UDC 003.26.09:519.2

Cryptographic attacks on AES based on side-channel information

Yevhenii Tolmachov[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

The topic of this work is the refinement of side-channel attacks, using the AES cipher as an example. Most such attacks are based on statistical methods and physical measurements of side-channel information, which is why the key obtained as a result of the attack may contain errors. The goal of this work is to investigate error correction algorithms for the key found during the attack. In the course of the work, two cryptographic models and attack algorithms on them are considered. The probability of success and the complexity of the attacks are theoretically derived and calculated.

Keywords: AES, symmetric cryptography, cryptoanalysis, side channel attacks, error correction

Intro

Due to its reliability and speed, the Advanced Encryption Standard (AES) [1] is currently one of the most widely used cryptographic ciphers. The cipher is even considered quantum-resistant. This is why concerns about its potential vulnerabilities remain relevant. Every cipher operates on physical processors, smart cards, phones, etc. These devices introduce sources of information about their operation that are not provided by the mathematical description of the cipher, such as temperature, caching, and electromagnetic emissions. This kind of information is known as side-channel information. Attacks that are based on such information are significantly more effective than purely mathematical ones. These are called side-channel attacks [2]. Attacks more effective than brute force have already been developed [3].

Previous work on this topic exists and usually focuses on the inner workings of specific ciphers. M. Brinkmann, C. Chuengsatiansup, A. May, J. Nowakowski and Y. Yarom proposed an approach to recover key with errors [4] for a contender for post-quantum schemes — McEliece cryptosystem — using public key with information from a Gaussian transformation leak.

Q. Guo, D. Nabokov, A. Nilsson and T. Johansson proposed [5] in their work a framework for usage of low-density parity-check (LDPC) codes for retrieval and decoding of symbols related to secret values, which offer error correction benefits, continuing the trend of using the LDPC approach for enhanced SCA-attacks on post-quantum ciphers.

In [6, 7] focus is on the recovery of the RSA private key. N. Heninger and H. Shacham proposed an algorithm for private key recovery in cases where public exponent e is small. The key is recovered based on knowledge about random fractions of the private key bits and general properties of private variables, which allows building a search tree to recover "erased" bits one by one. However, it requires having a certain fraction of correct bits, which is not always a realistic situation. Henecka W., May A. and Meurer A. proposed a Las-Vegas type algorithm capable of correcting errors in private key by applying similar logic to build a search tree for candidate blocks of bits.

The presented work approach can be applied to any retrieved key for any cipher. This work presents the results of previous studies on the topic [8], [9], and discusses three attack models with error correction and approximations of complexity and probability of success of the presented models.

This work is organized as follows. Section 1 focuses on the attack model with error correction in which an SCA-attack was conducted on the AES algorithm and the adversary retrieved a secret key with errors that has an error rate of p in every

bit and has an oracle to check whether the key is correct with the knowledge of a single pair of plaintext and ciphertext. Section 2 describes the model with error correction in which the adversary managed to recover several keys with the same constraints. Section 3 describes the attack model in which several keys were collected from several sources, and said keys have different error rates. Section 4 contains approximations for algorithm analysis using the Poisson limit theorem.

1. First Proposed Attack Model

It is assumed that a side-channel attack has been carried out on the AES algorithm. As a consequence, the retrieved key is likely to have errors in it. The following model of the attack will be referred to as Model 1. In all models considered, it is assumed that a side-channel attack (SCA) has been conducted on the AES algorithm.

Model 1 Definition

Model 1 can be defined as follows,

1. A side-channel attack based on ciphertext has occurred.

2. The adversary E, having access to a device using the AES cipher and possessing side-channel information about the execution of operations

$$C = AES(M, r), \quad (1)$$

$$\text{or} \quad M = InvAES(C, r), \quad (2)$$

where $AES(M, r)$ is the encryption operation of message M with the key r, and $InvAES(C, r)$ — decryption operation of ciphertext C with key r, has obtained bits of the secret key with the size of β bits with some error

$$\tilde{r} = \tilde{r}_{\beta-1},\tilde{r}_{\beta-2}, ...,\tilde{r}_2,\tilde{r}_1,\tilde{r}_0, \quad \tilde{r}_i \in \{0,1\}. \quad (3)$$

3. Assume that

$$\tilde{r_i} = r_i \oplus \varepsilon_i,$$

where $r_i \in \{0, 1\}$ — true value of the bit, $\varepsilon_i \in \{0, 1\}$ — independent random value. Probability of an error in each bit be defined as

$$\Pr\{\varepsilon_i = 1\} = p, \quad 0 \le p < \frac{1}{2}, \quad i = \overline{0, \beta - 1}.$$

If $p = 0$, there are no errors, and $\tilde{r}$ — is the true key r. If $p = \frac{1}{2}$, then it is impossible to derive any information about true key r from (3).

4. The adversary E can verify whether $\tilde{r}$ is the true key or a key with substitution errors by substituting it into equation (1) or (2).

Attack Algorithm

The goal of the second part of the attack is to find the true key r from the key with errors (3). According to (3), there may be $1, 2, ..., k, ..., \beta$ errors.

To construct this attack, first we need to define Cm_i — set of all bit strings of length $|\tilde{r}|$ with Hamming weight i. This set can be found with permutation generation algorithm. We will reffer to permutation generation algorithm as Algorithm 0 that takes parameters $|\tilde{r}|$ and i. Examples of such algorithms can be found in [10].

Algorithm 1. Error correction algorithm for up to k errors for Model 1. Input: $\tilde{r}$, M, C, k

Output: r

1. If $AES(M, \tilde{r}) = C$, then
2. $\quad r = \tilde{r}$, the algorithm terminates.
3. $i = 1$
4. While $i \le k$
5. $\quad Cm_i$ = Algorithm 0 with parameters $\tilde{r}, i$
6. $\quad$ For all j from Cm_i
7. $\quad\quad \tilde{r'} = \tilde{r} \oplus j$
8. $\quad\quad$ If $AES(M, \tilde{r'}) = C$, then
9. $\quad\quad\quad r = \tilde{r'}$, the algorithm terminates.
10. $\quad\quad i = i + 1$
11. Return error, the algorithm terminates.

As an equation to verify the correctness of the key, (2) can be used in addition to (1).

There may be more than k errors in the key, so the algorithm has a certain probability of success.

Algorithm Analysis

Theorem 1. *Probability of success of Algorithm 1 that fixes up to k errors is equal to*

$$\Pr\{\textit{Success}\} = \sum_{i=0}^{k} C_\beta^i \cdot p^i \cdot (1-p)^{\beta-i}$$

Proof. For an Algorithm that fixes up to k errors probability of success can be defined as follows:

$$\Pr\{\text{Success}\} = \Pr\{x \le k\},$$

where x is the number of errors in $\tilde{r}$.

$$\Pr\{x \le k\} = \sum_{i=0}^{k} \Pr\{x = i\} = \sum_{i=0}^{k} C_\beta^i \cdot p^i \cdot (1-p)^{\beta-i},$$

which concludes the proof. □

Probability of success with different parameters (β, p, k) presented within [11, Table 1].

Theorem 2. *Complexity T_k of Algorithm 1 counted in the amount of AES cipher calls in the worst-case scenario is equal to*

$$T_k = \sum_{i=0}^{k} C_\beta^k.$$

Proof. Number of AES operations needed exactly for fixing i errors — C_β^i. Then the number of operations required to correct up to k errors is $\sum_{i=0}^{k} C_\beta^k$, which represents the worst-case complexity. This concludes the proof. □

Theorem 3. *Average-case complexity of Algorithm 1*

$$\overline{T}_k = p_0 + \sum_{i=1}^{k} p_i \cdot \left(\sum_{j=0}^{i-1} C_\beta^j + \frac{1}{2} C_\beta^i \right) + \\ + \sum_{i=0}^{k} C_\beta^i \left(1 - \sum_{i=0}^{k} p_i \right),$$

where $p_i = C_\beta^i \cdot p^i \cdot (1-p)^{\beta - i}$.

Proof. The average complexity will be equal to the sum of the complexity for each specific case multiplied by the probability of that case.

Probability of $i \le k$ errors:

$$p_i = C_\beta^i \cdot p^i \cdot (1-p)^{\beta - i}$$

Probability of more than k errors:

$$\left(1 - \sum_{i=0}^{k} p_i \right)$$

Number of operations in case of i errors:

- $i = 0$: 1 call of AES;
- $i \le k : T_1^i = \sum_{j=0}^{i-1} C_\beta^j + \frac{1}{2} C_{\beta+1}^i$ calls of AES;
- $i > k : T_2^i = \sum_{i=0}^{k} C_\beta^i$ calls of AES.

Then the average number of operations required will be:

$$p_0 + \sum_{i=1}^{k} p_i \cdot T_1^i + \sum_{i=0}^{k} T_2^i \left(1 - \sum_{i=0}^{k} p_i \right).$$

This concludes the proof of the theorem. □

Complexity with different parameters (p, β, k) is presented in tables within [11, Table 2].

2. Second Proposed Attack Model

It is possible that the adversary gets several measurements of the key. The following model of the attack will be referred to as Model 2. Let's look into the second model. Several independent measurements of the key were conducted from the same source. Then the adversary E knows not just one but several equations of the type (1) and (2).

Model 2 Definition

The assumptions of Model 1 hold, but the analyst has m keys from a single source.

$$\tilde{r^j} = \tilde{r^j}_{\beta-1}, \tilde{r^j}_{\beta-2}, ..., \tilde{r^j}_2, \tilde{r^j}_1, \tilde{r^j}_0,$$
$$\tilde{r^j}_i \in \{0,1\}, \quad j \in \{0, m-1\},$$
$$\tilde{r_i^j} = r_i^j \oplus \varepsilon_i^j,$$

where $r_i^j \in \{0,1\}$ — true value of the bit, $\varepsilon_i^j \in \{0,1\}$ — random independent value,

$$\Pr\{\varepsilon_i^j = 1\} = p, \quad 0 \le p < \frac{1}{2}, \quad i = \overline{0, \beta - 1}.$$

Attack Algorithm

Algorithm 2. Error correction algorithm for up to k errors for Model 2.

Input: M, C, k, $\tilde{r}$, $j = \overline{1, n}$

Output: r

1. $i = 0$
2. While $i \le \beta$
3. $$\tilde{r_i} = \begin{cases} 1, & \sum_{j=0}^{m-1} \tilde{r_i}^{(j)} \ge \frac{m}{2} \\ 0, & \sum_{j=0}^{m-1} \tilde{r_i}^{(j)} < \frac{m}{2} \end{cases}$$
4. $i = i + 1$
5. Call Algorithm 1 with parameters $\tilde{r}$, M, C, and k

In this model the key may have more than k errors as well. So the algorithm has a probability of success.

Algorithm Analysis

Theorem 4. *Probability of success of algorithm 2 that fixes up to k errors is equal to*

$$\Pr\{\textit{Success}\} = \sum_{i=0}^{k} C_\beta^i \cdot q_m^i \cdot (1-q_m)^{\beta-i},$$

$$\textit{where} \qquad q_m = \sum_{i=0}^{\lfloor m/2 \rfloor} C_m^i \cdot p^{m-i} \cdot (1-p)^i$$

Proof.

$$\Pr\{\text{Success}\} = \Pr\{x \le k\},$$

where x is the amount of errors in $\tilde{r}$.

$$\Pr\{x \le k\} = \sum_{i=0}^{k} \Pr\{x = i\}$$

Since there are m equations, at least $\frac{m}{2}$ of them must have an error in the i-th bit for an error to occur in the bit $\tilde{r_i}$, therefore the probability that $\tilde{r_i} = r_i \oplus 1$ is equal to the probability that an error is present in at least half of the keys: $\tilde{r_i}^{(j)} = r_i^{(j)} \oplus 1$. Probability that an error is present in half of the keys is defined as q_m, then

$$q_m = \Pr\{y \ge \frac{m}{2}\} = \\ = \sum_{i=0}^{\lfloor m/2 \rfloor} C_m^i \cdot p^{m-i} \cdot (1-p)^i, \quad (4)$$

where y is the amount of errors in j-position bits of the key $\tilde{r_j}^{(1)}$,...,$\tilde{r_j}^{(r)}$

$$\Pr\{y = i\} = C_m^i \cdot p^{m-i} \cdot (1-p)^i$$

$$\Pr\{\text{Success}\} = \Pr\{x \le k\} = \\ = \sum_{i=0}^{k} C_\beta^i \cdot q_m^i \cdot (1-q_m)^{\beta-i},$$

which concludes the proof. □

Probability success with different parameters of (β, p, k, m) will be present in table within [11, Table 3].

Theorem 5. *Complexity T_k of Algorithm 2 counted in the amount of AES cipher calls and addition operations in the worst-case scenario is equal to*

$$\overline{T}_k = m \cdot \beta \quad \textit{additions} + \sum_{i=0}^{k} C_\beta^i \quad \textit{AES calls}$$

Proof. Number of needed additions — m additions for each of β bits. Addition complexity is — $O(1)$, so overall complexity for all additions is $O(m \cdot \beta)$. Proof for the amount of AES calls is equivalent to the one for Model 1. □

Complexity of additions can be neglected. Complexity in the worst-case scenario is presented in tables within [11, Table 3].

Theorem 6. *Average-case complexity of Algorithm 2 is*

$$\overline{T}_k = x_0 + \sum_{i=1}^{k} x_i \cdot \left(\sum_{j=0}^{i-1} C_\beta^j + \frac{1}{2} C_\beta^i \right) + \\ + \sum_{i=0}^{k} C_\beta^i \left(1 - \sum_{i=0}^{k} x_i \right) \quad (5)$$

where $x_i = C_\beta^i \cdot q_m^i \cdot (1-q_m)^{\beta-i}$,

$$q_m = \sum_{i=0}^{\rfloor m/2 \lfloor} C_m^i \cdot p^{m-i} \cdot (1-p)^i$$

Proof. Additions are done either way.

Proof for amount of calls is equivalent to Algorithm 1, with x_i having binomial distribution with parameters $n = \beta$ and $p = q_m$. □

Average-case complexity of Algorithm 2 with different parameters (β, p, k, m) are present in table within [11, Table 4].

Algorithm 2 also requires $m \cdot \beta$ additions. Complexity of said additions can be neglected. In that case, complexity in the worst-case scenario is equal to the complexity of Algorithm 1. However, the probability of success will be much higher. It should be noted that due to peculiarities of the third step of Algorithm 2, probability of success with $2k-1$ or $2k+1$ key measurements will be much higher than when using $2k$ measurements.

3. Third Proposed Attack Model

The following model of the attack will be referred to as Model 3. Let's describe the third model. Suppose several independent measurements of the key were conducted from different sources. Then the adversary E knows not just one but several equations of the type (1) and (2) from different sources.

Model 3 Definition

The assumptions of Model 1 hold, but the analyst has m keys from different sources.

$$\tilde{r^j} = \tilde{r^j}_{\beta-1}, \tilde{r^j}_{\beta-2}, ..., \tilde{r^j}_2, \tilde{r^j}_1, \tilde{r^j}_0,$$

$$\tilde{r^j}_i \in \{0,1\}, \quad j \in \{0, m-1\},$$

$$\tilde{r_i^j} = r_i^j \oplus \varepsilon_i^j,$$

where $r_i^j \in \{0,1\}$ — true value of bit, $\varepsilon_i^j \in \{0,1\}$ — random independent variables,

$$\Pr\{\varepsilon_i^j = 1\} = p_j, \quad 0 \le p_j < \frac{1}{2}, \quad i = \overline{0, \beta - 1}.$$

Attack Algorithm

Algorithm is equivalent to the one for Model 2.

In this model the key may have more than k errors as well. So the algorithm has a probability of success.

Algorithm Analysis

Theorem 7. *Probability of success of Algorithm 2 that fixes up to k errors is equal to*

$$\Pr\{Success\} = \sum_{i=0}^{k} C_\beta^i \cdot q_m^i \cdot (1 - q_m)^{k-i},$$

where

$$q_m = \sum_{i_1+i_2+\ldots+i_m \le \lfloor m/2 \rfloor} p_1^{1-i_1} \ldots p_n^{1-i_m}.$$

Proof. For an Algorithm that fixes up to k errors, probability of success can be defined as follows:

$$\Pr\{\text{Success}\} = \Pr\{x \le k\},$$

where x — number of errors in $\tilde{r}$.

$$\Pr\{x \le k\} = \sum_{i=0}^{k} \Pr\{x = i\}$$

Since we have m equations, at least $\frac{m}{2}$ of them should have an error in the i-position bit for there to be an error in $\tilde{r}_i$, so probability of $\tilde{r}_i = r_i \oplus 1$ is equal to the probability of an error occurring in half of the keys: $\tilde{r}_i^{(j)} = r_i^{(j)} \oplus 1$. Let the probability of an error in a key be q_m, then

$$q_m = \Pr\left\{y \ge \frac{m}{2}\right\} = \\ = \sum_{i_1+i_2+\ldots+i_m \le \lfloor m/2 \rfloor} p_1^{1-i_1} \ldots p_n^{1-i_m}, \quad (6)$$

where y — number of errors in j-position bits of the key $\tilde{r_j}^{(1)},\ldots,\tilde{r_j}^{(r)}$

$$\Pr\{y = j\} = p_1^{1-i_1} \ldots p_m^{1-i_m}$$

$$\Pr\{\text{Success}\} = \Pr\{x \le k\} = \\ = \sum_{i=0}^{k} C_\beta^i \cdot q_m^i \cdot (1 - q_m)^{k-i}, \quad (7)$$

which concludes the proof. □

Probability of success of this algorithm with various params (β, p, m, k) is in tables within [11, Table 5].

Theorem 8. *Complexity T_k of Algorithm 3 counted in the amount of AES cipher calls in the worst-case scenario is equal to*

$$T_k = \sum_{i=0}^{k} C_\beta^k$$

Proof is equivalent to the one provided for Algorithm 2. Complexity of additions can be neglected. Complexity is available in tables within [11, Table 6].

Theorem 9. *Average-case complexity of Algorithm 3 is*

$$\overline{T}_k = x_0 + \sum_{i=1}^{k} x_i \cdot \left(\sum_{j=0}^{i-1} C_\beta^j + \frac{1}{2} C_\beta^i \right) + \\ + \sum_{i=0}^{k} C_\beta^i \left(1 - \sum_{i=0}^{k} x_i \right).$$

where $x_i = C_\beta^i \cdot q_m^i \cdot (1 - q_m)^{\beta - i}$,

$$q_m = \Pr\left\{y \ge \frac{m}{2}\right\} = \\ = \sum_{i_1+i_2+\ldots+i_m \le \lfloor m/2 \rfloor} p_1^{1-i_1} \ldots p_m^{1-i_m}.$$

Proof. The average complexity will be equal to the sum of the complexity for each case multiplied by the probability of that case.

Probability of $i \le k$ errors:

$$x_i = \sum_{i=0}^{k} C_\beta^i \cdot q_m^i \cdot (1 - q_m)^{\beta - i}$$

where $q_m = \Pr\left\{y \ge \frac{m}{2}\right\} = \\ = \sum_{i_1+i_2+\ldots+i_m \le \lfloor m/2 \rfloor} p_1^{1-i_1} \ldots p_m^{1-i_m},$

Probability of more than k errors is

$$\left(1 - \sum_{i=0}^{k} x_i\right)$$

Number of operations in case of i errors:

- $i = 0$: 1 call of AES;
- $i \le k$: $T_1^i = \sum_{j=0}^{i-1} C_\beta^j + \frac{1}{2} C_{\beta+1}^i$ calls of AES;
- $i > k$: $T_2^i = \sum_{i=0}^{k} C_\beta^i$ calls of AES.

Then the average number of operations required will be:

$$x_0 \ + \ \sum_{i=1}^{k} x_i \ \cdot \ T_1^i \ + \ T_2^i \left(1 - \sum_{i=0}^{k} x_i\right)$$

AES calls. This concludes the proof. □

Algorithm 3 also requires $m \cdot \beta$ additions. Complexity of additions can be neglected. In that case, the worst-case scenario complexity is the same as Algorithm 1, and the probability of success will improve significantly. It should be noted that due to peculiarities of the third step of 2, probability of success with $2k-1$ or $2k+1$ key measurements will be much higher than when using $2k$ measurements. Differences in the complexity and probability of success between all 3 algorithms can be found in tables 1.

4. Limit Theorem for Approximating Algorithms That Fix Up To k Errors For Models 2 and 3

As the number of equations similar to equations (1) or (2) increases, analyzing the algorithms for Models 2 and 3 becomes increasingly difficult. The following section is therefore devoted to approximating a difficult to compute parameter using the Poisson limit theorem.

4.1. Theoretical Basis

Let's assume that we have a significant amount of equations 1 or 2. Calculating probability and complexity becomes significantly more difficult, especially for Model 3. The main problem is parameter q_m. It would be better to approximate probability instead. This subsection is mainly based on [12].

Given an independent test scheme $A_0, A_2, ...A_{m-1}$, from $P(A_k) = p_k, k = \overline{0,m-1}$, S_n is the number of successes in the tests. If as $n \longrightarrow \infty$ the sum $\sum_{k=0}^{n} p_k(1-p_k) \longrightarrow \infty$, then

$$\Pr\left\{\frac{S_n - \sum_{k=0}^{n} p_k}{\sqrt{\sum_{k=0}^{n} p_k(1-p_k)}} < x\right\} \longrightarrow \Phi(x) = \\ = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{-y^2}{2}} dy,$$

$$\text{where} \quad MS_n = \sum_{k=0}^{n} p_k, \tag{8}$$

$$DS_n = \sum_{k=0}^{n} p_k(1-p_k).$$

Let $n \longrightarrow \infty$ for any $k : p_k \geq 0$ and $\lambda = \sum_{i=0}^{m-1} p_i$.

$$\text{Then} \Pr\{S_n = h\} \longrightarrow \frac{\lambda_m^h e^{-\lambda_m}}{h!} \tag{9}$$

4.2. Approximating The Parameter q_m

Lemma 1. *For Model 2, parameter λ_m is*

$$\lambda_m = m \cdot p$$

Lemma 2. *For Model 3, parameter λ_m is*

$$\lambda_m = \sum_{i=0}^{m-1} p_i$$

Proof. We approximate binomial distribution with poisson one. Parameter λ_m can be inferred from 8. This concludes the proof. □

Theorem 10. *Parameter q_m for a large amount of equations can be approximated as*

$$q_m = 1 - \sum_{h=0}^{\lfloor m/2 \rfloor} \frac{\lambda_m^h e^{-\lambda_m}}{h!}.$$

Proof. q_m — probability of there being an error in a bit after the 3rd step of Algorithm 2. Then

$$q_m = \Pr\left\{S_n > \lfloor \frac{m}{2} \rfloor\right\} = 1 - \Pr\left\{S_n \leq \lfloor \frac{m}{2} \rfloor\}\right\},$$

from (9) $\Pr\{S_n = h\} \longrightarrow \frac{\lambda_m^h e^{-\lambda_m}}{h!}$, then

$$q_m = \sum_{h=\lceil m/2 \rceil}^{m} \frac{\lambda_m^h e^{-\lambda_m}}{h!} = 1 - \sum_{h=0}^{\lfloor m/2 \rfloor} \frac{\lambda_m^h e^{-\lambda_m}}{h!},$$

$$q_m = 1 - \sum_{h=0}^{\lfloor m/2 \rfloor} \frac{\lambda_m^h e^{-\lambda_m}}{h!}.$$

This concludes the proof. □

Conclusion

This work examines three cryptographic models and supporting attacks with error correction for them. The probability of success and the complexity of the attacks are calculated. When a adversary

Table 1
Comparative table for probability of success of the attack in 3 models with a key size $\beta = 256$, the presence of $m = 5$ measurements for the key with an error probability $p = 0.15$ for Models 1 and 2 and $p = [0.01, 0.08, 0.16, 0.24, 0.3], p_{mean} = 0.1567$ for Model 3, and k corrections.

k	1	2	5	10
$Algorithm1$	$2^{-54.49}$	$2^{-49.97}$	$2^{-39.33}$	$2^{-26.73}$
$Algorithm2$	0.008	0.0325	0.322	0.917
$Algorithm3$	0.0224	0.0775	0.5028	0.9719

Table 2
Comparative table for average-case complexity of the attack in 3 models with a key size $\beta = 256$, the presence of $m = 5$ measurements for the key with an error probability $p = 0.15$ for Models 1 and 2 and $p = [0.01, 0.08, 0.16, 0.24, 0.3], p_{mean} = 0.1567$ for Model 3, and k corrections.

k	1	2	5	10
$Algorithm1$	$2^{8.01}$	$2^{15.01}$	$2^{33.07}$	$2^{58.01}$
$Algorithm2$	$2^{7.96}$	$2^{14.87}$	$2^{32.14}$	$2^{53.55}$
$Algorithm3$	$2^{7.89}$	$2^{14.72}$	$2^{31.52}$	$2^{52.07}$

has several measurements of the key with errors from different sources, it is possible to significantly improve the probability of error correction and reduce the average execution complexity. Due to the peculiarities of the error correction algorithm, it is preferable to use an odd number of measured keys.

An approximation of the parameter q_m was also provided, which can be used to calculate the probability of success of attacks for a significantly larger number of equations.

The models described in this work highlight that an attacker can greatly increase the chance of recovering the correct key while reducing the time required for it by using several otherwise faulty measurements.

Overall, the presented models offer a flexible framework for assessing and improving error correction SCA attacks on AES, and they may serve as a basis for future research aimed at optimizing error-correction strategies and extending the analysis to other ciphers.

Acknowledgements

This work had not been possible without M. Savchuk. I would like to expresss gratitude for his mentorship, support, feedback, and guidance.

References

[1] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (aes)," 2001-11-26 2001. DOI: https://doi.org/10.6028/NIST.FIPS.197.

[2] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing." Cryptology ePrint Archive, Paper 2005/388, 2005. URL: https://eprint.iacr.org/2005/388.

[3] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, "Key recovery attacks of practical complexity on aes variants with up to 10 rounds." Cryptology ePrint Archive, Paper 2009/374, 2009. URL: https://eprint.iacr.org/2009/374.

[4] M. Brinkmann, C. Chuengsatiansup, A. May, J. Nowakowski, and Y. Yarom, "Leaky McEliece: Secret key recovery from highly erroneous side-channel information." Cryptology ePrint Archive, Paper 2023/1536, 2023. URL: https://eprint.iacr.org/2023/1536.

[5] Q. Guo, D. Nabokov, A. Nilsson, and T. Johansson, "SCA-LDPC: A code-based framework for key-recovery side-channel attacks

on post-quantum encryption schemes." Cryptology ePrint Archive, Paper 2023/294, 2023. URL: https://eprint.iacr.org/2023/294.

[6] N. Heninger and H. Shacham, "Reconstructing RSA private keys from random key bits." Cryptology ePrint Archive, Paper 2008/510, 2008. URL: https://eprint.iacr.org/2008/510.

[7] M. A. Henecka W., May A., "Correcting errors in rsa private keys: Annual cryptology conference," 2010. URL: https://probability.knu.ua/userfiles/yamnenko/Gnedenko.pdf.

[8] Y. Tolmachov, "Cryptographic attacks on aes based on information from a side-channel," 2024. URL: https://ela.kpi.ua/handle/123456789/54298.

[9] Y. Tolmachov, "Cryptographic attacks on aes based on information from a side-channel," 2024. URL: https://ela.kpi.ua/handle/123456789/69264.

[10] S. Robert, *Permutation generation methods*. 2008. URL: https://homepage.divms.uiowa.edu/~goodman/22m150.dir/2007/Permutation%20Generation%20Methods.pdf.

[11] Y. Tolmachov, "Cryptographic attacks on aes based on side channel information," 2025. URL: https://github.com/ZheZheDoshka/Cryptographic-attacks-on-AES-based-on-side-channel-information.

[12] B. Hnedenko, "Course in probability theory: Textbook," 2010. URL: https://probability.knu.ua/userfiles/yamnenko/Gnedenko.pdf.