On the Search for Differential Characteristics Last Change: November 7, 2023

In these notes, we introduce basic notions from differential cryptanalysis and discuss a new idea for a hybrid adiabatic-gatebased quantum algorithm for finding highly probable differential characteristics, as well as a counterexample for the existence of high probability differential characteristics with the Rijndael S-Box. Let $m, n \in \mathbb{N}_{\geq 1}$ throughout.

1 Differential Characteristics and the Boomerang Attack The main technique of differential cryptanalysis is to study the differences of texts across functions. This is formalized using *differential characteristics*.

Definition 1 (Differential Characteristics [1, p. 116])**.** Let $f\colon \{0,1\}^n \to \{0,1\}^m, \alpha \in \{0,1\}^n, \beta \in \{0,1\}^m, p \in [0,1]$. The quadruple (α, f, β, p) is called a *differential characteristic* of f, if

$$\Pr_{x,y\in\{0,1\}^n}(f(x) \oplus f(y) = \beta \mid x \oplus y = \alpha) = p \tag{1}$$

holds. We also denote the quadruple by $\alpha \to_p^f \beta$.

Since the addition of bitstrings is defined as taking the GF(2) addition componentwise and one bit can have only two states, a differential characteristic precisely states the possible changes of differences of a pair of texts. This is illustrated in Figure 1.

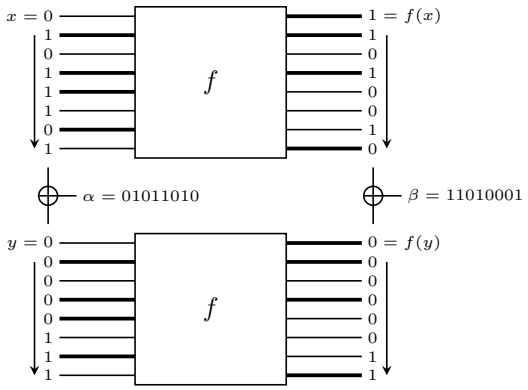

FIGURE 1. Representation of the differential behaviour of a function f on a byte, i.e. with $n = m = 8$. In each drawing of the byte strings, the most significant byte is on top. Since x and y are chosen with $x \oplus y = \alpha$, this diagram occurs with probability p.

Using differential characteristics, one can formulate the following general strategy for attacking a general cipher.

Algorithm 1 GENERAL DIFFERENTIAL ATTACK USING CHARACTERISTICS

Require: A function $E\colon \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^m$, $k \in \mathbb{N}_{\geq 1}$, with a characteristic $\alpha \to_p^{E(\cdot,\hat{k})} \beta$ to an unknown key $\hat{k}$ and $p \gg 0$.

Ensure: A candidate for $\hat{k}$.

1: Choose pairs $(x_1, y_1), ..., (x_{n_1}, y_{n_1}) \in \{0,1\}^{2n}$, $n_1 \in \mathbb{N}_{\geq 1}$, with $x_i \oplus y_i = \alpha \, \forall \, i \in [1, n]_{\mathbb{N}}$.

2: Choose keys $k_1, ..., k_{n_2} \in \{0,1\}^k$, $n_2 \in \mathbb{N}_{\geq 1}$, and count $e_{k_i} := |\{(x_j, y_j) \mid E(x_j, k_i) \oplus E(y_j, k_i) = E(x_j, k) \oplus E(y_j, k) = \beta\}|$ for each $i \in [1, n_2]_{\mathbb{N}}$.

3: **return** k_d, where $d := \arg\max_{i\in[1,n_2]_{\mathbb{N}}} e_{k_i}$.

This attack relies on replicating the differential behavior of $E(\cdot, k)$ wrt. $\alpha \to_p^{E(\cdot,k)} \beta$ as close as possible, it is very loosely formulated and the effectiveness depends on how the choice of the key affects the differential behavior of the cipher as well.

A different approach is to build more sophisticated structures of multiple characteristics, such as *quartets*, which are differential structures of four texts, not just pairs. In the following, we shall demonstrate the

boomerang attack, following [1, pp. 162-164]. Suppose a cipher $E = E_1 \circ E_0 \colon \{0,1\}^n \to \{0,1\}^n$ of invertible functions $E_0, E_1 \colon \{0,1\}^n \to \{0,1\}^n$ is given. We do not directly consider the key here. Denote $D_1 \coloneqq E_1^{-1}$ and $D_0 \coloneqq E_0^{-1}$. Suppose we have the characteristics

$$\alpha \overset{E_0}{\underset{p}{\to}} \beta, \gamma \overset{D_1}{\underset{q}{\to}} \delta, \beta \overset{D_0}{\underset{p'}{\to}} \alpha \tag{2}$$

where $p = p'$ may not necessarily hold by definition. The chosen plaintext-ciphertext attack is then performed the following way, following along Figure 2:

1. Choose $m_0 \in \{0,1\}^n$ and set $m_1 \coloneqq m_0 \oplus \alpha$.
2. Encrypt m_0 and m_1 to obtain ciphertexts c_0 and c_1, store u_0 and u_1. Set $c_2 \coloneqq c_0 \oplus \gamma$ and $c_3 \coloneqq c_1 \oplus \gamma$.
3. Compute u_2, u_3. We have $\Pr(\bigoplus_{i=0}^{3} u_i = 0) \geq q^2$.
4. Since $u_0 \oplus u_1 = \beta$ with probability p, we have $\Pr(u_2 \oplus u_3 = \beta) \geq pq^2$, giving $\Pr(m_2 \oplus m_3 = \alpha) = \Pr(\bigoplus_{i=0}^{3} m_i = 0) \geq pp'q^2$.

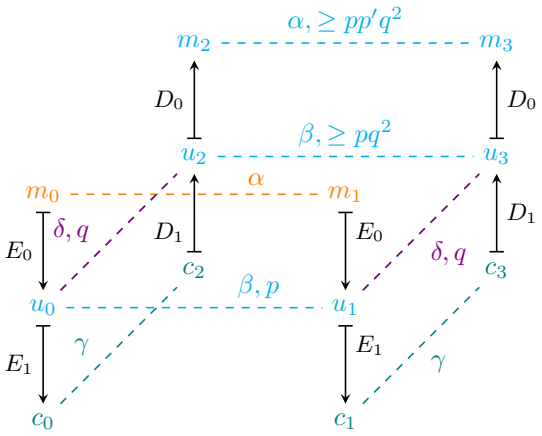

FIGURE 2. The general Boomerang attack.

The condition $\bigoplus_{i=0}^{3} m_i$ can then be used for attacking the key, see [2, pp. 161-162] for an example. The crucial condition for success here is whether $pp'q^2 \gg 0$.
The boomerang attack can be improved to only a chosen ciphertext attack with more available plaintexts, yielding the *amplified boomerang* and *rectangle* attacks [1, pp. 164-165]. The main conclusion to draw from this section is, that highly probable differential characteristics are crucial for successful attacks by differential cryptanalysis, as directly shown e.g. in the cryptanalysis of COCONUT98, where a precise analysis of the Feistel block cipher structure yielded a characteristic of probability $\approx 1/1900$ using texts with single one-entries each, breaking the cipher [2, pp. 160-161]. Furthermore, for some current research on quantum boomerang attacks, see [3, 4].

2 A Hybrid Adiabatic-Gatebased Quantum Attack Suppose a function $f \colon \{0,1\}^n \to \{0,1\}^m$ is given and our objective is to find one of the highest probable characteristic of it. Denote the oracles

$$U_{\oplus} \colon \mathbb{C}^{3N} \to \mathbb{C}^{3N}, |(x,y)\rangle |z\rangle \mapsto |(x,y)\rangle |z \oplus (x \oplus y)\rangle \tag{3}$$

$$U_{f \oplus f \times 0} \colon \mathbb{C}^{3N+M} \to \mathbb{C}^{3N+M}, |(x,y,z)\rangle |a\rangle \mapsto |(x,y,z)\rangle |a \oplus (f(x) \oplus f(y))\rangle \tag{4}$$

Then one may execute the following computations:

$$|0\rangle^{\otimes(3n+m)} \xmapsto{H^{\otimes 2n}\otimes E_{2M}} \frac{1}{N}\sum_{x,y\in\{0,1\}^n} |x\rangle\,|y\rangle\,|0\rangle^{\otimes(n+m)} = \frac{1}{N}\sum_{\alpha,x\in\{0,1\}^n} |x\rangle\,|x\oplus\alpha\rangle\,|0\rangle^{\otimes(n+m)} \tag{5}$$

$$\xmapsto{(U_{f\oplus f\times 0})(U_\oplus\otimes E_M)} \frac{1}{N}\sum_{\alpha,x\in\{0,1\}^n} |x\rangle\,|x\oplus\alpha\rangle\,|\alpha\rangle\,|f(x)\oplus f(x\oplus\alpha)\rangle \tag{6}$$

$$= \frac{1}{N}\sum_{(\alpha,\beta)\in\{0,1\}^{n+m}} \left(\sum_{x\in\{0,1\}^n, f(x)\oplus f(x\oplus\alpha)=\beta} |x\rangle\,|x\oplus\alpha\rangle\right)|\alpha\rangle\,|\beta\rangle \tag{7}$$

Our objective is to find a difference pair (α,β) with the highest number of pairs $(x, x\oplus\alpha)$ which admit to the associated characteristic. That corresponds to the highest probable result when measuring wrt. the observable $\{\mathrm{span}(\{|x\rangle\,|y\rangle\,|\alpha\rangle\,|\beta\rangle \mid x,y\in\{0,1\}^n\}) \mid (\alpha,\beta)\in\{0,1\}^{n+m}\}$, so the task may be reduced to the problem of finding the highest amplitude of a given state.
Consider the simplest case: A state $|\phi\rangle = \sum_{j=0}^{N-1}\alpha_j\,|j\rangle$ is given and we want to find $\arg\max_{j\in\{0,1\}^n}|\alpha_j|^2$. Our proposal is to use the following adiabatic quantum algorithm. We can observe

$$|\phi\rangle\langle\phi| = \sum_{j=0}^{N-1}|a_j|^2\,|j\rangle\langle j| \tag{8}$$

Thus

$$H_1 \coloneqq E_N - |\phi\rangle\langle\phi| = \sum_{j=0}^{N-1}(1-|\alpha_j|^2)\,|j\rangle\langle j| \tag{9}$$

We have $\sigma(H_1) = \{1-|\alpha_j|^2 \mid j\in\{0,1\}^n\}$, thus the problem reduces to find the ground state of the Hamiltonian H_1. We recall the necessary tools for such an adiabatic quantum algorithm: A proper initial Hamiltonian H_0, an appropriate schedule A and possibly a catalyst Hamiltonian A. Furthermore, one needs to find out how exactly to apply this algorithm to the problem from above, since there are still the first two registers in the state, so an observable encoding function χ needs to be given to the algorithm in an appropriate form. Also, of course, the analysis wrt. the rigorous adiabatic theorem must be performed.
Returning to the problem of finding characteristics, our hybrid adiabatic-gatebased quantum algorithm, in the end, would need to measure wrt. the canonical basis to get the highest probable characteristic differences and then perform amplitude estimation with runtime e.g. $O(\sqrt{N})$ [5, pp. 19-20] to approximate its probability, assuming the knowledge of it is needed.

3 The Rijndael S-Box Differential Property A counterexample to the existence of high probability characteristics for any function is the Rijndael S-Box. Recall the following concepts from the Rijndael algorithm: The factor ring $F \coloneqq \mathrm{GF}(2)[x]/(x^8+x^4+x^3+x+1)$ [6, pp. 10-11] is a field [7, pp. 313-314], which is bijective to $\mathrm{GF}(2)^8$ via the uniqueness of polynomial division in a polynomial ring over a field. Thus, we may represent a byte using such a polynomial via the canonical isomorphism of the additive groups. For the description of the Rijndael S-Box following [6, pp. 15-16], we now define the following *patched inverse* and affine linear transformation

$$\iota\colon F\to F, x\mapsto \begin{cases} x^{-1} & x\neq 0 \\ 0 & x=0 \end{cases} \qquad L_A \coloneqq \begin{pmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{pmatrix} \qquad v_A \coloneqq \begin{pmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{pmatrix} \tag{10}$$

from which the S-Box is then defined as

$$S\colon F\to F, x\mapsto (L\circ\iota)(x)+v_A \tag{11}$$

With $\oplus$ we shall denote the additive operation of $\mathrm{GF}(2)^8$, with $+$ the additive operation of F. The theorem of interest is now the following.

Theorem 1 (AES S-Box Differential Property [8, pp. 62-63])**.** Let $\alpha, \beta \in F \setminus \{0\} = F^*$ be arbitrary and loose. The following two statements hold.

(i) S possesses the following characteristics:

$$0 \xrightarrow[1]{S} 0, \alpha \xrightarrow[0]{S} 0, 0 \xrightarrow[0]{S} \beta \tag{12}$$

(ii) The characteristic $\alpha \to_p^S \beta$ has probability $p \in \{0, 2^{-7}, 2^{-6}\}$.

Proof. (i) Let $x \in F$ be loose. We consider the equation

$$S(x) \oplus S(x \oplus \alpha) = \beta \rightsquigarrow \iota(x) \oplus \iota(x \oplus \alpha) = L^{-1}(\beta) =: \hat{\beta} \tag{13}$$

For $\alpha = \beta = 0$, this reads

$$\iota(x) \oplus \iota(x) = 0 \tag{14}$$

which holds for all $x \in F$. For $\alpha \neq 0, \beta = 0$, we have

$$\iota(x) \oplus \iota(x \oplus \alpha) = 0 \rightsquigarrow \iota(x) = \iota(x \oplus \alpha) \tag{15}$$

$0 = 0$ would imply $\alpha = 0$, which is wrong $\lightning$. $x = 0$ or $x = \alpha$ is also not possible. $x^{-1} = (x \oplus \alpha)^{-1}$ gives $\alpha = 0$, which is also false. For $\alpha = 0, \beta \neq 0$, we get

$$0 = \hat{\beta} \tag{16}$$

which is false, as $\ker(L^{-1}) = \{0\}$.

(ii) We continue using Equation (13). We first consider the case $x(x \oplus \alpha) = 0$. Wlog. we consider $x = 0$, as the case $x = \alpha$ is dual. We thus have $\alpha = \hat{\beta}^{-1}$, so we may consider the probability p of the characteristic $\alpha \to_p^S L(\alpha^{-1})$. The condition gives

$$\iota(x) \oplus \iota(x \oplus \alpha) = \alpha^{-1} \tag{17}$$

$x = 0$ and $x = \alpha$ suffice the condition. Else we have

$$(x \oplus \alpha)^{-1} = x^{-1} \oplus \alpha^{-1} \rightsquigarrow x^2 \oplus \alpha x \oplus \alpha^2 = 0 \rightsquigarrow (x/\alpha)^2 \oplus x/\alpha \oplus 1 = 0 \tag{18}$$

Substituting $\hat{x} \coloneqq x/\alpha$, we reduce this problem to $\hat{x}^2 \oplus \hat{x} \oplus 1 = 0$ over F. This has either no or two solutions, totalling two to four, giving the claim.

Now we look at the case $x(x \oplus \alpha) \neq 0$. There we have

$$x^{-1} \oplus (x \oplus \alpha)^{-1} = \hat{\beta} \rightsquigarrow x^2 \oplus \alpha x \oplus \alpha\hat{\beta}^{-1} = 0 \tag{19}$$

Rewriting the equation as $(x/\alpha)^2 \oplus x/\alpha \oplus \hat{\beta}^{-1}/\alpha$, we may use a quantum algorithm for determining a solution of an equation of form $x^2 \oplus x \oplus d = 0$ [8, pp. 64-65]. The details shall be omitted here. This yields two solutions.

■

Theorem 1 (ii) gives, that the Rijndael S-Box has characteristics of comparatively low probability for non-trivial characteristics, even though 2^{-7} and 2^{-6} are still high enough complexities for cryptanalysis by computer, omitting at this point that the S-Box on its own is invertible, of course. The more important question that arises is how this can be used for the cryptanalysis of AES, which is considered as secure against differential cryptanalysis, and how this fact is connected with the rest of the algorithm. For more information see [8].

References

[1] Knudsen, L., *The Block Cipher Companion*, ISBN: 978-3-642-27111-3.

[2] Wagner, D., "The Boomerang Attack," DOI: 10.1007/3-540-48519-8_12.

[3] Frixons, P. and Naya-Plasencia, M. and Schrottenloher, A., "Quantum Boomerang Attacks and Some Applications," DOI: 10.1007/978-3-030-99277-4_16.

[4] Zou H. and Zou, J. and Luo, Y., "New results on quantum boomerang attacks," DOI: 10.1007/s11128-023-03921-6.

[5] Brassard, G. and Hoyer, P. and Mosca, M. and Tapp, A., "Quantum Amplitude Amplification and Estimation," DOI: https://doi.org/10.48550/arXiv.quant-ph/0005055.

[6] Dworkin, M. J., "Advanced Encryption Standard (AES)," Tech. Rep. DOI: https://doi.org/10.6028/NIST.FIPS.197-upd1.

[7] Fischer, G., *Lehrbuch der Algebra*, ISBN: 978-3-658-19217-4.

[8] Bonnetain, X. and Naya-Plasencia, M. and Schrottenloher, A., "Quantum Security Analysis of AES," DOI: https://doi.org/10.13154/tosc.v2019.i2.55-93.