Cryptanalysis of DCH-n

Dmitry Khovratovich and Ivica Nikolić

University of Luxembourg

Abstract. We present collision and preimage attacks on DCH-n. The attacks exploit a design weakness of the underlying compression function. Both attacks require 2^{45} computations and memory.

Description of DCH

The hash family DCH is based on the Merkle-Damgard design. Let H_i be a 512 bit intermediate chaining values, M_i be a 512 bit message block and f be the compression function. Then the new chaining value H_{i+1} is produced as follows:

$$H_{i+1} = f(H_i, M_i)$$

The compression function f is defined as:

$$f(H_i, M_i) = H_i + M_i + g(M_i),$$

where $g(M)$ is some transformation irrelevant for our attack.

Cryptanalysis of DCH

The author in [1] claims that he follows Miyaguchi-Preneel principle for design of compression functions:

$$H_i = E_{g(H_{i-1})}(M_i) \oplus H_{i-1} \oplus M_i$$

Yet, In DCH, the underlying block cipher does not take as a key H_{i-1}. It rather omits the key input. The compression scheme can be presented as:

$$\begin{aligned} H_i &= g(M_i) \oplus M_i \oplus H_{i-1} = g(M_i) \oplus M_i \oplus g(M_{i-1}) \oplus M_{i-1} \oplus H_{i-2} = \ldots \\ &= g(M_i) \oplus M_i \oplus g(M_{i-1}) \oplus \ldots \oplus g(M_1) \oplus M_1 \oplus H_0 \end{aligned}$$

Let $\mu(M) = g(M) \oplus M$. Then the above equation can be rewritten as ($H_0 = 0$):

$$H_i = \mu(M_i) \oplus \mu(M_{i-1}) \oplus \ldots \oplus \mu(M_1)$$

Wagner's generalized birthday algorithm

Wagner in [2] explained how to find solution for the equation:

$$x_1 \oplus x_2 \oplus \ldots \oplus x_k = C,$$

where $x_i \in L_i$. He stated that when $|L_i| \geq 2^{\frac{n}{1+\lg k}}$, a solution can be found with $k \cdot 2^{\frac{n}{1+\lg k}}$ computations and memory.

Collisions and Preimage attack on DCH

Implementing the Wagner's algorithm for finding collisions and preimages is trivial. For collisions we need two pairs of input messages $M^1 = M_1^1||M_2^1||\ldots||M_k^1$ and $M^2 = M_1^2||M_2^2||\ldots||M_k^2$ such that:

$$\mu(M_1^1) \oplus \mu(M_2^1) \oplus \ldots \oplus \mu(M_k^1) = \mu(M_1^2) \oplus \mu(M_2^2) \oplus \ldots \oplus \mu(M_k^2)$$

This equation can be rewritten as:

$$\mu(M_1^1) \oplus \ldots \oplus \mu(M_k^1) \oplus \mu(M_1^2) \oplus \mu(M_k^2) = 0$$

Thus we have obtained a generalized birthday problem with $2k$ components.
Finding preimages is rather similar. Let H^* be the target hash values. Then we have:

$$\mu(M_1) \oplus \mu(M_2) \oplus \ldots \oplus \mu(M_k) = H^*$$

Again, we have obtained a generalized birthday problem with k components.

Complexity and Memory requirements for the Attacks

Both, the collision search and the preimage, attacks requires $k \cdot 2^{\frac{512}{1+\lg k}}$ computations and memory, where k is the number of the message blocks of the colliding pairs (preimage). Hence, by increasing this number, we can change the expenses. The optimal results are obtained when $k = 2^{23}$. Then, the memory and complexity requirements are $2^{23} \cdot 2^{512/24} \approx 2^{45}$.

References

1. David A. Wilson:The DCH Hash Function. `http://web.mit.edu/dwilson/www/hash/dch/Supporting_Documentation/dch.pdf`
2. David Wagner:A Generalized Birthday Problem. CRYPTO 2002,LNCS 2442, Springer-Verlag, 2002, p. 288-303.