

# Security of Generalized TANDEM-DM

## – Abstract –

Ewan Fleischmann, Michael Gorski, Stefan Lucks  
{ewan.fleischmann,michael.gorski,stefan.lucks}@uni-weimar.de

Bauhaus-University Weimar, Germany

**Abstract.** At FSE'09 the first proof of security for TANDEM-DM was provided, one of the oldest and most well-known constructions for turning a block cipher with  $n$ -bit block length and  $2n$ -bit key length into a  $2n$ -bit cryptographic hash function. They proved, that when TANDEM-DM is instantiated with AES-256, *i.e.* a block cipher with block length 128 bits and key length 256 bits, any adversary that asks less than  $2^{120.4}$  queries cannot find a collision with success probability greater than  $1/2$ . Also, a weak preimage bound was stated. We generalize this result for applications of block ciphers with  $n + b$  bit keys with  $b > 1$ . This allows the use of, *e.g.*, AES-192 to be included in the security proof. We also tighten the FSE'09 result. We show that for any  $b > 1$ , no adversary asking less than  $2^{121.3}$  queries cannot find a collision with success probability greater than  $1/2$  (here assuming  $n = 128$ ). Interestingly, this result, mapped to the use of the block cipher SHACAL-1, gives the 'most efficient' *double block length hash function* currently known since it achieves a rate of 1.1 and resulting into a 320-bit hash function.

**Keywords:** Cryptographic hash function, block cipher based, proof of security, double-block length, ideal cipher model, Generalized Tandem-DM.

## 1 Introduction

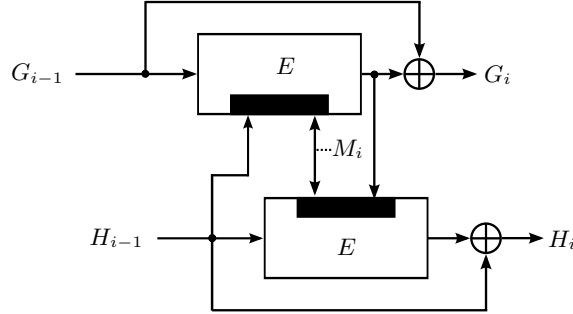
A cryptographic hash function is a function which maps an input of arbitrary length to an output of fixed length. It should satisfy at least collision-, preimage- and second-preimage resistance and is one of the most important primitives in cryptography [9].

*Block Cipher-Based Hash Functions.* Since their initial design by Rivest, MD4-family hash functions (*e.g.* MD4, MD5, RIPEMD, SHA-1, SHA2 [10–13]) have dominated cryptographic practice. But in recent years, a sequence of attacks on these type of functions [4, 6, 15, 16] has led to a generalized sense of concern about the MD4-approach. The most natural place to look for an alternative is in block cipher-based constructions, which in fact predate the MD4-approach [8]. Another reason for the resurgence of interest in block cipher-based hash functions is due to the rise of size restricted devices such as RFID tags or smart cards: A hardware designer has to implement only a block cipher in order to obtain an encryption function as well as a hash function. But since the output length of most practical encryption functions is far too short for a collision resistant hash function, *e.g.* 128-bit for AES, one is mainly interested in sound design principles for *double block length* (DBL) hash functions [1]. A DBL hash-function uses a block cipher with  $n$ -bit output as the building block by which it maps possibly long strings to  $2n$ -bit ones.

*Our Contribution.* Four 'classical' DBL hash functions are known: MDC-2, MDC-4, ABREAST-DM and TANDEM-DM [2, 3, 7]. At EUROCRYPT'07, Steinberger [14] proved the first security bound for the hash function MDC-2: assuming a hash output length of 256 bits, any adversary asking less than  $2^{74.9}$  queries cannot find a collision with probability greater than  $1/2$ . At FSE'09, Fleischmann et. al. [5] provided such a collision resistance bound for TANDEM-DM. They proved, that when TANDEM-DM is instantiated with AES-256, block length 128 bits and key length 256 bits, any adversary that asks less than  $2^{120.4}$  queries cannot find a collision with success probability greater than  $1/2$ . We generalize this result for applications of block ciphers with  $n + b$  bit keys with  $b > 1$ . We also tighten the FSE'09 result. We show that for any  $b > 1$ , no adversary asking less than  $2^{121.28}$  queries cannot find a collision with success probability greater than  $1/2$  (assuming  $n = 128$ ).

## 2 The G-Tandem-DM Compression Function

The TANDEM-DM compression function was proposed by Lai and Massey at EUROCRYPT'92 [7]. It uses two cascaded Davies-Meyer [1] schemes. We generalize TANDEM-DM for the use of  $(n, n + b)$  block ciphers, i.e. block ciphers with  $n$ -bit block length and  $n + b$  bit key length. This compression function, G-TANDEM-DM, is illustrated in Figure 1 and is formally given in Definition 1.



**Figure 1.** The compression function G-TANDEM-DM  $F^{GTDM}$  where  $E$  is an  $(n, n + b)$  block cipher, the small black rectangle inside the cipher rectangle indicates which input is used as key

**Definition 1.** Let  $F^{GTDM} : \{0, 1\}^{2n} \times \{0, 1\}^b \rightarrow \{0, 1\}^{2n}$  be a compression function such that  $(G_i, H_i) = F^{GTDM}(G_{i-1}, H_{i-1}, M_i)$  where  $G_i, H_i, G_{i-1}, H_{i-1} \in \{0, 1\}^n$  and  $M_i \in \{0, 1\}^b$ .  $F^{GTDM}$  is built upon an  $(n, n + b)$  block cipher  $E$  as follows:

$$\begin{aligned} W_i &= E(G_{i-1}, H_{i-1} | M_i) \\ G_i &= F_T(G_{i-1}, H_{i-1}, M_i) = W_i \oplus G_{i-1} \\ H_i &= F_B(G_{i-1}, H_{i-1}, M_i) = E(H_{i-1}, M_i | W_i) \oplus H_{i-1}. \end{aligned}$$

## 3 Collision Resistance – Security Results for G-Tandem-DM

Our discussion will result in a proof for the following upper bound:

**Theorem 1.** Let  $F := F^{TDM}$  be as in Definition 1 and  $n, q$  be natural numbers with  $q < 2^n$ . Let  $N' = 2^n - q$  and let  $\alpha$  be any positive number with  $eq/N' \leq \alpha$  and  $\tau = \alpha N'/q$  (and  $e^x$  being the exponential function). Then

$$\mathbf{Adv}_F^{\text{COLL}}(q) \leq q2^n e^{q\tau(1-\ln \tau)/N'} + 2q\alpha/N' + 3q\alpha/(N')^2 + q\alpha/(N')^3 + 6q/(N')^2.$$

The bound obtained by this theorem depends on a parameter  $\alpha$ . We do not require any specific value  $\alpha$  as any  $\alpha$  (meeting to the conditions mentioned in Theorem 1) leaves us with a correct bound. For Theorem 1 to give a *good* bound one must choose a suitable value for the parameter  $\alpha$ . Choosing large values of  $\alpha$  reduces the value of the first term but increases the value of the second term. There seems to be no good closed form for  $\alpha$  as these will change with every  $q$ . The meaning of  $\alpha$  will be explained in the proof. We will optimize the parameter  $\alpha$  numerically as given in the following corollary.

**Corollary 1.** For the compression function TANDEM-DM, instantiated e.g. with AES-256 or AES-192<sup>1</sup>, any adversary asking less than  $2^{121.28}$  (backward or forward) oracle queries cannot find a collision with probability greater than  $1/2$ . In this case,  $\alpha = 25.99$ .

<sup>1</sup> Formally, we model these block ciphers as ideal block ciphers.

## References

1. John Black, Phillip Rogaway, and Thomas Shrimpton. Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 320–335. Springer, 2002.
2. C. Meyer and S. Matyas. Secure program load with manipulation detection code, 1988.
3. D. Coppersmith, S. Pilpel, C. H. Meyer, S. M. Matyas, M. M. Hyden, J. Oseas, B. Bracht1, and M. Schilling. Data authentication using modification detection codes based on a public one way encryption function. U.S. Patent No. 4,908,861, March 13, 1990.
4. Bert den Boer and Antoon Bosselaers. Collisions for the Compression Function of MD5. In *EUROCRYPT*, pages 293–304, 1993.
5. Ewan Fleischmann, Michael Gorski, and Stefan Lucks. On the Security of Tandem-DM. In Matthew J. B. Robshaw, editor, *FSE*, volume 5??? of *Lecture Notes in Computer Science*, page ?? Springer, 2009.
6. H. Dobbertin. The status of MD5 after a recent attack, 1996.
7. Xuejia Lai and James L. Massey. Hash Function Based on Block Ciphers. In *EUROCRYPT*, pages 55–70, 1992.
8. M. Rabin. Digitalized Signatures. In R. DeMillo, D. Dobkin, A. Jones and R.Lipton, editors, *Foundations of Secure Computation*, Academic Press, pages 155–168, 1978.
9. Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
10. NIST National Institute of Standards and Technology. FIPS 180-1: Secure Hash Standard. April 1995. See <http://csrc.nist.gov>.
11. NIST National Institute of Standards and Technology. FIPS 180-2: Secure Hash Standard. April 1995. See <http://csrc.nist.gov>.
12. R. L. Rivest. *RFC 1321: The MD5 Message-Digest Algorithm*. Internet Activities Board, April 1992.
13. Ronald L. Rivest. The MD4 Message Digest Algorithm. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 303–311. Springer, 1990.
14. John P. Steinberger. The Collision Intractability of MDC-2 in the Ideal-Cipher Model. In Moni Naor, editor, *EUROCRYPT*, volume 4515 of *Lecture Notes in Computer Science*, pages 34–51. Springer, 2007.
15. Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu. Cryptanalysis of the Hash Functions MD4 and RIPEMD. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2005.
16. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding Collisions in the Full SHA-1. In Victor Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer, 2005.