Note on Streebog constants origin

V. Rudskoy

Abstract

Recent paper by AlTawy and Youssef [1] devoted to cryptanalysis of the new Russian cryptographic hash standard (GOST R 34.11-2012, a.k.a. Streebog) shows that a certain choice of randomly looking round constants for underlying block cipher of Streebog allows to mount a practical-time rebound attack on full Streebog-like hash function.

In support, the paper presents a modified version of Streebog, which is called «Malicious Streebog». The only difference between the original and the malicious versions lies in the set of round constants. Malicious Streebog turns out to be vulnerable to rebound attack and a collision is presented.

In order to remove suspicions on possible backdoors in Streebog, we provide the origin and the rationale for Streebog constants.

In this note we will use the notations from GOST R 34.11-2012 [2].

There are different design principles of round constants used in symmetric cryptographic algorithms. One of the possibilities is to generate them in random or pseudo-random way.

Cryptographic hash function can be seen as a pseudo-random function in the sense that a hash value provides no information on the input.

During the development of Streebog it was decided to generate pseudorandom constants with Streebog-like hash function, which we denote H_{init}, provided with 12 different natural language input messages. We present these inputs and the description of the H_{init} function below.

H_{init} function is almost equal to Streebog-512 (which we denote as H) except two minor differences: round constants and the linear transformation L. All constants of H_{init} are zero vectors: $C_i = 0^{512}$. Linear transformation L of H_{init} is defined the same way as for H – as a block-wise row by matrix multiplication over

$GF(2)$, – but with different matrix A_{init}. In turn A_{init} is obtained by reversing the *columns* order of matrix A, e.g. the first row of A is `8e20faa72ba0b470` (in hexadecimal notation), thus the first row of A_{init} is `0e2d05d4e55f0471`. Note that since A is an MDS matrix then A_{init} is an MDS matrix as well.

Finally, in table 1 we provide the input messages M, that were used for generation of round constants of Streebog.

$C_i = H_{init}(M)$	M (in hexadecimal notation)
C_1	`e2e5ede1e5f0c3`
C_2	`f7e8e2eef0e8ece8e4e0ebc220e9e5e3f0e5d1`
C_3	`f5f3ecc4`
C_4	`f7e8e2eef0e4ede0f1eae5ebc020e9e5f0e4edc0`
C_5	`ede8e3fbc4`
C_6	`f7e8e2eeebe9e0f5e8cc20f1e8ede5c4`
C_7	`ede8f5fef2e0cc`
C_8	`f7e8e2eef0eef2eae8c220e9e8f0f2e8ecc4`
C_9	`e9eeeaf1e4f3d0`
C_{10}	`f7e8e2e5f0eee3c820f0e8ece8e4e0ebc2`
C_{11}	`ede8eaf8e8d8`
C_{12}	`f7e8e2e5e5f1eae5ebc020e9e8ebe8f1e0c2`

Table 1: Messages used for generation of round constants

References

[1] *AlTawy, R.* Watch your Constants: Malicious Streebog / R. AlTawy, A. M. Youssef // *Cryptology ePrint Archive, Report 2014/879.* — 2014. — http://eprint.iacr.org/.

[2] GOST R 34.11-2012. Informational technology. Cryptographic data protection. Hash function. — Russian Federal Agency on Technical Regulation and Metrology, 2012.