AICR · OPEN PROBLEM

Tight Time-Space Tradeoffs for k-Collisions with Auxiliary Input

Status. Statement: AI-written, not yet formalized.

Category. Symmetric-Key Cryptography.

Finding collisions in hash functions under preprocessing (the Random Oracle Model with Auxiliary Input, AI-ROM) models realistic adversaries who execute unbounded offline computation to store an S-bit summary of a random oracle $H : [N] \to [N]$. While the exact tight tradeoff for 2-collisions ($k = 2$) is established as $S \cdot T^2 = \Theta(N)$, determining the exact asymptotic curve $S^a T^b = \Omega(N^c)$ for multicollisions ($k \geq 3$) remains an open problem in provable security.

1 Formal Model: AI-ROM

Let $H : [N] \to [N]$ be a uniformly random function, where $N = 2^n$.

Definition 1 (k-Collision Finding with Precomputation). A two-stage adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ operates as follows:

i. **Offline Phase**: $\mathcal{A}_1^H(1^n)$ has unbounded access to H and outputs an advice string $S \in \{0,1\}^S$ of size at most S bits.

ii. **Online Phase**: $\mathcal{A}_2^H(S)$ receives S, makes at most T query evaluations to H, and outputs a tuple of k distinct inputs $(x_1, x_2, \ldots, x_k)$.

The adversary wins if $H(x_1) = H(x_2) = \cdots = H(x_k)$ and $x_i \neq x_j$ for all $1 \leq i < j \leq k$.

2 The Open k-Collision Tradeoff Conjecture

Conjecture 1 (Tight k-Collision Time-Space Tradeoff). *Let $H : [N] \to [N]$ be a random oracle. For any $k \geq 3$, any adversary $(\mathcal{A}_1, \mathcal{A}_2)$ with S-bit advice and T online queries that finds a k-collision with success probability $\epsilon \geq 1/2$ must satisfy:*

$$S^{k-1} \cdot T^k \geq \Omega\left(N^{k-1}\right). \tag{1}$$

Specifically, for 3-collisions ($k = 3$), the optimal trade-off satisfies:

$$S^2 \cdot T^3 \geq \Omega\left(N^2\right). \tag{2}$$

3 Comparison of Known Upper and Lower Bounds

Collision Multiplicity (k)	**Known Lower Bound**	**Best Known Attack (Upper Bound)**	**Status**
$k = 2$ (2-Collision)	$S \cdot T^2 = \Omega(N)$	$S \cdot T^2 = O(N)$ (Hellman, 1980 / Coretti et al., 2018)	Tight
$k = 3$ (3-Collision)	$S \cdot T^3 = \Omega(N)$	$S^2 \cdot T^3 = O(N^2)$	**Gap of S**
General $k \geq 3$	$S \cdot T^k = \Omega(N)$	$S^{k-1}T^k = O(N^{k-1})$	**OPEN**

Table 1: Current state of knowledge for precomputation bounds in AI-ROM.

Why the Problem is Hard: Current lower-bound techniques (such as compression arguments or the bit-fixing model) fail to capture the multi-way combinatorial synergy when S advice bits store structural information about hypergraphs of preimages across k distinct points simultaneously.