict ourselves to only conditioning the input of a function; the case for conditioning the output is symmetric and is omitted for brevity. The discussion in this section is made from a mathematical point of view and is purposefully kept abstract. The implications for symmetric-key cryptanalysis and in particular the AES, are deferred to Sections 4–5.

3.1 Definition

A *conditional approximation* $(u, v)|_X$ for a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ comprises a linear approximation (u, v) with masks $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, and a vectorial Boolean function $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$. In this approximation, X is leveraged to create a partition $\mathcal{P}_X$ on the set of plaintexts $\mathbb{F}_2^n$ consisting of 2^r *classes*, with a class $\mathcal{P}_X^b := \{x \in \mathbb{F}_2^n \mid X(x) = b\}$ for each $b \in \mathbb{F}_2^r$. For each class, we are interested in

$$p_b := \mathbb{P}\big[u^\top x = v^\top F(x) \;\big|\; X(x) = b\big], \tag{7}$$

from which the definition of correlation naturally extends to the definition of *conditional correlation* as

$$C^F_{v,u}\Big|_{\mathcal{P}_X^b} := 2 \cdot \mathbb{P}\big[u^\top x = v^\top F(x) \;\big|\; x \in \mathcal{P}_X^b\big] - 1. \tag{8}$$

We furthermore refer to $C^F\Big|_{\mathcal{P}_X^b}$ as a *conditional correlation matrix*. Depending on the choice of X, it may be possible to achieve a conditional correlation in one or more classes that exceeds the correlation of the unconditioned linear approximation. In the following subsections, we provide some general properties of the conditional approximation and relate the conditional approximation to standard linear cryptanalysis. In Section 4, more specific properties will be discussed.

3.2 Properties

In [DGV95, Equation 15] it is demonstrated that for appropriate combinations of vectorial Boolean functions F and G, the correlation matrix $C^{G\circ F}$ can be computed as the matrix product $C^G \cdot C^F$. When using conditional correlation matrices instead, this equality is no longer satisfied. With Lemma 1 and 2 we demonstrate how this equation can be adapted for conditional approximations.

Lemma 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^p$, $G : \mathbb{F}_2^p \to \mathbb{F}_2^m$ and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$ be arbitrary vectorial Boolean functions. For all $b \in \mathbb{F}_2^r$ it holds that*

$$C^{G\circ F}\Big|_{\mathcal{P}_X^b} = C^G \cdot \Big(C^F\Big|_{\mathcal{P}_X^b}\Big).$$

Proof. The proof of this lemma is deferred to Appendix A.

Lemma 2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an arbitrary permutation, let $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$ be arbitrary vectorial Boolean functions. For all $b \in \mathbb{F}_2^r$ it holds that*

$$C^{G\circ F}\Big|_{\mathcal{P}^b_{X\circ F}} = C^G\Big|_{\mathcal{P}^b_X} \cdot C^F.$$

Proof. The proof of this lemma is deferred to Appendix A.

Note here that Lemma 2 only applies to the case that F is a *permutation*.

We furthermore discuss constructing a conditional approximation for the Cartesian product of functions. To this end, we present Lemma 3, where we use $\cdot|\cdot$ to denote vector concatenation and $\times$ to denote the Cartesian product of vectorial Boolean functions s.t. $(f \times g)(x|y) = f(x)|g(y)$.

Lemma 3. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $G : \mathbb{F}_2^r \to \mathbb{F}_2^p$, $X : \mathbb{F}_2^n \to \mathbb{F}_2^q$ and $Y : \mathbb{F}_2^r \to \mathbb{F}_2^s$ be arbitrary vectorial Boolean functions. It holds that*

$$C^F\big|_{\mathcal{P}^a_X} \otimes C^G\Big|_{\mathcal{P}^b_Y} = C^{F\times G}\Big|_{\mathcal{P}^{a|b}_{X\times Y}}$$

for all $a \in \mathbb{F}_2^q$ and $b \in \mathbb{F}_2^s$, where $\otimes$ denotes the Kronecker product.

Proof. The proof of this lemma is deferred to Appendix A.

Lastly, it was already observed in [BC14] that merging disjoint classes of the same size yields a new class with a conditional correlation that is the average of the original two. We present a generalization of this result in Lemma 4.

Lemma 4. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$ be arbitrary vectorial Boolean functions. For any $b, b' \in \mathbb{F}_2^r$ s.t. $b \neq b'$, it holds that*

$$C^F\Big|_{\mathcal{P}^b_X \cup \mathcal{P}^{b'}_X} = \frac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X| + |\mathcal{P}^{b'}_X|} \cdot C^F\Big|_{\mathcal{P}^b_X} + \frac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X| + |\mathcal{P}^{b'}_X|} \cdot C^F\Big|_{\mathcal{P}^{b'}_X}$$

when either $\mathcal{P}^b_X \neq \emptyset$ or $\mathcal{P}^{b'}_X \neq \emptyset$.

Proof. The proof of this lemma is deferred to Appendix A.

Note here in particular that when $|\mathcal{P}^b_X| = |\mathcal{P}^{b'}_X| \neq 0$, the correlation of the merged class is indeed the average of the original two.

3.3 Relation to Standard Linear Cryptanalysis

To provide an understanding of how this version of conditional cryptanalysis fits within the framework of standard linear cryptanalysis, we illustrate a relation between both approximation techniques when applied to Boolean permutations. To this end, we introduce Lemma 5.

Lemma 5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an arbitrary permutation and $u, v \in \mathbb{F}_2^n$ arbitrary masks. For all $b \in \mathbb{F}_2$ it holds that*

$$(-1)^b \cdot C^F_{v,0}\Big|_{\mathcal{P}^b_X} = C^F_{v,u},$$

when $X : \mathbb{F}_2^n \to \mathbb{F}_2 : x \mapsto u^\top x$.

Proof. The proof of this lemma is deferred to Appendix A.

It follows from this lemma that a conditional approximation $(0, v)|_{u^\top x}$ restricted to those plaintexts for which $u^\top x = 0$, is equivalent to the linear approximation (u, v) in the sense that both achieve the same correlation when used to approximate the same function. Furthermore, restricting $(0, v)|_{u^\top x}$ to $\mathcal{P}^1_{u^\top x}$ yields a conditional approximation achieving the same correlation as (u, v), but with opposite sign.

4 Conditional Analysis of the Multiplicative Inverse in $\mathbb{F}_{2^8}$

In this section, we analyze the vectorial Boolean function `inv`, which was introduced in Section 2.4 as an integral part of the AES s-box. First, we recall in Section 4.1 the seminal work by Nyberg [Nyb94] which provides an upper bound of $2^{1-n/2}$ on the correlation magnitude of any linear approximation for the inverse function on $\mathbb{F}_{2^n}$. We then recall the work of Keliher, Meijer, and Tavares [KMT01a, KMT01b] discussing the complete *Linear Approximation Table* (LAT) for the special case of $n = 8$, and observe that Nyberg's upper bound is tight in this case.

In symmetric-key folklore, these two results are understood to mean that any attempt to approximate this multiplicative inverse in $\mathbb{F}_{2^8}$ must incur a cost of 2^{-3} at the minimum (see *e.g.*, [AAB+20, GKM+09, MN17, JNPS21]). Conversely, we demonstrate in Section 4.3 how the conditional approximation technique can exhibit a higher correlation when properly applied to `inv`.

4.1 Linear Approximations of the Inversion Function

Nyberg proved in [Nyb94] that the inversion function on finite field $\mathbb{F}_{2^n}$ possesses properties that are highly desirable in cryptography. In particular, it is shown that the correlation of any linear approximation for this function is upper bounded by $2^{1-n/2}$. This property, among others, led Daemen and Rijmen to use it with $n = 8$ as part of the Rijndael s-box [DR20]. Recall that this particular instance of the inversion function was previously introduced in Section 2.4 as $\texttt{inv} : \mathbb{F}_2^8 \to \mathbb{F}_2^8$.

We briefly discuss the linear properties of the `inv` function. To this end, we construct its correlation matrix $C^{\texttt{inv}}$. This matrix is isomorphic to the Linear Approximation Table of `inv`, which was previously discussed in [KMT01a, KMT01b], and reveals a clear structure underlying the `inv` operation. In particular, it holds that the distribution of values in column $C^{\texttt{inv}}_{v,\cdot}$ is the same for any output mask $v \in \mathbb{F}_2^8 \setminus \{0\}$ [KMT01a, Lemma 2]. We recall this distribution in Table 1. For an arbitrary $v \in \mathbb{F}_2^8 \setminus \{0\}$, this table lists each value in $C^{\texttt{inv}}_{v,\cdot}$ along with the number ϕ of input masks for which this correlation is attained. Since `inv` is an involution, we additionally conclude that the same distribution arises when the input mask u is fixed and v varies instead.

Table 1 reveals that, regardless the choice of output mask $v \in \mathbb{F}_2^8 \setminus \{0\}$, there always exist exactly five input masks $u \in \mathbb{F}_2^8 \setminus \{0\}$ s.t. $C^{\texttt{inv}}_{v,u} = \frac{8}{64} = 2^{-3}$, where it should be noted that the exact values of these masks depend on the choice of v. Let us use $\Omega_v = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$ to denote the set containing these five masks moving forward.

Scanning these sets we find that, irrespective of the chosen output mask v, Ω_v always contains two masks that can be expressed as a linear combination of the other three. To be more precise: for any $v \in \mathbb{F}_2^8 \setminus \{0\}$, there exists an ordering on the elements in Ω_v such that $\omega_1 \oplus \omega_2 = \omega_4$ and $\omega_1 \oplus \omega_3 = \omega_5$. Since $a \oplus b = c \iff a \oplus c = b$, it follows that there are in fact eight such orderings. In the remaining analysis, we will assume any one of these eight to be applied to Ω_v; all results hold irrespective of the chosen ordering. An overview

Table 1: Frequency distribution of the correlation between linear combinations of bits in the `inv` input and output.

$C^{\texttt{inv}}_{v,u}$	$-\frac{7}{64}$	$-\frac{6}{64}$	$-\frac{5}{64}$	$-\frac{4}{64}$	$-\frac{3}{64}$	$-\frac{2}{64}$	$-\frac{1}{64}$	0
ϕ	8	16	8	18	24	16	32	17
$C^{\texttt{inv}}_{v,u}$	$\frac{1}{64}$	$\frac{2}{64}$	$\frac{3}{64}$	$\frac{4}{64}$	$\frac{5}{64}$	$\frac{6}{64}$	$\frac{7}{64}$	$\frac{8}{64}$
ϕ	16	20	16	16	16	20	8	5

of the masks $\omega_1, \omega_2, \omega_3 \in \Omega_v$ for each $v \in \mathbb{F}_2^8 \setminus \{0\}$ is provided as supplementary material.

4.2 Constructing a Conditional Approximation

In [BP18], Biham and Perle briefly discuss the strategies employed to construct the conditional approximations used in their attack for DES. From this discussion, it is evident that the authors primarily make use of heuristic methods and search algorithms, but provide no explicit construction techniques. In this section, we do present a construction method and demonstrate its value in the next subsection, where it is applied to `inv`.

When constructing a conditional approximation for some vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we propose to select an output mask $v \in \mathbb{F}_2^m$ that has multiple input masks $u_i \in \mathbb{F}_2^n$ for which $|C^F_{v,u_i}|$ is preferably high and at least non-zero, with $1 \leq i \leq r$ and $r \geq 2$. With these u_i and v, we construct the conditional approximation $(0, v)|_X$ with $X : \mathbb{F}_2^n \to \mathbb{F}_2^r : x \mapsto (u_1^\top x, \ldots, u_r^\top x)$.

In this construction, one must keep in mind only to include masks u_i that are linearly independent of one another; when a linearly dependent set is used, some of the classes in $\mathcal{P}_X$ will be empty. We can illustrate this with the example $X : \mathbb{F}_2^n \to \mathbb{F}_2^3 : x \mapsto (u_1^\top x, u_2^\top x, (u_1 \oplus u_2)^\top x)$, where the classes $\mathcal{P}_X^{(0,0,1)}$, $\mathcal{P}_X^{(0,1,0)}$, $\mathcal{P}_X^{(1,0,0)}$ and $\mathcal{P}_X^{(1,1,1)}$ are empty due to the linear dependency of the masks. When only linearly independent masks are used, X induces a partition consisting of 2^r classes that all have a size of 2^{n-r}.

We expect this conditional approximation to achieve an absolute correlation on class $\mathcal{P}_X^{\overline{b}}$ that is higher than $|C^F_{v,u_i}|$ for any u_i, when $\overline{b} \in \mathbb{F}_2^r$ s.t. $(-1)^{\overline{b}_i} = \mathtt{sgn}(C^F_{v,u_i})$ for all $1 \leq i \leq r$. Here, `sgn` is used to denote the *signum*-function. For the plaintexts x in this class, it namely holds that $u_i^\top x = \overline{b}_i$ and $\mathbb{P}\big[v^\top F(x) = 0 \;\big|\; u_i^\top x = \overline{b}_i\big] > \frac{1}{2}$ for all $1 \leq i \leq r$.

When the application of this technique yields two classes with the same absolute correlation, it is possible to merge these using Lemma 4 while maintaining the correlation magnitude. To account for the case that the classes one wishes to merge have correlations with opposing signs, we introduce Lemma 6.

Lemma 6. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an arbitrary vectorial Boolean function, $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$ arbitrary masks, and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r : x \mapsto (u_1^\top x, \ldots, u_r^\top x)$ an arbitrary linear vectorial Boolean function with $u_1, \ldots, u_r \in \mathbb{F}_2^n$ linearly independent. For all $b \in \mathbb{F}_2^r$ it holds that*

$$(-1)^{b_i} \cdot C^F_{v,u\oplus u_i}\Big|_{\mathcal{P}_X^b} = C^F_{v,u}\Big|_{\mathcal{P}_X^b}.$$

Proof. The proof of this lemma is deferred to Appendix A.

This lemma demonstrates that, with a properly chosen w in the span of the set $\{u_1, \ldots, u_r\}$, the signs of the correlations of the two classes one wishes to merge can be made the same when adding w to the input mask of the conditional approximation.

When constructing a conditional approximation for a cipher that starts with a key addition $\mathtt{A}_k : \mathbb{F}_2^n \to \mathbb{F}_2^n : x \mapsto x \oplus k$, using a *linear* conditioning function X to partition the plaintext space has another benefit. We can namely use Lemma 2 to see that

$$C^F\Big|_{\mathcal{P}_X^b} \cdot C^{\mathtt{A}_k} = C^{F\circ\mathtt{A}_k}\Big|_{\mathcal{P}^b_{X\oplus\mathtt{A}_k}} = C^{F\circ\mathtt{A}_k}\Big|_{\mathcal{P}^b_{X'}}, \tag{9}$$

where $X' : \mathbb{F}_2^n \to \mathbb{F}_2^r : x \mapsto X(x) \oplus X(k)$ constructs the same partition as X: adding k only rearranges the order of the classes such that $\mathcal{P}_X^b = \mathcal{P}_{X'}^{b\oplus X(k)}$. In this situation it thus suffices to construct a conditional approximation for F; the addition of k only influences *which* class achieves the large correlation.

4.3 Conditional Approximation for `inv`

We now construct a conditional approximation for `inv`. The technique presented in Section 4.2 lends itself exceptionally well to `inv` since we have seen in Section 4.1 that for any $v \in \mathbb{F}_2^8 \setminus \{0\}$ there are five input masks $\omega \in \Omega_v$ s.t. $C^{\texttt{inv}}_{v,\omega} = 2^{-3}$. We will, however, exclude the masks ω_4 and ω_5 from the conditioning function as we observed that they are linearly dependent on the masks ω_1, ω_2, and ω_3. Hence, we construct $X : \mathbb{F}_2^8 \to \mathbb{F}_2^3 : x \mapsto (\omega_1^\top x, \omega_2^\top x, \omega_3^\top x)$, which induces a partition with 8 classes that all contain 32 plaintexts. In Table 2 we present an overview of the conditional correlations achieved on each of these eight classes.

Table 2: $C^{\texttt{inv}}_{v,0}\big|_{\mathcal{P}^b_X}$ for each $b \in \mathbb{F}_2^3$.

$\omega_1^\top x$	0	0	0	0	1	1	1	1
$\omega_2^\top x$	0	0	1	1	0	0	1	1
$\omega_3^\top x$	0	1	0	1	0	1	0	1
$C^{\texttt{inv}}_{v,0}\big\|_{\mathcal{P}^b_X}$	2^{-1}	2^{-2}	2^{-2}	-2^{-1}	-2^{-3}	-2^{-3}	-2^{-3}	-2^{-3}

From this table we gather that the conditional approximation $(0, v)|_X$ achieves a conditional correlation of $\pm 2^{-1}$ for two plaintext classes. Note that this is a substantial increase when compared to the 2^{-3} correlation upper bound for the linear approximations (ω, v) with $\omega \in \Omega_v$, illustrating the utility of the conditional approximation.

4.4 Improving the Conditional Approximation

Since there are two classes with a correlation of magnitude 2^{-1}, we shall merge these by means of Lemma 4. Before performing this merge, we must first modify the approximation such that the signs of the conditional correlations of these two classes are the same. To this end we leverage Lemma 6 and observe that the correlation sign of the class $\mathcal{P}_X^{(0,1,1)}$ is inverted when we consider the conditional approximation $(\omega_3, v)|_X$ instead of $(0, v)|_X$. The correlations associated with this new conditional approximation are shown in Table 3.

With the signs of the correlations corresponding with $\mathcal{P}_X^{(0,0,0)}$ and $\mathcal{P}_X^{(0,1,1)}$ now the same, it is possible to modify X such that these two classes are merged. To this end, one needs to discover the linear properties that the classes have in common. Observe here that the value of $\omega_1^\top x$ is the same for the two classes of interest and that the value of $\omega_2^\top x \oplus \omega_3^\top x = (\omega_2 \oplus \omega_3)^\top x$ is moreover constant. This means that these two classes are merged when we instead partition on $X' : \mathbb{F}_2^n \to \mathbb{F}_2^2 : x \mapsto (\omega_1^\top x, \omega_6^\top x)$, where $\omega_6 := \omega_2 \oplus \omega_3$. The conditional correlations associated with the approximation $(\omega_3, v)|_{X'}$ are presented in Table 4 and shows that the linear approximation (ω_3, v) achieves a correlation of 2^{-1} on plaintext class corresponding with $\overline{b} = (0, 0)$.

It was previously mentioned in Section 4.2 that extending a conditional approximation to include a round-key addition function A_k yields that the conditional correlations are

Table 3: $C^{\texttt{inv}}_{v,\omega_3}\big|_{\mathcal{P}^b_X}$ for each $b \in \mathbb{F}_2^3$.

$\omega_1^\top x$	0	0	0	0	1	1	1	1
$\omega_2^\top x$	0	0	1	1	0	0	1	1
$\omega_3^\top x$	0	1	0	1	0	1	0	1
$C^{\texttt{inv}}_{v,\omega_3}\big\|_{\mathcal{P}^b_X}$	2^{-1}	-2^{-2}	2^{-2}	2^{-1}	-2^{-3}	2^{-3}	-2^{-3}	2^{-3}

Table 4: $C^{\mathtt{inv}}_{v,\omega_3}\Big|_{\mathcal{P}^b_{X'}}$ for each $b \in \mathbb{F}_2^2$.

$\omega_1^\top x$	0	0	1	1
$\omega_6^\top x$	0	1	0	1
$C^{\mathtt{inv}}_{v,\omega_3}\Big\|_{\mathcal{P}^b_{X'}}$	2^{-1}	0	0	0

permuted among the classes induced by X, depending on the value of k. This effect is illustrated in Table 5, where the conditional correlations for approximation $(\omega_3, v)|_{X'}$ with $\mathtt{inv} \circ \mathtt{A}_k$ are presented. We observe here that the class with the 2^{-1} correlation magnitude is indexed by $\overline{b} \oplus X'(k) = (\omega_1^\top k, \omega_6^\top k)$. It is moreover illustrated that the sign of the correlation is determined by the value of $(-1)^{\omega_3^\top k}$.

Table 5: $C^{\mathtt{inv}\circ\mathtt{A}_k}_{v,\omega_3}\Big|_{\mathcal{P}^b_{X'}}$ for $k \in \mathbb{F}_2^8$, $b \in \mathbb{F}_2^2$ and $X' : x \mapsto (\omega_1^\top x, \omega_6^\top x)$.

		$\omega_1^\top x$	0	0	1	1
		$\omega_6^\top x$	0	1	0	1
$\omega_3^\top k$	$\omega_1^\top k$	$\omega_6^\top k$				
0	0	0	2^{-1}	0	0	0
	0	1	0	2^{-1}	0	0
	1	0	0	0	2^{-1}	0
	1	1	0	0	0	2^{-1}
1	0	0	-2^{-1}	0	0	0
	0	1	0	-2^{-1}	0	0
	1	0	0	0	-2^{-1}	0
	1	1	0	0	0	-2^{-1}

5 Application to 4-round AES

It has been argued that the correlation contribution of a standard linear trail for four-round AES is upper bounded by 2^{-75} [DR20, Section 9.5.2], making it the smallest round-reduced version of this cipher that can withstand distinguishing attacks that rely on standard linear cryptanalysis. However, in symmetric-key folklore this is often incorrectly understood to mean that this round-reduced version of AES can withstand *any form* of linear cryptanalysis. In this section, we present a linear cryptanalysis distinguishing attack against four-round AES, highlighting the need for refining this understanding.

5.1 The four-round distinguisher

To construct a conditional distinguisher for four-round AES, one commences with the construction of a three-round linear trail (v, w) for $\mathtt{AES}_k^3$. This trail should be formed such that the first and third round have four active s-boxes, while the second round only has one. Moreover, one should make sure that the correlation of the trail over each of the nine s-boxes is 2^{-3}. When done correctly, this yields a trail with a correlation contribution of $(2^{-3})^9 = 2^{-27}$. In Figure 3, one such example is provided.

As a second step, one prepends to this the trail (u, v) for the function $\mathtt{MC} \circ \mathtt{SR}$, forming the $3\frac{1}{2}$-round trail (u, w) for $\mathtt{AES}_k^3 \circ \mathtt{MC} \circ \mathtt{SR}$. Note here that u should be chosen such that

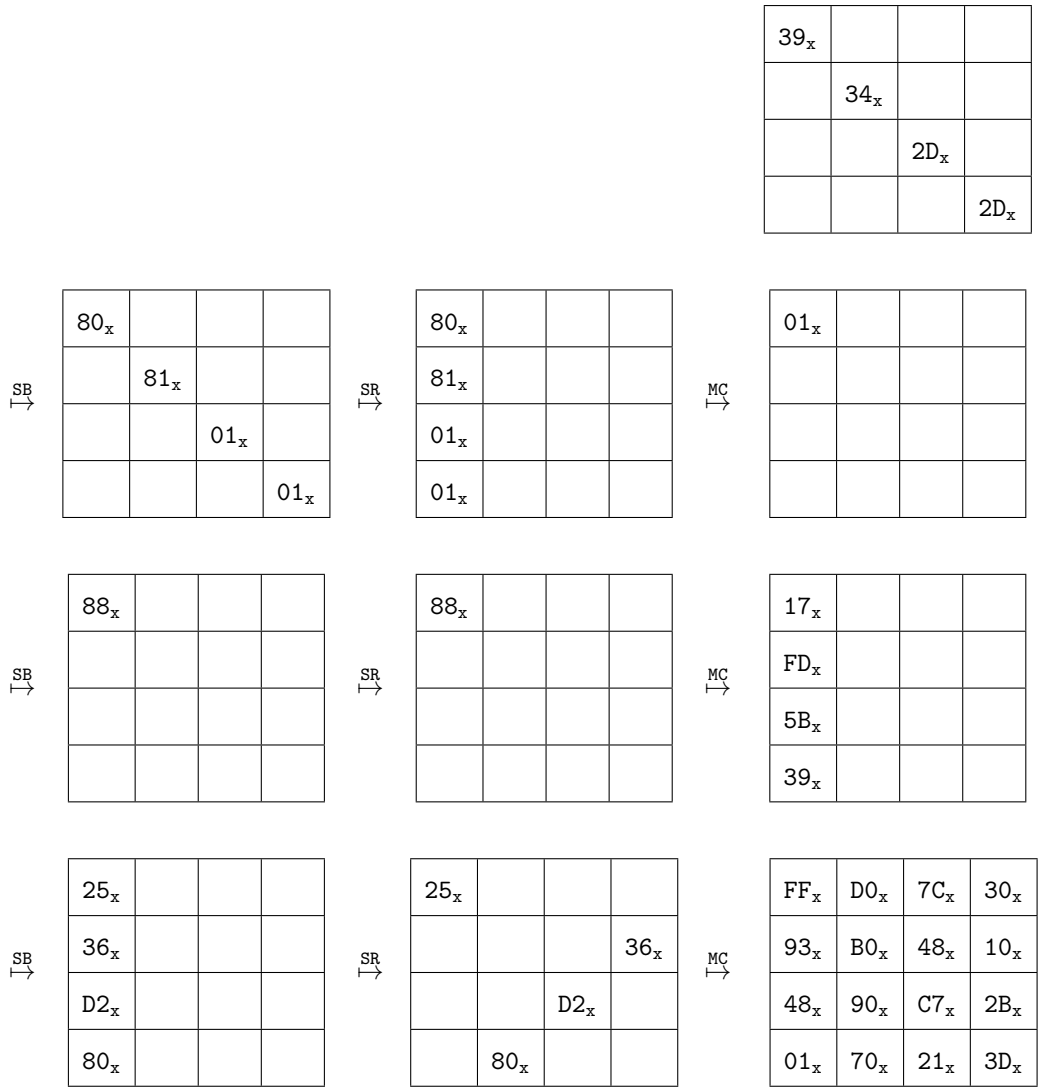

Figure 3: Linear trail (v, w) for three-round AES with 9 active s-boxes.

(u, v) achieves a correlation of 1 with $\texttt{MC} \circ \texttt{SR}$. Such a u always exists since both of these functions are linear. The resulting trail attains a correlation contribution of magnitude 2^{-27}. In Figure 4 the extension (u, v) for the example trail is presented.

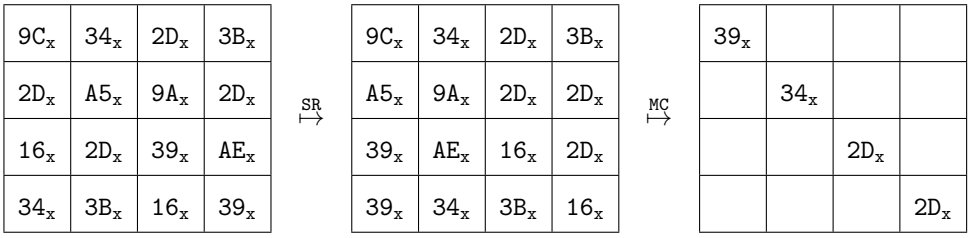

Figure 4: Linear trail (u, v) for `MixColumns` $\circ$ `ShiftRows`.

Third, one prepends a conditional approximation $(r, u)|_X$ for `SubBytes` to the trail,

forming the conditional trail $(r, w)|_X$ for $\texttt{AES}_k^3 \circ \texttt{MC} \circ \texttt{SR} \circ \texttt{SB}$. Using Lemma 3, we find that this conditional approximation can be formed using sixteen conditional trails $([r]_i, [u'']_i, [u']_i, [u]_i)|_{X_i}$ for the s-boxes S_i, where $1 \leq i \leq 16$. Since $S_i = \texttt{T} \circ \texttt{L} \circ \texttt{inv}$, with $\texttt{T}$ affine and $\texttt{L}$ linear, both $[u'']_i$ and $[u']_i$ can be chosen such that the trail $([u'']_i, [u]_i)$ achieves a correlation of magnitude 1 with $\texttt{T} \circ \texttt{L}$. Following this, one chooses the mask $[r]_i$ to be equal to $\omega_3 \in \Omega_{[u'']_i}$. Lastly, one constructs the conditioning function X_i as $x \mapsto (\omega_1^\top x, \omega_6^\top x)$ with $\omega_1, \omega_2, \omega_3 \in \Omega_{[u'']_i}$ and $\omega_6 = \omega_2 \oplus \omega_3$. Table 6 lists the conditioning masks ω_1 and ω_6 for each of the sixteen conditioning functions X_i, while Figure 5 presents the trail extension for the example (r, u).

Table 6: Masks ω_1 and ω_6 for partitioning functions $X_i : x \mapsto (\omega_1^\top x, \omega_6^\top x)$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ω_1	$\texttt{E5}_\texttt{x}$	$\texttt{93}_\texttt{x}$	$\texttt{62}_\texttt{x}$	$\texttt{7D}_\texttt{x}$	$\texttt{7D}_\texttt{x}$	$\texttt{C0}_\texttt{x}$	$\texttt{93}_\texttt{x}$	$\texttt{79}_\texttt{x}$	$\texttt{93}_\texttt{x}$	$\texttt{94}_\texttt{x}$	$\texttt{7A}_\texttt{x}$	$\texttt{62}_\texttt{x}$	$\texttt{79}_\texttt{x}$	$\texttt{93}_\texttt{x}$	$\texttt{9D}_\texttt{x}$	$\texttt{7A}_\texttt{x}$
ω_6	$\texttt{3A}_\texttt{x}$	$\texttt{20}_\texttt{x}$	$\texttt{19}_\texttt{x}$	$\texttt{EA}_\texttt{x}$	$\texttt{EA}_\texttt{x}$	$\texttt{6B}_\texttt{x}$	$\texttt{20}_\texttt{x}$	$\texttt{CE}_\texttt{x}$	$\texttt{20}_\texttt{x}$	$\texttt{49}_\texttt{x}$	$\texttt{F9}_\texttt{x}$	$\texttt{19}_\texttt{x}$	$\texttt{CE}_\texttt{x}$	$\texttt{20}_\texttt{x}$	$\texttt{F2}_\texttt{x}$	$\texttt{F9}_\texttt{x}$

$\texttt{93}_\texttt{x}$	$\texttt{80}_\texttt{x}$	$\texttt{A9}_\texttt{x}$	$\texttt{AA}_\texttt{x}$		$\texttt{AF}_\texttt{x}$	$\texttt{E6}_\texttt{x}$	$\texttt{87}_\texttt{x}$	$\texttt{BC}_\texttt{x}$		$\texttt{9C}_\texttt{x}$	$\texttt{34}_\texttt{x}$	$\texttt{2D}_\texttt{x}$	$\texttt{3B}_\texttt{x}$
$\texttt{A9}_\texttt{x}$	$\texttt{9C}_\texttt{x}$	$\texttt{58}_\texttt{x}$	$\texttt{A9}_\texttt{x}$	$\overset{\texttt{inv}}{\mapsto}$	$\texttt{87}_\texttt{x}$	$\texttt{F0}_\texttt{x}$	$\texttt{8B}_\texttt{x}$	$\texttt{87}_\texttt{x}$	$\overset{\texttt{ToL}}{\mapsto}$	$\texttt{2D}_\texttt{x}$	$\texttt{A5}_\texttt{x}$	$\texttt{9A}_\texttt{x}$	$\texttt{2D}_\texttt{x}$
$\texttt{3C}_\texttt{x}$	$\texttt{A9}_\texttt{x}$	$\texttt{C1}_\texttt{x}$	$\texttt{D9}_\texttt{x}$		$\texttt{3B}_\texttt{x}$	$\texttt{87}_\texttt{x}$	$\texttt{5F}_\texttt{x}$	$\texttt{6D}_\texttt{x}$		$\texttt{16}_\texttt{x}$	$\texttt{2D}_\texttt{x}$	$\texttt{39}_\texttt{x}$	$\texttt{AE}_\texttt{x}$
$\texttt{80}_\texttt{x}$	$\texttt{AA}_\texttt{x}$	$\texttt{3C}_\texttt{x}$	$\texttt{C1}_\texttt{x}$		$\texttt{E6}_\texttt{x}$	$\texttt{BC}_\texttt{x}$	$\texttt{3B}_\texttt{x}$	$\texttt{5F}_\texttt{x}$		$\texttt{34}_\texttt{x}$	$\texttt{3B}_\texttt{x}$	$\texttt{16}_\texttt{x}$	$\texttt{39}_\texttt{x}$

Figure 5: Linear trail (r, u) for `SubBytes` in first round.

It now follows from Section 4.4 that $([r]_i, [u'']_i)|_{X_i}$ achieves a conditional correlation with S_i of magnitude 2^{-1} when restricted to the plaintexts in $\mathcal{P}^0_{X_i}$, while achieving a correlation of 0 when restricted to the other classes. Recalling Lemma 3, we find that one can combine these sixteen conditioning functions as $\bigtimes_{i=1}^{16} X_i$ to form X. The resulting approximation $(r, u)|_X$ now achieves a conditional correlation with `SubBytes` of magnitude $(2^{-1})^{16} = 2^{-16}$ on plaintext class $\mathcal{P}^0_X$ and 0 on all other classes. Leveraging Lemma 1, we find that $(r, w)|_X$ achieves a conditional correlation with $\texttt{AES}_k^3 \circ \texttt{MC} \circ \texttt{SR} \circ \texttt{SB}$ of magnitude $2^{-27} \cdot 2^{-16} = 2^{-43}$ on plaintext class $\mathcal{P}^0_X$.

Finally, Equation 15 shows that prepending the round key addition function A_{k_0} yields that $(r, w)|_X$ achieves a conditional correlation with $\texttt{AES}_k^4$ of magnitude 2^{-43} on plaintext class $\mathcal{P}^{b^*}_X$, where $b^* := X(k_0)$. Moving forward, we will refer to $\mathcal{P}^{b^*}_X$ as the *substantial* plaintext class.

Completing the example, Figure 6 presents the full four-round trail (r, w) and Equation 10 lists the complete conditioning function X.

$\texttt{93}_\texttt{x}$	$\texttt{80}_\texttt{x}$	$\texttt{A9}_\texttt{x}$	$\texttt{AA}_\texttt{x}$		$\texttt{FF}_\texttt{x}$	$\texttt{D0}_\texttt{x}$	$\texttt{7C}_\texttt{x}$	$\texttt{30}_\texttt{x}$
$\texttt{A9}_\texttt{x}$	$\texttt{9C}_\texttt{x}$	$\texttt{58}_\texttt{x}$	$\texttt{A9}_\texttt{x}$	$\overset{\texttt{AES}_k^4}{\mapsto}$	$\texttt{93}_\texttt{x}$	$\texttt{B0}_\texttt{x}$	$\texttt{48}_\texttt{x}$	$\texttt{10}_\texttt{x}$
$\texttt{3C}_\texttt{x}$	$\texttt{A9}_\texttt{x}$	$\texttt{C1}_\texttt{x}$	$\texttt{D9}_\texttt{x}$		$\texttt{48}_\texttt{x}$	$\texttt{90}_\texttt{x}$	$\texttt{C7}_\texttt{x}$	$\texttt{2B}_\texttt{x}$
$\texttt{80}_\texttt{x}$	$\texttt{AA}_\texttt{x}$	$\texttt{3C}_\texttt{x}$	$\texttt{C1}_\texttt{x}$		$\texttt{01}_\texttt{x}$	$\texttt{70}_\texttt{x}$	$\texttt{21}_\texttt{x}$	$\texttt{3D}_\texttt{x}$

Figure 6: Linear trail (r, w) for four-round AES with 25 active s-boxes.

$$
\begin{aligned}
X : \mathbb{F}_2^{128} \to \mathbb{F}_2^{32} :\ x \mapsto\ & \\
(&\texttt{E5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 93 00 00 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 62 00 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 7D 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 7D 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 C0 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 93 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 79 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 93 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 94 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 7A 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 62 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 79 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 93 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7A}^{\top}_{\texttt{x}} x, \qquad (10) \\
&\texttt{3A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 19 00 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 EA 00 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 EA 00 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 6B 00 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 CE 00 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 49 00 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 F9 00 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 CE 00 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 00 F2 00}^{\top}_{\texttt{x}} x, \\
&\texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F9}^{\top}_{\texttt{x}} x)
\end{aligned}
$$

5.2 Distinguishing property

We may thus construct a conditional approximation $(u, v)|_X$ with X linear, which, when applied to four-round AES, achieves a correlation of magnitude 2^{-43} when conditioning on the substantial class, while yielding 0 on the other $2^{32} - 1$ classes. We will argue that

this property is highly unique for a 128-bit permutation and thus allows us to distinguish four-round AES from a random permutation.

First, observe that a conditional approximation using a linear conditioning function is akin to considering the correlation of a linear approximation where a number of bits of the input is fixed. In the case of four-round AES, we have shown a set of 32 input bits for which the linear approximation achieves a correlation magnitude of 2^{-43} for a single class (which we refer to as *the substantial class*) and 0 for all other classes; which class is the substantial one depends on the first round-key. To illustrate that this property is unique to AES, it thus suffices to show that when fixing 32 bits of the input of a random permutation, it is highly unlikely that any linear approximation will achieve a correlation of 2^{-43} when restricted to a certain data class.

When fixing 32-bits of the input of a 128-bit permutation P, we can view this function as a set of vectorial Boolean functions $P_1, \ldots, P_{2^{32}} : \mathbb{F}_2^{96} \to \mathbb{F}_2^{128}$, one for each of the 2^{32} possible fixations of the input bits. When P is a random permutation, we argue that these functions P_i are themselves reasonably approximated as random vectorial Boolean functions. It was shown in [DR07] that the correlation of a linear approximation with any vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is distributed according to the normal distribution $\mathcal{N}(0, 2^{-n})$. For the functions P_i, this distribution thus evaluates to $N := \mathcal{N}(0, 2^{-96})$. The probability that an arbitrary P_i yields a correlation with magnitude greater than or equal to 2^{-43} with the constructed trail then follows as

$$\mathbb{P}\left[|X| \geq 2^{-43}\right] = 2 \cdot \mathbb{P}\left[X \geq 2^{-43}\right] = 2 \cdot \mathbb{P}\left[2^{48} \cdot X \geq 2^5\right] = 2 \cdot \Phi(-2^5) < 2^{-743.987},$$

where $X \sim N$ and Φ denotes the cumulative density function for the standard normal distribution. Given that the arbitrary permutation P is composed of the 2^{32} functions P_i, the probability that at least one of these P_i achieves the desired correlation can be closely approximated as $2^{-743} \cdot 2^{32} = 2^{-711}$. This probability is small enough to conclude that observing a correlation of 2^{-43} on one of the 2^{32} classes constructed by a linear conditioning function X is a distinguishing property for four-round AES.

5.3 Key-recovery attack

In addition to constructing a distinguishing attack, the conditional approximation $(r, w)|_X$ can be leveraged to construct a key-recovery attack against 4-round AES. We have namely seen that the value of the first round key k_0 fully determines which plaintext class in $\mathcal{P}_X$ becomes substantial. In particular, the substantial class can be indexed by the value of $b^* = X(k_0)$. Since $X : \mathbb{F}_2^{128} \to \mathbb{F}_2^{32}$, one can thus recover 32 bits of information on this first round key k_0 by determining which class is substantial.

We will demonstrate how the substantial class can be determined in both the chosen and known-plaintext model, as well as derive the data complexity of either attack. Note that these complexity bounds also illustrate the time complexity of both attacks since the data complexity and time complexity are identical in this instance.

5.3.1 Chosen plaintext attack

To determine which plaintext class is substantial, we closely approximate the conditional correlation of all 2^{32} classes and conclude that the greatest absolute correlation corresponds with the substantial class. To construct this approximation in the chosen plaintext model, one selects a sufficient number of plaintext-ciphertext pairs t for each class in the plaintext-ciphertext space partition induced by X, and uses this to compute an empirical approximation of the conditional correlation. To compute the value of t, we can use [Sel08, Corollary 1]. Although Selçuk introduces this formula for computing the data complexity of Matsui's Algorithm 2 attack, it can also be applied here: the only difference between this and an Algorithm 2 attack is that our attack seeks to find the plaintext class achieving

the non-zero correlation, whereas Algorithm 2 seeks to find the class of keys achieving a non-zero correlation. Since this attack computes correlations with different data sets and a static key, instead of different keys and a static data set, the formula now yields the data complexity per plaintext class. A reformulated version of Selçuk's corollary is presented in Corollary 1.

Corollary 1 (Corollary 1, [Sel08])**.**

$$N = \left(\Phi^{-1}(P_S) + \Phi^{-1}(1 - 2^{-a-1})\right)^2 \cdot C^{-2} \tag{11}$$

plaintext blocks are needed in a linear attack to accomplish an a-bit advantage with a success probability of P_S using a linear approximation achieving a correlation of C.

We determine the number of chosen plaintext-ciphertext pairs necessary to correctly identify the substantial class with 95% certainty. In Table 7, an overview for the data complexity per class t for fixed success probability $P_S = 0.95$ and varying advantages a is presented. Based on this table, we can conclude that with 2^{92} plaintext-ciphertext pairs per class one should be able to correctly discern the non-zero correlation plaintext class in at least 95% of experiments. This thus implies a total data complexity of $2^{32} \cdot 2^{92} = 2^{124}$ chosen plaintext-ciphertext pairs for this attack.

Table 7: Data complexity per plaintext class of a chosen plaintext attack in terms of advantage.

a	1	8	16	32
$\log_2(t)$	88.43	90.36	91.16	91.99

5.3.2 Known-plaintext attack

The data complexity for the known-plaintext attack is identical, except for the evaluation of the complete data complexity from the complexity per class. In the case of a known-plaintext attack, one has to account for the fact that at least t samples must be encountered for each class even though the samples are drawn from the complete codebook.

This is in fact the problem known as the *dixie-cup problem*. Here, one attempts to obtain m copies of n unique objects by uniformly sampling these objects with replacement. It was shown by Newman [New60] that the expected number of objects $E_m(n)$ one must sample before obtaining m instances of each of the n types equals

$$E_m(n) = n \ln n + (m-1) \cdot n \ln \ln n + \mathcal{O}(1) \tag{12}$$

as n approaches infinity. In our situation, we attempt to encounter $m = t$ samples for $n = 2^{32}$ plaintext classes and are thus interested in the total number of necessary samples $t^* = E_m(n)$. We present the value of t^* in terms of the advantage a in Table 8. From this table we conclude that $2^{125.62}$ known plaintext-ciphertext pairs will allow one to correctly identify the substantial class with 95% certainty.

Table 8: Expected data complexity in terms of advantage.

a	1	8	16	32
$\log_2(t^*)$	122.06	123.99	124.79	125.62

5.4 Experimental validation

We experimentally validate the conditional approximation presented in Section 5.1. Given that the time complexity of the full key recovery attack is $2^{125.62}$, and therefore beyond what we can compute in reasonable time, we instead validate two parts of $(r, w)|_X$ independently.

5.4.1 Experiment 1

The first experiment restricts itself to the conditional approximation used in the first round of the distinguisher. This approximation with sixteen active s-boxes is expected to achieve a correlation of magnitude 2^{-16} when restricted to data from the substantial class, while achieving a correlation of 0 when restricted to data from other classes.

As such, the experiment generates a random key k and uses this to compute the value of $b^* = X(k_0)$. In addition to this correct class index, fifteen incorrect classes $b_1, \ldots, b_{15}$ are randomly selected. For each of the sixteen data classes, $2^{35.62}$ plaintext-ciphertext pairs are generated and used to approximate the conditional correlation for each class. Applying Equation (1) we can deduce that this amount of data would result in the substantial class having the highest correlation among all 16 classes with probability 0.95.

Results The experiment was repeated sixteen times. In fifteen of the sixteen runs, the substantial class was correctly identified. Furthermore, the magnitudes of the correlation observed for the substantial class fell in the interval $[2^{-16.2620}, 2^{-15.3295}]$ with one outlier at $2^{-17.0648}$. We deem this evidence sufficient to support the claim that the substantial conditional correlation of the conditional approximation $(r, u)|_X$ with $\texttt{AES}_k^1$ is greater than or equal to 2^{-16}. The details of this experiment and its results are attached as supplementary material.

5.4.2 Experiment 2

To show that a conditional approximation can be followed by (*i.e.*, prepended to) a "standard" linear approximation, we devised a second experiment covering two rounds. We restrict ourselves to a trail $(\overline{r}, \overline{v})|_{\overline{X}}$ which includes eight active S-boxes in the first round and two active S-boxes in the second. The conditional approximation is applied only to the S-boxes in the first round whereas the S-boxes in the second round are approximated in the standard way. The s-boxes have been chosen such that this approximation is expected to achieve a correlation with $\texttt{AES}_k^2$ of magnitude 2^{-14} when restricted to data from the substantial class, while achieving a correlation of 0 when restricted to data from other classes.

The setup of the experiment is identical to that of Experiment 1, except that the data complexity per class is reduced to $2^{31.62}$.

Results The experiment was executed sixteen times. In fourteen of the sixteen runs, the substantial class was correctly identified. Furthermore, the magnitudes of the correlation observed for the substantial class fell in the interval $[2^{-15.0900}, 2^{-13.4589}]$. We deem this evidence sufficient to support the claim that the substantial conditional correlation of the conditional approximation $(\overline{r}, \overline{u})|_X$ with $\texttt{AES}_k^2$ is greater than or equal to 2^{-14}. The details of this experiment and its results are furthermore attached as supplementary material.

6 Discussion and Conclusion

Let us recall that, according to the WTS, the number of rounds r for a cipher should be chosen such that the absolute correlation contribution of all linear trails is smaller than $\kappa^{-1} \cdot 2^{-n/2}$. For AES-128, this bound evaluates to $\frac{1}{128} \cdot 2^{-128/2} = 2^{-71}$, while for four-round AES, it has been shown that any linear trail has an absolute correlation contribution smaller than or equal to 2^{-75}, which is clearly smaller than 2^{-71}. It is thus argued that four-round AES is not vulnerable to attacks based on *standard* linear cryptanalysis. However, we observe that in literature this argument is often understood to apply to *all* forms of linear cryptanalysis. The presented statistical distinguisher and key-recovery attack demonstrate that this generalization does not apply.

We have observed that `inv`, the inversion function on 2^8 elements, has five input masks ω for every output mask $v \in \mathbb{F}_2^8 \setminus \{0\}$ s.t. $C_{v,\omega}^{\texttt{inv}} = 2^{-3}$. This allowed for the construction of a conditional approximation that achieves a conditional correlation of 2^{-1} when applied to `inv`. This approximation was then expanded to encompass a full round of the AES, which was used to construct a statistical distinguisher for four-round AES in the known-plaintext model; the existence of which was often understood to be impossible. We have moreover demonstrated a key-recovery attack capable of extracting 32 bits of information on the key using only $2^{125.62}$ data. To validate this attack, two small-scale experiments were performed that demonstrated that the conditional approximation can be used to achieve a 4-bit advantage when approximating one-round AES with sixteen active s-boxes and sampling $2^{35.62}$ data for all sixteen plaintext classes, and when approximating two-round AES with 10 active s-boxes while sampling $2^{31.62}$ per class.

With the distinguisher established and validated, this work demonstrates that four-round AES is statistically distinguishable from a random permutation in the known-plaintext model. In addition to illustrating that this round-reduced version is unsafe, this result furthermore presents a potential weakness in any cipher using it as a subroutine (*e.g.*, [MN17, WP13]). Even more impacting is the fact that the vulnerability in four-round AES stems from a caveat in the security argument of the Wide Trail Strategy. This security argument implicitly assumed that, in the case of AES, the correlation magnitude of an approximation for the s-box is upper bounded by 2^{-3}. As such, the conditional approximation forms a threat to the security of any of the multitude of ciphers constructed in recent years according to this design framework (*e.g.*, [AAB+20, BBI+15, BKL+07, GNL11, GKR+21, JNPS21], *etc.*).

References

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of symmetric-key primitives for advanced cryptographic protocols. *IACR Trans. Symmetric Cryptol.*, 2020(3):1–45, 2020.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436. Springer, 2015.

[BBK+13] Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013*, pages 142–158, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[BC14] Eli Biham and Yaniv Carmeli. An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X. In Antoine Joux and Amr Youssef, editors, *Selected Areas in Cryptography – SAC 2014*, pages 59–76, Cham, 2014. Springer International Publishing.

[Bih95] Eli Biham. On Matsui's linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 341–355, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[BP18] Eli Biham and Stav Perle. Conditional Linear Cryptanalysis – Cryptanalysis of DES with Less Than 2^{42} Complexity. *IACR Transactions on Symmetric Cryptology*, 2018(3):215–264, Sep. 2018.

[Dae95] Joan Daemen. *Cipher and hash function design, strategies based on linear and differential cryptanalysis, PhD Thesis*. K.U.Leuven, 1995. http://jda.noekeon.org/.

[DBN+01] Morris Dworkin, Elaine Barker, James Nechvatal, James Foti, Lawrence Bassham, E. Roback, and James Dray. *Advanced Encryption Standard (AES)*, November 2001.

[DGV95] Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation matrices. In Bart Preneel, editor, *Fast Software Encryption*, pages 275–285, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[DKR97] Joan Daemen, Lars Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *Fast Software Encryption*, pages 149–165, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[DR00] Joan Daemen and Vincent Rijmen. The Block Cipher BKSQ. In Jean-Jacques Quisquater and Bruce Schneier, editors, *Smart Card Research and Applications*, pages 236–245, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[DR01] Joan Daemen and Vincent Rijmen. The Wide Trail Design Strategy. In Bahram Honary, editor, *Cryptography and Coding*, pages 222–238, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[DR07] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Math. Cryptol.*, 1(3):221–242, 2007.

[DR20] Joan Daemen and Vincent Rijmen. *The Design of Rijndael*. Springer, 2 edition, 2020.

[GKM+09] Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen. Grøstl - a SHA-3 candidate. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography, 11.01. - 16.01.2009*, volume 09031 of *Dagstuhl Seminar Proceedings*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2009.

[GKR+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In Michael Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 519–535. USENIX Association, 2021.

[GNL11] Zheng Gong, Svetla Nikova, and Yee Wei Law. KLEIN: A new family of lightweight block ciphers. In Ari Juels and Christof Paar, editors, *RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers*, volume 7055 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2011.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The photon family of lightweight hash functions. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, pages 222–239, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw. The LED Block Cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, pages 326–341, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[HCN19] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Linear Cryptanalysis. *Journal of Cryptology*, 32(1):1–34, Jan 2019.

[HM97] Carlo Harpes and James L. Massey. Partitioning cryptanalysis. In Eli Biham, editor, *Fast Software Encryption*, pages 13–27, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[HN11] Miia Hermelin and Kaisa Nyberg. Linear Cryptanalysis Using Multiple Linear Approximations. *IACR Cryptol. ePrint Arch.*, page 93, 2011.

[JNPS21] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. The deoxys AEAD family. *J. Cryptol.*, 34(3):31, 2021.

[KMT01a] Liam Keliher, Henk Meijer, and Stafford Tavares. Improving the Upper Bound on the Maximum Average Linear Hull Probability for Rijndael. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography*, pages 112–128, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[KMT01b] Liam Keliher, Henk Meijer, and Stafford E. Tavares. New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 420–436. Springer, 2001.

[LMM91] Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 17–38, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[Mat93] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 386–397, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[MN17] Bart Mennink and Samuel Neves. Optimal prfs from blockcipher designs. *IACR Trans. Symmetric Cryptol.*, 2017(3):228–252, 2017.

[MY92] Mitsuru Matsui and Atsuhiro Yamagishi. A New Method for Known Plaintext Attack of FEAL Cipher. In *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, volume 658 of *Lecture Notes in Computer Science*, pages 81–91. Springer, 1992.

[New60] Donald J. Newman. The Double Dixie Cup Problem. *The American Mathematical Monthly*, 67(1):58–61, 1960.

[Nyb94] Kaisa Nyberg. Differentially uniform mappings for Cryptography. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 55–64, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[RDP+96] Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win. The cipher SHARK. In Dieter Gollmann, editor, *Fast Software Encryption*, pages 99–111, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[Sel08] Ali Aydın Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. *Journal of Cryptology*, 21(1):131–147, Jan 2008.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[WP13] Hongjun Wu and Bart Preneel. AEGIS: A fast authenticated encryption algorithm. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 185–201. Springer, 2013.

A Proofs

In this appendix, we present the proofs for all lemmas presented in this work. The proofs are provided in the same order as the lemmas are presented.

Lemma 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^p$, $G : \mathbb{F}_2^p \to \mathbb{F}_2^m$ and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$ be arbitrary vectorial Boolean functions. For all $b \in \mathbb{F}_2^r$ it holds that*

$$C^{G\circ F}\Big|_{\mathcal{P}_X^b} = C^G \cdot \left(C^F\Big|_{\mathcal{P}_X^b}\right).$$

Proof. Let us first observe that for any combination of masks $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, the correlation of approximation (u, v) with any vectorial Boolean function $H : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be computed as

$$C_{v,u}^H = \frac{1}{|\mathbb{F}_2^n|} \sum_{x\in\mathbb{F}_2^n} (-1)^{u^\top x \oplus v^\top H(x)}, \tag{13}$$

while conditional correlation can be computed as

$$C_{v,u}^H\Big|_{\mathcal{P}_X^b} = \frac{1}{|\mathcal{P}_X^b|} \sum_{x\in\mathcal{P}_X^b} (-1)^{u^\top x \oplus v^\top H(x)}. \tag{14}$$

We can use these equalities to see that for any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, it holds that

$$\begin{aligned}
&\sum_{z\in\mathbb{F}_2^p} C_{v,z}^G \cdot C_{z,u}^F\Big|_{\mathcal{P}_X^b} \\
&= \sum_{z\in\mathbb{F}_2^p} \left[\frac{1}{|\mathbb{F}_2^p|} \sum_{x\in\mathbb{F}_2^p} (-1)^{z^\top x \oplus v^\top G(x)}\right] \left[\frac{1}{|\mathcal{P}_X^b|} \sum_{y\in\mathcal{P}_X^b} (-1)^{u^\top y \oplus z^\top F(y)}\right] \\
&= \frac{1}{|\mathbb{F}_2^p|}\frac{1}{|\mathcal{P}_X^b|} \sum_{x\in\mathbb{F}_2^p}\sum_{y\in\mathcal{P}_X^b} (-1)^{u^\top y \oplus v^\top G(x)} \sum_{z\in\mathbb{F}_2^n} (-1)^{z^\top (x\oplus F(y))} \\
&\overset{(1)}{=} \frac{1}{|\mathbb{F}_2^p|}\frac{1}{|\mathcal{P}_X^b|} \sum_{x\in\mathbb{F}_2^p}\sum_{y\in\mathcal{P}_X^b} (-1)^{u^\top y \oplus v^\top G(x)} \cdot |\mathbb{F}_2^p| \cdot \delta_{x,F(y)} \\
&= \frac{1}{|\mathcal{P}_X^b|} \sum_{y\in\mathcal{P}_X^b} (-1)^{u^\top y \oplus v^\top G(F(y))} \\
&= C_{v,u}^{G\circ F}\Big|_{\mathcal{P}_X^b},
\end{aligned}$$

where step (1) follows from the fact that the parity function $z^\top \cdot$ is balanced. □

Lemma 2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an arbitrary permutation, let $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$ be arbitrary vectorial Boolean functions. For all $b \in \mathbb{F}_2^r$ it holds that*

$$C^{G\circ F}\Big|_{\mathcal{P}_{X\circ F}^b} = C^G\Big|_{\mathcal{P}_X^b} \cdot C^F.$$

Proof. We start with the observation that for any $x \in \mathbb{F}_2^n$ it holds that

$$\begin{aligned}
&F(x) \in \mathcal{P}_X^b \\
&\iff F(x) \in \{z \mid X(z) = b\} \\
&\iff x \in \{F^{-1}(z) \mid X(z) = b\} \\
&\iff x \in \{y \mid X(F(y)) = b\} \\
&\iff x \in \{y \mid y \in \mathcal{P}_{X\circ F}^b\} \\
&\iff x \in \mathcal{P}_{X\circ F}^b.
\end{aligned} \tag{15}$$

Let us furthermore recall Equation 13 and 14 for computing correlation and conditional correlation, listed in the proof of Lemma 1. We can use these equalities to see that

$$
\begin{aligned}
&\sum_{z\in\mathbb{F}_2^n} C^G_{v,z}\Big|_{\mathcal{P}_X^b} \cdot C^F_{z,u} \\
&= \sum_{z\in\mathbb{F}_2^n} \left[\frac{1}{|\mathcal{P}_X^b|}\sum_{x\in\mathcal{P}_X^b}(-1)^{z^\top x\oplus v^\top G(x)}\right]\left[\frac{1}{|\mathbb{F}_2^n|}\sum_{y\in\mathbb{F}_2^n}(-1)^{u^\top y\oplus z^\top F(y)}\right] \\
&= \frac{1}{|\mathcal{P}_X^b|}\frac{1}{|\mathbb{F}_2^n|}\sum_{x\in\mathcal{P}_X^b}\sum_{y\in\mathbb{F}_2^n}(-1)^{u^\top y\oplus v^\top G(x)}\sum_{z\in\mathbb{F}_2^n}(-1)^{z^\top(x\oplus F(y))} \\
&\overset{(1)}{=} \frac{1}{|\mathcal{P}_X^b|}\frac{1}{|\mathbb{F}_2^n|}\sum_{x\in\mathcal{P}_X^b}\sum_{y\in\mathbb{F}_2^n}(-1)^{u^\top y\oplus v^\top G(x)}\cdot|\mathbb{F}_2^n|\cdot\delta_{x,F(y)} \\
&= \frac{1}{|\mathcal{P}_X^b|}\frac{1}{|\mathbb{F}_2^n|}\sum_{x\in\mathcal{P}_X^b}\sum_{y\in\mathbb{F}_2^n}(-1)^{u^\top y\oplus v^\top G(x)}\cdot|\mathbb{F}_2^n|\cdot\delta_{F^{-1}(x),y} \\
&\overset{(2)}{=} \frac{1}{|\mathcal{P}_X^b|}\sum_{x\in\mathcal{P}_X^b}(-1)^{u^\top F^{-1}(x)\oplus v^\top G(x)} \\
&= \frac{1}{|\mathcal{P}_X^b|}\sum_{F(y)\in\mathcal{P}_X^b}(-1)^{u^\top y\oplus v^\top G(F(y))} \\
&\overset{(3)}{=} \frac{1}{|\mathcal{P}_X^b|}\sum_{z\in\mathcal{P}_{X\circ F}^b}(-1)^{u^\top z\oplus v^\top G(F(z))} \\
&\overset{(4)}{=} C^{G\circ F}_{v,u}\Big|_{\mathcal{P}_{X\circ F}^b},
\end{aligned}
$$

where step (1) follows from the fact that the parity function $z^\top\cdot$ is balanced, (2) from the fact that F is a permutation, (3) from Equation 15, and (4) from the fact that $|\mathcal{P}_X^b| = |\mathcal{P}_{X\circ F}^b|$. □

Lemma 3. *Let $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$, $G:\mathbb{F}_2^r\to\mathbb{F}_2^p$, $X:\mathbb{F}_2^n\to\mathbb{F}_2^q$ and $Y:\mathbb{F}_2^r\to\mathbb{F}_2^s$ be arbitrary vectorial Boolean functions. It holds that*

$$C^F\big|_{\mathcal{P}_X^a}\otimes C^G\Big|_{\mathcal{P}_Y^b} = C^{F\times G}\Big|_{\mathcal{P}_{X\times Y}^{a|b}}$$

for all $a\in\mathbb{F}_2^q$ and $b\in\mathbb{F}_2^s$, where $\otimes$ denotes the Kronecker product.

Proof. Let us first observe that $|\mathcal{P}_X^a|\cdot|\mathcal{P}_Y^b| = |\mathcal{P}_{X\times Y}^{a|b}|$ and that

$$y|z\in\mathcal{P}_{X\times Y}^{a|b} \iff y\in\mathcal{P}_X^a \text{ and } z\in\mathcal{P}_Y^b$$

for any $y \in \mathbb{F}_2^n$ and $z \in \mathbb{F}_2^r$. Let $v := v_1|v_2$ and $w := w_1|w_2$ be arbitrary. It then holds that

$$\begin{aligned}
C^{F\times G}_{v,w}\Big|_{\mathcal{P}^{a|b}_{X\times Y}} &= \frac{1}{|\mathcal{P}^{a|b}_{X\times Y}|}\sum_{x\in\mathcal{P}^{a|b}_{X\times Y}} (-1)^{w^\top x \oplus v^\top (F\times G)(x)} \\
&= \frac{1}{|\mathcal{P}^a_X|}\cdot\frac{1}{|\mathcal{P}^b_Y|}\sum_{y|z\in\mathcal{P}^{a|b}_{X\times Y}} (-1)^{(w_1|w_2)^\top (y|z)\oplus (v_1|v_2)^\top (F(y)|G(z))} \\
&= \frac{1}{|\mathcal{P}^a_X|}\cdot\frac{1}{|\mathcal{P}^b_Y|}\sum_{y\in\mathcal{P}^a_X}\sum_{z\in\mathcal{P}^b_Y} (-1)^{w_1^\top y\oplus w_2^\top z\oplus v_1^\top F(y)\oplus v_2^\top G(z)} \\
&= \left[\frac{1}{|\mathcal{P}^a_X|}\sum_{y\in\mathcal{P}^a_X}(-1)^{w_1^\top y\oplus v_1^\top F(y)}\right]\cdot\left[\frac{1}{|\mathcal{P}^b_Y|}\sum_{z\in\mathcal{P}^b_Y}(-1)^{w_2^\top z\oplus v_2^\top G(z)}\right] \\
&= C^F_{v_1,w_1}\big|_{\mathcal{P}^a_X}\cdot C^G_{v_2,w_2}\Big|_{\mathcal{P}^b_Y}
\end{aligned}$$

with $y \in \mathbb{F}_2^n$ and $z \in \mathbb{F}_2^m$. □

Lemma 4. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r$ be arbitrary vectorial Boolean functions. For any $b, b' \in \mathbb{F}_2^r$ s.t. $b \neq b'$, it holds that*

$$C^F\Big|_{\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X} = \frac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|}\cdot C^F\Big|_{\mathcal{P}^b_X} + \frac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|}\cdot C^F\Big|_{\mathcal{P}^{b'}_X}$$

when either $\mathcal{P}^b_X \neq \emptyset$ or $\mathcal{P}^{b'}_X \neq \emptyset$.

Proof. Let $s := |\mathcal{P}^b_X|$. Observe that

$$\begin{aligned}
&\mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x\in\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X\Big] \\
&= \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x\in\mathcal{P}^b_X\setminus\mathcal{P}^{b'}_X\Big]\cdot\mathbb{P}\Big[x\in\mathcal{P}^b_X\setminus\mathcal{P}^{b'}_X \;\Big|\; x\in\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X\Big] \\
&\quad + \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x\in\mathcal{P}^{b'}_X\setminus\mathcal{P}^b_X\Big]\cdot\mathbb{P}\Big[x\in\mathcal{P}^{b'}_X\setminus\mathcal{P}^b_X \;\Big|\; x\in\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X\Big] \\
&\quad + \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x\in\mathcal{P}^{b'}_X\cap\mathcal{P}^b_X\Big]\cdot\mathbb{P}\Big[x\in\mathcal{P}^{b'}_X\cap\mathcal{P}^b_X \;\Big|\; x\in\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X\Big] \\
&\overset{(1)}{=} \mathbb{P}\big[u^\top x = v^\top F(x) \;\big|\; x\in\mathcal{P}^b_X\big]\cdot\mathbb{P}\Big[x\in\mathcal{P}^b_X \;\Big|\; x\in\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X\Big] \\
&\quad + \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x\in\mathcal{P}^{b'}_X\Big]\cdot\mathbb{P}\Big[x\in\mathcal{P}^{b'}_X \;\Big|\; x\in\mathcal{P}^b_X\cup\mathcal{P}^{b'}_X\Big] \\
&= \mathbb{P}\big[u^\top x = v^\top F(x) \;\big|\; x\in\mathcal{P}^b_X\big]\cdot\tfrac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} \\
&\quad + \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x\in\mathcal{P}^{b'}_X\Big]\cdot\tfrac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|}
\end{aligned}$$

where step (1) follows from the assumption that $b \neq b'$ and $\mathcal{P}_F$ is a partition. This equality

can now be used to show that for any $u, v \in \mathbb{F}_2^n$ it holds that

$$\begin{aligned}
&C^F_{v,u}\Big|_{\mathcal{P}^b_X \cup \mathcal{P}^{b'}_X} \\
&= 2 \cdot \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x \in \mathcal{P}^b_X \cup \mathcal{P}^{b'}_X\Big] - 1 \\
&= 2\Big(\mathbb{P}\big[u^\top x = v^\top F(x) \;\big|\; x \in \mathcal{P}^b_X\big] \cdot \tfrac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} \\
&\quad + \mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x \in \mathcal{P}^{b'}_X\Big] \cdot \tfrac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|}\Big) - 1 \\
&\overset{(2)}{=} \tfrac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} \cdot \big(2\mathbb{P}\big[u^\top x = v^\top F(x) \;\big|\; x \in \mathcal{P}^b_X\big] - 1\big) \\
&\quad + \tfrac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} \cdot \Big(2\mathbb{P}\Big[u^\top x = v^\top F(x) \;\Big|\; x \in \mathcal{P}^{b'}_X\Big] - 1\Big) \\
&= \tfrac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} \cdot C^F_{v,u}\Big|_{\mathcal{P}^b_X} + \tfrac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} \cdot C^F_{v,u}\Big|_{\mathcal{P}^{b'}_X},
\end{aligned}$$

where step (2) involves the fact that $\frac{|\mathcal{P}^b_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} + \frac{|\mathcal{P}^{b'}_X|}{|\mathcal{P}^b_X|+|\mathcal{P}^{b'}_X|} = 1$. Since this holds for all u and v, the lemma follows. □

Lemma 5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an arbitrary permutation and $u, v \in \mathbb{F}_2^n$ arbitrary masks. For all $b \in \mathbb{F}_2$ it holds that*

$$(-1)^b \cdot C^F_{v,0}\Big|_{\mathcal{P}^b_X} = C^F_{v,u},$$

when $X : \mathbb{F}_2^n \to \mathbb{F}_2 : x \mapsto u^\top x$.

Proof. Note first of all that it follows from Lemma 4 that

$$C^F_{v,0}\Big|_{\mathcal{P}^0_X} + C^F_{v,0}\Big|_{\mathcal{P}^1_X} = 2 \cdot C^F_{v,0}\Big|_{\mathcal{P}^0_X \cup \mathcal{P}^1_X} = 2 \cdot C^F_{v,0} \overset{(1)}{=} 0,$$

where step (1) follows from the fact that F is a permutation. In particular, note that $C^F_{v,0}\Big|_{\mathcal{P}^0_X} = -C^F_{v,0}\Big|_{\mathcal{P}^1_X}$. Note furthermore that $|\mathcal{P}^0_X| = |\mathcal{P}^1_X| = |\mathbb{F}_2^n|/2$ since X is a balanced function. Subsequently,

$$\begin{aligned}
&C^F_{v,0}\Big|_{\mathcal{P}^0_X} - C^F_{v,0}\Big|_{\mathcal{P}^1_X} \\
&= \left[\frac{1}{|\mathcal{P}^0_X|} \sum_{x \in \mathcal{P}^0_X} (-1)^{0^\top x \oplus v^\top F(x)}\right] - \left[\frac{1}{|\mathcal{P}^1_X|} \sum_{x \in \mathcal{P}^1_X} (-1)^{0^\top x \oplus v^\top F(x)}\right] \\
&\overset{(2)}{=} \left[\frac{1}{|\mathcal{P}^0_X|} \sum_{x \in \mathcal{P}^0_X} (-1)^{u^\top x \oplus v^\top F(x)}\right] - \left[-\frac{1}{|\mathcal{P}^1_X|} \sum_{x \in \mathcal{P}^1_X} (-1)^{u^\top x \oplus v^\top F(x)}\right] \\
&= \frac{2}{|\mathbb{F}_2^n|} \sum_{x \in \mathbb{F}_2^n} (-1)^{u^\top x \oplus v^\top F(x)} \\
&= 2 \cdot C^F_{v,u},
\end{aligned}$$

where step (2) multiplies the summations with $(-1)^{u^\top x}$, which equals 1 for all $x \in \mathcal{P}^0_X$ and -1 for $x \in \mathcal{P}^1_X$. Combining these two results then gives that

$$C^F_{v,u} = \frac{1}{2}\Big(C^F_{v,0}\Big|_{\mathcal{P}^0_X} - C^F_{v,0}\Big|_{\mathcal{P}^1_X}\Big) = \frac{1}{2}\Big(C^F_{v,0}\Big|_{\mathcal{P}^0_X} + C^F_{v,0}\Big|_{\mathcal{P}^0_X}\Big) = C^F_{v,0}\Big|_{\mathcal{P}^0_X} \tag{16}$$

and also $C^F_{v,u} = -C^F_{v,0}\Big|_{\mathcal{P}^1_X}$. □

Lemma 6. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an arbitrary vectorial Boolean function, $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$ arbitrary masks, and $X : \mathbb{F}_2^n \to \mathbb{F}_2^r : x \mapsto (u_1^\top x, \ldots, u_r^\top x)$ an arbitrary linear vectorial Boolean function with $u_1, \ldots, u_r \in \mathbb{F}_2^n$ linearly independent. For all $b \in \mathbb{F}_2^r$ it holds that*

$$(-1)^{b_i} \cdot C^F_{v,u\oplus u_i}\Big|_{\mathcal{P}_X^b} = C^F_{v,u}\Big|_{\mathcal{P}_X^b}.$$

Proof. Let recall Equation 14 provided in the proof of Lemma 1. We can use this to show that

$$\begin{aligned}
C^F_{v,u}\Big|_{\mathcal{P}_X^b} &= \frac{1}{|\mathcal{P}_X^b|} \sum_{x\in\mathcal{P}_X^b} (-1)^{u^\top x \oplus v^\top F(x)} \\
&= \frac{1}{|\mathcal{P}_X^b|} \sum_{x\in\mathcal{P}_X^b} (-1)^{u^\top x \oplus v^\top F(x)} \cdot (-1)^{u_i^\top x} \cdot (-1)^{u_i^\top x} \\
&\overset{(1)}{=} (-1)^{b_i} \cdot \frac{1}{|\mathcal{P}_X^b|} \sum_{x\in\mathcal{P}_X^b} (-1)^{(u\oplus u_i)^\top x \oplus v^\top F(x)} \\
&= (-1)^{b_i} \cdot C^F_{v,u\oplus u_i}\Big|_{\mathcal{P}_X^b}.
\end{aligned}$$

Here, step (1) follows from the observation that $u_i^\top x = b_i$ for all $x \in \mathcal{P}_X^b$ and that $a^\top x \oplus b^\top x = (a \oplus b)^\top x$. □

Supplementary material

B $M_{\mathtt{H}}$

In Section 2.4, the algebraic description of the `MixColumns` function is presented. This function can be decomposed into the application of the function `H` to each column of the state. The matrix representation $M_{\mathtt{H}}$ of this function is presented below. To improve its readability, all one-entries in this matrix are printed in bold, while all zero-entries are represented with a dot. Moreover, three horizontal and three vertical lines have been included to aid in understanding the effect of applying this matrix to a four-byte column of the state.

$$M_{\mathtt{H}} = \left[\begin{array}{cccc|cccc|cccc|cccc}
\cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot \\
\cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot \\
\mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} \\
\mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\hline
\mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot \\
\cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot \\
\cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} \\
\cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\hline
\mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot \\
\cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot \\
\cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} \\
\cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} \\
\cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} \\
\hline
\mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot \\
\cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot \\
\cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot & \mathbf{1} \\
\mathbf{1} & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \cdot \\
\mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot \\
\mathbf{1} & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \mathbf{1} & \cdot & \mathbf{1} & \cdot & \cdot & \mathbf{1} \\
\mathbf{1} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1} & \cdot & \cdot & \cdot & \mathbf{1} & \mathbf{1} & \cdot & \cdot & \cdot
\end{array}\right]$$

C Lookup Tables

Table 9: Look-up table for inv(xy).

x \ y	· 0	· 1	· 2	· 3	· 4	· 5	· 6	· 7	· 8	· 9	· A	· B	· C	· D	· E	· F
0 ·	00_x	01_x	$8D_x$	$F6_x$	CB_x	52_x	$7B_x$	$D1_x$	$E8_x$	$4F_x$	29_x	$C0_x$	$B0_x$	$E1_x$	$E5_x$	$C7_x$
1 ·	74_x	$B4_x$	AA_x	$4B_x$	99_x	$2B_x$	60_x	$5F_x$	58_x	$3F_x$	FD_x	CC_x	FF_x	40_x	EE_x	$B2_x$
2 ·	$3A_x$	$6E_x$	$5A_x$	$F1_x$	55_x	$4D_x$	$A8_x$	$C9_x$	$C1_x$	$0A_x$	98_x	15_x	30_x	44_x	$A2_x$	$C2_x$
3 ·	$2C_x$	45_x	92_x	$6C_x$	$F3_x$	39_x	66_x	42_x	$F2_x$	35_x	20_x	$6F_x$	77_x	BB_x	59_x	19_x
4 ·	$1D_x$	FE_x	37_x	67_x	$2D_x$	31_x	$F5_x$	69_x	$A7_x$	64_x	AB_x	13_x	54_x	25_x	$E9_x$	09_x
5 ·	ED_x	$5C_x$	05_x	CA_x	$4C_x$	24_x	87_x	BF_x	18_x	$3E_x$	22_x	$F0_x$	51_x	EC_x	61_x	17_x
6 ·	16_x	$5E_x$	AF_x	$D3_x$	49_x	$A6_x$	36_x	43_x	$F4_x$	47_x	91_x	DF_x	33_x	93_x	21_x	$3B_x$
7 ·	79_x	$B7_x$	97_x	85_x	10_x	$B5_x$	BA_x	$3C_x$	$B6_x$	70_x	$D0_x$	06_x	$A1_x$	FA_x	81_x	82_x
8 ·	83_x	$7E_x$	$7F_x$	80_x	96_x	73_x	BE_x	56_x	$9B_x$	$9E_x$	95_x	$D9_x$	$F7_x$	02_x	$B9_x$	$A4_x$
9 ·	DE_x	$6A_x$	32_x	$6D_x$	$D8_x$	$8A_x$	84_x	72_x	$2A_x$	14_x	$9F_x$	88_x	$F9_x$	DC_x	89_x	$9A_x$
A ·	FB_x	$7C_x$	$2E_x$	$C3_x$	$8F_x$	$B8_x$	65_x	48_x	26_x	$C8_x$	12_x	$4A_x$	CE_x	$E7_x$	$D2_x$	62_x
B ·	$0C_x$	$E0_x$	$1F_x$	EF_x	11_x	75_x	78_x	71_x	$A5_x$	$8E_x$	76_x	$3D_x$	BD_x	BC_x	86_x	57_x
C ·	$0B_x$	28_x	$2F_x$	$A3_x$	DA_x	$D4_x$	$E4_x$	$0F_x$	$A9_x$	27_x	53_x	04_x	$1B_x$	FC_x	AC_x	$E6_x$
D ·	$7A_x$	07_x	AE_x	63_x	$C5_x$	DB_x	$E2_x$	EA_x	94_x	$8B_x$	$C4_x$	$D5_x$	$9D_x$	$F8_x$	90_x	$6B_x$
E ·	$B1_x$	$0D_x$	$D6_x$	EB_x	$C6_x$	$0E_x$	CF_x	AD_x	08_x	$4E_x$	$D7_x$	$E3_x$	$5D_x$	50_x	$1E_x$	$B3_x$
F ·	$5B_x$	23_x	38_x	34_x	68_x	46_x	03_x	$8C_x$	DD_x	$9C_x$	$7D_x$	$A0_x$	CD_x	$1A_x$	41_x	$1C_x$

Table 10: Look-up table for the AES s-box function $S(xy)$

x \ y	· 0	· 1	· 2	· 3	· 4	· 5	· 6	· 7	· 8	· 9	· A	· B	· C	· D	· E	· F
0 ·	63_x	$7C_x$	77_x	$7B_x$	$F2_x$	$6B_x$	$6F_x$	$C5_x$	30_x	01_x	67_x	$2B_x$	FE_x	$D7_x$	AB_x	76_x
1 ·	CA_x	82_x	$C9_x$	$7D_x$	FA_x	59_x	47_x	$F0_x$	AD_x	$D4_x$	$A2_x$	AF_x	$9C_x$	$A4_x$	72_x	$C0_x$
2 ·	$B7_x$	FD_x	93_x	26_x	36_x	$3F_x$	$F7_x$	CC_x	34_x	$A5_x$	$E5_x$	$F1_x$	71_x	$D8_x$	31_x	15_x
3 ·	04_x	$C7_x$	23_x	$C3_x$	18_x	96_x	05_x	$9A_x$	07_x	12_x	80_x	$E2_x$	EB_x	27_x	$B2_x$	75_x
4 ·	09_x	83_x	$2C_x$	$1A_x$	$1B_x$	$6E_x$	$5A_x$	$A0_x$	52_x	$3B_x$	$D6_x$	$B3_x$	29_x	$E3_x$	$2F_x$	84_x
5 ·	53_x	$D1_x$	00_x	ED_x	20_x	FC_x	$B1_x$	$5B_x$	$6A_x$	CB_x	BE_x	39_x	$4A_x$	$4C_x$	58_x	CF_x
6 ·	$D0_x$	EF_x	AA_x	FB_x	43_x	$4D_x$	33_x	85_x	45_x	$F9_x$	02_x	$7F_x$	50_x	$3C_x$	$9F_x$	$A8_x$
7 ·	51_x	$A3_x$	40_x	$8F_x$	92_x	$9D_x$	38_x	$F5_x$	BC_x	$B6_x$	DA_x	21_x	10_x	FF_x	$F3_x$	$D2_x$
8 ·	CD_x	$0C_x$	13_x	EC_x	$5F_x$	97_x	44_x	17_x	$C4_x$	$A7_x$	$7E_x$	$3D_x$	64_x	$5D_x$	19_x	73_x
9 ·	60_x	81_x	$4F_x$	DC_x	22_x	$2A_x$	90_x	88_x	46_x	EE_x	$B8_x$	14_x	DE_x	$5E_x$	$0B_x$	DB_x
A ·	$E0_x$	32_x	$3A_x$	$0A_x$	49_x	06_x	24_x	$5C_x$	$C2_x$	$D3_x$	AC_x	62_x	91_x	95_x	$E4_x$	79_x
B ·	$E7_x$	$C8_x$	37_x	$6D_x$	$8D_x$	$D5_x$	$4E_x$	$A9_x$	$6C_x$	56_x	$F4_x$	EA_x	65_x	$7A_x$	AE_x	08_x
C ·	BA_x	78_x	25_x	$2E_x$	$1C_x$	$A6_x$	$B4_x$	$C6_x$	$E8_x$	DD_x	74_x	$1F_x$	$4B_x$	BD_x	$8B_x$	$8A_x$
D ·	70_x	$3E_x$	$B5_x$	66_x	48_x	03_x	$F6_x$	$0E_x$	61_x	35_x	57_x	$B9_x$	86_x	$C1_x$	$1D_x$	$9E_x$
E ·	$E1_x$	$F8_x$	98_x	11_x	69_x	$D9_x$	$8E_x$	94_x	$9B_x$	$1E_x$	87_x	$E9_x$	CE_x	55_x	28_x	DF_x
F ·	$8C_x$	$A1_x$	89_x	$0D_x$	BF_x	$E6_x$	42_x	68_x	41_x	99_x	$2D_x$	$0F_x$	$B0_x$	54_x	BB_x	16_x

D Masks

Table 11: The masks $\omega_1, \omega_2, \omega_3 \in \Omega_v$ for every $v \in \mathbb{F}_2^8 \setminus \{0\}$.

v	ω_1	ω_2	ω_3
01_x	84_x	63_x	$F3_x$
02_x	$7C_x$	$A2_x$	$D2_x$
03_x	42_x	31_x	$F9_x$
04_x	$3E_x$	69_x	$D1_x$
05_x	$5A_x$	CD_x	FD_x
06_x	$D4_x$	$9A_x$	61_x
07_x	$A1_x$	18_x	FC_x
08_x	80_x	97_x	DA_x
09_x	$9F_x$	AB_x	68_x
$0A_x$	AD_x	53_x	CB_x
$0B_x$	$4C_x$	89_x	93_x
$0C_x$	AE_x	$A2_x$	$A0_x$
$0D_x$	EA_x	CD_x	$B0_x$
$0E_x$	$D0_x$	DC_x	AE_x
$0F_x$	$C9_x$	44_x	54_x
10_x	47_x	33_x	$7B_x$
11_x	40_x	$8B_x$	ED_x
12_x	$4F_x$	$9A_x$	FB_x
13_x	$9E_x$	$1B_x$	43_x
14_x	$9A_x$	60_x	61_x
15_x	56_x	$A9_x$	$B3_x$
16_x	$A6_x$	$E2_x$	$C9_x$
17_x	CA_x	08_x	$2C_x$
18_x	57_x	50_x	$D1_x$
19_x	$7F_x$	$F2_x$	$C9_x$
$1A_x$	$1E_x$	99_x	92_x
$1B_x$	75_x	13_x	$D8_x$
$1C_x$	$E8_x$	BF_x	86_x
$1D_x$	$C4_x$	$4A_x$	78_x
$1E_x$	$1A_x$	20_x	$6C_x$
$1F_x$	64_x	22_x	AA_x
20_x	23_x	$3D_x$	99_x
21_x	$4D_x$	$6A_x$	EA_x
22_x	$F6_x$	$E9_x$	DB_x
23_x	20_x	76_x	$E5_x$
24_x	$A7_x$	$6A_x$	DA_x
25_x	54_x	$3B_x$	$D9_x$
26_x	43_x	85_x	94_x
27_x	CF_x	$C2_x$	21_x
28_x	$C5_x$	$3A_x$	93_x
29_x	CD_x	30_x	$B0_x$
$2A_x$	$2B_x$	54_x	$D9_x$
$2B_x$	$2A_x$	$6D_x$	51_x
$2C_x$	DA_x	CD_x	30_x
$2D_x$	$D3_x$	$F1_x$	64_x
$2E_x$	65_x	$E1_x$	$F3_x$
$2F_x$	$F5_x$	71_x	82_x
30_x	$C2_x$	29_x	$2C_x$
31_x	AB_x	$A8_x$	68_x
32_x	$3F_x$	79_x	$5B_x$
33_x	$6F_x$	10_x	$E2_x$
34_x	$8A_x$	09_x	$C1_x$
35_x	$8F_x$	43_x	49_x
36_x	$3A_x$	$6C_x$	89_x
37_x	$C8_x$	38_x	$B2_x$
38_x	$F4_x$	$C3_x$	AB_x
39_x	$B9_x$	$F8_x$	$E4_x$
$3A_x$	36_x	28_x	$B1_x$
$3B_x$	62_x	25_x	$3C_x$
$3C_x$	$8D_x$	10_x	$3B_x$
$3D_x$	89_x	20_x	56_x
$3E_x$	04_x	$B9_x$	$E0_x$
$3F_x$	32_x	55_x	91_x
40_x	11_x	$9E_x$	CC_x
41_x	50_x	39_x	$D6_x$
42_x	03_x	$5C_x$	68_x
43_x	26_x	13_x	53_x
44_x	$7B_x$	74_x	$6D_x$
45_x	69_x	$E8_x$	86_x
46_x	78_x	67_x	32_x
47_x	10_x	$3B_x$	$E2_x$
48_x	$D9_x$	$B6_x$	$A6_x$
49_x	53_x	35_x	ED_x
$4A_x$	AA_x	$1D_x$	EC_x
$4B_x$	68_x	34_x	$A8_x$
$4C_x$	$0B_x$	$A4_x$	$B1_x$
$4D_x$	21_x	$C2_x$	CA_x
$4E_x$	$E7_x$	$E1_x$	90_x
$4F_x$	12_x	90_x	$F5_x$
50_x	41_x	18_x	$E4_x$
51_x	$E2_x$	$C9_x$	$9D_x$
52_x	66_x	98_x	$D8_x$
53_x	49_x	$0A_x$	$9E_x$
54_x	25_x	$2A_x$	$7B_x$
55_x	95_x	AA_x	79_x
56_x	15_x	23_x	28_x
57_x	18_x	04_x	$E4_x$
58_x	ED_x	$8B_x$	98_x
59_x	$B8_x$	50_x	$D6_x$
$5A_x$	05_x	08_x	CA_x
$5B_x$	$E9_x$	32_x	78_x
$5C_x$	$B2_x$	$F0_x$	$F9_x$
$5D_x$	86_x	81_x	39_x
$5E_x$	$F2_x$	$C9_x$	54_x
$5F_x$	$7A_x$	38_x	$C1_x$
60_x	$E1_x$	14_x	96_x
61_x	77_x	71_x	63_x
62_x	$3B_x$	$9D_x$	$D9_x$
63_x	$D5_x$	01_x	61_x
64_x	$1F_x$	32_x	$A3_x$
65_x	$2E_x$	$9B_x$	FA_x
66_x	52_x	58_x	49_x
67_x	$B7_x$	88_x	$F1_x$
68_x	$4B_x$	09_x	31_x
69_x	45_x	41_x	$E0_x$
$6A_x$	$C7_x$	21_x	$E3_x$
$6B_x$	$C1_x$	42_x	$B2_x$
$6C_x$	BA_x	$A4_x$	$8C_x$
$6D_x$	$9D_x$	$2B_x$	$D9_x$
$6E_x$	$E4_x$	$F8_x$	59_x
$6F_x$	33_x	25_x	48_x
70_x	AC_x	$D0_x$	$D2_x$
71_x	FA_x	$D5_x$	61_x
72_x	DC_x	72_x	$A0_x$
73_x	$9C_x$	03_x	$6B_x$
74_x	$B6_x$	10_x	$F2_x$
75_x	$1B_x$	58_x	94_x
76_x	$B1_x$	$1E_x$	92_x
77_x	61_x	60_x	$4E_x$
78_x	46_x	$5B_x$	88_x

v	ω_1	ω_2	ω_3
79_x	BC_x	32_x	$E9_x$
$7A_x$	$5F_x$	68_x	$9F_x$
$7B_x$	44_x	10_x	$2B_x$
$7C_x$	02_x	70_x	DC_x
$7D_x$	$E6_x$	$C2_x$	29_x
$7E_x$	DE_x	$D0_x$	70_x
$7F_x$	19_x	$2A_x$	48_x
80_x	08_x	CF_x	$E6_x$
81_x	$F8_x$	45_x	$5D_x$
82_x	$B5_x$	$9A_x$	FA_x
83_x	$A8_x$	$9C_x$	$6B_x$
84_x	01_x	$2E_x$	$B4_x$
85_x	98_x	13_x	BE_x
86_x	$5D_x$	18_x	41_x
87_x	93_x	89_x	$A9_x$
88_x	$8E_x$	$E9_x$	78_x
89_x	$3D_x$	$0B_x$	BA_x
$8A_x$	34_x	$C0_x$	$C3_x$
$8B_x$	94_x	11_x	58_x
$8C_x$	FF_x	$1A_x$	93_x
$8D_x$	$3C_x$	33_x	19_x
$8E_x$	88_x	$1D_x$	79_x
$8F_x$	35_x	40_x	$D8_x$
90_x	$9B_x$	$D5_x$	$D4_x$
91_x	EC_x	$D3_x$	$5B_x$
92_x	$A9_x$	$1A_x$	76_x
93_x	87_x	$0B_x$	28_x
94_x	$8B_x$	AD_x	75_x
95_x	55_x	DB_x	$A3_x$
96_x	$B4_x$	$9A_x$	60_x
97_x	EB_x	05_x	08_x
98_x	85_x	52_x	58_x
99_x	DF_x	$1A_x$	20_x
$9A_x$	14_x	12_x	82_x
$9B_x$	90_x	$F5_x$	71_x
$9C_x$	73_x	$F0_x$	$C8_x$
$9D_x$	$6D_x$	62_x	51_x
$9E_x$	13_x	40_x	AD_x
$9F_x$	09_x	$7A_x$	$C8_x$
$A0_x$	$A0_x$	AC_x	$D2_x$
$A1_x$	07_x	$B8_x$	$D1_x$
$A2_x$	$D2_x$	$D0_x$	$0C_x$
$A3_x$	$F1_x$	CE_x	64_x
$A4_x$	$B3_x$	$4C_x$	$6C_x$
$A5_x$	$D1_x$	50_x	$B8_x$

v	ω_1	ω_2	ω_3
$A6_x$	16_x	48_x	62_x
$A7_x$	24_x	21_x	EB_x
$A8_x$	83_x	31_x	$C8_x$
$A9_x$	92_x	15_x	$3D_x$
AA_x	$4A_x$	55_x	BC_x
AB_x	31_x	38_x	$C8_x$
AC_x	70_x	$A0_x$	DC_x
AD_x	$0A_x$	11_x	94_x
AE_x	$0C_x$	02_x	72_x
AF_x	$E5_x$	$A9_x$	93_x
$B0_x$	EE_x	$E3_x$	29_x
$B1_x$	76_x	$3A_x$	$B3_x$
$B2_x$	$5C_x$	$6B_x$	$A8_x$
$B3_x$	$A4_x$	$B1_x$	92_x
$B4_x$	96_x	12_x	63_x
$B5_x$	82_x	84_x	65_x
$B6_x$	74_x	19_x	48_x
$B7_x$	67_x	$4A_x$	91_x
$B8_x$	59_x	$F8_x$	FC_x
$B9_x$	39_x	$3E_x$	$D6_x$
BA_x	$6C_x$	20_x	89_x
BB_x	$C3_x$	$C0_x$	$9C_x$
BC_x	79_x	64_x	AA_x
BD_x	BF_x	81_x	$D1_x$
BE_x	CC_x	49_x	52_x
BF_x	BD_x	$A1_x$	$E0_x$
$C0_x$	$F0_x$	$4B_x$	$7A_x$
$C1_x$	$6B_x$	34_x	$F4_x$
$C2_x$	30_x	27_x	$7D_x$
$C3_x$	BB_x	31_x	38_x
$C4_x$	$1D_x$	$D3_x$	$F1_x$
$C5_x$	28_x	23_x	99_x
$C6_x$	FE_x	$D8_x$	CB_x
$C7_x$	$6A_x$	80_x	$B0_x$
$C8_x$	37_x	AB_x	$9F_x$
$C9_x$	$0F_x$	19_x	51_x
CA_x	17_x	$5A_x$	EA_x
CB_x	$D7_x$	$0A_x$	11_x
CC_x	BE_x	$8B_x$	40_x
CD_x	29_x	$2C_x$	24_x
CE_x	DB_x	$C4_x$	78_x
CF_x	27_x	$5A_x$	80_x
$D0_x$	$0E_x$	70_x	$A2_x$
$D1_x$	$A5_x$	$A1_x$	18_x
$D2_x$	$A2_x$	$A0_x$	70_x

v	ω_1	ω_2	ω_3
$D3_x$	$2D_x$	91_x	$E9_x$
$D4_x$	06_x	63_x	90_x
$D5_x$	63_x	71_x	90_x
$D6_x$	$E0_x$	41_x	59_x
$D7_x$	CB_x	ED_x	98_x
$D8_x$	DD_x	$1B_x$	52_x
$D9_x$	48_x	$6D_x$	$2A_x$
DA_x	$2C_x$	08_x	EB_x
DB_x	CE_x	22_x	$5B_x$
DC_x	72_x	$7C_x$	AC_x
DD_x	$D8_x$	13_x	40_x
DE_x	$7E_x$	02_x	$A2_x$
DF_x	99_x	92_x	$A4_x$
$E0_x$	$D6_x$	$E8_x$	69_x
$E1_x$	60_x	$4E_x$	$9B_x$
$E2_x$	51_x	16_x	62_x
$E3_x$	FD_x	$B0_x$	$6A_x$
$E4_x$	$6E_x$	39_x	50_x
$E5_x$	AF_x	BA_x	23_x
$E6_x$	$7D_x$	$6A_x$	80_x
$E7_x$	$4E_x$	01_x	FB_x
$E8_x$	$1C_x$	59_x	$E0_x$
$E9_x$	$5B_x$	79_x	88_x
EA_x	$0D_x$	21_x	CA_x
EB_x	97_x	30_x	DA_x
EC_x	91_x	$4A_x$	$C4_x$
ED_x	58_x	49_x	$D7_x$
EE_x	$B0_x$	97_x	30_x
EF_x	FC_x	$F8_x$	$B9_x$
$F0_x$	$C0_x$	$F7_x$	$9C_x$
$F1_x$	$A3_x$	$2D_x$	$C4_x$
$F2_x$	$5E_x$	19_x	$2A_x$
$F3_x$	FB_x	01_x	$D5_x$
$F4_x$	38_x	$B2_x$	$C1_x$
$F5_x$	$2F_x$	60_x	$9B_x$
$F6_x$	22_x	88_x	95_x
$F7_x$	$F9_x$	$F0_x$	$8A_x$
$F8_x$	81_x	$B8_x$	$6E_x$
$F9_x$	$F7_x$	03_x	AB_x
FA_x	71_x	14_x	82_x
FB_x	$F3_x$	$E1_x$	14_x
FC_x	EF_x	$E8_x$	$B8_x$
FD_x	$E3_x$	05_x	29_x
FE_x	$C6_x$	$0A_x$	52_x
FF_x	$8C_x$	99_x	28_x

E Experiment details

This appendix discusses the three experiments in detail and presents the results of each.

E.1 Experiment 1

The first experiment verifies the conditional approximation $(r, u)|_X$ used for the first round. We present the linear trail part (r, u) of this approximation in Figure 7. Note that this trail is formed as the concatenation of the trails presented in figures 5 and 4. The conditioning function X is identical to the one found in Equation 10.

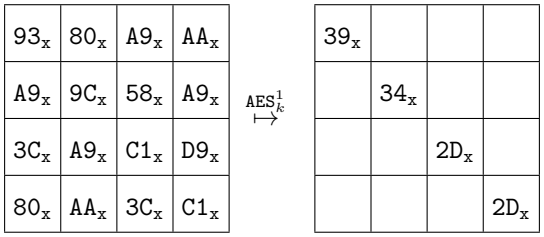

Figure 7: Linear trail (u, v) for one-round AES with 16 active s-boxes.

For this experiment, it was decided to compute an approximation of the correlation of (r, u) with $\texttt{AES}^1_k$ for sixteen of the 2^{32} data classes induced by X: $X(k_0)$, the class expected to achieve a 2^{-16} conditional correlation, and fifteen arbitrary classes, each expected to achieve a correlation of 0. Leveraging Corollary 1, we find that sampling

$$\begin{aligned} N &= \left(\Phi^{-1}(P_S) + \Phi^{-1}(1 - 2^{-a-1})\right)^2 \cdot C^{-2} \\ &= \left(\Phi^{-1}(0.95) + \Phi^{-1}(1 - 2^{-a-1})\right)^2 \cdot (2^{-16})^{-2} \\ &= 12.31 \cdot 2^{32} \approx 2^{35.62} \end{aligned}$$

uniformly random sampled plaintext-ciphertext pairs per class, should allow $X(k_0)$ to achieve the greatest correlation magnitude of all sixteen classes with a probability of 0.95 if its correlation is indeed 2^{-16} and 0 for the other, arbitrarily chosen classes. Thus, we

1. sample $2^{35.62}$ data for each class,
2. use this data to approximate the correlation of (u, v) with $\texttt{AES}^1_k$ for each class, and
3. verify that the correlation corresponding with the correct data class has the greatest magnitude of the sixteen classes.

The experiment was run sixteen times. The randomly generated encryption keys k as well as the IDs of the classes $X(k_0)$ for each run are presented in Table 12. An overview of the observed correlation approximations for each class are found in Tables 13–16.

E.2 Experiment 2

The second experiment verifies the conditional approximation $(\overline{r}, \overline{v})|_{\overline{X}}$ used for the first two rounds. We present the linear trail part $(\overline{r}, \overline{v})$ of this approximation in Figure 8. Note that this trail is formed as an extension of partial the concatenation of the trails presented in figures 5, and 4, and is expected to achieve a correlation of 2^{-14} on the substantial class. The conditioning function X is a modified version of the one found in Equation 10, and is presented in Equation 17.

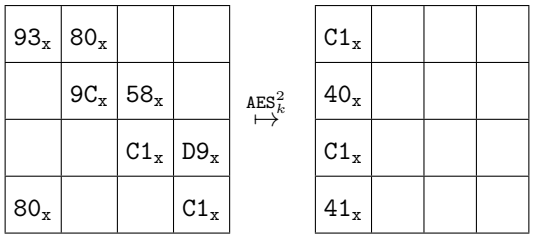

Figure 8: Linear trail $(\overline{r}, \overline{v})$ for two-round AES with 10 active s-boxes.

$$
\begin{aligned}
X : \mathbb{F}_2^{128} \to \mathbb{F}_2^{16} :\ x \mapsto\ & \\
(&\texttt{E5}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{7D}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{7D}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{C0}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{94}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{7A}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{9D}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{7A}_{\mathtt{x}}^{\top} x, \\
&\texttt{3A}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{EA}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{EA}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{6B}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{49}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{F9}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{F2}\ \texttt{00}_{\mathtt{x}}^{\top} x, \\
&\texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{00}\ \texttt{F9}_{\mathtt{x}}^{\top} x)
\end{aligned}
\tag{17}
$$

For this experiment, it was decided to compute an approximation of the correlation of $(\overline{r}, \overline{v})$ with $\texttt{AES}_k^2$ for sixteen of the 2^{32} data classes induced by X: $X(k_0)$: the substantial class and fifteen arbitrary classes expected to achieve a correlation of 0. Leveraging Corollary 1, we find that sampling

$$
\begin{aligned}
N &= \left(\Phi^{-1}(P_S) + \Phi^{-1}(1 - 2^{-a-1})\right)^2 \cdot C^{-2} \\
&= \left(\Phi^{-1}(0.95) + \Phi^{-1}(1 - 2^{-a-1})\right)^2 \cdot (2^{-14})^{-2} \\
&= 12.31 \cdot 2^{28} \approx 2^{31.62}
\end{aligned}
$$

uniformly random sampled plaintext-ciphertext pairs per class, should allow the substantial class to achieve the greatest correlation magnitude of all sixteen classes with a probability of 0.95 if its correlation is indeed 2^{-14} and 0 for the other, arbitrarily chosen classes.

The experiment was run sixteen times. The randomly generated encryption keys k as well as the IDs of the classes $X(k_0)$ for each run are presented in Table 17. An overview of the observed correlation approximations for each class are found in tables 18 and 19.

Table 12: Settings Experiment 1

run	key k	substantial class $X(k_0)$
1	88 0E E0 4B BF 21 F4 33 13 A3 8D FE 49 59 3B FB_x	$D9FB9362_x$
2	8B 7A EB E0 59 3F 1B C7 69 05 9B 19 A6 98 56 $2F_x$	$22E950DB_x$
3	D6 B6 42 AF 31 1F C6 E3 0A 11 6A 19 89 02 B3 CE_x	$C9C74D71_x$
4	34 73 51 C4 88 FD 52 31 3E A4 BF 25 81 58 70 89_x	$691F40BB_x$
5	5C 75 EF 33 F4 83 1C 39 2D 50 8A 7D 23 E7 61 $2A_x$	$36C749DC_x$
6	6E 24 F2 80 74 B3 DD B1 AC 1C 69 AE 87 CF 3A $E4_x$	$A7ACF5DB_x$
7	79 F4 39 C6 0E E0 A9 25 A7 2A 55 6F C1 25 63 99_x	$A096F3E6_x$
8	FB 1B 90 FE F3 6A FE E9 7A 14 B0 BA EF EB 51 $D3_x$	$560533AC_x$
9	3C A5 5A 91 15 CF E2 17 36 9C 77 61 F1 94 CF 89_x	$0841D2D3_x$
10	40 B7 FE 84 B3 C2 E6 CB 17 5A 59 DF 6A 9B 62 13_x	$B9E85A1A_x$
11	5C E2 A9 5B 40 85 49 F5 49 7D C5 A9 23 17 95 $9B_x$	$2EB55D68_x$
12	F3 A3 74 6B 7C 95 34 2B 08 A4 CB 07 85 78 CA 43_x	$4F3CEE16_x$
13	68 D8 84 4F EB 86 F0 85 28 A0 06 17 F5 11 21 $B6_x$	$05731E8B_x$
14	F8 29 2B 7E A4 06 98 88 B3 2A 02 98 DD B1 88 29_x	$D124C4C7_x$
15	88 C0 B6 C1 34 7B 85 C0 6A E3 B6 3E A2 B4 0C 35_x	$CDE8ACA5_x$
16	5D FA 71 65 47 00 57 D6 8E EC 35 C1 7D 62 73 69_x	$CA1D403C_x$

Table 13: Results Experiment 1, run 1-3

Run 1		Run 2		Run 3	
Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.
$D9FB9362_x$	$2^{-15.4999}$	$22E950DB_x$	$2^{-16.1102}$	$C9C74D71_x$	$-2^{-15.9625}$
$D818A478_x$	$2^{-19.1573}$	$CE3417E4_x$	$2^{-18.1270}$	$5B05CFDC_x$	$-2^{-19.3660}$
$E605FB82_x$	$-2^{-17.9155}$	$B8CB982E_x$	$2^{-19.8481}$	$D4F596BC_x$	$2^{-17.2500}$
$B2674FB6_x$	$-2^{-17.6730}$	04857711_x	$-2^{-18.5216}$	$8E3CEED7_x$	$-2^{-18.0353}$
$8A3B6341_x$	$2^{-17.5305}$	$0E9736CE_x$	$2^{-17.9451}$	$2527A236_x$	$2^{-21.0380}$
$01AAA9D9_x$	$2^{-19.5722}$	$30C1E6DA_x$	$2^{-17.7053}$	$BEAA017C_x$	$2^{-19.7306}$
$3E3CCD29_x$	$-2^{-17.7783}$	$E715387C_x$	$-2^{-17.6672}$	$FE483590_x$	$2^{-17.4687}$
$4C4E58B7_x$	$-2^{-22.4873}$	$F854C41D_x$	$-2^{-17.9095}$	$8EE41D6D_x$	$-2^{-18.2623}$
$7DCDAD8B_x$	$2^{-19.7293}$	$03FA8B0E_x$	$2^{-17.8999}$	$462E26EE_x$	$-2^{-19.2456}$
$748D48A9_x$	$2^{-17.3644}$	$CFF74618_x$	$2^{-21.4722}$	$1C0B28EB_x$	$2^{-17.9268}$
$BE90D164_x$	$-2^{-17.6962}$	$146146C7_x$	$-2^{-18.5509}$	$DBAFA19B_x$	$2^{-17.4078}$
$4527B12D_x$	$-2^{-17.5678}$	$CA06AB96_x$	$-2^{-22.9214}$	$845A6D19_x$	$-2^{-18.1232}$
$987ABE46_x$	$-2^{-18.0745}$	$A6846144_x$	$2^{-18.6522}$	$90E62B87_x$	$-2^{-16.8759}$
$83945F76_x$	$2^{-17.3502}$	$394B5D83_x$	$-2^{-16.5908}$	$A77796EB_x$	$-2^{-16.9372}$
$E9B0845F_x$	$2^{-18.0487}$	$1CC311A6_x$	$-2^{-18.5728}$	$A62113EF_x$	$2^{-17.8797}$
$A087006E_x$	$-2^{-18.1554}$	$F7AA8286_x$	$-2^{-20.4581}$	$12BC7FF7_x$	$-2^{-18.6994}$

Table 14: Results Experiment 1, run 4-12

Run 4

Class	Cond. corr.
$\texttt{691F40BB}_\texttt{x}$	$-2^{-15.7756}$
$\texttt{16E3FDBE}_\texttt{x}$	$2^{-23.7022}$
$\texttt{B3897963}_\texttt{x}$	$2^{-18.7780}$
$\texttt{93CFEF88}_\texttt{x}$	$2^{-17.3957}$
$\texttt{A7B89A0C}_\texttt{x}$	$-2^{-16.8270}$
$\texttt{FB5C4923}_\texttt{x}$	$-2^{-17.1264}$
$\texttt{4B257145}_\texttt{x}$	$2^{-18.7155}$
$\texttt{59C4690F}_\texttt{x}$	$-2^{-18.0092}$
$\texttt{E75E61C7}_\texttt{x}$	$2^{-18.1044}$
$\texttt{7108E4AF}_\texttt{x}$	$2^{-19.0402}$
$\texttt{508A71FF}_\texttt{x}$	$-2^{-19.2861}$
$\texttt{F8ED0A0B}_\texttt{x}$	$2^{-18.7207}$
$\texttt{F24337B1}_\texttt{x}$	$-2^{-18.8501}$
$\texttt{0C34BDF3}_\texttt{x}$	$-2^{-17.4189}$
$\texttt{398233B0}_\texttt{x}$	$2^{-17.6361}$
$\texttt{83FB82ED}_\texttt{x}$	$2^{-18.6361}$

Run 5

Class	Cond. corr.
$\texttt{36C749DC}_\texttt{x}$	$2^{-16.2046}$
$\texttt{FBCFEAC8}_\texttt{x}$	$2^{-18.3684}$
$\texttt{61CA4EFA}_\texttt{x}$	$2^{-19.1917}$
$\texttt{66F33BE1}_\texttt{x}$	$2^{-19.5200}$
$\texttt{E4C79FDF}_\texttt{x}$	$2^{-18.5953}$
$\texttt{51B30397}_\texttt{x}$	$-2^{-20.0508}$
$\texttt{6E6105C0}_\texttt{x}$	$2^{-17.9348}$
$\texttt{CC14343D}_\texttt{x}$	$-2^{-18.8991}$
$\texttt{89A6C359}_\texttt{x}$	$2^{-19.5868}$
$\texttt{4921655D}_\texttt{x}$	$2^{-17.4314}$
$\texttt{B5DAA46B}_\texttt{x}$	$2^{-17.2169}$
$\texttt{411ED3B3}_\texttt{x}$	$2^{-21.0006}$
$\texttt{BBE96696}_\texttt{x}$	$-2^{-18.1351}$
$\texttt{32A5DEAF}_\texttt{x}$	$-2^{-16.8141}$
$\texttt{FFD6F2AE}_\texttt{x}$	$2^{-17.2869}$
$\texttt{E97815C2}_\texttt{x}$	$-2^{-19.7837}$

Run 6

Class	Cond. corr.
$\texttt{A7ACF5DB}_\texttt{x}$	$-2^{-15.3295}$
$\texttt{3723281B}_\texttt{x}$	$2^{-19.9286}$
$\texttt{A7791C20}_\texttt{x}$	$2^{-17.6121}$
$\texttt{57D0D38A}_\texttt{x}$	$-2^{-20.2062}$
$\texttt{2E8AA8D0}_\texttt{x}$	$-2^{-17.9525}$
$\texttt{AF73613D}_\texttt{x}$	$-2^{-18.0425}$
$\texttt{2127A29C}_\texttt{x}$	$2^{-18.3473}$
$\texttt{B999CDA8}_\texttt{x}$	$2^{-18.4215}$
$\texttt{9B722706}_\texttt{x}$	$2^{-17.0399}$
$\texttt{ABB3564F}_\texttt{x}$	$2^{-17.9552}$
$\texttt{0DC239A7}_\texttt{x}$	$2^{-20.5299}$
$\texttt{94E844C3}_\texttt{x}$	$-2^{-20.1235}$
$\texttt{F6148C2A}_\texttt{x}$	$-2^{-18.3755}$
$\texttt{5EB3E9BB}_\texttt{x}$	$2^{-18.3688}$
$\texttt{396A0040}_\texttt{x}$	$2^{-23.1944}$
$\texttt{24EC1390}_\texttt{x}$	$2^{-20.9910}$

Run 7

Class	Cond. corr.
$\texttt{A096F3E6}_\texttt{x}$	$-2^{-16.0597}$
$\texttt{D0A9D240}_\texttt{x}$	$-2^{-18.3818}$
$\texttt{46373DFE}_\texttt{x}$	$2^{-18.1380}$
$\texttt{15895B21}_\texttt{x}$	$-2^{-19.3119}$
$\texttt{5A403D62}_\texttt{x}$	$-2^{-18.5704}$
$\texttt{2E66E414}_\texttt{x}$	$2^{-21.1715}$
$\texttt{04DD66C5}_\texttt{x}$	$2^{-21.0084}$
$\texttt{2BB84DFD}_\texttt{x}$	$2^{-19.7062}$
$\texttt{BAE4A96E}_\texttt{x}$	$-2^{-17.4475}$
$\texttt{5507078F}_\texttt{x}$	$2^{-18.9505}$
$\texttt{B299AD82}_\texttt{x}$	$2^{-17.7568}$
$\texttt{6B639FC2}_\texttt{x}$	$-2^{-18.9349}$
$\texttt{1E04D922}_\texttt{x}$	$-2^{-18.7995}$
$\texttt{2CB164AE}_\texttt{x}$	$-2^{-19.9789}$
$\texttt{782AC4B9}_\texttt{x}$	$2^{-19.8064}$
$\texttt{B2C73118}_\texttt{x}$	$-2^{-17.9784}$

Run 8

Class	Cond. corr.
$\texttt{560533AC}_\texttt{x}$	$-2^{-15.9254}$
$\texttt{F8E3E4FB}_\texttt{x}$	$-2^{-19.8774}$
$\texttt{DC190EF0}_\texttt{x}$	$-2^{-17.8428}$
$\texttt{A5155394}_\texttt{x}$	$2^{-16.1876}$
$\texttt{01061496}_\texttt{x}$	$2^{-16.8843}$
$\texttt{3FB87759}_\texttt{x}$	$-2^{-17.1370}$
$\texttt{E08EBDF0}_\texttt{x}$	$2^{-19.8748}$
$\texttt{2DDF9477}_\texttt{x}$	$2^{-18.2082}$
$\texttt{FDC770D4}_\texttt{x}$	$2^{-21.4741}$
$\texttt{0B38CBE3}_\texttt{x}$	$-2^{-18.8104}$
$\texttt{C703D7F9}_\texttt{x}$	$2^{-20.0152}$
$\texttt{01B81B61}_\texttt{x}$	$2^{-21.1555}$
$\texttt{C3A5180C}_\texttt{x}$	$2^{-19.2615}$
$\texttt{AB74FC57}_\texttt{x}$	$2^{-17.1102}$
$\texttt{0969D431}_\texttt{x}$	$2^{-20.6310}$
$\texttt{702CB326}_\texttt{x}$	$-2^{-19.3912}$

Run 9

Class	Cond. corr.
$\texttt{0841D2D3}_\texttt{x}$	$-2^{-15.5616}$
$\texttt{2A6A80BB}_\texttt{x}$	$-2^{-19.0762}$
$\texttt{72A6FCD6}_\texttt{x}$	$2^{-20.3500}$
$\texttt{CAB51EF7}_\texttt{x}$	$2^{-17.2106}$
$\texttt{D1B4AE5D}_\texttt{x}$	$2^{-17.8585}$
$\texttt{21284C10}_\texttt{x}$	$2^{-18.0342}$
$\texttt{D9BD6A99}_\texttt{x}$	$2^{-19.2286}$
$\texttt{131D8ABD}_\texttt{x}$	$2^{-18.4165}$
$\texttt{040D421A}_\texttt{x}$	$-2^{-17.3171}$
$\texttt{1F7590A3}_\texttt{x}$	$2^{-17.0995}$
$\texttt{0BC17C43}_\texttt{x}$	$-2^{-17.0447}$
$\texttt{94A8D2D6}_\texttt{x}$	$2^{-18.6436}$
$\texttt{3F9CA5E4}_\texttt{x}$	$2^{-17.6383}$
$\texttt{A64226DE}_\texttt{x}$	$2^{-18.3055}$
$\texttt{814D89A2}_\texttt{x}$	$-2^{-19.4767}$
$\texttt{40C22B2A}_\texttt{x}$	$2^{-21.6249}$

Run 10

Class	Cond. corr.
$\texttt{B9E85A1A}_\texttt{x}$	$2^{-17.0648}$
$\texttt{DD399B66}_\texttt{x}$	$2^{-18.2499}$
$\texttt{C4712160}_\texttt{x}$	$2^{-17.6473}$
$\texttt{0E845DE9}_\texttt{x}$	$-2^{-17.8888}$
$\texttt{F5697A15}_\texttt{x}$	$2^{-16.6692}$
$\texttt{20AE2D1E}_\texttt{x}$	$-2^{-18.6498}$
$\texttt{4E1A9439}_\texttt{x}$	$-2^{-20.4738}$
$\texttt{A692CF68}_\texttt{x}$	$-2^{-25.7297}$
$\texttt{2D6E74B9}_\texttt{x}$	$-2^{-19.1425}$
$\texttt{4BA432CE}_\texttt{x}$	$2^{-24.1769}$
$\texttt{908FB0E1}_\texttt{x}$	$2^{-16.1571}$
$\texttt{87D2C47D}_\texttt{x}$	$-2^{-17.7923}$
$\texttt{45BBB748}_\texttt{x}$	$2^{-17.2851}$
$\texttt{EF778233}_\texttt{x}$	$-2^{-17.9270}$
$\texttt{AB448DE7}_\texttt{x}$	$2^{-19.0715}$
$\texttt{B35C0B5E}_\texttt{x}$	$-2^{-18.4746}$

Run 11

Class	Cond. corr.
$\texttt{2EB55D68}_\texttt{x}$	$2^{-15.8385}$
$\texttt{8DA98656}_\texttt{x}$	$2^{-21.5538}$
$\texttt{7F5C9161}_\texttt{x}$	$2^{-20.5999}$
$\texttt{E2E3F48B}_\texttt{x}$	$-2^{-19.3037}$
$\texttt{3D9CD58A}_\texttt{x}$	$2^{-21.4999}$
$\texttt{E3232ED1}_\texttt{x}$	$-2^{-17.1821}$
$\texttt{D215324F}_\texttt{x}$	$2^{-21.3974}$
$\texttt{68CB1CBB}_\texttt{x}$	$2^{-21.0152}$
$\texttt{6E3AF545}_\texttt{x}$	$2^{-17.3588}$
$\texttt{E06121A4}_\texttt{x}$	$-2^{-19.7149}$
$\texttt{F5DA598A}_\texttt{x}$	$-2^{-17.7904}$
$\texttt{9E0718E9}_\texttt{x}$	$2^{-23.8105}$
$\texttt{FE5FB280}_\texttt{x}$	$-2^{-18.7501}$
$\texttt{8650F29D}_\texttt{x}$	$-2^{-19.6677}$
$\texttt{52EEFA5D}_\texttt{x}$	$2^{-18.6606}$
$\texttt{DDBBBCC6}_\texttt{x}$	$2^{-19.1039}$

Run 12

Class	Cond. corr.
$\texttt{4F3CEE16}_\texttt{x}$	$2^{-15.8386}$
$\texttt{6118C102}_\texttt{x}$	$2^{-20.1948}$
$\texttt{5EDE09FA}_\texttt{x}$	$2^{-16.4085}$
$\texttt{C6D23AF3}_\texttt{x}$	$-2^{-19.3290}$
$\texttt{917BDE76}_\texttt{x}$	$2^{-19.2828}$
$\texttt{DB9D1706}_\texttt{x}$	$-2^{-16.6047}$
$\texttt{B52017DF}_\texttt{x}$	$-2^{-17.9765}$
$\texttt{E932226C}_\texttt{x}$	$-2^{-17.3126}$
$\texttt{798D01C6}_\texttt{x}$	$2^{-17.5631}$
$\texttt{8C374DF8}_\texttt{x}$	$2^{-17.3292}$
$\texttt{CC6C8D7F}_\texttt{x}$	$-2^{-17.0031}$
$\texttt{431CAB81}_\texttt{x}$	$2^{-17.5546}$
$\texttt{5D4A703F}_\texttt{x}$	$-2^{-18.0655}$
$\texttt{C0C4F6E0}_\texttt{x}$	$-2^{-18.2996}$
$\texttt{FF5CC8D0}_\texttt{x}$	$2^{-19.7086}$
$\texttt{8AEE31A7}_\texttt{x}$	$2^{-21.3384}$

Table 15: Results Experiment 1, run 13-14

Run 13		Run 14	
Class	Cond. corr.	Class	Cond. corr.
$\texttt{05731E8B}_\texttt{x}$	$-2^{-16.2620}$	$\texttt{D124C4C7}_\texttt{x}$	$2^{-15.9330}$
$\texttt{5DB0E778}_\texttt{x}$	$-2^{-17.5226}$	$\texttt{1EAB8149}_\texttt{x}$	$2^{-18.2779}$
$\texttt{1978A847}_\texttt{x}$	$2^{-16.4214}$	$\texttt{D096E50A}_\texttt{x}$	$-2^{-16.8167}$
$\texttt{0714A162}_\texttt{x}$	$2^{-17.4079}$	$\texttt{F63D83A0}_\texttt{x}$	$2^{-16.7964}$
$\texttt{E427DDA1}_\texttt{x}$	$-2^{-19.0854}$	$\texttt{58DD999F}_\texttt{x}$	$-2^{-19.6575}$
$\texttt{F1043FF0}_\texttt{x}$	$2^{-18.4435}$	$\texttt{687BD459}_\texttt{x}$	$2^{-17.2279}$
$\texttt{2063BF16}_\texttt{x}$	$2^{-18.2604}$	$\texttt{7ED57159}_\texttt{x}$	$-2^{-18.1704}$
$\texttt{72FEEE44}_\texttt{x}$	$2^{-16.8421}$	$\texttt{3E16ED13}_\texttt{x}$	$-2^{-19.2129}$
$\texttt{84FB3EB8}_\texttt{x}$	$2^{-18.1412}$	$\texttt{AB7C3CDF}_\texttt{x}$	$2^{-20.4807}$
$\texttt{D460EBE6}_\texttt{x}$	$2^{-19.2130}$	$\texttt{5B44777F}_\texttt{x}$	$2^{-17.3261}$
$\texttt{8B520DDC}_\texttt{x}$	$-2^{-18.5055}$	$\texttt{EB21F368}_\texttt{x}$	$2^{-17.1960}$
$\texttt{62AD0B93}_\texttt{x}$	$2^{-17.6416}$	$\texttt{8D37614E}_\texttt{x}$	$-2^{-18.7395}$
$\texttt{49724508}_\texttt{x}$	$2^{-18.2654}$	$\texttt{D8D92EA8}_\texttt{x}$	$2^{-18.2482}$
$\texttt{961235FB}_\texttt{x}$	$2^{-18.9537}$	$\texttt{53E8CFA4}_\texttt{x}$	$2^{-21.3423}$
$\texttt{1B2DF449}_\texttt{x}$	$-2^{-16.7523}$	$\texttt{4BFDC6C2}_\texttt{x}$	$2^{-19.8957}$
$\texttt{9439837B}_\texttt{x}$	$2^{-17.2473}$	$\texttt{F0873852}_\texttt{x}$	$-2^{-17.5521}$

Table 16: Results Experiment 1, run 15-16

Run 15		Run 16	
Class	Cond. corr.	Class	Cond. corr.
$\texttt{CDE8ACA5}_\texttt{x}$	$-2^{-16.5740}$	$\texttt{CA1D403C}_\texttt{x}$	$-2^{-15.6369}$
$\texttt{CAED06DE}_\texttt{x}$	$-2^{-17.8129}$	$\texttt{269AEC23}_\texttt{x}$	$2^{-17.6759}$
$\texttt{54B90F29}_\texttt{x}$	$2^{-18.5584}$	$\texttt{18A8ABD9}_\texttt{x}$	$2^{-20.1006}$
$\texttt{4CA9E3D1}_\texttt{x}$	$2^{-18.3883}$	$\texttt{F6624A07}_\texttt{x}$	$2^{-17.8805}$
$\texttt{6CDE2F4A}_\texttt{x}$	$2^{-19.2274}$	$\texttt{39526EEB}_\texttt{x}$	$-2^{-18.4606}$
$\texttt{EA60B0CC}_\texttt{x}$	$-2^{-19.0488}$	$\texttt{86EC1AFE}_\texttt{x}$	$2^{-16.7075}$
$\texttt{71848C19}_\texttt{x}$	$2^{-19.7642}$	$\texttt{E7D25F0A}_\texttt{x}$	$-2^{-17.4129}$
$\texttt{4B2F81CD}_\texttt{x}$	$-2^{-18.2663}$	$\texttt{79C1D69B}_\texttt{x}$	$2^{-18.2451}$
$\texttt{F202E2B0}_\texttt{x}$	$2^{-17.9375}$	$\texttt{794E2396}_\texttt{x}$	$-2^{-18.2178}$
$\texttt{A799466F}_\texttt{x}$	$-2^{-17.3837}$	$\texttt{08966969}_\texttt{x}$	$2^{-17.8062}$
$\texttt{2EF92DBD}_\texttt{x}$	$-2^{-20.7477}$	$\texttt{D6D50228}_\texttt{x}$	$-2^{-19.1594}$
$\texttt{177B5383}_\texttt{x}$	$2^{-16.9851}$	$\texttt{4FD5EEF1}_\texttt{x}$	$2^{-17.6230}$
$\texttt{3ED126D7}_\texttt{x}$	$2^{-16.7947}$	$\texttt{F2D8D95A}_\texttt{x}$	$2^{-17.8633}$
$\texttt{6F7C522C}_\texttt{x}$	$2^{-17.9543}$	$\texttt{8DE104EC}_\texttt{x}$	$-2^{-20.9480}$
$\texttt{3B690371}_\texttt{x}$	$2^{-19.4156}$	$\texttt{AE59DF9B}_\texttt{x}$	$2^{-16.6174}$
$\texttt{398B8EAE}_\texttt{x}$	$-2^{-17.8491}$	$\texttt{9CDF42F0}_\texttt{x}$	$-2^{-18.5145}$

Table 17: Settings Experiment 2

run	key k	substantial class $\overline{X}(k_0)$
1	D2 E7 BD 7E 06 4A 6F 15 AE 5D 39 B9 56 FA 50 $C1_x$	7739_x
2	AB 78 62 7C 36 16 BB 8B F3 7D 55 BB 00 D0 F7 $9A_x$	$E1DF_x$
3	CA 43 A2 7A B5 4B 67 77 D5 65 E3 4C 98 FD 0A 01_x	$1E03_x$
4	5C FF CC D5 A7 C6 B5 DF 3D 08 74 66 4B B5 5F 05_x	$242F_x$
5	87 25 84 F0 51 5B BD 45 82 75 B1 F7 37 98 40 31_x	$F0E3_x$
6	FD AC D1 33 A2 EB 0D C5 07 48 00 33 51 C2 61 $0E_x$	$E2B1_x$
7	E2 79 A6 01 48 F7 74 F9 78 8C E9 02 D5 A6 25 DA_x	$C40E_x$
8	62 AC EC 54 68 92 18 B4 F7 DD 92 8E D1 66 D4 $2D_x$	$7A7B_x$
9	06 93 63 2A 8A 34 1A E9 E9 00 24 3B 4C 77 CD BE_x	$A4F4_x$
10	10 49 22 10 34 A5 68 63 2E A5 BE 17 96 90 C5 76_x	$72A9_x$
11	40 C3 EE A1 05 55 F5 C5 1C 78 C8 69 35 32 61 BB_x	$9A05_x$
12	AA 95 B1 8D AF 97 00 36 84 2B BF 8D 3F F4 6C $D2_x$	5185_x
13	82 3B 85 7F 4C 12 9A 8A E1 12 8D 1C 2C C9 1D 45_x	$AD96_x$
14	81 05 9B F3 F8 7F 8F 8C 87 D3 4E 97 0B 29 DB 97_x	1411_x
15	06 0A 9E 84 FF 39 1B EF 5B 4E 05 FC 32 8F EE $A4_x$	$CBF4_x$
16	32 91 C5 32 60 EF D4 B3 9C FA DD A7 1C 4D 85 04_x	8696_x

Table 18: Results Experiment 2, run 1-4

Run 1		Run 2		Run 3		Run 4	
Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.
7739_x	$2^{-14.7755}$	$E1DF_x$	$2^{-14.4051}$	$1E03_x$	$-2^{-14.2988}$	$242F_x$	$2^{-14.3707}$
$0BA7_x$	$-2^{-15.1016}$	$DECD_x$	$2^{-14.7583}$	$BA93_x$	$2^{-15.4010}$	$388E_x$	$2^{-14.6176}$
$C56D_x$	$-2^{-15.9418}$	$8BD2_x$	$2^{-15.9473}$	$95E2_x$	$-2^{-15.5154}$	$C034_x$	$2^{-16.1970}$
$E0A4_x$	$-2^{-17.5555}$	$8F18_x$	$-2^{-16.6231}$	$47F4_x$	$-2^{-16.1295}$	$632E_x$	$-2^{-17.6330}$
$B205_x$	$-2^{-16.7841}$	$7CDF_x$	$-2^{-15.9235}$	5722_x	$2^{-17.3693}$	$E279_x$	$2^{-18.7117}$
$DBCF_x$	$-2^{-14.9386}$	$911B_x$	$2^{-18.5230}$	$322D_x$	$2^{-15.8003}$	$B28C_x$	$2^{-15.4069}$
$94A2_x$	$-2^{-15.9209}$	$F4DB_x$	$-2^{-15.4753}$	$EF5B_x$	$-2^{-17.0102}$	$26C4_x$	$-2^{-18.8490}$
$E406_x$	$2^{-16.3749}$	$FE17_x$	$-2^{-16.0871}$	$D8AD_x$	$2^{-18.5977}$	$CB00_x$	$-2^{-16.4241}$
$C716_x$	$-2^{-15.4192}$	$3B8A_x$	$-2^{-19.1257}$	8555_x	$-2^{-18.7710}$	$2CCF_x$	$-2^{-16.1990}$
$3D7C_x$	$-2^{-16.1821}$	6731_x	$2^{-17.3923}$	$9EFB_x$	$-2^{-20.1980}$	$86F8_x$	$2^{-14.8792}$
$DFC8_x$	$-2^{-20.0540}$	$AEF9_x$	$-2^{-16.2686}$	$E725_x$	$2^{-15.8796}$	$4E16_x$	$-2^{-19.1657}$
$CE69_x$	$-2^{-15.0659}$	$264F_x$	$-2^{-17.1391}$	$A5DB_x$	$-2^{-15.4151}$	$F68E_x$	$-2^{-16.1821}$
$E317_x$	$-2^{-19.4358}$	$D568_x$	$2^{-16.3593}$	$6F63_x$	$-2^{-15.6374}$	$DC87_x$	$-2^{-15.2997}$
$ABB9_x$	$2^{-18.2686}$	$1C8C_x$	$2^{-16.2737}$	$C883_x$	$-2^{-16.7736}$	$4D0B_x$	$2^{-14.3464}$
$EA58_x$	$-2^{-16.5159}$	$57A9_x$	$2^{-16.0766}$	$BC3C_x$	$2^{-16.6672}$	$F52F_x$	$-2^{-16.4191}$
$68A3_x$	$2^{-18.4225}$	$6BF4_x$	$2^{-16.5487}$	$8F28_x$	$2^{-18.9721}$	$CA7D_x$	$-2^{-17.5357}$

Table 19: Results Experiment 2, run 5-16

Run 5		Run 6		Run 7		Run 8	
Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.
$\texttt{F0E3}_x$	$2^{-14.0013}$	$\texttt{E2B1}_x$	$2^{-14.3716}$	$\texttt{C40E}_x$	$2^{-14.4449}$	$\texttt{7A7B}_x$	$-2^{-14.8248}$
$\texttt{DB7E}_x$	$-2^{-15.7332}$	$\texttt{8CA5}_x$	$2^{-20.0693}$	$\texttt{E7A6}_x$	$2^{-16.8690}$	$\texttt{42BE}_x$	$-2^{-17.1346}$
$\texttt{DB49}_x$	$-2^{-16.4554}$	$\texttt{5722}_x$	$2^{-15.0597}$	$\texttt{C134}_x$	$-2^{-15.3590}$	$\texttt{A34A}_x$	$2^{-18.5138}$
$\texttt{BCE7}_x$	$-2^{-17.4877}$	$\texttt{B362}_x$	$2^{-14.9223}$	$\texttt{935D}_x$	$2^{-15.4809}$	$\texttt{C238}_x$	$-2^{-15.0471}$
$\texttt{B219}_x$	$2^{-20.7283}$	$\texttt{A6FF}_x$	$2^{-16.5127}$	$\texttt{7478}_x$	$-2^{-16.4987}$	$\texttt{EDE1}_x$	$-2^{-21.9871}$
$\texttt{35EC}_x$	$2^{-14.6546}$	$\texttt{17A2}_x$	$-2^{-15.6205}$	$\texttt{190B}_x$	$-2^{-15.0138}$	$\texttt{F6B0}_x$	$2^{-16.1473}$
$\texttt{3A19}_x$	$2^{-16.6525}$	$\texttt{80E6}_x$	$2^{-18.5839}$	$\texttt{7DC3}_x$	$2^{-16.3652}$	$\texttt{0BE1}_x$	$-2^{-16.8602}$
$\texttt{ECC4}_x$	$-2^{-15.5898}$	$\texttt{0C8E}_x$	$2^{-14.6881}$	$\texttt{4B0B}_x$	$2^{-16.8354}$	$\texttt{1F33}_x$	$2^{-16.0671}$
$\texttt{C1E4}_x$	$2^{-15.0888}$	$\texttt{9689}_x$	$-2^{-16.8477}$	$\texttt{B242}_x$	$-2^{-16.6587}$	$\texttt{6EE5}_x$	$2^{-17.2484}$
$\texttt{2043}_x$	$-2^{-16.3024}$	$\texttt{87E0}_x$	$-2^{-15.1826}$	$\texttt{1AA0}_x$	$2^{-15.8424}$	$\texttt{A1F7}_x$	$2^{-16.3617}$
$\texttt{F1C9}_x$	$2^{-16.2757}$	$\texttt{A6C3}_x$	$2^{-15.4206}$	$\texttt{214B}_x$	$-2^{-18.2526}$	$\texttt{0B3E}_x$	$2^{-15.7595}$
$\texttt{6CBC}_x$	$-2^{-16.2378}$	$\texttt{3385}_x$	$2^{-18.8934}$	$\texttt{4317}_x$	$-2^{-15.8732}$	$\texttt{A420}_x$	$-2^{-15.5446}$
$\texttt{2815}_x$	$-2^{-16.2954}$	$\texttt{CD7F}_x$	$-2^{-18.9379}$	$\texttt{1D46}_x$	$-2^{-16.8654}$	$\texttt{EA4B}_x$	$2^{-14.9606}$
$\texttt{475F}_x$	$-2^{-16.1167}$	$\texttt{6E2E}_x$	$2^{-16.8961}$	$\texttt{2CFC}_x$	$-2^{-16.9402}$	$\texttt{3880}_x$	$-2^{-15.8658}$
$\texttt{697A}_x$	$-2^{-15.2881}$	$\texttt{E2DA}_x$	$2^{-17.4384}$	$\texttt{24F4}_x$	$2^{-15.9180}$	$\texttt{16B1}_x$	$2^{-19.0984}$
$\texttt{988D}_x$	$-2^{-16.9645}$	$\texttt{530C}_x$	$2^{-15.6815}$	$\texttt{BC3B}_x$	$2^{-15.1942}$	$\texttt{FC8A}_x$	$-2^{-16.5374}$

Run 9		Run 10		Run 11		Run 12	
Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.
$\texttt{A4F4}_x$	$-2^{-14.4412}$	$\texttt{72A9}_x$	$-2^{-15.0900}$	$\texttt{9A05}_x$	$2^{-13.9470}$	$\texttt{5185}_x$	$2^{-13.9585}$
$\texttt{19A8}_x$	$-2^{-17.2236}$	$\texttt{6FEC}_x$	$2^{-18.3103}$	$\texttt{BAFE}_x$	$-2^{-15.2182}$	$\texttt{F7EC}_x$	$-2^{-15.2780}$
$\texttt{3B6D}_x$	$-2^{-14.5100}$	$\texttt{C936}_x$	$2^{-16.7246}$	$\texttt{0203}_x$	$-2^{-15.5227}$	$\texttt{B9AE}_x$	$2^{-18.4358}$
$\texttt{AC88}_x$	$-2^{-16.3749}$	$\texttt{3598}_x$	$-2^{-15.5514}$	$\texttt{3ED5}_x$	$2^{-15.2702}$	$\texttt{9AAA}_x$	$2^{-17.0183}$
$\texttt{37D2}_x$	$-2^{-17.7640}$	$\texttt{CF43}_x$	$-2^{-16.0569}$	$\texttt{CA16}_x$	$-2^{-18.3100}$	$\texttt{C141}_x$	$2^{-14.5610}$
$\texttt{1150}_x$	$2^{-15.6985}$	$\texttt{868B}_x$	$-2^{-15.8424}$	$\texttt{8524}_x$	$2^{-16.1654}$	$\texttt{7C9D}_x$	$-2^{-15.5436}$
$\texttt{5F5F}_x$	$2^{-16.0560}$	$\texttt{0FA7}_x$	$-2^{-14.9989}$	$\texttt{68AB}_x$	$2^{-18.6388}$	$\texttt{2161}_x$	$2^{-18.0580}$
$\texttt{BBCB}_x$	$-2^{-15.0803}$	$\texttt{2F07}_x$	$-2^{-22.2192}$	$\texttt{435F}_x$	$-2^{-18.9816}$	$\texttt{48E9}_x$	$2^{-15.6957}$
$\texttt{BC5C}_x$	$-2^{-15.2454}$	$\texttt{45B6}_x$	$-2^{-16.5485}$	$\texttt{4A7F}_x$	$2^{-17.6849}$	$\texttt{404B}_x$	$-2^{-15.6813}$
$\texttt{B564}_x$	$2^{-14.9222}$	$\texttt{243A}_x$	$2^{-15.2239}$	$\texttt{47BF}_x$	$2^{-14.7445}$	$\texttt{42AF}_x$	$2^{-15.5912}$
$\texttt{1293}_x$	$-2^{-16.1343}$	$\texttt{DB15}_x$	$-2^{-15.8345}$	$\texttt{3951}_x$	$2^{-17.2349}$	$\texttt{BE9D}_x$	$2^{-17.0223}$
$\texttt{21D1}_x$	$-2^{-18.2133}$	$\texttt{51F4}_x$	$-2^{-14.8893}$	$\texttt{371A}_x$	$-2^{-18.2964}$	$\texttt{174A}_x$	$-2^{-15.6898}$
$\texttt{5D60}_x$	$-2^{-16.2374}$	$\texttt{1358}_x$	$-2^{-15.6970}$	$\texttt{C3B9}_x$	$2^{-17.2509}$	$\texttt{E7C5}_x$	$-2^{-18.7995}$
$\texttt{F344}_x$	$-2^{-16.5596}$	$\texttt{2315}_x$	$2^{-15.9978}$	$\texttt{DDE4}_x$	$-2^{-18.0504}$	$\texttt{2A2C}_x$	$-2^{-15.9797}$
$\texttt{9CF2}_x$	$-2^{-15.5289}$	$\texttt{8A7F}_x$	$-2^{-17.4412}$	$\texttt{6E09}_x$	$2^{-18.7562}$	$\texttt{9C3D}_x$	$-2^{-15.5690}$
$\texttt{BD63}_x$	$2^{-14.2884}$	$\texttt{44B1}_x$	$-2^{-15.8216}$	$\texttt{4ABD}_x$	$2^{-18.1714}$	$\texttt{2FC7}_x$	$-2^{-16.4663}$

Run 13		Run 14		Run 15		Run 16	
Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.	Class	Cond. corr.
$\texttt{AD96}_x$	$2^{-14.1913}$	$\texttt{1411}_x$	$-2^{-13.4589}$	$\texttt{CBF4}_x$	$2^{-13.8074}$	$\texttt{8696}_x$	$2^{-13.7917}$
$\texttt{FF04}_x$	$-2^{-18.6912}$	$\texttt{775C}_x$	$2^{-15.7345}$	$\texttt{7DB0}_x$	$-2^{-17.2316}$	$\texttt{F63F}_x$	$-2^{-15.7935}$
$\texttt{908D}_x$	$-2^{-15.3723}$	$\texttt{01A3}_x$	$-2^{-17.8515}$	$\texttt{3B6A}_x$	$2^{-16.4807}$	$\texttt{63E2}_x$	$2^{-14.6600}$
$\texttt{BD3C}_x$	$2^{-19.0892}$	$\texttt{65E1}_x$	$2^{-15.1726}$	$\texttt{7B79}_x$	$2^{-16.0247}$	$\texttt{404F}_x$	$-2^{-16.3921}$
$\texttt{2684}_x$	$-2^{-14.8869}$	$\texttt{FB61}_x$	$2^{-14.9914}$	$\texttt{9D17}_x$	$2^{-19.4792}$	$\texttt{62E4}_x$	$2^{-15.5395}$
$\texttt{4622}_x$	$-2^{-17.4602}$	$\texttt{C750}_x$	$-2^{-17.0675}$	$\texttt{3CB1}_x$	$-2^{-16.5038}$	$\texttt{97D7}_x$	$2^{-17.1093}$
$\texttt{B95E}_x$	$-2^{-18.4386}$	$\texttt{4714}_x$	$2^{-14.8149}$	$\texttt{8570}_x$	$-2^{-15.8811}$	$\texttt{00C0}_x$	$-2^{-17.1480}$
$\texttt{3409}_x$	$-2^{-17.0849}$	$\texttt{CA10}_x$	$-2^{-19.6321}$	$\texttt{FC18}_x$	$-2^{-15.0194}$	$\texttt{A35A}_x$	$-2^{-18.0227}$
$\texttt{A1E8}_x$	$-2^{-16.8910}$	$\texttt{C2B3}_x$	$-2^{-17.9569}$	$\texttt{C44B}_x$	$-2^{-16.7061}$	$\texttt{61E0}_x$	$-2^{-20.2835}$
$\texttt{B4AB}_x$	$-2^{-17.1547}$	$\texttt{E9AE}_x$	$2^{-16.3241}$	$\texttt{CE37}_x$	$2^{-16.1367}$	$\texttt{1D38}_x$	$-2^{-16.7416}$
$\texttt{C844}_x$	$2^{-15.8789}$	$\texttt{5B12}_x$	$-2^{-18.0958}$	$\texttt{EADE}_x$	$-2^{-16.8083}$	$\texttt{7C57}_x$	$-2^{-15.6409}$
$\texttt{417A}_x$	$2^{-18.2304}$	$\texttt{BB3B}_x$	$-2^{-14.4584}$	$\texttt{AFC3}_x$	$-2^{-17.6059}$	$\texttt{1A3D}_x$	$2^{-21.1668}$
$\texttt{152B}_x$	$2^{-16.5412}$	$\texttt{04A8}_x$	$2^{-18.2655}$	$\texttt{CC21}_x$	$-2^{-14.7704}$	$\texttt{3548}_x$	$2^{-16.1807}$
$\texttt{F68F}_x$	$-2^{-16.4105}$	$\texttt{684F}_x$	$-2^{-16.3141}$	$\texttt{3EA8}_x$	$-2^{-17.2445}$	$\texttt{8A66}_x$	$-2^{-19.0099}$
$\texttt{D00F}_x$	$-2^{-18.5125}$	$\texttt{9648}_x$	$2^{-17.7090}$	$\texttt{1A4D}_x$	$-2^{-22.6600}$	$\texttt{F063}_x$	$-2^{-17.0442}$
$\texttt{49A0}_x$	$-2^{-16.0733}$	$\texttt{F1D2}_x$	$-2^{-16.4496}$	$\texttt{C6CD}_x$	$-2^{-16.1096}$	$\texttt{BB46}_x$	$-2^{-16.0631}$