A Practical Limit of Security Proof in the Ideal Cipher Model : Possibility of Using the Constant As a Trapdoor In Several Double Block Length Hash Functions

Donghoon Chang

Center for Information Security Technologies(CIST),
Korea University, Korea
dhchang@cist.korea.ac.kr

Abstract. Recently, Shoichi Hirose [2] proposed several double block length (DBL) hash functions. Each DBL hash function uses a constant which has a role to make the DBL hash function collision-resistant in the ideal cipher model. However, we have to instantiate a block cipher. In this paper, we show that the constant may be used as a trapdoor to help a attacker to find a collision easily. In case of 256-bit output size, we can find a collision with the complexity 2^{64}. This is a gap between the security of the DBL hash function in the ideal cipher model and the security of the DBL hash function based on any block cipher.

Keywords : Hash Function, Collision Attack, Block Cipher, Double Block Length Hash Function, Constant, Trapdoor.

1 Introduction.

John Black [1] exhibited a block cipher based hash function that is collision resistant in the ideal cipher model but trivially insecure when instantiated by any block cipher. His example is unrealistic but meaningful theoretically. In this paper, we show that several double block length hash functions based on any block cipher may have a trapdoor to help a attacker to find a collision easily. This is a practical limitation of the proof in the ideal cipher model.

2 DBL Compression Functions

In Fig. 1 $\sim$ 4, e is a block cipher with n-bit block and $2n$-bit key. g_{i-1}, h_{i-1} and m_i are n-bit. c is a non-zero n-bit constant. In Fig. 5 and 6, e is a block cipher with n-bit block and $\frac{3n}{2}$-bit key. $g_{i-1}(= g_{i-1}^{(1)}||g_{i-1}^{(2)})$, h_{i-1} are n-bit and m_i is $\frac{n}{2}$-bit. c is a non-zero n-bit constant. Shoichi Hirose [2] showed that the the compression functions in Fig. 1 $\sim$ 6 are optimal collision resistant in the ideal cipher model.

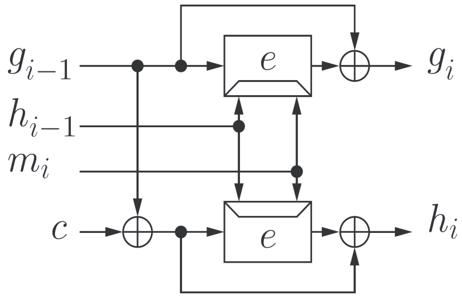

Fig. 1. Double Block Length Compression Function 1

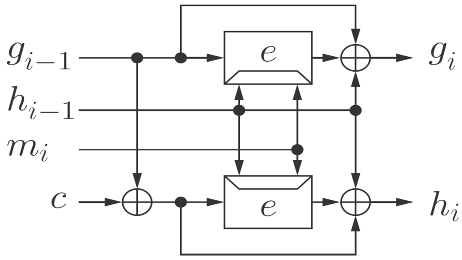

Fig. 2. Double Block Length Compression Function 2

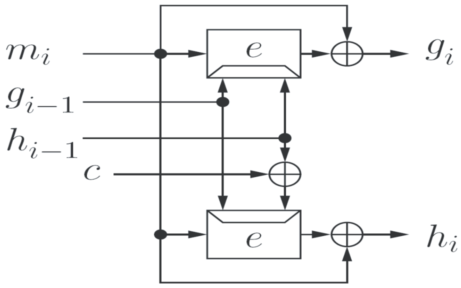

Fig. 3. Double Block Length Compression Function 3

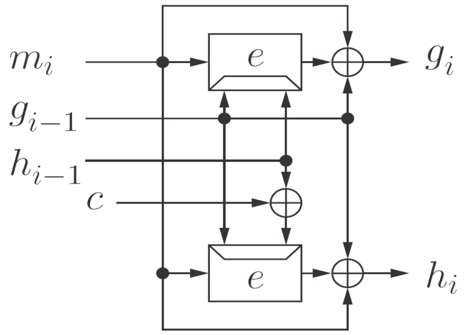

Fig. 4. Double Block Length Compression Function 4

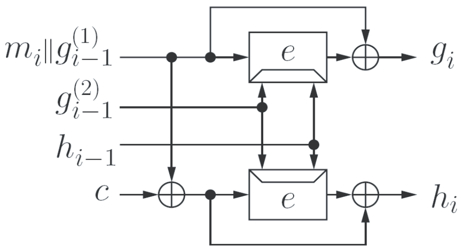

Fig. 5. Double Block Length Compression Function 5

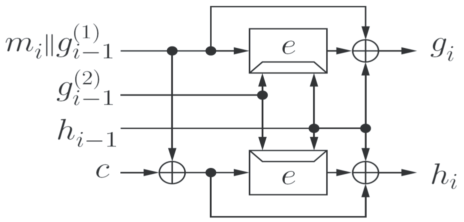

Fig. 6. Double Block Length Compression Function 6

3 Possibility of Using the Constant As a Trapdoor In Several Double Block Length Hash Functions

In the ideal cipher model, the constant in DBL hash functions can be any constant to give a security proof of them because the ideal cipher is an oracle chosen uniformly and randomly from the set of all block ciphers. On the other hand, in the practical point of view, we have to instantiate a known block cipher such as AES which is not an oracle. In the ideal cipher model, the constant enables us to prove the security of DBL hash functions. However, in the practice, the constant may be used as a trapdoor to help an attacker to find a collision easily.

Analysis of DBL Compression Functions in Fig. 1 and 2 With the birthday attack comprexity $2^{n/2}$, we can find x and x' ($x \neq x'$) with high probability such that $e_{a||b}(x) \oplus x = e_{a||b}(x') \oplus x'$ and a and b are fixed values. If $g_{i-1} = x$ and $g'_{i-1} = x'$ and $h_{i-1} = h'_{i-1} = a$ and $m_i = m'_i = b$ and $c = x \oplus x'$, then $g_i = g'_i$ and $h_i = h'_i$. This means that we can find a collision of DBL compression functions in Fig. 1 and 2. So, if $c = x \oplus x'$, c is a trapdoor. This means that c should be chosen randomly and publicly so that there is no trapdoor.

Analysis of DBL Compression Functions in Fig. 3 and 4 With the birthday attack comprexity $2^{n/2}$, we can find x and x' ($x \neq x'$) with high probability such that $e_{a||x}(b) \oplus b = e_{a||x'}(b) \oplus b$ and a and b are fixed values. If $h_{i-1} = x$ and $h'_{i-1} = x'$ and $g_{i-1} = g'_{i-1} = a$ and $m_i = m'_i = b$ and $c = x \oplus x'$, then $g_i = g'_i$ and $h_i = h'_i$. This means that we can find a collision of DBL compression functions in Fig. 3 and 4. So, if $c = x \oplus x'$, c is a trapdoor. This means that c should be chosen randomly and publicly so that there is no trapdoor.

Analysis of DBL Compression Functions in Fig. 5 and 6 With the birthday attack comprexity $2^{n/2}$, we can find x and x' ($x \neq x'$) with high probability such that $e_{a||b}(x||d) \oplus (x||d) = e_{a||b}(x'||d) \oplus (x'||d)$ and a ($n/2$ bits) and b (n bits) and d ($n/2$ bits) are fixed values. If $m_i = x$ and $m'_i = x'$ and $h_{i-1} = h'_{i-1} = b$ and $g_{i-1} = g'_{i-1} = (d||a)$ and $c = (x \oplus x')||0$, then $g_i = g'_i$ and $h_i = h'_i$. This means that we can find a collision of DBL compression functions in Fig. 5 and 6. So, if $c = (x \oplus x')||0$, c is a trapdoor. This means that c should be chosen randomly and publicly so that there is no trapdoor.

Analysis of DBL Hash Functions in Fig. 5 and 6 In case of DBL hash functions in Fig. 5 and 6, when the initial value $g_0||h_0$ is $d||a||b$ and $c = (x \oplus x')||0$, $(x||M,\ x'||M)$ is a collision for any M. So, if $c = (x \oplus x')||0$, c is a trapdoor. This means that c should be chosen randomly and publicly so that there is no trapdoor of the hash functions.

4 Conclusion

In this paper, we show that a constant c of DBL hash functions can be used as a trapdoor. This is meaningful practically and theoretically. Practically, we have to choose the constant carefully and publicly. Theoretically, this result shows a limitation of security proof in the ideal cipher model. We encourage cryptographers to design double block length hash functions which have no trapdoor.

References

1. J. Black, *The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function*, FSE'06, LNCS 4047, Springer-Verlag, pp. 328-340, 2006.
2. S. Hirose, *How to Construct Double-Block-Length Hash Functions*, In second Hash Workshop, 2006.