Quantum rebound attack to D-M structure based on ARIA algorithm

Shanque Dou1,2, Ming Mao1, Yanjun Li1,2, Dongying Qiu1*
1Beijing Electronic Science and Technology Institute, Beijing, 100070, China,
2Guangxi Key Laboratory of cryptography and information security, Guilin University of Electronic Science and technology, Guilin 541004
*Corresponding author’s e-mail: dsqdky@163.com

Abstract. With the increasing application of quantum computing, quantum technology is increasingly used in the security analysis and research of multiple symmetric cryptographic algorithms such as block ciphers and hash functions. In 2020, Sasaki et al. proposed a dedicated quantum collision attack against hash functions in EUROCRYPT. Some differential trajectories with a probability of $2^{-2n/3}$ that cannot be used in the classical environment may be used to launch collision attacks in the quantum environment. The ARIA algorithm is a block cipher proposed by the Korean researcher Kwon et al. on ICISC 2003. The block cipher algorithm is similar to AES in structure. This article mainly analyzes the security of Davies-Meyer structure, and uses AIRA as the permutation function to construct ARIA hash function based on the DM hash model. A new AIRA differential path was found based on MILP, and 7 rounds of ARIA-DM hash function quantum rebound attacks were given.

1. Introduction

With the advent of the post-quantum era, the cryptography community pays much attention to quantum security. The security of public-key cryptographic schemes is often reduced to some mathematical problems. For example, the periodic function can be successfully solved by the quantum algorithm Shor. Symmetric cryptographic algorithms have also been threatened by quantum computing in recent years. In 2010, Kuwakad and Mori [1] pointed out that the use of the Simon algorithm under the quantum computing model enables three rounds of Feistel to be distinguished only by polynomial queries. After that, the researchers also applied Grover's algorithm [2] to symmetric ciphers, using its square root-level search capability under traditional time complexity to reduce complexity.

The ARIA algorithm is a block cipher proposed by South Korean researcher Daesung Kwon et al [3,4] in 2003. The algorithm uses the SPN structure (replacement-replacement network structure). In 2004, it was identified as South Korea by the Ministry of Energy, the Ministry of Commerce and the Ministry of Industry. Standard block cipher algorithm. So far, the algorithm has been revised and proposed three versions, the latest version 1.0 has been confirmed as the standard by the Korean Government Standards Organization (KATS).

With the widespread application of modern technology, hash functions are applied to the key technologies of various scenarios, occupying a pivotal position. As the MD5 and SHA algorithms have been cracked one after another, it has become more and more important to evaluate the security of the hash function. At present, the analysis methods of hash function mainly include: birthday attack [4], differential attack [5], pre-image attack [6], meet-in-the-middle attack [7], etc. In the quantum environment,
the complexity of finding collisions in general quantum algorithms like BHT algorithm\cite{8} is $O(2^{n/3})$. Using quantum algorithms to find a pair of messages satisfying the differential trajectory with probability $p$ can be generated with a complexity of $p^{1/2}$. This makes the differential trajectory with a probability of $2^{-2n/3}$ that cannot be used in the classical environment may be used to launch collision attacks in the quantum environment. But there is not much attention to the specific hash function. Until 2020, Sasaki et al\cite{9}, first proposed a dedicated quantum collision attack against the hash functions of AES-MMO and WHIRLPOOL in EUROCRYPT, using a quantum version of the rebound attack. Later, Dong et al\cite{10}, applied the quantum version of the non-full super s-box technology to the quantum rebound attack of AES-MMO and Grøstl, which significantly reduced qRAM, and the performance of this attack was better than the general collision attack given by Chailloux et al. Because the structure of the ARIA algorithm is very similar to the structure of AES, scholars have conducted a lot of security analysis on the algorithm\cite{11}, but there is no security analysis on the hash function based on the ARIA algorithm. This paper constructs a hash function of D-M structure based on ARIA algorithm, and further analyzes its security under the quantum computing model.

The structure of this paper is as follows: The second part is preliminary knowledge, which will briefly introduce the structure of ARIA algorithm. Part 3 presents Grover algorithm and BHT algorithm in quantum computing. Part 4 mainly introduces the Davies-Meyer model. The fifth part is a quantum rebound attack on the DM-ARIA hash function. Part 6 is the conclusion part.

2. ARIA block cipher

ARIA is a block cipher with a block length of 128 bits, which is similar to the advanced encryption standard AES structure design. It uses a substitution-permutation network (SPN). Its key length is 128 bits, 192 bits and 256 bits, and the corresponding round numbers are respectively 12 rounds, 14 rounds and 16 rounds. The round function is composed of three basic parts: round key addition (RKA), confusion layer (SL) and diffusion layer (DL).

Add Round Key: First, we initialize, we use the master key $K$ to generate the initial key $KL || KR = K || 0...0$ according to the key expansion algorithm, and then bring the initial key into the formula to generate $W_0, W_1, W_2, W_3$ The relevant formula is:

$$W_0 = KL$$
$$W_1 = F_0(W_0, CK_1) \oplus KR$$
$$W_2 = F_1(W_1, CK_2) \oplus W_0$$
$$W_3 = F_2(W_2, CK_3) \oplus W_1$$

Then bring the generated $W_0, W_1, W_2, W_3$ into the formula in Table 1 to generate the required round key.

| $RK_1$ | $RK_2$ |
|--------|--------|
| $W_0 \oplus (W_1 \ggg 19)$ | $W_1 \oplus (W_2 \ggg 19)$ |
| $W_2 \oplus (W_3 \ggg 19)$ | $W_3$ |
| $W_0 \oplus (W_1 \ggg 31)$ | $W_1 \oplus (W_2 \ggg 31)$ |
| $W_2 \oplus (W_3 \ggg 31)$ | $W_3$ |
| $W_0 \oplus (W_1 \lll 61)$ | $W_1 \oplus (W_2 \lll 61)$ |
| $W_2 \oplus (W_3 \lll 61)$ | $W_3$ |
| $W_0 \oplus (W_1 \lll 31)$ | $W_1 \oplus (W_2 \lll 31)$ |
| $W_2 \oplus (W_3 \lll 31)$ | $W_3$ |
| $W_0 \oplus (W_1 \ggg 19)$ | $W_1 \oplus (W_2 \ggg 19)$ |

Table 1. Round key generation

Substitution Layer: Substitution Layer is composed of 4 different $8 \times 8$ S boxes. These are $S_1$ and $S_2$ and their inverses $S_1^{-1}$ and $S_2^{-1}$. This transformation is a byte-oriented transformation, and its generation method is similar to the S-box of AES. It uses polynomials to define operations on the finite field $GF(2^8)$. The polynomial expression method is to regard a byte $b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$ as a polynomial with degree less than 8 in the binary field $GF(2)$, namely:

$$b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$$
The internal state of ARIA is to divide 128 bits into 16 bytes, and write them into a $4 \times 4$ matrix as shown in Table 2. For the parity of the number of rounds, there are different confusion layers, respectively:

$SL_1 = S_1 S_2 S_3 S_4 S_5 S_6 S_7 S_8 S_9 S_{10} S_{11} S_{12} S_{13} S_{14} S_{15}$

$SL_2 = S_1^{-1} S_2^{-1} S_3^{-1} S_4^{-1} S_5^{-1} S_6^{-1} S_7^{-1} S_8^{-1} S_9^{-1} S_{10}^{-1} S_{11}^{-1} S_{12}^{-1} S_{13}^{-1} S_{14}^{-1} S_{15}^{-1}$

The two kinds of confusion are used interchangeably, the odd-numbered wheel uses $SL_1$ confusion layer, and the even-number theory uses $SL_2$. Table 3 shows the specific arrangement of the two confusion layers of $SL_4$ and $SL_2$

| 0 | 4 | 8 | 12 |
|---|---|---|----|
| 1 | 5 | 9 | 13 |
| 2 | 6 | 10 | 14 |
| 3 | 7 | 11 | 15 |

Table 3. Odd number wheel $SL_4$ (a), even number theory $SL_2$ (b)

| $S_1$ | $S_2$ | $S_3$ | $S_4$ | $S_5$ | $S_6$ | $S_7$ | $S_8$ | $S_9$ | $S_{10}$ | $S_{11}$ | $S_{12}$ | $S_{13}$ | $S_{14}$ | $S_{15}$ |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $S_1^{-1}$ | $S_2^{-1}$ | $S_3^{-1}$ | $S_4^{-1}$ | $S_5^{-1}$ | $S_6^{-1}$ | $S_7^{-1}$ | $S_8^{-1}$ | $S_9^{-1}$ | $S_{10}^{-1}$ | $S_{11}^{-1}$ | $S_{12}^{-1}$ | $S_{13}^{-1}$ | $S_{14}^{-1}$ | $S_{15}^{-1}$ |

Diffusion Layer: ARIA uses a byte-oriented linear transformation on the binary domain, which is a 16-bit to 16-bit mapping, which is: $GF(2^8)^{16} \rightarrow GF(2^8)^{16}$, $(x_0,x_1,\ldots,x_{15}) \rightarrow (y_0,y_1,\ldots,y_{15})$

Table 4: Linear transformation table of diffusion layer

\[
\begin{align*}
  y_0 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \\
  y_1 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\
  y_2 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \\
  y_3 &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\
  y_4 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \\
  y_5 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\
  y_6 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \\
  y_7 &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\
  y_8 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \\
  y_9 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\
  y_{10} &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \\
  y_{11} &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\
  y_{12} &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \\
  y_{13} &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\
  y_{14} &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \\
  y_{15} &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5
\end{align*}
\]

3. Quantum computing

3.1. Grover algorithm:

The Grover algorithm [13] was proposed by Grover in 1996. For an unordered data set with N data, if it passes the classic algorithm, it needs $O(N)$ times. However, if the Grover algorithm is used, it only needs to search $O(N^{1/2})$ times. It can be seen through such collections. The Grover quantum algorithm speeds up the search speed of the classic algorithm and poses a threat to password security.

Grover problem: Suppose the Boolean function $F: \{0,1\}^n \rightarrow \{0,1\}$, suppose $F$ is pointed out as a black box. Then find an x such that $F(x) = 1$. 

\[\]
The Grover algorithm starts with the initial state of n qubits $|0\rangle^n$, and then uses the Hadamard transform to superpose $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, and then continue to use Grover algorithm iteratively for quantum search. Through the iterative Grover algorithm $R = \left\lceil \frac{\sqrt{N/M}}{4} \right\rceil$ times, a solution probability of the problem can be searched for $O(1)$.

3.2. BHT algorithm:
The first general quantum collision algorithm is the BHT algorithm developed by Brassard, Høyer, and Tapp\cite{8}. The author proposes that when quantum random access memory (qRAM) is available, it will pass $O(2^{n/3})$ quantum query. The collision is found at time $O(2^{n/3})$. Quantum random storage allows us to access data through quantum superposition.

Suppose our goal is to find the collision of the random function $f: \{0,1\}^n \rightarrow \{0,1\}^n$. The BHT algorithm is composed of two parts. The first step is to perform pre-calculation, select a set $X \subset \{0,1\}^n$ and $|X| = 2^{n/3}$, calculate the corresponding $f(x)$ for all $x \in X$, this need to query and time in $O(2^{n/3})$. Store these $2^{n/3}$ pairs of data $L = \{(x, f(x))\}$ in qRAM so that it can be accessed under quantum superposition. The second step uses Grover algorithm search to find $x' \in \{0,1\}^n \setminus X$ such that $f(x') = f(x)$. The average running time is $O\left(\sqrt{2^n/|L|}\right) = O(2^{n/3})$. If we find such $x'$, this will find a collision of $f$ for us $f(x') = f(x)$.

4. Davies-Meyer structure permutation hash function
The designers of Simpira proposed several applications of Simpira replacement, such as block ciphers using Even-Mansour structure\cite{13}, wide pipe encryption algorithms and so on. One of the special applications is to use a feedforward single-block, keyless hash function of the Davies-Meyer structure to calculate the hash function $H(x)$ of $x$, as shown in Figure 1. We can express it like this: $H(x) = \text{trunc}(\pi(x) \oplus x)$

![Figure 1. Davies-Meyer structure](image)

Among them, we replace the $\pi$ function with ARIA permutation. This method provides an effective construction method for hash input of limited length, which is required by many applications.

Through the research on the Davies-Meyer (DM) model, we found that the n-digit block cipher $E_k(m)$ is constructed as a compression function: $h^E: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$, $h^E(iv, m) = E_{iv}(m) \oplus m$. The compression function can be constructed by using difference construction methods to construct the hash function (for example, Merkle-Damgard). DM-ARIA is a new ARIA hash function constructed based on ARIA as the compression function. The goal of the attacker’s collision attack on the hash function is to find the message $m, m' \in \{0,1\}^n$ such that $h^E(iv, m) = h^E(iv, m')$ (Where $E$ is ARIA), any given $iv \in \{0,1\}^n$. If we can launch such a collision attack on $h^E$, we can extend it to the entire hash function, which is not safe.

5. Quantum rebound attack of DM-ARIA hash
Construct a hash function based on ARIA algorithm. $m$ is the plaintext input, the key input $k$ is fixed to the initial value $iv$, and the output is calculated as $E_K(p) \oplus p$. $E_K$ is ARIA. Suppose there is a differential trajectory of $E_{iv}$ with probability $p$, and the input and output differences share a common value $\Delta$. Given about $1/p$ pairs of input messages with a difference $\Delta$, we expect a pair of $(m, m \oplus \Delta)$ to follow this difference trajectory: $E_{iv}(m) \oplus E_{iv}(m \oplus \Delta) = \Delta$. If the ciphertext XOR matches the plaintext XOR, the output value of the MMO mode is 0 after the feedback operation, that is $(m \oplus E_{iv}(m)) \oplus \Delta$.
\( (m \oplus E_i (m \oplus \Delta)) = \Delta \oplus \Delta = 0 \). In other words, if the effective byte positions at the beginning and the end and the actual difference are the same, collisions will occur when offsetting through the feedforward operation.

Here we use the MILP algorithm to search for a differential path with a 7-round ARIA probability of \(2^{-120}\). Through the research of the differential path, the differential path satisfies the same conditions as the input and output difference required for our above-mentioned collisions, and can be used for 7 rounds of ARIA-MMO collision attacks. The differential trace is shown in Figure 2. Each 4\times4 square shows the active bytes of each round. The 7-byte cancellation probability of the feedforward operation is \(2^{-56}\).

Regarding the 7-round ARIA differential path of the ARIA algorithm, we propose how to use this path in a quantum environment to perform a rebound attack on the 7-round DM-ARIA.

![Figure 2. 7 rounds of ARIA differential path](image)

In order to realize the rebound attack on a quantum computer, we use Grover search for the Boolean function \(F(\Delta in, \Delta out)\) defined as \(F(\Delta in, \Delta out) = 1\), if and only if the following two conditions are met:

- For each of the \(2^{56}\) possible differences of X3.
- For each of the \(2^{56}\) possible differences of Y3. Since \(\Delta Z3 = \Delta X4\), we can get a satisfying route Y3-Z3-X4-Y4-Z4.
- From the values at state Z4, we can get the values at X3 and X5. Then check the following equations: \(\Delta [SL(X3)] = \Delta Y3, \Delta [SL(X5)] = \Delta Y5\)
- As shown in the Figure 1, we know: \(P=X1=X3, X5=X7=X8\), in this differential path, the probability of collision between the input difference and the output difference is \(2^\times(-112)\times2^\times(-56)=2^\times(-168)\).

If we find the solutions of the above two equations, it means that we have found a pair of values that satisfy the difference from round 3 to round 5. For any triples \((\Delta Y3, \Delta Z4, \Delta Y5)\), the probability that the above two equations are true is \(2^{-112}\).

Degrees of freedom: the number of triples \((\Delta Y3, \Delta Z4, \Delta Y5)\) is \(2^{56}\times3 = 2^{168}\). Therefore, we have enough degrees of freedom to get a collision.
Next, we will carry out a quantum collision attack on it. First, we made several assumptions about quantum collision attacks.

- The computational complexity of 7 rounds of ARIA is approximately 160 S-boxes (encryption function 16*7=112 S-boxes, key arrangement 16*3=48 S-boxes).
- The complexity of one access to the qRAM of the storage table is equivalent to one S-box calculation.
- The realization of an inverse S-box is an S-box.

This quantum attack consists of two stages, called the inbound and outbound stages. The inbound phase is similar to an effective meet-in-the-middle phase, which uses truncated difference to satisfy the low probability part of the difference. In the outbound phase, the matching of the inbound phase is calculated backward and forward, and a collision attack on the hash function is obtained.

The core of quantum collision attack is to apply Grover algorithm to search space, in which relevant elements are marked by an efficient and computable Boolean function f. We define a function f, and represent the instantiated inbound input-output difference pair as(Δin, Δout). The goal of the inbound phase of the rebound attack is to generate data pairs about the inbound difference.

Define $F_{56}^2 \times F_2^5 \rightarrow F_2$, if and only if the starting point is (Δin, Δout), the function F satisfies the forward and backward outbound difference. Therefore, the application of Grover’s search algorithm is mapped to the quantum Oracle UF: |Δin, Δout⟩ is mapped to |y ⊕ F (Δin, Δout)⟩, we can pass about $\frac{\pi}{4} \sqrt{2^{56}}$ times of the query found a collision. Next, in order to estimate the overall complexity, we need to clarify the complexity brought by UF.

Now we need some additional functions to implement UF. We define a function G(i), which marks the solution of a given difference (Δin, Δout). Apply the Grover search algorithm to the G(i) of the given(Δin, Δout), and find the value of 7 ≈ 56 bits, you need to execute $\frac{\pi}{4} \times \sqrt{2^{56}} \approx 2^{27.65}$ for oracle UG(i) queries. Among them, UG(i) needs to evaluate 16 S boxes. Therefore, the complexity of 7 rounds of DM-ARIA is $2^{27.65} \times 16 \times \frac{1}{160} \approx 2^{24.45}$.

UF complexity: We need to calculate 2 rounds forward and 2 rounds backward to meet the outbound difference in the inbound phase (Δin, Δout). Therefore, the UF complexity of 7 rounds of DM-ARIA is $\frac{16\times4\times7}{160} + 7 \times 2^{24.45} \approx 2^{27.45}$.

Find the complexity of the collision: In order to identify a 112-bit value (Δin, Δout) ∈ $F_2^5 \times F_2^5$, searching for $F(\Delta in, \Delta out) = 1$ through Grover, we need to perform $\frac{\pi}{4} \sqrt{2^{112}}$ on UF Inquire. Therefore, the time complexity of 7 rounds of DM-ARIA to find collisions is $\frac{\pi}{4} \sqrt{2^{112}} \times 2^{27.45} = 2^{83.1}$.

6. Summarize

This paper mainly studies the security of the hash model DM based on the ARIA algorithm. Through the study of DM, it is found that if the plaintext XOR value in the hash function matches the ciphertext XOR value, the feedforward operation of the DM structure will lead to the output result. If the hash function satisfies the above conditions, such a hash function is not safe. Therefore, in order to prevent attackers from using this property to attack the hash function, we instantiate the DM structure of the hash model and perform security analysis on it, and use the ARIA algorithm as the replacement function to construct the ARIA hash. The round DM-ARIA hash function launched a quantum collision attack, and it was discovered that the security of the ARIA hash function of the 7-round differential route would be reduced.

Through the security research of ARIA hash function, we can know that when we use ARIA as the hash function of the round function, the security of the round number is greater than 7 is greatly improved. Therefore, research on various block cipher algorithms as the hash function of the permutation function provides the minimum number of safe rounds for the hash function. It is greater than the minimum number of safe rounds, such a hash function is safe.
References
[1] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings, pages 2682–2685, 2010.
[2] Grover L K . A fast quantum mechanical algorithm for database search[J]. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, 212-219. [DOI: 10.1145/237814.237866]
[3] Kwon D , Kim J , Park S , et al. New block cipher: ARIA[C]// Icisc. DBLP, 2003: 1-15. [DOI: 10.1007/978-3-540-24691-6_32]
[4] Mihir Bellare, Tadayoshi Kohno. Hash Function Balance and it Impact on Birthday Attacks. In: EUROCRYPT04, LNCS3027, Springer Verlag, 2004:410–418.
[5] Chabaud F,Joux A.Differential Collisions in SHA-0.Advances in Cryptology-Crypto’98,volume 1462 of Lecture Notes in Computer Science, Springer-Verlag,1998:56–71.
[6] Y.Sasaki, K.Aoki.Preimage Attacks on Step-Reduced MD5. ACISP2008. LNCS5107. 2008:282–296
[7] MJ Saarinen, A Meeting-in-the-Middle Collision Attack Against the New FORK-256. INDOCRYPT2007. LNCS4859, 2007, 10–17.
[8] Gilles Brassard, Peter Hoyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In LATIN ’98, Campinas, Brazil, April, 20-24, 1998,Proceedings, pages 163–169, 1998.
[9] Akinori Hosoyamada and Yu Sasaki. Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In Anne Canteaut and Yuval Ishai, editors, Advances in Cryptology EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14,2020. Proceedings, Part II, volume 12106 of Lecture Notes in Computer Science,pages 249–279. Springer, 2020.
[10] Ni, B., Dong, X., Jia, K., & You, Q. (2021).(Quantum) collision attack on simplified Simpira v2. IACR Symmetric Cryptography Transactions, 2021 (2), 222-248.
[11] Birjukov A,Ors S B, Preneel B. Security and Performance Analysis of Aria[J]. Technical report, Katholieke Universiteit Leuven, Belgium, 2007: 1-58.
[12] Akshima, Chang D, Ghosh M, Goel A, et al. Improved Meet-in-the-Middle Attacks on 7 and 8-Round ARIA-192 and ARIA-256[J]. International Conference on Cryptology in India. Springer, Cham, 2015, 198-217. [DOI:10.1007/978-3-319-26617-6_11]
[13] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In ISITA 2012, Honolulu, HI, USA, October 28-31,2012, pages 312–316, 2012.