DE GRUYTER
OPEN

TATRA MOUNTAINS
Mathematical Publications
DOI: 10.1515/tmmp-2015-0050
Tatra Mt. Math. Publ. **64** (2015), 217–231

HYPOTHESIS TESTING AND ADVANCED DISTINGUISHERS IN DIFFERENTIAL CRYPTANALYSIS OF BLOCK CIPHERS

Theodosis Mourouzis—Nicolas Courtois

ABSTRACT. Distinguishing distributions is a major part during cryptanalysis of symmetric block ciphers. The goal of the cryptanalyst is to distinguish two distributions; one that characterizes the number of certain events which occur totally at random and another one that characterizes same type of events but due to propagation inside the cipher. This can be realized as a hypothesis testing problem, where a source is used to generate independent random samples in some given finite set with some distribution P, which is either R or W, corresponding to propagation inside the cipher or a random permutation respectively. Distinguisher's goal is to determine which one is most likely the one which was used to generate the sample. In this paper, we study a general *hypothesis-testing* based approach to construct statistical distinguishers using truncated differential properties. The observable variable in our case is the expected number of pairs that follow a certain truncated differential property of the form $\Delta X \to \Delta Y$ after a certain number of rounds. As a proof of concept, we apply this methodology to GOST and SIMON 64/128 block ciphers and present distinguishers on 20 and 22 rounds respectively.

1. Introduction

In cryptanalysis, we very often study the problem of distinguishing distributions, one distribution that describes the number of events occurring due to a random permutation and another one describing the same variable but due to propagation inside the cipher. The aim of crypto designers is to construct cryptographic primitives that resemble the properties of a random permutation to the highest achievable degree. On the other hand, the cryptanalyst's aim is to design an algorithm (or a distinguisher) that would allow him to distinguish a given a cipher from a random permutation by capturing as much as possible

2010 Mathematics Subject Classification: 94A60, 68P25.
Keywords: differential cryptanalysis, hypothesis, testing, distinguisher, SIMON, GOST, truncated differentials,

of the cipher's structure. Such a distinguishing attack might reveal information which can be used to reduce the space of the key candidates. This might lead to an attack faster than exhaustive search either against a large number of rounds or even against the whole block cipher. Some good examples of of this are differential attacks on GOST described in [9], [10], [14].

We should also note that the behaviour which we expect for a random permutation, is also expected to work for almost any permutation, also from some very specific distribution dues for example to incorrect guesses in a key recovery attack. In other words cases in which the assumptions made by the attacker are not true, are assumed to behave as a random permutation, even though we know that they are not a random permutation.

Distinguishing attacks can be summarized as follows. Suppose that a source is used to generate independent random samples with some distribution $\mathcal{P}$, which is either R or W. A distinguisher is an algorithm used to determine which one is the most likely the one which was used to generate the sample. Hence, the overall attack based on distinguishers considers the following underlying statistical hypothesis testing problem,

$$\textbf{Null hypothesis: } H_0 : \mathcal{P} = W,$$

$$\textbf{Alternative hypothesis: } H_1 : \mathcal{P} = R.$$

This can be seen as a hypothesis-testing problem of distinguishing the two distributions as shown in Figure 1, page 219.

Assuming that we have two random normally distributed variables $\mathcal{W}$ and $\mathcal{R}$ with parameters $\big(E(W), V(W)\big)$ and $\big(E(R), V(R)\big)$, respectively. Our aim is given an observation of the variable of our interest to determine from which distribution this sample is more likely to be taken.

Note that for cryptanalytic purposes, we assume that distribution $\mathcal{W}$ corresponds to a wrong assumption or a wrong key, i.e., to a random permutation, while $\mathcal{R}$ corresponds to a right assumption or the right key. To be precise, the attacker can make any assumption on they key and the data inside the cipher, not only an assumption on the key, see the first stages of the complex attack described in [9, 10] for a specific example. For simplicity throughout this paper we will just speak about assumptions about the key, a simpler case which is also a lot more common in cryptanalysis. The distribution $\mathcal{R}$ is the most interesting one to study and it has a lot of interesting properties which the attacker can deduce from his assumptions. This is related to the notion of "propagation" of differentials inside the cipher[1].

[1] A random permutation can also have input and output properties assumed by the attacker, however this will be accidental. For a permutation which satisfies all the assumptions of the

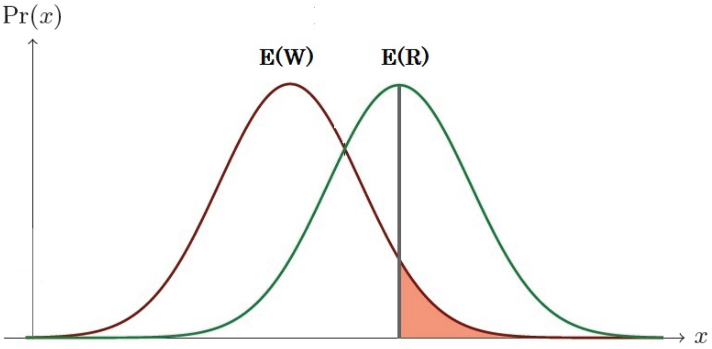

Figure 1. The two Gaussian distributions corresponding to wrong key guess (red) and right key guess (green). The red-shaded region corresponds to the probability of false positives or Type I error value.

The probability density function of the distribution of the variable $\mathcal{W}$ is given by

$$f_{\mathcal{W}}(x) = \frac{1}{\sqrt{2\pi V(W)}} \exp^{-\frac{1}{2V(W)}(x-E(W))^2}. \tag{1}$$

Assume that based on our experiments we have observed x events of our interest. From Figure 1 we observe that if $x > E(R)$, we can assume with probability $\frac{1}{2}$ that this observation corresponds to the right key.

On the other hand, the probability of accepting the wrong key as correct (false positive or Type I error) is represented by the red-shaded region in Figure 1. Type I error is computed by the following formulae,

$$P(\mathcal{W} > \mathcal{R}) = \int\limits_{E(R)}^{\infty} f_{\mathcal{W}}(x)\, \mathrm{dx} = \frac{1}{2}\left(1 - \mathrm{erf}\left(\frac{E(R) - E(W)}{\sqrt{2V(W)}}\right)\right), \tag{2}$$

where $erf(x)$ is the Gaussian error function given by

$$erf(x) = \frac{2}{\sqrt{\pi}} \int\limits_{0}^{x} \exp^{-t^2}\ \mathrm{dt}. \tag{3}$$

In terms of Type II error (right key rejection) we set it to constant probability $\frac{1}{2}$. Our scope is to study this hypothesis problem applied to differential cryptanalysis and its variants, especially using truncated differentials. The variable of our interest is the number of plaintext pairs with difference lying

attacker on the outside, and on the inside, we expect a strong path of correlated differential events inside the cipher which we call “propagation”, see Figure 2 on the page 221.

in a set ΔX and their difference after r rounds lies in a particular truncated differential set ΔY. We aim to use particular sets of differences which capture the mathematical structure of the cipher.

In this paper, we describe a general framework for constructing such distinguishers. As a proof of concept we apply this methodology to construct distinguishers that could be used to distinguish a large number of rounds for two well-known ciphers, GOST and SIMON. Based on this technique we construct a 20-round and a 22-round distinguisher for GOST and SIMON, respectively. Similar distinguishers can be found in [5], [9], [10], [14], [15].

2. Differential cryptanalysis

Differential Cryptanalysis (DC) is a general form of probabilistic or statistical cryptanalytic technique that belongs to the category of chosen-plaintext attacks. It was developed and popularized by Eli Biham and Adi Shamir [2] even though the attack has been known for much longer, see [11] for a short historical survey. It is a generic attack that could applied to any cryptographic primitive.

In DC, the main idea is to study the propagation of differences inside an iterated block cipher and compare with the case of a random permutation. Thus, we discover how and where the cipher exhibits non-random behaviour. The task is to discover specific differences that propagate with comparatively higher probability as in the case of a random permutation. By exploiting these properties further an attacker can recover parts of the secret key or the full key with time complexity lower than an exhaustive search.

In such attacks, the first step is to find pairs of input and output differences over sufficiently many rounds, that propagate with relatively high probability. Usually, we search for differences with their propagation round after round, cf. left hand side in Figure 2, on the page 221. Otherwise, we fix a number of rounds and search for events which occur for the whole block of rounds in a black box way, totally ignoring intermediate differences. The latter is known as a differential, cf. right hand side in Figure 2.

2.1. Truncated Differentials

Truncated Differential Cryptanalysis is a generalization of DC developed by Lars Knudsen [4]. In traditional DC we study the propagation of single differences, while in truncated DC we consider differences that are partially determined, i.e., we are interested only in some parts of the difference. This technique has been successfully applied to many block ciphers such as SAFER, IDEA, Skipjack, Twofish and many others.

We define the truncation TRUNC(a) of a n-bit string a as in Definition 1.

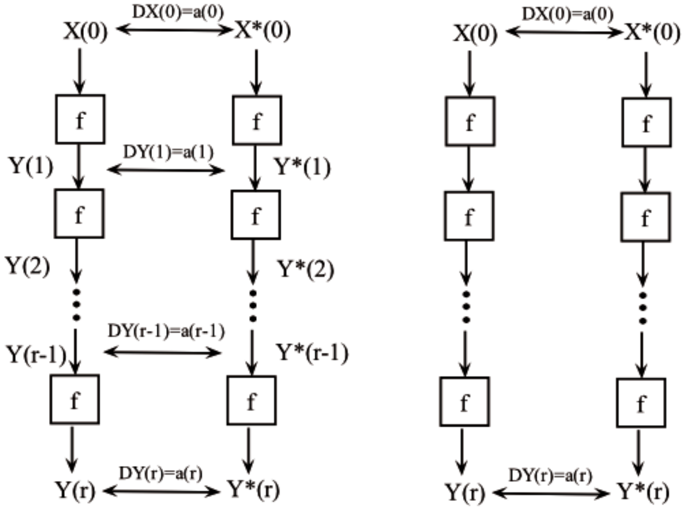

Figure 2. The left diagram illustrates a propagation of differences through different rounds, which is called *a differential characteristic*. On the right side, *a differential*, where only input-output differences are considered and middle differences are ignored.

Definition 1 (Truncation, [4]). Let $a = a_0a_1 \ ldotsa_{n-1}$ be an n-bit string, then its truncation is the n-bit string b given by

$$b_0b_1 \dots b_{n-1} = \mathrm{TRUNC}(a_0a_1 \dots a_{n-1}), \quad \text{where either } b_i = a_i \text{ or } b_i = *,$$

for all $0 \leq i \leq n-1$ and $*$ is an unknown value.

The notion of truncated differentials (cf. Definition 2) extends naturally to differences.

Definition 2 (Truncated Differentials, [4]). Let (α, β) be an i-round differential, then if α' and β' are truncations of α and β respectively, then (α', β') is an i-round truncated differential.

Note that we always need to exclude the zero difference from our set of differences which are allowed.

Example 1. The truncated differential on 8 bytes of the form 0000000000$*$00000 (in hexadecimal representation), where $* = x_1x_2x_3x_4$, is a set of differences of size $16-1$ (excluding the zero difference).

A truncated characteristic predicts only part of the difference in a pair of texts after each round of encryption. A truncated differential is a collection of truncated characteristics. Truncated differentials proved to be a very useful cryptanalytic tool against many block ciphers which at first glance seem secure against basic differential cryptanalysis.

In the next section we employ a simple heuristic discovery algorithm for discovering truncated differential properties which propagate with sufficiently high probability. In a later stage we combine these properties to construct a large round distinguisher which we use to mount a differential attack on a larger number of rounds.

3. Applications

In this section, we describe a general framework for the construction of efficient distinguishers, which is based on propagations of well-chosen propagations. This methodology is heuristic and it does not guarantee that the best possible distinguisher is obtained.

Our construction works as follows. Suppose we obtained the sets X_1, $X_2, \dots, X_r$ which propagate with sufficiently high probability for m rounds for an iterated block cipher (cf. Figure 3, page 223).

Then, we compute the cumulative probability of a transition from any difference in $\{X_1, X_2, \dots, X_r\}$ to itself for the middle $n-2m$ rounds. We select X_i, X_j as the input and output differences, which maximize the cumulative probability of the distinguisher. This methodology was introduced and was also studied earlier in [5], [6], [10], [14].

The aim is to distinguish a reduced version of an n-bit block cipher from a random permutation. In this paper we are interested in $n = 64$.

For a random permutation on 64 bits we compute the probability $X_i \to X_j$, where X_i and X_j are sets of differences with sizes $|X_i|$ and $|X_j|$, respectively, as follows (cf. Lemma 1).

Lemma 1 (Random Permutation Property on 64 bits for sets). *Let $P:\{0,1\}^{64} \to \{0,1\}^{64}$ be a uniformly random permutation. Given all pairs of inputs (P_i, P_j) with $P_i \oplus P_j \in X_i$, where X_i is a set of non-zero differences, then the average number of resulting pairs $\big(P(P_i), P(P_j)\big)$ that satisfy $P(P_i) \oplus P(P_j) \in X_j$, denoted by E_{ref}, where X_j is a set of non-zero differences, is given by,*

$$E_{\text{ref}} = \frac{|X_i| \cdot |X_j|}{2}. \tag{4}$$

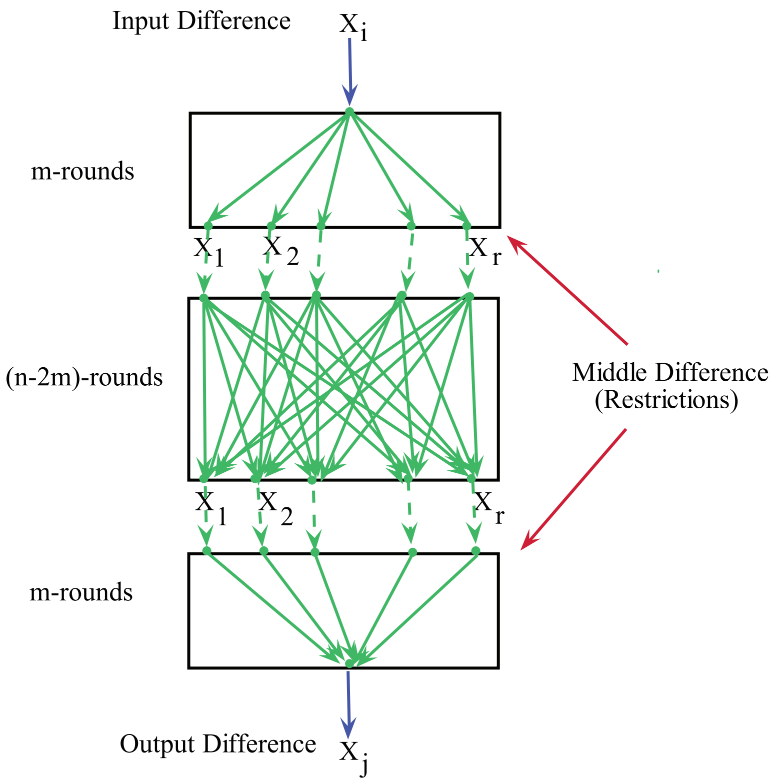

FIGURE 3. General construction of a distinguisher based on individual transitional probabilities.

Proof. For a random permutation P we have that every single combination of an input differential on 64 bits, and of an output differential on 64 bits, is expected to occur about $\frac{1}{2}$ times on average. This is because we have in total 2^{127} pairs of inputs and about 2^{128} possible sets of two differentials.

For a pair of input output differences X_i,X_j we have $|X_i| \cdot |X_j|$ possibilities and each has expected frequency of $\frac{1}{2}$ times on average. Overall, we expect to obtain $\frac{1}{2} \cdot |X_i| \cdot |X_j|$ pairs of inputs (P_i, P_j) with $P_i \oplus P_j \in X_i$ such that $P(P_i) \oplus P(P_j) \in X_j$. □

Subsequently, we need to compute the number of expected pairs with this input and output difference due to propagation inside the cipher.

Lemma 2 (Cumulative Probability of Distinguisher)**.** *The expected number of pairs (P_i, P_j) with input difference in X_i which follow the differential characteristic shown in Figure 3 is approximately given by:*

$$E_{ij} = 2^{63} \cdot |X_i| \cdot \sum_{m,n} \big(P(X_i \to X_m) \cdot P(X_m \to X_n) \cdot P(X_n \to X_j)\big). \tag{5}$$

Proof. The expected number of pairs (P_i, P_j) with $P_i \oplus P_j$ in open set X_i is given by $2^{64} \cdot |X_i| \cdot \frac{1}{2}$. Any difference in the set X_i is mapped to any difference in X_j over random key with probability (using Markov Property, cf. [14])

$$p_{ij} = \sum_{m',n'} \big(P(X_i \to X_{m'}) \cdot P(X_{m'} \to X_{n'}) \cdot P(X_{n'} \to X_j)\big).$$

Then, the expected number of output pairs is given by

$$E_{ij} = 2^{63} \cdot |X_i| \cdot p_{ij}. \tag{6}$$

□

Our aim is to distinguish the two distributions; one corresponding to a random permutation (or naturally occurred) and one due to propagation with additionally have the middle differences (propagation).

In the first case, we expect on average E_{ref} pairs, while in the second case we expect $E_{i,j} + E_{\text{ref}} - E_{\text{inter}}$ pairs, where E_{inter} is the number of pairs which occur naturally but also have this middle difference property. If this number is non-negligible, then the analysis becomes more complex. However, these middle differences can be used to make the two sets entirely disjoint and thus assume that E_{inter} is negligible.

Assuming that the sets are entirely disjoint, the distributions of the sample means $\mathcal{E}_{\text{ref}}$ and $\mathcal{E}_{i,j} + \mathcal{E}_{\text{ref}}$ can be approximated by Normal Distributions

$$\mathcal{X} \sim \mathcal{N}(E_{\text{ref}}, E_{\text{ref})} \quad \text{and} \quad \mathcal{Y} \sim \mathcal{N}(E_{i,j} + E_{\text{ref}}, E_{i,j} + E_{\text{ref}}),$$

respectively. In our case, since we use intermediate difference, we can assume that the intersection of the two sets is negligible. The variance in both cases equals the mean since we approximate the distributions of the variable of number of pairs by Poisson distribution.

We define the advantage of the distinguisher as a measure of expressing the number of standard deviations that the mean of distribution $\mathcal{X}$ deviates from that of $\mathcal{Y}$. In cryptography an 'advantage' is typically a difference in success probability in two experiments in which an adversary distinguishes between an idealized and real situation. Our particular definition is rescaled to provide a standardized measure of success of a distinguisher for the purpose of judging the validity of an assumption on key bits (or another type of attacker assumption).

Definition 3 (Advantage of Distinguisher)**.** The advantage of a distinguisher $\mathcal{A}$ for distinguishing $\mathcal{X} \sim \mathcal{N}(\mu_1, \sigma_1^2)$ over $\mathcal{Y} \sim \mathcal{N}(\mu_2, \sigma_2^2)$ is given by

$$\mathrm{ADV} = \frac{(\mu_2 - \mu_1)}{\sigma_1}. \tag{7}$$

We know that by Central Limit Theorem (CLT) that the sample mean distribution will be approximately Normal with mean equal to the variance. Thus, the advantage is given by $\frac{E_{i,j}}{\sqrt{E_{\mathrm{ref}}}}$.

Note that, in order to compute the probability of a transition we use a very simple algorithm that simply counts the number of events of our interest for a given fixed number of trials. We assume that the distribution of the number of events of our interest follows (approximately) a Poisson distribution. We use this distribution as we have experimentally observed that for all cases we have tried.

- We have a discrete distribution of small integers.
- In all cases we have tried and are included in this paper the variance is relatively close to the mean.

For a sample of size N if x denotes the number of events that were observed (approximated by Poisson with parameter Poisson mean Np, where p is the true mean), then the approximated Standard Deviation (SD) of the variable $\frac{x}{N}$, where N is assumed to be constant and p the observed mean, is given by $\sqrt{Np}/N = \sqrt{p/N}$. This is because the variance equals to the mean in case of a Poisson distribution.

Let I_1 be the interval $[p - t\sqrt{p'/N},\, p + t\sqrt{p/N}]$, where t a parameters of our choice, expressing how accurately we would like to search. In our simulations we would like I_1 to be contained in the interval

$$I_2 = \left[p \cdot 2^{-a},\, p \cdot 2^{a}\right],$$

where a is an error we allow in the exponent of the mean as a power of 2. For example $a = 0.1$ is a frequent choice. We assume that the true mean that we are aiming to approximate by simulations is bigger than some probability value p_0 in order to ensure that our algorithm terminates in reasonable time. The inclusion of sets implies that we need to run $N > N_0$ simulations, where N_0 is given by

$$N_0 = \frac{2^{2a} t^2}{(2^a - 1)^2} . \frac{1}{p_0} \tag{8}$$

in order to achieve the desired precision. Since we record the mean $\frac{x}{N}$ we expect by Central Limit Theorem that the distribution of our mean converges to a Normal Distribution. Thus, for the results presented in the next section we run simulations for at least N_0 times in order to get desired precision, e.g., $a = 0.1$ in the exponents of probabilities which are of interest to the attacker.

3.1. Application A: SIMON

SIMON is a lightweight block cipher designed by NSA, with the aim to have optimal hardware performance [13]. It follows the classical Feistel design paradigm and operates on two n-bit halves in each round.

The basic version SIMON 64/128 has 44 rounds. Each round of SIMON applies a non-linear, non-bijective function

$$F : GF(2)^n \to GF(2)^n \quad \text{to the left half of the state.}$$

The operations used are as follows:

(1) bitwise XOR,

(2) bitwise AND, and

(3) left circular shift, S^j by j bits.

We denote the input to the ith round by $L^{i-1}||R^{i-1}$ and in each round the left word L^{i-1} is used as input to the round function F defined by

$$F(L^{i-1}) = (L^{i-1} <<< 1) \cdot (L^{i-1} <<< 8) \oplus (L^{i-1} <<< 2), \tag{9}$$

where '$\cdot$' is the bitwise AND operator.

The next state $L_i||R_i$ is computed in the following way

$$L^i = R^{i-1} \oplus F(L^{i-1}) \oplus K^{i-1}, \tag{10}$$

$$R^i = L^{i-1}. \tag{11}$$

The output of the last round is the ciphertext after applying the round function for 44 times for the particular variant SIMON 64/128. More details are out of scope of this paper and can be found in [13].

3.2. SIMON 64/128: 22-round distinguishers

In this section we combine several truncated differential properties in order to construct a 22-round distinguisher. In particular, we combine two transitions discovered to propagate with sufficiently high probability for 10 and 2 rounds. The transitions are presented in Result A.

Following precisely this methodology we end up in the problem of distinguishing the following two Gaussian distributions.

- Natural Propagation: X: N $(2^{12}, 2^6)$.
- SIMON: Y: N $(2^{12} + 2^7, \sqrt{(2^{12} + 2^7)})$.

Result A.

$$\begin{array}{r}[0000002200000080]\\ \downarrow(10\mathrm{R})\\ [002EFF9A00022E4C]\\ \downarrow(10\mathrm{R})\\ [0000002200000800]\\ \downarrow(2\mathrm{R})\\ [0A50002209010008]\end{array}$$

is a 22 rounds distinguisher with 2 standard deviations for this variant of SIMON.

Justification. We have in total $2^{63} \cdot 2^{3} = 2^{66}$ pairs of plaintexts (P, P') that satisfy $P \oplus P' \in [0000002200000080]$. A proportion $2^{10}/2^{64}$ is expected to have a ciphertext difference

$$C \oplus C' \in [0A50002209010008]$$

by accident (random permutation) after either a large number of rounds or by simply at random, which implies 2^{12} pairs. Now in case of SIMON we expect $2^{66-17\cdot 0-38\cdot 0-4\cdot 0} = 2^{7}$ to follow this truncated differential path with the specified differences in the middle. Since these distributions converge to Gauss distributions, but the underlying source for observed samples is approximated by Poisson, we can assume that the standard deviation can be computed by the square root of the mean.

The other problem that we need to consider is the problem of the number of pairs that by accident have also this intermediate differences after 10 and 20 rounds as specified by the distinguisher. For this particular example, we have that

$$2^{16} \cdot 2^{-17-38} \approx 2^{-39}$$

are expected to have these intermediate differences. We need to stress that we are NOT looking at a random permutation, but at a real SIMON with 22 rounds and at events which occur at random on the outside (input and output), whether they can propagate on the inside as predicted (which would mean that random events interfere with non-random events). This is expected to be zero events in common in most cases, sometimes 1 and 2^{-39} on average, and thus the two sets of events are completely disjoint in practice.

Note that we follow the following hypothesis testing; if the number of pairs observed during the attack exceeds $2^{12} + 2^{7}$, then we accept the key assumption as correct, otherwise we reject it. This implies that the Type II error of our attack is automatically set to half. That implies that we have to repeat twice our attack in order to retrieve the correct key.

3.3. Application B: GOST

GOST is a block cipher with a simple 32-round Feistel structure which encrypts a 64-bit block using a 256-bit key [1, 3]. Each round of GOST contains a key addition modulo 2^{32}, a set of 8 bijective S-boxes on 4 bits and a simple rotation by 11 positions to the left. The image of any 64-bit block of the form $L||R$ (where L and R the left and the right half, respectively) after 1 round of GOST is given by

$$(L, R) \to \big(R, L \oplus F_i(R)\big), \tag{12}$$

where F_i is the internal function used in each round. GOST has a very simple key schedule. The 256-bit key is divided into eight 32-bit words $k_0, k_1, \ldots, k_7$, where the first 24 rounds use the keys in this order and only the last 8 rounds use them in the reverse order, as shown in Table 1, on the page 228.

Table 1. Key schedule in GOST.

R1–R8	R9–R16
$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$	$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$
R17–R24	R25–R32
$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$	$k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$

3.4. GOST: 20-round distinguisher

In this section we present the results obtained when our methodology is applied to the GOST which uses the standard set of S-boxes.

Result B.

$$\begin{tikzcd}
{[8078000000000700]} \arrow[d, "(7R)"] \\
{[8070070080700700]} \arrow[d, "(6R)"] \\
{[8070070080700700]} \arrow[d, "(7R)"] \\
{[0000070080780000]}
\end{tikzcd}$$

is a 20-round distinguisher with approx. 69 standard deviations for this variant of GOST.

Justification.
We have $(2^8-1)(2^8-1)$ possibilities of type: [8078000000000700)] → (after some permutation OR 20 inner rounds of GOST) → [0000070080780000]. For a typical permutation[2] on 64-bits we expect that there are $0.5 \cdot 2^{8+8} = 2^{15}$ pairs (P_i, P_j) with such differences. The distribution of this number can be approximated by a Gaussian with a standard deviation $2^{7.5}$.

Following [12] or Fact 3.4.1 in page 13 of [10] and given $2^{64+14-1}$ pairs with the initial difference, we have $2^{77-18.7} = 2^{58.3}$ pairs for the middle 6 rounds.

Then following Fact 3.4.2 in page 13 of [10] the propagation in the next 7 rounds occurs with probability $2^{-22.2}$ on average over GOST keys. Since this is a permutation, the same propagation can be applied backwards in the preceding 7 rounds. Overall, we expect that $2^{58.3-44.4} = 2^{13.9}$ pairs survive.

Now we show that with large probability none of these $2^{13.9}$ pairs P_i, P_j is a member of the set of 2^{15} established beforehand. For any of the 2^{15} cases which occur naturally at random, we have a non-zero input differential [8078000000000700]. Then, a computer simulation shows that a differential of type [807007008070070] CAN occurs at 7 rounds later but only with probability of $2^{-16.2}$. Similarly, it can also occur 7 rounds from the end, but only with probability of $2^{-16.2}$. Overall we expect that only about $2^{15-16.2-16.2} = 2^{-17}$ pairs P_i, P_j on average will have the "*propagation*" characteristics as shown above. Therefore, the two sets are entirely disjoint with a very high probability.

As in Result A the standard deviation is expected to be equal exactly to the square root of their expected average number of $2^{15} + 2^{13.9}$, which will be about $2^{7.8}$. The $2^{13.9}$ additional events divided by $2^{7.8}$ means that we get a distinguisher which works at $2^{6.1} \approx 69$ standard deviations.

We refer to [9], [10] to show how to transform this distinguisher into a complex multiple stage attack on full 32 round GOST with running time of 2^{179}.

4. Conclusion

The main task in symmetric cryptanalysis is to use structure of the block cipher in order to construct distinguishers which can be used to distinguish a large number of rounds from a random permutation. In this paper, we described a hypothesis-testing framework for constructing such distinguishers, using truncated differential properties inside the cipher. We apply this methodology to two well-known ciphers, GOST and SIMON, to construct a 20-round and a 22-round

[2] It does not have to be a random permutation, it can be GOST with more rounds are any other permutation somewhat artificially constructed by an attacker when his assumptions are incorrect.

distinguishers respectively. In our additional works which are published separately we have successfully built various distinguishers of similar kind for GOST and SIMON and demonstrate how to transform such distinguishers to develop key recovery attacks against (up to) the full round ciphers [5], [7]–[10], [14]. Our best truncated differential result on GOST leads to an attack in 2^{179} which is described in full in [9], [10]. In [5], [6], [10], [14] and in the present paper we explain in detail how such attacks can be constructed with a mix of insights, heuristics and a careful analysis of numerous possible variants.

REFERENCES

[1] POSCHMANN, A.—LING, S.—WANG, H.: *256 bit standardized crypto for 650 GE-GOST revisited*. In: CHES 2010, Lect. Notes. in Comput. Sci. Vol. 6225, Springer, Berlin, Heidelberg, New York, 2010, pp. 219–233.

[2] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of DES-like cryptosystems*. J. Cryptology, **4** (1991) 3–72.

[3] GOST: A Russian reference implementation of GOST implemented as an extension of TLS v1.0, available in: OpenSSL library, 2005.

[4] KNUDSEN, L.: *Truncated and higher order differentials*. In: FSE 1994, Lect. Notes. in Comput. Sci. Vol. 1008, Springer-Verlag, Berlin, Heidelberg, New York, 1995. pp. 196–211.

[5] COURTOIS, N.—MOUROUZIS, T.: *Enhanced truncated dfferential cryptanalysis of GOST*. In: SECRYPT 2013, `http://www.nicolascourtois.com/papers/sec13.pdf`

[6] COURTOIS, N.—MOUROUZIS, T.: *Propagation of truncated differentials in GOST*. In: SECURWARE 2013,
`http://www.thinkmind.org/download.php?articleid=securware_2013_7_20_30119`

[7] COURTOIS, N.—MOUROUZIS, T.—GROCHOLEWSKA-CZURYLO, A.—QUISQUATER, J-J.: *On optimal size in truncated differential attacks*. In: CECC 2014, Studia Sci. Math. Hungar. **52** (2015), no. 2, 246-256.

[8] COURTOIS, N.: *Algebraic Complexity Reduction and Cryptanalysis of GOST*. Monograph study on GOST cipher, 2015, `http://eprint.iacr.org/2011/626`

[9] COURTOIS, N.: *An improved differential attack on full GOST*. In: Lect. Notes. in Comput Sci. Vol. 9100, Springer, Berlin, Heidelberg, New York, 2016 (to appear).

[10] COURTOIS, N.: *An improved differential attack on full GOST*. Preprint 2015, available at: `http://eprint.iacr.org/2012/138`

[11] COURTOIS, N.—MOUROUZIS, T.—MISZTAL, M.—QUISQUATER, J-J.—SONG, G.: *Can GOST be made secure against differential cryptanalysis?* Cryptologia, **39** (2015), no. 2, 145–156.

[12] COURTOIS, N.—MISZTAL, M.: *Aggregated differentials and cryptanalysis of PP-1 and GOST*. In: CECC 2011, Period. Math. Hungar. **65** (2012), no. 2, 11-26.

[13] BEAULIEU, R.—SHORS, D.—SMITH, J.—TREATMAN-CLARK, S.—WEEKS, B.—WINGERS, L.: *The SIMON and SPEK families of lightweight block ciphers*. Cryptology ePrint Archive, Report 2013/404, 2013.

[14] MOUROUZIS, T.: *Optimizations in Algebraic and Differential Cryptanalysis*. UCL PhD Thesis, 2014. `http://discovery.ucl.ac.uk/`

[15] MOUROUZIS, T.—SONG, G.—COURTOIS, N.—CHRISTOFI, M.: *Advanced differential cryptanalysis of reduced-round SIMON 64/128 using large-round statistical distinguishers*. Cryptology ePrint Archive, Report 2053/481, 2015.

Received November 10, 2015

Theodosis Mourouzis
InfoLab, (CIIM)
Cyprus International Institute
of Management
21 Academias, Ave Aglandjia
Nicosia 2107
CYPRUS
E-mail: theodosis@ciim.ac.cy

Nicolas Courtois
University College London
Gower street
London WC1E 6BT
UNITED KINGDOM
E-mail: ncourtois@cs.ucl.ac.uk