Information Processing Letters 114 (2014) 655–662

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

# Cryptanalysis of GOST R hash function ☆

Zongyue Wang [a], Hongbo Yu [b,*], Xiaoyun Wang [a,b,c]

[a] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[b] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[c] Institute for Advanced Study, Tsinghua University, Beijing 10084, China

ARTICLE INFO

*Article history:*
Received 8 May 2013
Received in revised form 9 April 2014
Accepted 7 July 2014
Available online 22 July 2014
Communicated by S.M. Yiu

*Keywords:*
Cryptography
Hash function
GOST R
Rebound attack
Multi-collision

ABSTRACT

GOST R 34.11-2012 is the new Russian hash function standard. This paper presents some cryptanalytic results on GOST R. Using the rebound attack technique, we achieve collision attacks on the reduced round compression function. Result on up to 9.5 rounds is proposed, the time complexity is $2^{176}$ and the memory requirement is $2^{128}$ bytes. Based on the 9.5-round collision result, a limited birthday distinguisher is presented. More over, a $k$-collision on 512-bit version of GOST R is constructed which shows the weakness of the structure used in GOST R.



## 1. Introduction

Hash functions are taking important roles in cryptography and have been used in many applications, e.g., digital signatures, authentications and message integrity. Since the break of MD5 and SHA-1 [1,2], cryptographers have been searching for secure and efficient hash functions. Stribog [3] is proposed by Grebnev et al. It was selected as the new Russian hash standard (GOST R 34.11-2012) in August 2012. Similar as the structure of Whirlpool [4], it also uses an AES-like block cipher in its compression function.

Rebound attack is a freedom degrees utilized technique which can be applied to find collisions in both permutation based and block cipher based hash constructions. This technique was firstly proposed by Mendel et al. to achieve collision attacks on reduced Whirlpool and Grøstl [5]. It aims to find a pair of values that follows a pre-determined truncated differential efficiently. The searching procedure is divided into two phase: the inbound phase and the outbound phase. In inbound phase the attacker makes full use of the available degrees of freedom and generates sufficiently many paired values that satisfy the truncated differential path of the inbound phase as starting points. The subsequent outbound phase tests these starting points in order to find paired values that satisfy the truncated differential path of the outbound phase.

Giving better results on Whirlpool, Lamberger et al. improved this technique in [6]. Available degrees of freedom of the key schedule are used to extended the inbound phase of the rebound attack by up to two rounds. The best result of [6] is near-collision attack on 9.5 rounds of the compression function with a complexity of $2^{176}$. And this result is further turned into the first distinguishing attack for the full 10 round compression function of Whirlpool. As an independent work, Gilbert et al. bring in Super-Sbox technique to rebound attack in [7] where two rounds of AES-like permutations were viewed as a layer of Super-Sbox. Besides, the rebound technique can also be applied to analysis AES and AES-like block ciphers [8,9] as well as ARX ciphers [10]. Recently, using techniques adapted from

☆ Supported by 973 program (No. 2013CB834205), the National Natural Science Foundation of China (Nos. 61133013 and 61373142), the Tsinghua University Initiative Scientific Research Program (No. 20111080970) and "12th Five-year plan" the National Development Foundation for Cryptological Research (No. MMJJ201401009).

* Corresponding author.

http://dx.doi.org/10.1016/j.ipl.2014.07.007
0020-0190/

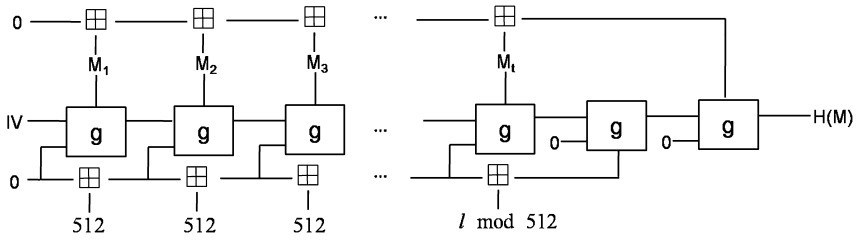


**Fig. 1.** The GOST R hash function.

**Table 1**
Summary of results for GOST R compression function. The complexity in brackets refer to modified attacks using a precomputed table taking $2^{128}$ time/memory to set up.

| Rounds | Complexity time/memory | Type | Source |
|---|---|---|---|
| 4.5 | $2^{64}/2^{16}$ | collision | Section 3.3 |
| 5.5 | $2^{64}/2^{64}$ | collision | Section 3.4 |
| 7.5 | $2^{128}/2^{16}$ | collision | Section 3.5 |
| 9.5 | $2^{240}/2^{16}(2^{176}/2^{128})$ | collision | Section 3.6 |

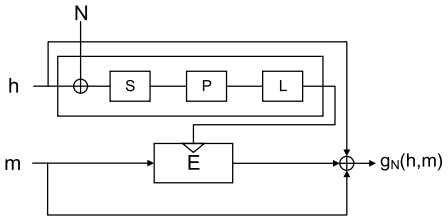


**Fig. 2.** Compression function of GOST R.

the rebound attack, Duc et al. constructed differential characteristics on Keccak in [11].

In contrary to finding collisions for hash functions, Joux proposed a method to construct multicollisions in [12]. He argued that for iterated hash functions, to find a multicollisions is not even harder than finding ordinary collisions. Gauravaram et al. improved this method and achieve generic attack on Damgård–Merkle variants with linear-XOR or additive checksums [13,14].

During the revision of this paper, we notice an independent but similar work by AlTawy et al. They achieved 7.75, 8.75 and 9.75 round semi free-start near collision on GOST R using rebound technique. For more details, we refer the reader to [15].

### 1.1. Our contributions

As the similarity between GOST R and Whirlpool, the rebound techniques used in [6] to analyze Whirlpool can also applied to GOST R. However, GOST R replace of the ShiftRows operation in AES-based designs with the matrix transposition. We show that this difference brings more weakness.

In this paper, we present the analysis on GOST R. More precisely, by applying the rebound attack techniques similar as in [6], we give collision attacks on 4.5, 5.5, 7.5 and 9.5 rounds GOST R compression function respectively. Our collision attacks on GOST R compression function are summarized in Table 1. Then we show that the result of 9.5 rounds can be further converted to a 10-round distinguisher. In addition, we construct multicollisions on full 512-bit version of GOST R employing technique proposed in [13,14]. This result shows that the structure used in GOST R is not an ideal one.

### 1.2. Outline of the paper

The paper is organized as follows: in Section 2, we briefly describe the GOST R hash function. Then we illustrate rebound attack in detail in Section 3; a limited birthday distinguisher is given in Section 4. In Section 5, we construct multicollisions. Finally, in Section 6, we conclude this paper.

## 2. The GOST R hash function

GOST R is the Russian hash function standard [3]. It accepts message block size of 512 bits and produces a hash value of 512 or 256 bits. An $l$-bits message is first padded into a multiple of 512 bits. The bit '1' is appended to the end of the message, followed by $512-1-(l \bmod 512)$ zero bits. Let $M = M_t \parallel M_{t-1} \parallel \ldots \parallel M_1$ be a $t$-block message (after padding) which is represented in big Endian form. As illustrated in Fig. 1, the computation of $H(M)$ can be described as follow:

$$h_0 = IV, \qquad N = 0, \qquad \Sigma = 0 \tag{1}$$

$$h_j = g_N(h_{j-1}, M_j), \qquad N = N \boxplus 512, \qquad \Sigma = \Sigma \boxplus M_j \quad \text{for } 0 < j < t \tag{2}$$

$$h_t = g_N(h_{t-1}, M_t), \qquad N = N \boxplus (l \bmod 512), \quad \Sigma = \Sigma \boxplus M_t \tag{3}$$

$$h_{t+1} = g_0(h_t, N) \tag{4}$$

$$H(M) = g_0(h_{t+1}, \Sigma) \tag{5}$$

where $IV$ is a predefined initial value and '$\boxplus$' means addition operation in the ring $Z_{2^{512}}$. Defined in (6), $g_N(h, m)$ is the compress function of GOST R whose structural is illustrated in Fig. 2.

$$g_N(h, m) = E\big(L \circ P \circ S(h \oplus N), m\big) \oplus h \oplus m \tag{6}$$

As shown in Fig. 3, the block cipher $E$ used in GOST R is a variant of AES which update an $8 \times 8$ state[1] of 64 bytes and round key in 12 rounds. In one round, the state is updated by the round transformation $r_i$ as follows:

$$r_i \equiv X[k_{i+1}] \circ L \circ P \circ S$$

[1] The state is also $64 \times 64$ over the field $GF(2)$.