Preimage attack on Sarmal-512

Ivica Nikolić

University of Luxembourg

Abstract. We present a preimage attack on Sarmal-512 that requires $max(2^{512-s}, 2^{256+s})$ computations and 2^s memory.

1 Description of Sarmal-n

Sarmal-n [3] is a hash family based on the HAIFA design. After the standard padding procedure, the padded message is divided into blocks of 1024 bits each, i.e. $M = M_1||M_2||\ldots||M_k, |M_i| = 1024, i = 1, \ldots, k$. Each block is processed by the compression functions. HAIFA design implies that the compression function f has four input arguments: a previous chain value h_{i-1}, a message block M_i, a salt s, and a block index t_i. Hence, Sarmal-n can be described as (IV is some initial value):

$h_0 = IV$
for$(1 \leq i \leq k)$
{
$h_i = f(h_{i-1}, M_i, s, t_i)$
}
output h_k

The last chaining value h_k is the hash value of the message M. The chaining value h_i has 512 bits. Let us denote the left and the right half of h_i as L_i and R_i respectively, i.e. $h_i = L_i||R_i$. The salt s has 256 bits (similarly let $s = s_1||s_2$), and the block index t_i has 64 bits. Then, the compression function of Sarmal-n can be defined as:

$$f(h_{i-1}, M_i, s, t_i) = \mu(L_{i-1}||s_l||c_1||t_i) \oplus \nu(R_{i-1}||s_r||c_2||t_i) \oplus h_{i-1}, \quad (1)$$

where μ and ν are functions that output 512 bit values, and c_1, c_2 are some constants. The exact definition of these functions is irrelevant for our attack.

2 Free Start Preimage attack on the Compression Function of Sarmal-512

First let us try to find a free start preimage attack for the compression function of Sarmal-512.
Definition. Let $f(h, M, s, t)$ be the compression function for some hash function. Then (h^*, M^*, s^*, t^*) is a free start preimage of the hash value H^* if $f(h^*, M^*, s^*, t^*) = H^*$.
Further, we will show how to find a free start preimage, for any values of the message, salt, and the block index.
From (1) we get:

$$\begin{aligned}
&f\ (\ h_{i-1}, M_i, s, t_i) = \\
&= \mu\ (L_{i-1}||s_l||c_1||t_i) \oplus \nu(R_{i-1}||s_r||c_2||t_i) \oplus h_{i-1} = \\
&= \mu\ (L_{i-1}||s_l||c_1||t_i) \oplus \nu(R_{i-1}||s_r||c_2||t_i) \oplus L_i||R_i = \\
&= \mu\ (L_{i-1}||s_l||c_1||t_i) \oplus \nu(R_{i-1}||s_r||c_2||t_i) \oplus L_i||0 \oplus 0||R_i = \\
&= (\mu\ (L_{i-1}||s_l||c_1||t_i) \oplus L_i||0) \oplus (\nu(R_{i-1}||s_r||c_2||t_i) \oplus 0||R_i)
\end{aligned}$$

Let us fix the values of M_i, s, and t_i. Then, we can introduce the functions $F(L_{i-1}) = \mu(L_{i-1}||s_l||c_1||t_i) \oplus L_i||0$, and $G(R_{i-1}) = \nu(R_{i-1}||s_r||c_2||t_i) \oplus 0||R_i$. Let H^* be the target hash value. Then we get the equation:

$$F(L) \oplus G(R) = H^*$$

If we generate 2^{256} different values for $F(L)$ and the same amount for $G(R)$, then, by the birthday paradox, with high probability we can expect the get at least one pair $(F(L_l), G(R_m)$ that will satisfy the above equation and therefore find a preimage with $h = L_l||R_m$.
A memoryless version of the attack can be obtained by introducing the function $\tilde{F}(L) = F(L) \oplus H^*$, and launching the memoryless meet-in-the-middle attack [2] on $\tilde{F}$ and G. This attack requires 2^{256} computations and negligible memory.

3 Preimage attack on the Full Sarmal-512

Since we can freely chose the message, the salt, and the block index, neither the padding nor the sequential increase of the block index can affect the attack. Therefore extending the free start preimage attack to a full preimage attack is trivial. We simply create a set S of 2^s different free start preimages for the target hash H^*. Then by taking different one block messages and applying the compression function to them, we try to obtain some chaining value from the set S. If we generate 2^{512-s} different chaining values then with high probability we can expect that one of these values will be in the set S. For generating the set S we need 2^{256+s} computations and 2^s memory. For example, if we take $s = 128$, we get an attack that requires 2^{384} computations and 2^{128} memory.
More advanced ways of extending a free start preimage attack to a full preimage attack are presented at [1].

References

1. C.D. Canière, C. Rechberger: Preimages for reduced SHA-0 and SHA-1, Advances in Cryptology - CRYPTO 2008, LNCS 5157, Springer-Heidelberg, 2008, p. 179-202.
2. H. Morita, K. Ohta, S. Miyaguchi: A switching closure test to analyze cryptosystems, Advances in Cryptology_ CRYPTO 1991, LNCS 576, Springer-Verlag, 1992, p. 183-193.
3. K.Varıcı, O. Özen, Ç. Kocair:Sarmal: SHA-3 Proposal. `http://www.metu.edu.tr/~e127761/Supporting_Documentation/SarmaL.pdf`