A Collision Attack on a Double-Block-Length Hash Proposal ⋆

Norbert Pramstaller and Vincent Rijmen

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria
{Norbert.Pramstaller,Vincent.Rijmen}@iaik.tugraz.at

Abstract. At FSE 2006 Shoichi Hirose proposed a construction for double-block-length hash functions [2]. This construction only requires a block cipher where the key length is greater than the block length. In this article we present a collision attack on the proposal with DESX as underlying block cipher.
Keywords: hash functions, double-block-length hash functions, cryptanalysis, collision

1 The Double-Block-Length Proposal

Shoichi Hirose proposed a double-block-length hash function defined as following [2]:

$$g_i = e_k(h_{i-1}||m_i) \oplus g_{i-1} \tag{1}$$
$$h_i = e_k(h_{i-1}||m_i \oplus c) \oplus g_{i-1} \oplus c, \tag{2}$$

where c is an arbitrary constant ($c \neq 0$), and e_k any block cipher. The construction is shown in Figure 1.

In their paper they give two examples how AES-192 or AES-256 can be used as underlying block cipher e_k but they do not explicitly forbid to use another cipher. The only requirement for their scheme is that the key length has to be greater than the block length of the cipher.

2 The collision attack

Assume that DESX is used as underlying block cipher with the following settings (see also figure 2):

$$y = DES_k(x \oplus k_1) \oplus k_2, \tag{3}$$

where $k_1 = h_{i-1}$, k are the first 56 bits of the input message block and k_2 are the remaining 64 bits of the input message block, i.e. $m = k||k_2$ and $|m| = 120$, $|k| = 56$, and $|k_2| = 64$. For DESX we have $|g_i| = |h_i| = |c| = 64$.

⋆ The work in this paper has been supported by the Austrian Science Fund (FWF), project P18138.

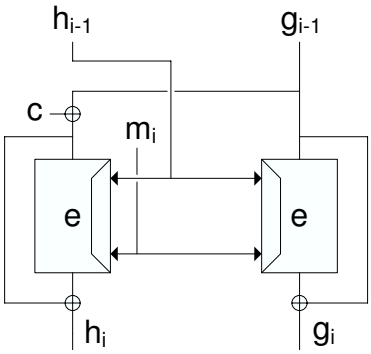

Fig. 1. The proposed scheme for any block cipher e_k

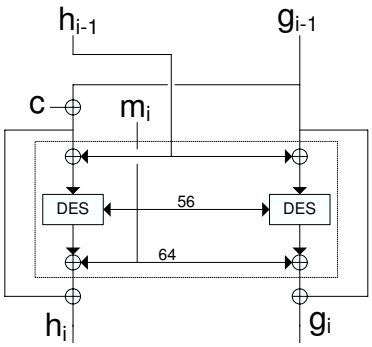

Fig. 2. The proposed scheme with DESX

For this setting we can easily construct a two-block collision for the DBL hash proposal. We stick to the convention of [1] to denote a difference by $h' = h \oplus h^*$.

For the first iteration the input message block has an arbitrary difference in the right-most 64 bits (k_2):

$$m_1 = u||v \tag{4}$$
$$m_1^* = u||v^* \tag{5}$$
$$m_1' = 0||v', \tag{6}$$

where u is an arbitrary 56-bit value and v' is an arbitrary difference. To construct the two-block collision we only have to choose the second message block with the same difference as for the first message block where the first 56 bits can be any value z:

$$m_2 = z||v \tag{7}$$
$$m_2^* = z||v^* \tag{8}$$
$$m_2' = 0||v' \ . \tag{9}$$

If we do so we have a collision after two iterations. After this iteration we can start with the same attack again. So the only restriction we have is that we need two message blocks that have the same difference in the right-most 64 bits. The DES keys in both iterations can be different.

The same attack can be applied if a block cipher following the Even-Mansour construction [3] is used as underlying block cipher.

3 Conclusion and Further Work

We have shown that for the proposal of Shoichi Hirose the underlying block cipher is important for the security against collision attacks. For DESX as underlying block cipher we can easily create collisions. This is work in progress.

References

1. Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4(1):3–72, 1991.
2. Shoichi Hirose. Some Plausible Constructions of Double-Block-Length Hash Functions. In Matt Robshow, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Pre-Proceedings*.
3. Shimon Even and Yishay Mansour. A Construction of a Cipher From a Single Pseudorandom Permutation. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan, November 11-14, 1991, Proceedings*, volume 739 of *LNCS*, pages 210–224. Springer, 1991.