# A 2nd-Preimage Attack on AURORA-512

Yu Sasaki

NTT Information Sharing Platform Laboratories, NTT Corporation
3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan
sasaki.yu@lab.ntt.co.jp

**Abstract.** In this note, we present a 2nd-preimage attack on AURORA-512, which is one of the candidates for SHA-3. Our attack can generate 2nd-preimages of any given message, in particular, the attack complexity becomes optimal when the message length is 9 blocks or more. In such a case, the attack complexity is approximately $2^{290}$ AURORA-512 operations, which is less than the brute force attack on AURORA-512, namely, $2^{512-\log_2 9} \approx 2^{508}$. Our attack exploits some weakness in the mode of operation.

**keywords**: AURORA, DMMD, 2nd-preimage, multi-collision

## 1 Description of AURORA-512

We briefly describe the specification of AURORA-512. Please refer to Ref. [1] for details. An input message is padded to be a multiple of 512 bits by the standard MD message padding, then, the padded message is divided into 512-bit message blocks $(M_0, M_1, \ldots, M_{N-1})$.

In AURORA-512, compression functions $F_k : \{0,1\}^{256} \times \{0,1\}^{512} \rightarrow \{0,1\}^{256}$ and $G_k : \{0,1\}^{256} \times \{0,1\}^{512} \rightarrow \{0,1\}^{256}$, two permutations $MF : \{0,1\}^{512} \rightarrow \{0,1\}^{512}$ and $MFF : \{0,1\}^{512} \rightarrow \{0,1\}^{512}$, and two initial 256-bit chaining values $H_0^U$ and $H_0^D$ are defined[1].

The algorithm to compute a hash value is as follows.

1. `for` $k$=0 to $N-1$ {
2. $\quad H_{k+1}^U \leftarrow F_k(H_k^U, M_k)$.
3. $\quad H_{k+1}^D \leftarrow G_k(H_k^D, M_k)$.
4. $\quad$ `If` $k$ `mod` $8 = 7$ {
5. $\quad\quad$ `temp` $\leftarrow H_{k+1}^U \| H_{k+1}^D$
6. $\quad\quad H_{k+1}^U \| H_{k+1}^D \leftarrow MF($`temp`$)$.
7. $\quad$ }
8. }
9. Output $MFF(H_N^U \| H_N^D)$.

[1] $F_k$ and $F_{k'}$ are identical if $k \equiv k' \bmod 8$. $G_k$ and $G_{k'}$ also follow the same rule.

## 2 Attack Description

Our attack can generate 2nd-preimages of any given message, in particular, the attack complexity becomes optimal when the message length is 9 blocks or more, in which case it is approximately $2^{290}$ AURORA-512 operations. Strictly speaking, the attack complexity depends on the output distribution of the compression function. We first assume that the output distribution is perfectly balanced, then discuss other cases later.

The attack procedure for a 9-block message $X_0\|X_1\|\cdots\|X_8$ is as follows. The attack is also illustrated in Fig. 1

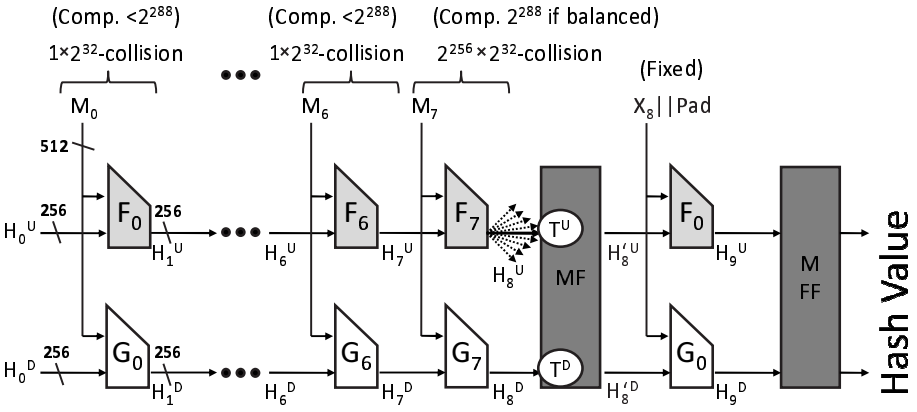


**Fig. 1.** 2nd-preimage construction for a 9-block message in AURORA-512

1. Compute a hash value of the given message. Let $T^U$ and $T^D$ be $H_8^U$ and $H_8^D$ for the given message, respectively.
2. Choose an $M_0$ and compute $H_1^U \leftarrow F_0(H_0^U, M_0)$. Repeat this computation with changing $M_0$ until a $2^{32}$-collision of $H_1^U$ is obtained.
3. Following the first block, we apply the Joux's attack [2] to $M_1$ through $M_6$. In total, we obtain a $2^{32\times 7} = 2^{224}$-collision of $H_7^U$.
4. Compute $H_8^U \leftarrow F_7(H_7^U, M_7)$ for $2^{288}(= 2^{256} \cdot 2^{32})$ different $M_7$s. If the output distribution of $F_7$ is perfectly balanced with respect to $M_7$, namely, the output distribution of $F_7(H_7^U, \cdot)$ is balanced, we obtain $2^{32}$-collisions for all possible values of $H_8^U$. Therefore, we obtain a $2^{32}$-collision of $M_7$ that maps $H_7^U$ to $T^U$. Consequently, we obtain $2^{256}(= 2^{224} \cdot 2^{32})$ messages $M_0\|M_1\|\cdots\|M_7$ that produce $T^U$.
5. Compute $H_{k+1}^D \leftarrow G_k(H_k^D, M_k), 0 \le k \le 7$ for all $M_0\|M_1\|\cdots\|M_7$ obtained at Step 4. Since we have $2^{256}$ different choices, we expect that one of them will match $T^D$. Let $M_0^*\|M_1^*\|\cdots\|M_7^*$ be the matched message, then, $M_0^*\|M_1^*\|\cdots\|M_7^*\|X_8$ is a second preimage of the given message.

### 2.1 Complexity evaluation

At Steps 2 and 3, if we try $2^{288}(= 2^{256} \cdot 2^{32})$ different $M_k$ for each block, we obtain a $2^{32}$-collision due to the pigeonhole principle. The time complexity is at most $7 \cdot 2^{288}$ $F_k$ operations and the success probability is 1. Step 4 costs exactly $2^{288}$ $F_7$-operations if the output distribution of $F_7(H_7^U, \cdot)$ is perfectly balanced. Step 5 costs $8 \cdot 2^{256}$ $G_k$-operations. Therefore, the total time complexity of this attack is $7 \cdot 2^{288} + 2^{288} + 8 \cdot 2^{256} \approx 2^{291}$ $F_k$ or $G_k$-operations, which is approximately $2^{290}$ AURORA-512 operations.

At Steps 2 and 3, we need to prepare $2^{288} \times 512$ bits of memory.

### 2.2 Remarks on output distribution

At Steps 2 and 3, we need only one $2^{32}$-collision. Therefore, the attack complexity becomes less if the distribution is not balanced. At Step 4, we need one $2^{32}$-collision that produces $T^U$. If the distribution is not balanced and $T^U$ is produced more frequently than other values, the complexity becomes less. However, if $T_U$ is not produced as much as other values, $2^{288}$ trials may not be enough to produce a desired $2^{32}$-collision. In such a case, one solution is simply trying more messages until we obtain a $2^{32}$-collision. Another solution is keeping other multi-collisions of $H_7^U$ at Step 3, and start to compute $F_7$ by replacing the value of $H_7^U$.

## 3 Conclusion

In this note, we presented a 2nd-preimage attack on AURORA-512 with a complexity of $2^{290}$. Our attack exploits the weakness in the mode of operation and efficiently finds a 2nd-preimage by generating many multi-collisions. We note that a collision attack is also presented at Ref. [3].

## References


1. Tetsu Iwata, Kyoji Shibutani, Taizo Shirai, Shiho Moriai, and Toru Akishita. *AURORA: A Cryptographic Hash Algorithm Family.* AURORA home page `http://www.sony.net/Products/cryptography/aurora/index.html`, (Also available at NIST home page: `http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`).
2. Antoine Joux. Multicollisions in iterated hash functions. application to cascaded constructions. In Matt Franklin, editor, *Advances in Cryptology — CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 306–316, Berlin, Heidelberg, New York, 2004. Springer-Verlag.
3. Yu Sasaki. A collision attack on AURORA-512. Cryptology ePrint Archive, Report 2009/131, 2009. `http://eprint.iacr.org/2009/131`.