

# Design and Analysis of Block Cipher with Variable Word-Size Based on Dedicated Hash Functions: SHACAL-V

Yong-Sork HER\*, Kouichi SAKURAI

Graduate School of Information Science and Electrical Engineering , Kyushu University  
6-10-1, Hakozaki, Higashiku, Fukuoka, 812-8581, JAPAN

[ysher@tcslab.csce.kyushu-u.ac.jp](mailto:ysher@tcslab.csce.kyushu-u.ac.jp)

[sakurai@csce.kyushu-u.ac.jp](mailto:sakurai@csce.kyushu-u.ac.jp)

**Abstract.** In this paper, we propose block cipher based on SHA-V, namely *SHACAL-V*. SHACAL-V as block cipher has variable word sizes, which is 128, 160, 192, 224, 256, 288, and 320-bit. SHACAL-V has variable key values, and a fixed number of rounds. For the security of SHACAL-V, we discuss the security of SHACAL-V against amplified boomerang attack. Moreover, we compare SHACAL-V with RC5/6 on the security.

A block cipher using hash function was proposed by H.Handschuh and D.Naccache. Exactly, they designed block cipher, called SHACAL-1 and SHACAL-2, using SHA-1 and SHA-256, as a submission to NESSIE (New European Schemes for Signatures Integrity and Encryption). SHACAL-1 is a 160-bit block cipher based on the hash standard SHA-1. In 2001, they introduced SHACAL-2 based on SHA-256. In the third NESSIE workshop, Kim et al. proposed amplified boomerang attack of reduced-round SHACAL with various key sizes.

We proposed hash function with a variable output length, namely *SHA-V*, based on SHA-1 and HAVAL. We use initial values of SHA-V as a plaintext and messages of SHA-V as secret key. The structure of SHACAL-V similar to SHA-V is two parallel lines, denoted as the *Left-line* and *Right-line*, consisting of 80 steps each. The size of input message is 320 bits and the size of output message is from 128 bits to 320 bits by a 32-bit. A key which consists of two parallel lines is fixed, as 1024 bits, but key values are variable. So, each of the round steps is invertible in the round variables. The new message in each round is created in combination with input message and step operation.

There are block ciphers, RC5 and RC6, which have a variable word size, a variable number of rounds, and a variable length secret key. In the number of round, SHACAL-V has 160 rounds, RC5 and RC6 are from 0 to 255 rounds. The input (output) sizes of RC5 are 256 bits or 384 bits or 512 bits, and the input (output) sizes of RC6 are 512 bits or 768 bits or 1024 bits. But, the input (output) size of SHACA-V is the fixed 320 bits.

**Keyword** Cryptography, Block cipher, SHACAL-V, SHACAL-1, RC5, RC6, Amplified boomerang attack, Dedicated hash functions