Open access • Book Chapter • DOI:10.1007/3-540-57220-1_91

An Attack on Two Hash Functions by Zheng-Matsumoto-Imai — Source link

Bart Preneel, René Govaerts, Joos Vandewalle

Institutions: Katholieke Universiteit Leuven

Published on: 13 Dec 1992 - Theory and Application of Cryptographic Techniques

Topics: MDC-2, Collision attack, Collision resistance, SHA-2 and Hash function

An Attack on Two Hash Functions by Zheng-Matsumoto-Imai

Bart Preneel*, René Govaerts, and Joos Vandewalle

Katholieke Universiteit Leuven, Laboratorium ESAT-COSIC,
Kardinaal Mercierlaan 94, B–3001 Heverlee, Belgium

Abstract. In [ZMI89,ZMI90] two constructions for a collision resistant hash function were proposed. The first scheme is based on a block cipher, and the second scheme uses modular arithmetic. It is shown in this paper that both proposals have serious weaknesses.

1 Introduction

For an informal definition of a collision resistant hash function the reader is referred to [PGV92]. The following model will be used to described iterated hash functions:

$$H_i = f(X_i, H_{i-1}) \quad i = 1, 2, \ldots t\,.$$

Here f is the round function, X_i are the t message blocks, H_i are the chaining variables, H_0 is equal to the initial value, that should be specified together with the scheme, and H_t is the hashcode. It was shown by I. Damgård [Dam89] that if the round function f is a collision resistant function, h is a collision resistant hash function. The authors of [ZMI89,ZMI90] claim that their constructions yield a collision resistant round function. It will be demonstrated that in both cases the round function is not collision resistant, and that in some cases collisions for h can be constructed.

2 The Hash Function Based on a Block Cipher

The round function f compresses a 224-bit input to a 128-bit output and is based on xDES^1. This block cipher is one of the extensions of DES [Fi46] that has been proposed in [ZMI89b]. xDES^1 is a three round Feistel cipher with block length 128 bits, key size 168 bits and with the F function equal to DES. One round is defined as follows:

$$C1_{i+1} = C2_i \quad \text{and} \quad C2_{i+1} = C1_i \oplus \text{DES}(K_i, C2_i) \quad i = 0, 1, 2.$$

The variables $C1_i$ and $C2_i$ are 64-bit blocks, and K_i are 56-bit keys. The block cipher is then written as

$$C2_3 \parallel C1_3 = \text{xDES}^1(K_1 \| K_2 \| K_3, C1_0 \| C2_0)\,.$$

* NFWO aspirant navorser, sponsored by the National Fund for Scientific Research (Belgium).

Appeared in *Advances in Cryptology – ASIACRYPT 1992*, Lecture Notes in Computer Science 718, J. Seberry, and Y. Zheng (eds.), Springer-Verlag, pp. 535–538.

Here $C1_0$ and $C2_0$ are the first and second part of the plaintext, and $C2_3$ and $C1_3$ are the first and second part of the ciphertext. The collision resistant function consists of 2 xDES^1 operations:

$$f(Y1\|Y2) = \text{xDES}^1\left(\text{chop}_{72}\left(\text{xDES}^1(\beta\|Y1,\alpha)\right)\|Y2,\alpha\right) .$$

Here $Y1$ and $Y2$ are 112-bit blocks, α is a 128-bit constant, β is a 56-bit initialization variable and chop_r drops the r least significant (or rightmost) bits of its argument. The complete hash function has the following form: $H_i = f(H_{i-1}\|X_i)$, where H_{i-1} is a 128-bit block, and X_i is a 96-bit block. The rate of this scheme is equal to 4, which means that 4 DES encryptions are required to hash 64 bits.

The scheme has two weaknesses, that allow to produce collisions for the round function f. First only 56 bits are kept from the first xDES^1 encryption, and hence a birthday attack will require only 2^{29} operations to produce a collision for the intermediate value and hence for the function f. The second problem is that if $\beta = K_1$ and $Y_1 = K_2\|K_3$, one can use the key collision search algorithm described in [QD89] to produce key collisions for the DES plaintext equal to the second part of α. This yields a collision for f in about 2^{33} operations.

The scheme can be strengthened however by distributing β equally over K_1, K_2, and K_3, and by increasing the size of β [Zhe92]. It will be shown that independently of the size of β, the security level can not be larger than 44 bits. If the size of β is equal to v bits (in the original proposal $v = 56$), the number of fixed bits of β that enter the key port of a single DES block is equal to $v/3$ (it will be assumed that v is divisible by 3). It can be shown that the rate of this scheme is then equal to $R = \frac{6\cdot 64}{208-2v}$. The number of bits of Y_1 that enter the key port will be denoted with y, hence $y + v/3 = 56$. Two attacks are now considered.

For the fixed value of the right part of α and of the first $v/3$ bits of β, one can calculate and store a set of 2^z different ciphertexts. The probability that a collision will be found in this set is approximately equal to 2^{2z-65}. If $y > 32$, implying $v < 72$, a value of $z = 33$ is clearly sufficient to obtain a collision. If on the other hand $y \leq 32$, one will take $z = y$, and the probability of success is smaller than one. One can however repeat this procedure, (e.g., if one attacks a DES block different from the first one, a different value can be chosen for the value of the bits of Y_1 that enter the first DES), and the expected number of operations for a single collision is equal to 2^{65-y}, while the required storage is equal to 2^y. An extension of the Quisquater algorithm [QD89] could be used to eliminate the storage. If the security level S is expressed in bits, it follows that $S = \max\{65 - y, 33\}$. With the relation between y and v, one obtains $S = \max\{9 + v/3, 33\}$.

A second attack follows from the observation that only v bits are kept from the output of the first xDES^1 operation (hence the chop operation is chopping $128 - v$ bits). It is clear that finding a collision for the remaining v bits requires only $2^{v/2+1}$ operations, or $S \leq v/2 + 1$ bits. This attack is more efficient than the first attack if $v < 64$ bits.

The relation between S and v can be summarized as follows: if $v < 64$ then $S = v/2 + 1$, if $64 \leq v < 72$ then S=33, and if $72 \leq v < 104$ then $S = v/3 + 9$.

Appeared in *Advances in Cryptology – ASIACRYPT 1992*, Lecture Notes in Computer Science 718, J. Seberry, and Y. Zheng (eds.), Springer-Verlag, pp. 535–538.

One can conclude that producing a collision for the proposed round function requires less than 2^{44} operations. Depending on the allocation of the bits of X_i and H_{i-1} to Y_1 and Y_2, it might also be feasible to produce a collision for the hash function with a fixed initial value: it is certainly possible to produce a collision for the hash function if there is a single DES block where all key bits are selected from X_i.

3 The Hash Function Based on Modular Arithmetic

In this case the round function f consists of 2 modular squarings with an n-bit modulus (with $n = 500$):

$$f(Y1\|Y2) = \left(chop'_{450}\left((\beta\|Y1)^2 \bmod N\right)\|Y2\right)^2 \bmod N\,,$$

where $\text{chop'}_r(x)$ drops the r most significant bits of x, $Y1$ and $Y2$ are 450-bit blocks, and β is a 50-bit initialization variable. The complete hash function has the following form: $H_i = f(H_{i-1}\|X_i)$, where H_{i-1} is a 500-bit block, and X_i is a 400-bit block. The security of this scheme is based on the fact that $O(\log N)$ bits of squaring modulo N is hard if N is a Blum integer, i.e., $N = pq$ with $p \equiv q \equiv 3 \bmod 4$. From this it is wrongly concluded that finding two integers such that their squares agree at the 50 least significant positions is hard (a trivial collision for x is $x' = -x$). As only 50 bits of the first squaring are used as input to the second squaring, it follows that collisions can be found with a birthday attack in 2^{26} operations. It can be shown that one can find a second preimage and hence a collision for f even if $k = n/4$ bits are selected, or $3n/4$ bits are chopped. The algorithm is the same as the one presented in [Gir87] to break a related scheme with redundancy in the least significant positions.

References

[Dam89] I.B. Damgård, "A design principle for hash functions," *Advances in Cryptology, Proc. Crypto'89, LNCS 435*, G. Brassard, Ed., Springer-Verlag, 1990, pp. 416–427.

[Fi46] *"Data Encryption Standard,"* Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[Gir87] M. Girault, "Hash-functions using modulo-n operations," *Advances in Cryptology, Proc. Eurocrypt'87, LNCS 304*, D. Chaum and W.L. Price, Eds., Springer-Verlag, 1988, pp. 217–226.

[PGV92] B. Preneel, R. Govaerts, and J. Vandewalle, "On the power of memory in the design of collision resistant hash functions," these proceedings.

[QD89] J.-J. Quisquater and J.-P. Delescaille, "How easy is collision search ? Application to DES," *Advances in Cryptology, Proc. Eurocrypt'89, LNCS 434*, J.-J. Quisquater and J. Vandewalle, Eds., Springer-Verlag, 1990, pp. 429–434.

[ZMI89] Y. Zheng, T. Matsumoto, and H. Imai, "Duality between two cryptographic primitives," *Papers of technical group for information security, IEICE of Japan*, March 16, 1989, pp. 47–57.

Appeared in *Advances in Cryptology – ASIACRYPT 1992*, Lecture Notes in Computer Science 718, J. Seberry, and Y. Zheng (eds.), Springer-Verlag, pp. 535–538.

[ZMI89b] Y. Zheng, T. Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypothesis," *Advances in Cryptology, Proc. Crypto'89, LNCS 435*, G. Brassard, Ed., Springer-Verlag, 1990, pp. 461–480.

[ZMI90] Y. Zheng, T. Matsumoto, and H. Imai, "Duality between two cryptographic primitives," *Proc. 8th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, LNCS 508*, S. Sakata, Ed., Springer-Verlag, 1991, pp. 379–390.

[Zhe92] Y. Zheng, personal communication, 1992.

Appeared in *Advances in Cryptology – ASIACRYPT 1992*, Lecture Notes in Computer Science 718, J. Seberry, and Y. Zheng (eds.), Springer-Verlag, pp. 535–538.