

# The Security of Abreast-DM in the Ideal Cipher Model

Jooyoung Lee, Daesung Kwon

The Attached Institute of Electronics and Telecommunications Research Institute  
Yuseong-gu, Daejeon, Korea 305-390  
jlee05@ensec.re.kr, ds\_kwon@ensec.re.kr

**Abstract.** In this paper, we give a security proof for ABREAST-DM in terms of collision resistance and preimage resistance. As old as TANDEM-DM, the compression function ABREAST-DM is one of the most well-known constructions for double block length compression functions. The bounds on the number of queries for collision resistance and preimage resistance are given by  $O(2^n)$ . Based on a novel technique using *query-response cycles*, our security proof is simpler than those for MDC-2 and TANDEM-DM. We also present a wide class of ABREAST-DM variants that enjoy a birthday-type security guarantee with a simple proof.

## 1 Introduction

A cryptographic hash function takes a message of arbitrary length, and returns a bit string of fixed length. The most common way of hashing variable length messages is to iterate a fixed-size compression function according to the Merkle-Damgård paradigm. The underlying compression function can either be constructed from scratch, or be built upon off-the-shelf cryptographic primitives such as blockciphers. Recently, the blockcipher-based construction is attracting renewed interest, as many dedicated hash functions, including those most common in practical applications, exhibit serious security weaknesses [1, 6, 14, 15, 20, 24–26]. Conveniently choosing an extensively studied blockcipher in the blockcipher-based construction, one can easily transfer the trust in the existing algorithm to the hash function. This approach is particularly useful in highly constrained environments such as RFID systems, since a single implementation of a blockcipher can be used for both a blockcipher and a hash function. Compared to blockciphers, the most dedicated hash functions require significant amounts of state and the operations in their designs are not hardware friendly [3].

Compression functions based on blockciphers have been widely studied [2, 4, 8–11, 13, 16–19, 21–23]. The most common approach is to construct a  $2n$ -to- $n$  bit compression function using a single call to an  $n$ -bit blockcipher. However, such a function, called a *single block length* (SBL) compression function, might be vulnerable to collision attacks due to its short output length. For example, one could successfully mount a birthday attack on a compression function based on AES-128 using approximately  $2^{64}$  queries. This observation motivated substantial research on *double block length* (DBL) compression functions, where the output length is twice the block length of the underlying blockciphers.

Unfortunately, it turned out that a wide class of DBL compression functions of rate 1 are not optimally secure in terms of collision resistance and preimage resistance [8, 9, 12]. The most classical DBL compression functions of rate less than 1 include MDC-2, MDC-4, TANDEM-DM and ABREAST-DM [5, 13]. In 2007, 20 years after its original proposal, Steinberger first proved the collision resistance of MDC-2 in the ideal cipher model [23]. The author showed that an adversary asking less than  $2^{3n/5}$  queries has only a negligible chance of finding a collision. Motivated by this work, Fleischmann et. al. proved the security of TANDEM-DM [7]. Similar to MDC-2, the security of TANDEM-DM is estimated in terms of a parameter, say,  $\alpha$ . Optimizing the parameter, they proved the collision resistance of TANDEM-DM up to the birthday bound. Currently, TANDEM-DM and the Hirose’s scheme [11] are the only rate 1/2 DBL compression functions that are known to have a birthday-type security guarantee.

**Results** We give a security proof for ABREAST-DM in terms of collision resistance and preimage resistance. As old as TANDEM-DM, the compression function ABREAST-DM is known to be more advantageous than TANDEM-DM in that two encryptions involved can be computed in parallel. The bounds on the number of queries for collision resistance and preimage resistance are given by  $O(2^n)$ . Our security proof using certain cyclic structures, called *query-response cycles*, is much simpler than those for MDC-2 and TANDEM-DM. The query-response cycle technique also allows us to present a wide class of ABREAST-DM variants that enjoy a birthday-type security guarantee with a simple proof. It is shown that this class includes the Hirose’s scheme [11] as a special case. We note, however, this technique does not apply directly to MDC-2 and TANDEM-DM, since two encryptions in these compression functions are computed in serial and hence it is infeasible to define query-response cycles. The underlying blockcipher of ABREAST-DM use  $2n$ -bit keys, while MDC-2 accepts  $n$ -bit keys. For this reason, it seems to be natural that the security proof of MDC-2 is more challenging.

## 2 Preliminaries

**General Notations** For a positive integer  $n$ , we let  $I_n = \{0, 1\}^n$  denote the set of all bitstrings of length  $n$ . For two bitstrings  $A$  and  $B$ ,  $A|B$  and  $\bar{A}$  denote the concatenation of  $A$  and  $B$ , and the bitwise complement of  $A$ , respectively. For a set  $U$ , we write  $u \stackrel{\$}{\leftarrow} U$  to denote uniform random sampling from the set  $U$  and assignment to  $u$ .

**Ideal Cipher Model** For positive integers  $n$  and  $k$ , let

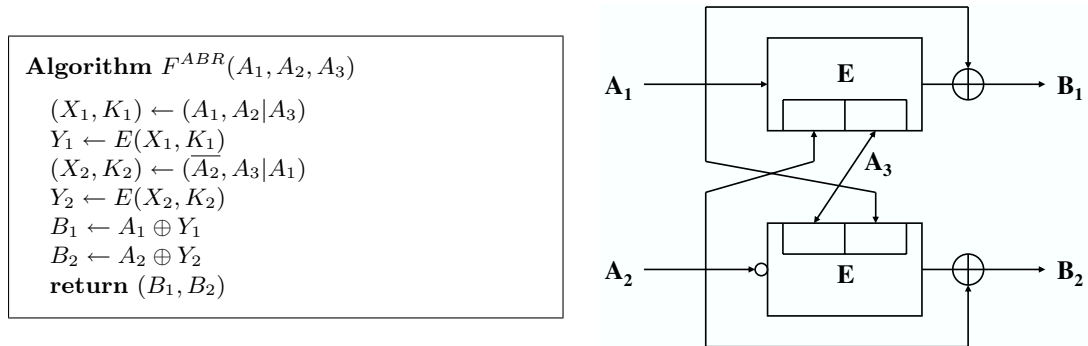
$$BC(n, k) = \{E : I_n \times I_k \rightarrow I_n : \forall K \in I_k, E(\cdot, K) \text{ is a permutation on } I_n\}.$$

In the ideal cipher model, an  $(n, k)$ -blockcipher  $E$  is chosen from  $BC(n, k)$  uniformly at random. It allows for two types of oracle queries  $E(X, K)$  and  $E^{-1}(Y, K)$  for  $X, Y \in I_n$  and  $K \in I_k$ . Here,  $X, Y$  and  $K$  are called a plaintext, a ciphertext and a key, respectively. The response to an inverse query  $E^{-1}(Y, K)$  is  $X \in I_n$  such that  $E(X, K) = Y$ .

**The Abreast-DM Compression Function** In the ideal cipher model, the ABREAST-DM compression function

$$F^{ABR} : I_n^3 \longrightarrow I_n^2$$

has oracle access to an ideal cipher  $E \in BC(n, 2n)$ , and computes  $F^{ABR}(A_1, A_2, A_3)$ ,  $(A_1, A_2, A_3) \in I_n^3$ , by the algorithm described in Figure 1.



**Fig. 1.** The ABREAST-DM compression function

**Collision Resistance and Preimage Resistance** Let  $F := F^{ABR}$  be the ABREAST-DM compression function based on an ideal blockcipher  $E \in BC(n, 2n)$ , and let  $\mathcal{A}$  be an information-theoretic adversary with oracle access to  $E$  and  $E^{-1}$ . Then we execute the experiment  $\mathbf{Exp}_{\mathcal{A}}^{\text{coll}}$  described in Figure 2(a), in order to quantify the collision resistance of  $F$ . The experiment records the queries that the adversary  $\mathcal{A}$  makes into a *query history*  $\mathcal{Q}$ . A pair  $(X, K, Y)$  is in the query history if  $\mathcal{A}$  asks for  $E(X, K)$  and gets back  $Y$ , or it asks for  $E^{-1}(Y, K)$  and gets back  $X$ . For  $A = (A_1, A_2, A_3) \in I_n^3$  and  $B = (B_1, B_2) \in I_n^2$ , we write

$$A \vdash_{\mathcal{Q}} B,$$

if there exist query-response pairs  $(X_1, K_1, Y_1), (X_2, K_2, Y_2) \in \mathcal{Q}$ , satisfying the following equations.

$$(X_1, K_1) = (A_1, A_2 | A_3), \quad (1)$$

$$(X_2, K_2) = (\overline{A_2}, A_3 | A_1), \quad (2)$$

$$B_1 = A_1 \oplus Y_1, \quad (3)$$

$$B_2 = A_2 \oplus Y_2. \quad (4)$$

Informally,  $A \vdash_{\mathcal{Q}} B$  means that the query history  $\mathcal{Q}$  determines the evaluation  $F : A \mapsto B$ . Now the *collision-finding advantage* of  $\mathcal{A}$  is defined to be

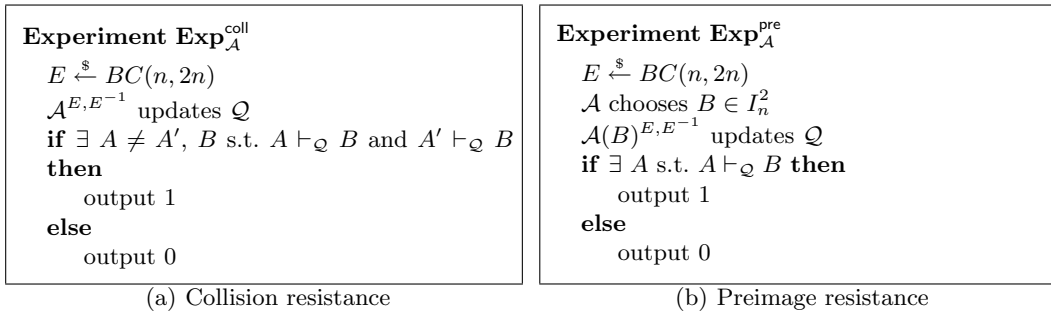
$$\mathbf{Adv}_F^{\text{coll}}(\mathcal{A}) = \Pr [\mathbf{Exp}_{\mathcal{A}}^{\text{coll}} = 1]. \quad (5)$$

The probability is taken over the random blockcipher  $E$  and  $\mathcal{A}$ 's coins (if any). For  $q > 0$ , we define  $\mathbf{Adv}_F^{\text{coll}}(q)$  as the maximum of  $\mathbf{Adv}_F^{\text{coll}}(\mathcal{A})$  over all adversaries  $\mathcal{A}$  making at most  $q$  queries.

The preimage resistance of  $F$  is quantified similarly using the experiment  $\mathbf{Exp}_{\mathcal{A}}^{\text{pre}}$  described in Figure 2(b). The adversary  $\mathcal{A}$  chooses a single target image  $B \in I_n^2$  before it begins making queries to  $E^{\pm 1}$ . The *preimage-finding advantage* of  $\mathcal{A}$  is defined to be

$$\mathbf{Adv}_F^{\text{pre}}(\mathcal{A}) = \Pr [\mathbf{Exp}_{\mathcal{A}}^{\text{pre}} = 1]. \quad (6)$$

For  $q > 0$ ,  $\mathbf{Adv}_F^{\text{pre}}(q)$  is the maximum of  $\mathbf{Adv}_F^{\text{pre}}(\mathcal{A})$  over all adversaries  $\mathcal{A}$  making at most  $q$  queries. The security definitions given in this section can be extended easily to any compression function built upon ideal primitives by appropriately defining the relation “ $\vdash_{\mathcal{Q}}$ ”.



**Fig. 2.** Experiments for quantification of collision resistance and preimage resistance

### 3 Security of Abreast-DM

#### 3.1 Query-response Cycle and Modified Adversary

Let  $F := F^{ABR}$  be the ABREAST-DM compression function based on a blockcipher  $E \in BC(n, 2n)$ , and let  $\mathcal{Q}$  be the query history obtained by oracle access to  $E$  and  $E^{-1}$ . Now we associate the

query history  $\mathcal{Q}$  with a direct graph  $\mathcal{G}$  on  $\mathcal{Q}$ , where  $\overrightarrow{QQ'} \in \mathcal{G}$  if and only if  $Q = (A_1, A_2|A_3, Y_1)$  and  $Q' = (\overline{A_2}, A_3|A_1, Y_2)$  for some  $A_s$ 's and  $Y_t$ 's. A (direct) cycle in  $\mathcal{G}$  is called a *query-response cycle*. The following properties can be easily proved.

*Property 1.* If query-response pairs  $Q$  and  $Q'$  are obtained by the first blockcipher call and the second blockcipher call, respectively, in an evaluation of  $F$ , then  $\overrightarrow{QQ'} \in \mathcal{G}$ . Conversely, each edge in  $\mathcal{G}$  represents a valid evaluation of  $F$ .

*Property 2.* Each query-response cycle in  $\mathcal{G}$  is of length 2 or length 6. If  $\Delta = (Q_1, \dots, Q_6) \in \mathcal{G}$  is a cycle of length 6, then we have

$$\begin{aligned} Q_1 &= (A_1, A_2|A_3, Y_1), & Q_2 &= (\overline{A_2}, A_3|A_1, Y_2), & Q_3 &= (\overline{A_3}, A_1|\overline{A_2}, Y_3), \\ Q_4 &= (\overline{A_1}, \overline{A_2}|\overline{A_3}, Y_4), & Q_5 &= (A_2, \overline{A_3}|\overline{A_1}, Y_5), & Q_6 &= (A_3, \overline{A_1}|A_2, Y_6), \end{aligned}$$

for some  $A_s$ 's and  $Y_t$ 's. If  $\Delta = (Q_1, Q_2) \in \mathcal{G}$  is a cycle of length 2, then we have  $Q_1 = (A_1, A_1|\overline{A_1}, Y_1)$  and  $Q_2 = (\overline{A_1}, \overline{A_1}|A_1, Y_2)$  for some  $A_1, Y_1$  and  $Y_2$ . Here we see that the first three blocks of the query-response pairs are moving cyclically under the permutation

$$\begin{aligned} \pi : I_n^3 &\longrightarrow I_n^3 \\ (A_1, A_2, A_3) &\longmapsto (\overline{A_2}, A_3, A_1). \end{aligned}$$

*Property 3.* For query-response cycles  $\Delta$  and  $\Delta'$ , either  $\Delta = \Delta'$  or  $\Delta \cap \Delta' = \emptyset$ .

Given an adversary  $\mathcal{A}$  with oracle access to  $E$  and  $E^{-1}$ , one can transform  $\mathcal{A}$  into an adversary  $\mathcal{B}$  that records its query history in terms of query-response cycles. The modified adversary  $\mathcal{B}$  is described in Figure 3. We can easily check the following properties of  $\mathcal{B}$ .

*Property 4.* If  $\mathcal{A}$  makes at most  $q$  queries, then the corresponding adversary  $\mathcal{B}$  makes at most  $6q$  queries, and records at most  $q$  query-response cycles.

*Property 5.*  $\mathbf{Adv}_F^{\text{sec}}(\mathcal{A}) \leq \mathbf{Adv}_F^{\text{sec}}(\mathcal{B})$  for  $\text{sec} \in \{\text{coll}, \text{pre}\}$ .

## 3.2 Security Results

Given Property 5, we will analyze the security of the ABREAST-DM compression function with respect to the modified adversary  $\mathcal{B}$ . We denote the query history of  $\mathcal{B}$  by

$$\mathcal{Q}_\Delta = \{\Delta^i : 1 \leq i \leq q\},$$

where we write  $\Delta^i = (Q_1^i, Q_2^i, Q_3^i, Q_4^i, Q_5^i, Q_6^i)$  or  $(Q_1^i, Q_2^i)$  for  $1 \leq i \leq q$ . Here we assume that query-response pair  $Q_j^i$  is obtained after  $Q_{j'}^i$ , if  $j > j'$ .

**Collision Resistance** Let  $\mathcal{E}$  denote the event that  $\mathcal{B}$  makes a collision of  $F$ . Then, by definition,  $\mathbf{Adv}_F^{\text{coll}}(\mathcal{B}) = \Pr[\mathcal{E}]$ . In order to estimate  $\Pr[\mathcal{E}]$ , we decompose  $\mathcal{E}$  as follows.

$$\mathcal{E} = \bigcup_{i=1}^q \left( \mathcal{E}^i \cup \bigcup_{j=1}^{i-1} \mathcal{E}^{i,j} \right), \quad (7)$$

where

$$\mathcal{E}^i \Leftrightarrow \text{two evaluations from a single cycle } \Delta^i \text{ determines a collision,} \quad (8)$$

$$\mathcal{E}^{i,j} \Leftrightarrow \text{two evaluations from } \Delta^i \text{ and } \Delta^j \text{ determine a collision.} \quad (9)$$

Then it follows that

$$\Pr[\mathcal{E}] = \sum_{i=1}^q \left( \Pr[\mathcal{E}^i] + \sum_{j=1}^{i-1} \Pr[\mathcal{E}^{i,j}] \right). \quad (10)$$

**Algorithm  $\mathcal{B}^{E, E^{-1}}$**

```

 $\mathcal{Q}_\Delta \leftarrow \emptyset$ 
Run  $\mathcal{A}$ 
if  $\mathcal{A}$  makes a fresh query for  $E(A_1, A_2|A_3)$  then
  Make queries for
   $Y_1 = E(A_1, A_2|A_3), \quad Y_2 = E(\overline{A_2}, A_3|A_1), \quad Y_3 = E(\overline{A_3}, A_1|\overline{A_2}),$ 
   $Y_4 = E(\overline{A_1}, \overline{A_2}|\overline{A_3}), \quad Y_5 = E(A_2, \overline{A_3}|\overline{A_1}), \quad Y_6 = E(A_3, \overline{A_1}|A_2),$ 

   $\mathcal{Q}_\Delta \leftarrow \mathcal{Q}_\Delta \cup \{\Delta\}$  ( $\Delta$ =the cycle defined by the above six queries)
  Return  $Y_1$  to  $\mathcal{A}$ 
else if  $\mathcal{A}$  makes a fresh query for  $E^{-1}(Y_1, A_2|A_3)$  then
  Make queries for
   $A_1 = E^{-1}(Y_1, A_2|A_3), \quad Y_2 = E(\overline{A_2}, A_3|A_1), \quad Y_3 = E(\overline{A_3}, A_1|\overline{A_2}),$ 
   $Y_4 = E(\overline{A_1}, \overline{A_2}|\overline{A_3}), \quad Y_5 = E(A_2, \overline{A_3}|\overline{A_1}), \quad Y_6 = E(A_3, \overline{A_1}|A_2),$ 

   $\mathcal{Q}_\Delta \leftarrow \mathcal{Q}_\Delta \cup \{\Delta\}$ 
  Return  $A_1$  to  $\mathcal{A}$ 
else
  Return the response using query history  $\mathcal{Q}_\Delta$ 

```

**Fig. 3.** Modified algorithm  $\mathcal{B}$ . A query is called “fresh” if its response is not obtained from the query history of  $\mathcal{B}$

**Lemma 1.** Let  $N' = 2^n - 6q \geq 15$  and  $1 \leq i < j \leq q$ . Then,

1.  $\Pr[\mathcal{E}^i] \leq 1/N'$ ,
2.  $\Pr[\mathcal{E}^{i,j}] \leq 36/(N')^2$ .

*Proof.* Inequality 1: First, assume that  $\Delta^i$  consists of two distinct query-response pairs. A collision within this cycle implies that  $Q_1^i = (A_1, A_1|\overline{A_1}, Y_1)$ ,  $Q_2^i = (\overline{A_1}, \overline{A_1}|A_1, Y_2)$  and  $(A_1 \oplus Y_1, \overline{A_1} \oplus Y_2) = (\overline{A_1} \oplus Y_2, A_1 \oplus Y_1)$  for some  $A_1, Y_1$  and  $Y_2$ . Since the second query-response pair  $Q_2^i$  is obtained by a forward query, and  $Y_2$  should be equal to  $\overline{Y_1}$ , the probability that this type of collision occurs is not greater than  $1/N'$ .

Next, assume that  $\Delta^i$  consists of six distinct query-response pairs. Suppose that, say,  $\overrightarrow{Q_1^i Q_2^i}$  and  $\overrightarrow{Q_2^i Q_3^i}$  determines a collision. With the notations in Property 2, it should be the case that  $(A_1 \oplus Y_1, \overline{A_2} \oplus Y_2) = (\overline{A_2} \oplus Y_2, \overline{A_3} \oplus Y_3)$ . In this case, we have  $Y_2 = A_1 \oplus Y_1 \oplus \overline{A_2}$  and  $Y_3 = \overline{A_2} \oplus Y_2 \oplus \overline{A_3}$ . The probability that  $Y_2$  and  $Y_3$  satisfy these equations is not greater than  $(1/N')^2$ . The same argument applies to every pair of edges in  $\Delta^i$ . Since the number of such pairs is  $\binom{6}{2} = 15$  and  $15/(N')^2 \leq 1/N'$  for  $N' \geq 15$ , the first inequality is proved.

Inequality 2: Let  $\overrightarrow{Q_h^i Q_{h+1}^i}$  and  $\overrightarrow{Q_{h'}^j Q_{h'+1}^j}$  be edges contained in  $\Delta^i$  and  $\Delta^j$ , respectively. Then we can write

$$\begin{aligned} Q_h^i &= (A_1, A_2|A_3, Y_1), & Q_{h+1}^i &= (\overline{A_2}, A_3|A_1, Y_2), \\ Q_{h'}^j &= (A'_1, A'_2|A'_3, Y'_1), & Q_{h'+1}^j &= (\overline{A'_2}, A'_3|A'_1, Y'_2), \end{aligned}$$

for some  $A_s$ 's,  $A'_s$ 's,  $Y_t$ 's and  $Y'_t$ 's. If two edges  $\overrightarrow{Q_h^i Q_{h+1}^i}$  and  $\overrightarrow{Q_{h'}^j Q_{h'+1}^j}$  determine a collision, then it should be the case that  $(A_1 \oplus Y_1, \overline{A_2} \oplus Y_2) = (A'_1 \oplus Y'_1, \overline{A'_2} \oplus Y'_2)$ , or equivalently  $Y'_1 = A_1 \oplus Y_1 \oplus A'_1$  and  $Y'_2 = \overline{A_2} \oplus Y_2 \oplus \overline{A'_2}$ . The probability that such an event occurs is not greater than  $(1/N')^2$ . Since each cycle contains at most 6 edges, we obtain  $\Pr[\mathcal{E}^{i,j}] \leq 36/(N')^2$ .  $\square$

By Lemma 1, equality (10) and Property 5, we obtain the following theorem.

**Theorem 1.** *Let  $F^{ABR}$  be the compression function ABREAST-DM and let  $q > 0$ . Then,*

$$\mathbf{Adv}_{F^{ABR}}^{\text{coll}}(q) \leq \frac{q}{(2^n - 6q)} + \frac{18q^2}{(2^n - 6q)^2}.$$

**Preimage Resistance** Suppose that a modified adversary  $\mathcal{B}$  is given a target image  $B = (B_1, B_2)$ . Let  $\mathcal{E}$  denote the event that  $\mathcal{B}$  makes an evaluation  $F(A_1, A_2, A_3) = (B_1, B_2)$  for some  $A_s$ 's. Then, by definition,  $\mathbf{Adv}_F^{\text{pre}}(\mathcal{B}) = \Pr[\mathcal{E}]$ . Define

$$\mathcal{E}^i \Leftrightarrow \Delta^i \text{ determines a preimage of } B. \quad (11)$$

Then it follows that

$$\Pr[\mathcal{E}] = \sum_{i=1}^q \Pr[\mathcal{E}^i]. \quad (12)$$

Let  $\overrightarrow{Q_h^i Q_{h+1}^i}$  be an edge contained in  $\Delta^i$ . Then we can write  $Q_h^i = (A_1, A_2 | A_3, Y_1)$  and  $Q_{h+1}^i = (\overline{A_2}, A_3 | A_1, Y_2)$  for some  $A_s$ 's and  $Y_t$ 's. If  $\overrightarrow{Q_h^i Q_{h+1}^i}$  determines a preimage of  $B = (B_1, B_2)$ , then it should be the case that  $(A_1 \oplus Y_1, \overline{A_2} \oplus Y_2) = (B_1, B_2)$ , or equivalently  $Y_1 = B_1 \oplus A_1$  and  $Y_2 = B_2 \oplus \overline{A_2}$ . The probability that such an event occurs is not greater than  $(1/N')^2$ . Since each cycle contains at most 6 edges, we obtain  $\Pr[\mathcal{E}^i] \leq 6/(N')^2$  for  $1 \leq i \leq q$ , and the following theorem.

**Theorem 2.** *Let  $F^{ABR}$  be the compression function ABREAST-DM and let  $q > 0$ . Then,*

$$\mathbf{Adv}_{F^{ABR}}^{\text{pre}}(q) \leq \frac{6q}{(2^n - 6q)^2}.$$

## 4 Abreast-DM Variants

In this section, we present a wide class of ABREAST-DM variants that enjoy a birthday-type security guarantee. Let  $\pi$  be a permutation on  $I_n^3 (\equiv I_n \times I_n^2)$  such that every cycle in  $\pi$  is of length  $2 \leq l \leq L$  for a positive integer  $L$ . Then we can associate the permutation  $\pi$  with an ABREAST-DM variant  $F_\pi^{ABR}$  as follows.

$$F_\pi^{ABR} : I_n^3 \longrightarrow I_n^2 \\ (A_1, A_2, A_3) \longmapsto (E(X_1, K_1) \oplus X_1, E(X_2, K_2) \oplus X_2), \quad (13)$$

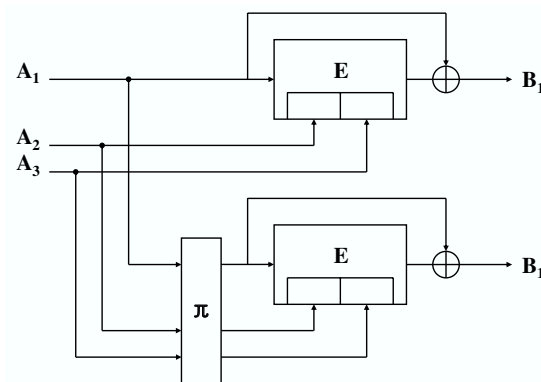
where  $(X_1, K_1) = (A_1, A_2 | A_3)$  and  $(X_2, K_2) = \pi(A_1, A_2, A_3)$ . An ABREAST-DM variant is illustrated in Figure 4. By essentially the same argument as the previous section, we can prove the following theorem.

**Theorem 3.** *Let  $F_\pi^{ABR}$  be the compression function defined in (13), and let  $2^n \geq q + \binom{L}{2}$ . Then,*

$$\mathbf{Adv}_{F_\pi^{ABR}}^{\text{coll}}(q) \leq \frac{q}{(2^n - Lq)} + \frac{L^2 q^2}{2(2^n - Lq)^2}, \\ \mathbf{Adv}_{F_\pi^{ABR}}^{\text{pre}}(q) \leq \frac{Lq}{(2^n - Lq)^2}.$$

If  $\pi$  contains no cycle of length 2, then

$$\mathbf{Adv}_{F_\pi^{ABR}}^{\text{coll}}(q) \leq \frac{L^2(q + q^2)}{2(2^n - Lq)^2}.$$



**Fig. 4.** ABREAST-DM variant

We conclude this section with some examples.

*Example 1.* Let  $\pi : (A_1, A_2, A_3) \mapsto (A_1 \oplus C, A_2, A_3)$  for a constant  $C \in I_n$ . Then  $F_\pi^{ABR}$  is reduced to the Hirose's scheme [11].

*Example 2.* Let  $\pi : (A_1, A_2, A_3) \mapsto (\overline{A_1}, A_3, \overline{A_2})$ . Then every cycle in  $\pi$  is of length 4. By Theorem 3, we have

$$\mathbf{Adv}_{F_\pi^{ABR}}^{\text{coll}}(q) \leq \frac{8(q + q^2)}{(2^n - 4q)^2}.$$

In numerical terms with  $n = 128$ , any adversary asking less than  $2^{125.0}$  queries cannot find a collision with probability greater than  $1/2$ .

## 5 Conclusion

In this paper, we analyzed collision resistance and preimage resistance of ABREAST-DM with a novel technique using query-response cycles. As a result, we have shown that ABREAST-DM is both collision resistant and preimage resistant up to  $O(2^n)$  query complexity. With essentially the same proof as ABREAST-DM, we also presented a wide class of ABREAST-DM variants that enjoy a birthday-type security guarantee. We note that, however, our result for preimage resistance might not be optimal, since a truly random function with a  $2n$ -bit output would require  $O(2^{2n})$  queries to find any preimage. For this reason, it will be an interesting further research to improve the security proof for preimage resistance.

## References

1. E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet and W. Jalby. Collisions of SHA-0 and reduced SHA-1. Eurocrypt 2005, LNCS 3494, pp. 36–57, Springer-Verlag, 2005.
2. J. Black, M. Cochran and T. Shrimpton. On the impossibility of highly-efficient blockcipher-based hash functions. Eurocrypt 2005, LNCS 3494, pp. 526–541, Springer-Verlag, 2005.
3. A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw and Y. Seurin. Hash functions and RFID tags: mind the gap. CHES 2008, LNCS 5154, pp. 283–299, Springer-Verlag, 2008.
4. J. Black, P. Rogaway and T. Shrimpton. Black-box analysis of the block-cipher-based hash-function construction from PGV. Crypto 2002, LNCS 2442, pp. 320–325, Springer-Verlag, 2002.
5. B. Brachtel, D. Coppersmith, M. Heyden, S. Matyas, C. Meyer, J. Oseas, S. Pilpel and M. Schilling. Data authentication using modification detection codes based on a public one-way encryption function. US Patent #4,908,861. Awarded March 13, 1990 (filed August 28, 1987).

6. De. Canniere and C. Rechberger. Preimages for reduced SHA-0 and SHA-1. *Crypto 2008*, LNCS 5157, pp. 179–202, Springer-Verlag, 2008.
7. E. Fleischmann, M. Gorski and S. Lucks. On the security of TANDEM-DM. *Preproceedings of FSE 2009*, pp. 85–105, 2009.
8. M. Hattori, S. Hirose and S. Yoshida. Analysis of double block length hash functions. *IMA 2003*, LNCS 2898, pp. 290–302, Springer-Verlag, 2003.
9. S. Hirose. A security analysis of double-block-length hash functions with the rate 1. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E89-A, NO. 10, pp. 2575–2582, 2006.
10. S. Hirose. Provably secure double-block-length hash functions in a black-box model. *ICISC 2004*, LNCS 3506, pp. 330–342, Springer-Verlag, 2005.
11. S. Hirose. Some plausible construction of double-block-length hash functions. *FSE 2006*, LNCS 4047, pp. 210–225, Springer-Verlag, 2006.
12. L. R. Knudsen, J. L. Massey and B. Preneel. Attacks on fast double block length hash functions. *Journal of Cryptology*, Vol. 11, NO. 1, pp. 59–72, 1998.
13. X. Lai and J. L. Massey. Hash function based on block ciphers. *Eurocrypt 1992*, LNCS 658, pp. 55–70, Springer-Verlag, 1993.
14. G. Leurent. MD4 is not one-way. *FSE 2008*, LNCS 5086, pp. 412–428, Springer-Verlag, 2008.
15. F. Mendel, N. Pramstaller, C. Rechberger and V. Rijmen. Analysis of step-reduced SHA-256. *FSE 2006*, LNCS 4047, pp. 126–143, Springer-Verlag, 2006.
16. B. Preneel, R. Govaerts and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. *Crypto 1993*, LNCS 773, pp. 368–378, Springer-Verlag, 1994.
17. T. Ristenpart and T. Shrimpton. How to build a hash function from any collision-resistant function. *Asiacrypt 2007*, LNCS 4833, pp. 147–163, Springer-Verlag, 2007.
18. P. Rogaway and J. Steinberger. Constructing cryptographic hash functions from fixed-key blockciphers. *Crypto 2008*, LNCS 5157, pp. 433–450, Springer-Verlag, 2008.
19. P. Rogaway and J. Steinberger. Security/efficiency tradeoffs for permutation-based hashing. *Eurocrypt 2008*, LNCS 4965, pp. 220–236, Springer-Verlag, 2008.
20. Y. Sasaki and K. Aoki. Finding preimages in full MD5 faster than exhaustive search. *Eurocrypt 2009*, LNCS 5479, pp. 134–152, Springer-Verlag, 2008.
21. T. Shrimpton and M. Stam. Building a collision-resistant function from non-compressing primitives. *ICALP 2008*, LNCS 5126, pp. 643–654, Springer-Verlag, 2008.
22. M. Stam. Beyond uniformity: Better security/efficiency tradeoffs for compression functions. *Crypto 2008*, LNCS 5157, pp. 397–412, Springer-Verlag, 2008.
23. J. Steinberger. The collision intractability of MDC-2 in the ideal-cipher model. *Eurocrypt 2007*, LNCS 4515, pp. 34–51, Springer-Verlag, 2008.
24. X. Wang, X. Lai, D. Feng, H. Chen and X. Yu. Cryptanalysis of the hash functions MD4 and RIPEMD. *Eurocrypt 2005*, LNCS 3494, pp. 1–18, Springer-Verlag, 2005.
25. X. Wang, X. Lai and H. Yu. Finding collisions in the full SHA-1. *Crypt0 2005*, LNCS 3621, pp. 17–36, Springer-Verlag, 2005.
26. X. Wang and H. Yu. How to break MD5 and other hash functions. *Eurocrypt 2005*, LNCS 3494, pp. 19–35, Springer-Verlag, 2005.