# A Collision Attack on AURORA-512

Yu Sasaki

NTT, 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan

**Abstract.** In this note, we present a collision attack on AURORA-512, which is one of the candidates for SHA-3. The attack complexity is approximately $2^{236}$ AURORA-512 operations, which is less than the birthday bound of AURORA-512, namely, $2^{256}$. Our attack exploits some weakness in the mode of operation.

**keywords**: AURORA, DMMD, collision, multi-collision

## 1 Description of AURORA-512

We briefly describe the specification of AURORA-512. Please refer 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 $F_k : \{0,1\}^{256} \times \{0,1\}^{512} \to \{0,1\}^{256}$ and $G_k : \{0,1\}^{256} \times \{0,1\}^{512} \to \{0,1\}^{256}$, two permutations $MF : \{0,1\}^{512} \to \{0,1\}^{512}$ and $MFF : \{0,1\}^{512} \to \{0,1\}^{512}$, 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.

```
for k=0 to N − 1 {
        H^U_{k+1} ← F_k(H^U_k, M_k).
        H^D_{k+1} ← G_k(H^D_k, M_k).
        If k mod 8 = 7 {
                temp ← H^U_{k+1} || H^D_{k+1}
                H^U_{k+1} || H^D_{k+1} ← MF(temp).
        }
}
Output MFF(H^U_N || H^D_N).
```

For example, we show the computation of AURORA-512 for a 10-block message in Fig. 1.

## 2 Attack Description

Our attack finds collisions of 8-block messages with a complexity of $2^{236}$. The attack procedure is as follows. The attack is also illustrated in Fig. 2

[1] $F_k$ and $F'_k$ are identical if $k \equiv k' \bmod 8$. $G_k$ and $G'_k$ also follow the same rule.

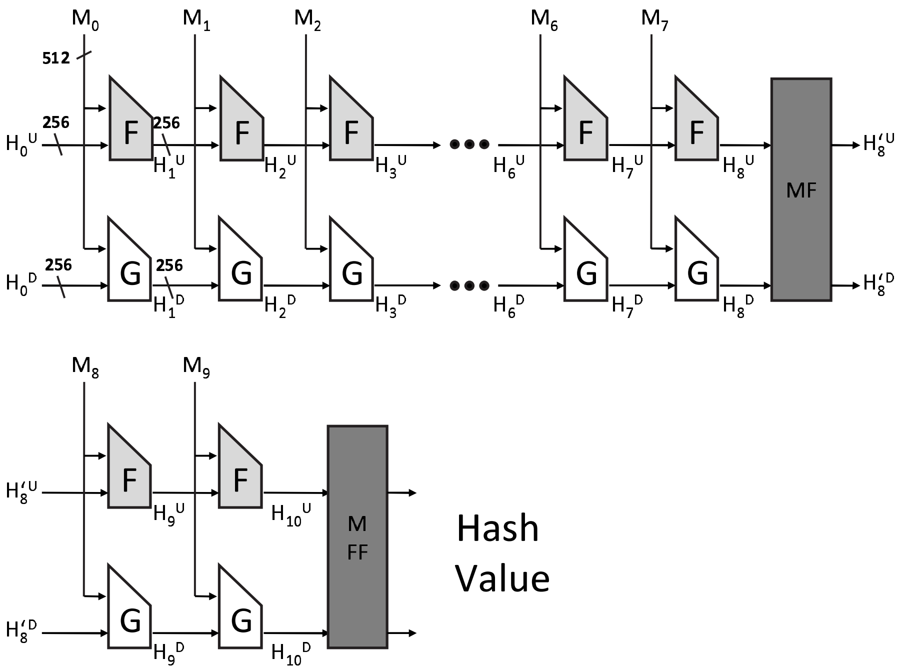


**Fig. 1.** AURORA-512 computation for a 10-block message

1. Randomly choose $2^{224} (= 2^{256 \cdot \frac{7}{8}})$ $M_0$, and compute $H_1^U \leftarrow F_k(H_0^U, M_0)$ for each $M_0$. This yields an 8-collision (=$2^3$-collision) of $H_1^U$.
2. By applying the Joux's attack [2] to $M_1$ through $M_6$, we obtain a $2^{21}$-collision of $H_7^U$. Let these 7-block messages yielding the $2^{21}$-collision be $M_{[06]}^{(i)}, 0 \leq i \leq 2^{21} - 1$.
3. Compute $H_{k+1}^D \leftarrow G_k(H_k^D, M_k^{(i)}), 0 \leq k \leq 6$ for all $i$. Let the corresponding $2^{21}$ $H_7^D$s be $H_7^{D(i)}$.
4. Set $M_7$ to be a randomly chosen value, and compute $H_8^{D(i)} = G_k(H_7^{D(i)}, M_7)$ for all $i$. Check whether or not a collision exists among $2^{21}$ $H_8^{D(i)}$.
5. If not, go back to Step 4 and try a different $M_7$. If a collision is found, let the corresponding '$i$'s be $i1$ and $i2$, and corresponding $M_7$ be $M_7^{(j)}$. Then, $M_{[06]}^{(i1)} \| M_7^{(j)}$ and $M_{[06]}^{(i2)} \| M_7^{(j)}$ are the colliding pair.

At Step 4, since there are $2^{21}$ $H_8^{D(i)}$, we can make roughly $2^{41} (= (2^{21})^2/2)$ pairs of $H_8^{D(i)}$. Therefore, the probability that a collision is found is $2^{-215} (= 2^{-256} \cdot 2^{41})$. As a result, after $2^{215}$ iterations of Step 4, we expect to obtain a colliding pair.

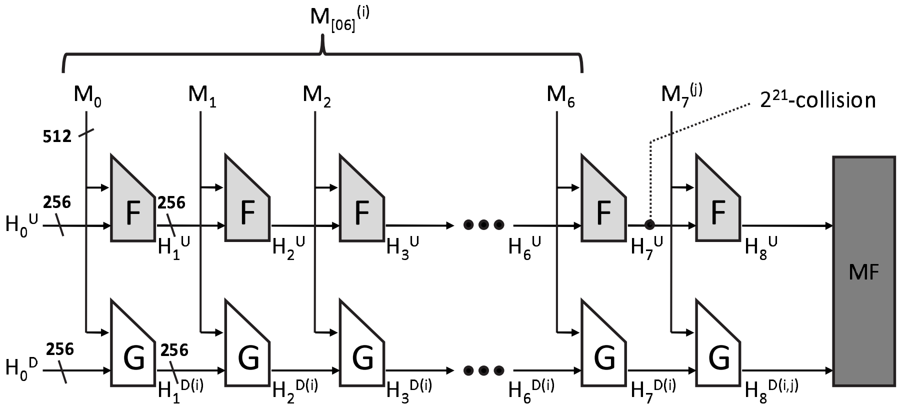


**Fig. 2.** Collision construction on AURORA-512

### 2.1 Complexity evaluation

Steps 1 and 2 cost $7 \cdot 2^{224}$ $F_k$-operations. Step 3 costs $7 \cdot 2^{21}$ $G_k$-operations. At Steps 4 and 5, the complexity of Step 4 for a chosen $M_7$ is $2^{21}$ $G_k$-operations. Therefore, $2^{215}$ iterations cost $2^{236}(= 2^{21} \cdot 2^{215})$ $G_k$-operations. Hence, the time complexity of this collision attack is $7 \cdot 2^{224} + 7 \cdot 2^{21} + 2^{236} \approx 2^{236}$ AURORA-512 operations.

At Steps 1 and 2, we need to prepare $2^{236} \times 512$ bits of memory.

### 2.2 Remarks on success probability of generating multi-collision

At Step 2 of the attack procedure, the success probability of generating multi-collisions is much lower than 1/2. Ref. [3] gives us the complexity for finding $s$-collisions of $n$-bit value with a probability of approximately 1/2:

$$(s!)^{1/s} \times (2^{n \cdot \frac{s-1}{s}}) + s - 1. \tag{1}$$

The value of this equation is $2^{225.91} \approx 2^{226}$ when $n = 256$ and $s = 2^3$. However, by considering that our attack generates $2^3$-collisions 7 times at Steps 1 and 2, we need to increase the success probability much more. For this purpose, our attack computes $2^{230}$ $F_k$-operations for each block. Since $2^{230-226} = 16$, the success probability for Step 2 becomes $(1 - (1/2)^{16})^7 \approx 1$.

Under this strategy, the attack complexity is $7 \cdot 2^{230} + 7 \cdot 2^{21} + 2^{236} = 2^{236.150} \approx 2^{236}$ AURORA-512 operations.

## 3 Conclusion

In this note, we presented a collision attack on AURORA-512 with a complexity of $2^{236}$. Our attack uses the Joux's multi-collision attack [2] to find a $2^{21}$-collision of the first seven blocks. We emphasize that the presented attack is the first attack on AURORA-512.

## Remarks

Our attack succeeds due to the long (8 steps) interval of the $MF$ function, namely, the computations of $H_k^U$ and $H_k^D$ are independent in up to 8 steps.

## References


1. Tetsu Iwata, Kyoji Shibutani, Taizo Shirai, Shiho Moriai, and Toru Akishita. AURORA: A cryptographic hash algorithm family. *AURORA home page*, 2009. `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. Kazuhiro Suzuki, Dongvu Tonien, Kaoru Kurosawa, and Koji Toyota. Birthday paradox for multi-collisions. E91-A(1):39–45, 2008.