

Key Recovery Attack on full GOST Block Cipher with Zero Time and Memory

Ewan Fleischmann, Michael Gorski, Jan-Hendrik Hühne, and Stefan Lucks

Bauhaus-University Weimar, Germany

{Ewan.Fleischmann, Michael.Gorski, Jan.Huehne, Stefan.Lucks}@uni-weimar.de

Abstract. The GOST block cipher was developed in the 1970s and is a standard currently used in the Russian government. In this paper we present a new attack on the GOST block cipher that uses only $2^{7.5}$ chosen plaintexts and ciphertexts and runs in time $2^{7.5}$. Due to the very low complexity we state that our attack is memoryless and runs in nearly zero time. In this way we present the best attack on the full 32-round GOST block cipher that can be used for key recovery.

Keywords: differential cryptanalysis, related-key rectangle attack, GOST block cipher.

1 Introduction

The GOST [9] block cipher is defined in the standard GOST 28147-89 and is a Soviet and Russian government standard for an symmetric key block cipher. As well the GOST hash function is based on the block cipher. After the dissolution of the USSR, it was released to the public in 1994. GOST 28147 was the Soviet alternative to DES, the United States standard symmetric key encryption algorithm.

It has a very simple key schedule and iterates 32 times a round function F . In each round function GOST uses a key addition modulo 2^{32} , so the probability depends on the value of the round key and the value of the input differences and not only on the input-out differences. So as to reduce the effect of the round key addition, H. Seki et al. introduced a specific set of differential characteristics and proposed a differential on 13 rounds of GOST as well as a related key differential attack on 21 rounds of GOST. A summary of existing attacks on GOST is shown in Table 1.

References

- [1] Eli Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. Cryptology*, 7(4):229–246, 1994.
- [2] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-Key Boomerang and Rectangle Attacks. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 507–525. Springer, 2005.
- [3] Eli Biham, Orr Dunkelman, and Nathan Keller. Improved slide attacks. In Alex Biryukov, editor, *FSE*, volume 4593 of *Lecture Notes in Computer Science*, pages 153–166. Springer, 2007.
- [4] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.
- [5] Orhun Kara. Reflection Cryptanalysis of Some Ciphers. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT*, volume 5365 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2008.

Table 1. Summary of Attacks on the GOST block cipher

Attack	# rounds	data	time	source
A set of Diff. Char.	13	2^{51}	Not mentioned.	[9]
RK Differential	21	2^{56}	Not mentioned.	[9]
RK Differential	24	theoretical	theoretical	[6]
Slide*	24	2^{64}	2^{64}	[3]
Slide	30	2^{64}	$2^{253.7}$	[3]
Reflection [†]	30	2^{32}	2^{224}	[5]
RK Differential	31	2^{26}	2^{39}	[7]
Distinguishing [‡]	full	2	2	[7]
RK Boomerang	full	$2^{11.5}$	$2^{11.5}$	this paper
Reflection	full	2^{32}	2^{192}	[5]
Slide ²	full	2^{64}	2^{64}	[3]
RK Differential	full	2^{35}	2^{36}	[7]

[†] Under the assumption that its S-Boxes are bijective the attack works on approximately 2^{224} keys.

[‡] Cannot be used for key recovery attacks.

* The attack works with unknown S-Boxes.

² The attack works for a weak key class of GOST containing 2^{128} weak keys and with unknown S-Boxes.

- [6] John Kelsey and Bruce Schneier. Key-schedule cryptanalysis of deal. In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 118–134. Springer, 1999.
- [7] Youngdai Ko, Seokhie Hong, Wonil Lee, Sangjin Lee, and Ju-Sung Kang. Related key differential attacks on 27 rounds of xtea and full-round gost. In Bimal K. Roy and Willi Meier, editors, *FSE*, volume 3017 of *Lecture Notes in Computer Science*, pages 299–316. Springer, 2004.
- [8] Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Related-Key Rectangle Attack on 42-Round SHACAL-2. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 85–100. Springer, 2006.
- [9] Haruki Seki and Toshinobu Kaneko. Differential cryptanalysis of reduced rounds of gost. In Douglas R. Stinson and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 2012 of *Lecture Notes in Computer Science*, pages 315–323. Springer, 2000.
- [10] YongSup Shin, Jongsung Kim, Guil Kim, Seokhie Hong, and Sangjin Lee. Differential-Linear Type Attacks on Reduced Rounds of SHACAL-2. In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *ACISP*, volume 3108 of *Lecture Notes in Computer Science*, pages 110–122. Springer, 2004.
- [11] Gosudarstvennyi standard 28146-89. Cryptographic Protection for Data Processing Systems, 1989.
- [12] David Wagner. The Boomerang Attack. In Lars R. Knudsen, editor, *Fast Software Encryption*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.