Time-Space Tradeoffs for Bounded-Length collisions in Merkle-Damgård hashing

Ashrujit Ghoshal
University of Washington

Ilan Komargodski
Hebrew University and NTT Research

CRYPTO 2022
Iterative hashing

Hash functions need to handle variable input lengths
- password hashing
- hash and sign
- commitments

Cannot design a different hash for every length

Construct a VIL hash function from an underlying FIL primitive

e.g., Merkle Damgård hashing \([\text{Mer89, Dam89}], \text{sponge [BDPV07]}\)
**Merkle-Damgård**

Given a random salt $a$, hard to find $M \neq M'$ such that $\text{MD}_h(a, M) = \text{MD}_h(a, M')$.

Used in MD5, SHA-1, SHA-2
Complexity of finding collisions

• Model $h$ as a random oracle

• Using $T \approx \sqrt{N}$ queries, can find collisions
  • This is necessary

• What about adversaries with large preprocessing?
  • birthday-style attack no longer optimal
  • Scenario studied by [Hellman80, Fiat-Naor99, Unruh07,...]
Auxiliary-input random oracle model (AI-ROM) [Unruh07]

\[ (A_1, A_2) \]

\[ \begin{align*} A \quad &\quad \Downarrow \quad A_1 \quad \Downarrow h \quad \rightarrow \quad A_2 \quad \Downarrow M, M' \quad \rightarrow \quad h \\ &\quad \Downarrow S \text{ bits} \quad \Downarrow T \text{ queries} \quad \Downarrow \end{align*} \]

“pre-processing” phase \hspace{1cm} “online” phase

\[ A \text{ wins if } M' \neq M, \text{MD}_h(a, M) = \text{MD}_h(a, M') \]

\[ \text{Adv}_N(S,T) = \max_{(S,T) \text{ adv}_A} \text{Pr}[A \text{ wins}] \]
Prior work

Theorem. [CDGS18] \( \text{Adv}_N(S, T) = \Theta \left( \frac{ST^2}{N} \right) \)

An observation: the attack finds collisions of length \( \Omega(T) \)!

Say, \( T \approx 2^{60} \Rightarrow \) petabytes sized collision!

Shorter collisions are provably harder to find

Theorem. [ACDW20] \( \text{Adv}_{N,2}(S, T) \leq O \left( \frac{ST}{N} + \frac{T^2}{N} \right) \)
Theorem (STB attack). [ACDW20] \( \text{Adv}_{N,B}(S,T) \geq \tilde{\Omega}\left(\frac{STB}{N} + \frac{T^2}{N}\right) \)

The STB conjecture [ACDW20]

“the optimal attack for finding \( B \)-block collisions has advantage at most \( \tilde{O}\left(\frac{STB}{N} + \frac{T^2}{N}\right)\)”

Was unresolved for \( 3 \leq B \ll T \)
This work:

Proof of the STB conjecture for

- $B = O(1)$  
- $S^4B^2 \in \tilde{O}(T)$

Recently improved by Akshima, Guo, Liu [AGL22]
Main theorem

**Theorem.** [this work]

\[
\text{Adv}_{N,B}(S,T) \leq O\left(\frac{STB^2 \log S}{N} + \frac{T^2}{N}\right)
\]

For constant \(B\),

\[
\text{Adv}_{N,B}(S,T) \leq \tilde{\Omega}\left(\frac{ST}{N} + \frac{T^2}{N}\right)
\]

Proof via multi-instance framework [IK10, CGLQ20, ACDW20]
Multi-instance framework \([\text{CGLQ20, ACDW20}]\)

\[a_1, a_2, ..., a_u \leftarrow [N]\]

\[\begin{align*}
(0^s, a_1) & \quad \rightarrow \quad A_2 \quad \downarrow T \text{ queries} \quad \rightarrow \quad (M_1, M'_1) \\
(0^s, a_2) & \quad \rightarrow \quad A_2 \quad \downarrow T \text{ queries} \quad \rightarrow \quad (M_2, M'_2) \\
(0^s, a_u) & \quad \rightarrow \quad A_2 \quad \downarrow T \text{ queries} \quad \rightarrow \quad (M_u, M'_u)
\end{align*}\]

\(A_2\) wins if \(\forall i \in [u]\)

1. \(M_i \neq M'_i\)  
2. \(\text{MD}_h(a_i, M_i) = \text{MD}_h(a_i, M'_i)\)  
3. \(|M_i|, |M'_i| \leq B\)
Multi-instance lemma. Let \( u = S + \log N \). Define \( \varepsilon := \max_{A_2} \Pr[A_2 \text{ wins}] \). Then

\[
\text{Adv}_{N,B}(S,T) \leq \frac{1}{\varepsilon u}
\]

Will prove:

\[
\varepsilon \leq \left( O \left( \frac{uT B^2 (\log u)^B}{N} + \frac{T^2}{N} \right) \right)^u
\]

For constant \( B \), \( u = S + \log N \)

\[
\varepsilon \leq \left( \tilde{O} \left( \frac{ST}{N} + \frac{T^2}{N} \right) \right)^u
\]

From multi-instance lemma, it follows

\[
\text{Adv}_{N,B}(S,T) \leq \tilde{O} \left( \frac{ST}{N} + \frac{T^2}{N} \right)
\]
Upper bounding multi-instance advantage

Technique: compression argument

Lemma [GT00, DTT10]. Let $\varepsilon := \Pr_{x,r}[\text{Dec(Enc}(x, r), r) = x]$. Then

$$\log|Y| \geq \log|X| - \log \frac{1}{\varepsilon}$$
$a_1, a_2, \ldots, a_u \leftarrow [N]$

$A_2$ (0^s, a_1) \quad h \quad T \text{ queries} \quad (M_1, M_1')$

$A_2$ (0^s, a_2) \quad h \quad T \text{ queries} \quad (M_2, M_2')$

$A_2$ (0^s, a_u) \quad h \quad T \text{ queries} \quad (M_u, M_u')$

Our strategy: Encode $h, \{a_1, a_2, \ldots, a_u\}$ using $A_2$ that always wins.

Compression lemma $\Rightarrow$ upper bound $\Pr[A_2 \text{ wins}]$

Simplifying assumption: Only queries of the form $h(a_i,\ast)$ when $A_2$ run on $a_i$
Encoding

\((0^s, a_1)\)

\[ A_2 \xrightarrow{(x_k, y_k)} z_k \]

\[ z_j = z_k \]

\[ a_1 \ldots a_u \]

\[ z_1 \ldots z_k \ldots j \ldots z_T \ldots \]

Unqueried entries of \(h\)

\[ (j, k) \ldots (p, q) \]

\[ (0^s, a_u) \]

\[ A_2 \xleftarrow{} \]

\[ h \]
Decoding

Using the compression lemma,

\[ \varepsilon \leq \left( \frac{1}{N} \right) \]

Collision for every salt

\[ \Rightarrow \text{Savings} = u \left( \log N - 2 \log T \right) \]

Unqueried entries of \( h \)

\[ (0^s, a_1) \]

\[ A_2 \]

\[ \frac{(x_j, y_j)}{z_j z_k} \]

\[ h \]

\[ (0^s, a_u) \]

\[ A_2 \]

\[ \frac{}{h} \]

However, cannot assume only queries of the form \( h(a_i, *) \) are made when \( A_2 \) run on \( a_i \)

\[ (j, k) \]

\[ (p, q) \]
Query graph

Graph grows across all of $A_2$’s runs

Note: $A_2$ may repeat queries across different runs

Assume wlog $A_2$ makes all $h$ queries needed to compute collision

How do $B$-block collisions look like?
Collision structure

The mouse structure

- Tail
- Body
- Tip

- $a$

- $\leq B$

- No lower body
- Self loop body
- No tail

Isolate one mouse structure per salt
Types of queries

- **New** queries: queries made for the first time
  - wlog no queries repeated in single $A_2$ run
  - query not made in any previous $A_2$ run ⇒ **new** query

- Repeated queries
  - **repeated-mouse** queries: query present in some earlier mouse structure
  - **repeated-non-mouse** queries: other queries

Assume: Before running $A_2$ on $a_i, h(a_i,*)$ not queried
⇒ every mouse structure has a new query
Classifying mouse structures

1) Colliding new queries

2) Self loop body

3) New query touching repeated-mouse query
Classifying mouse structures (2)

4. At least one repeated-mouse query

5. No repeated-mouse query
Goal: for every mouse structure save at least

\[ \delta = \min\left\{ \log \frac{N}{T^2}, \log \frac{N}{uTB^2 (\log u)^B} \right\} \text{ bits} \]

Total savings \( \geq u \cdot \delta \) bits

Using the compression lemma,

\[ \varepsilon \leq \max \left\{ \frac{T^2}{N}, \frac{4uTB^2 (3 \log u)^B}{N} \right\} \leq \left( O \left( \frac{uTB^2 (\log u)^B}{N} + \frac{T^2}{N} \right) \right)^u \]
Recall assumption: Before running $A_2$ on $a_i$, $h(a_i, \ast)$ not queried

Why is it reasonable?

Because otherwise save on $a_i$

That suffices!

Savings = $\log N - \log uT \geq \delta$

omit $a_i$

add query index of $h(a_i, \ast)$
Easy case examples

Colliding new queries

Say $q_2$ after $q_1$

Savings:
$$\log N - 2\log T \geq \delta$$

“local” indices of $q_1, q_2$

New query touching repeated-mouse query

Savings:
$$\log N - \log T - \log uB \geq \delta$$

answer of $q_2$

index of $q_4$

index of $q_3$
Hard case example

At least one repeated-mouse query

Strategy:
Omit answer of $q_2$,
Remember:
- index of $q_1$
- index of $q_2$
- path back from $q_1$ to $q_2$

No large multi-collision if:
$\leq \log u$ incoming edges for all nodes

no large multi-collision $\Rightarrow$ path encoding needs at most
$\log B + B \log(\log u)$

# of edges on path which edge to take on path back
Strategy:
Omit answer of $q_2$,
Remember:
• index of $q_1$
• index of $q_2$
• path back from $q_1$ to $q_2$

$$\text{Savings} \geq \log N - (\log uB + \log T + \log(\log u)^B + \log B) \geq \delta$$

But, what if there are large multi-collisions?

Key idea: Save from the large multi-collision!
**Saving from multi-collisions**

**Strategy:**
Remember answer of first of $m$ queries, indices of rest

$m$- multi-collision

**Savings:**

$$(m - 1) \log N - \log \binom{uT}{m}$$

When $m \geq \log u$,

$$(m - 1) \log N - \log \binom{uT}{m} \geq \log N - 2 \log T \geq \delta$$
Conclusion

• STB conjecture true for all constant $B$, when $S^4 B^2 \in \tilde{O}(T)$

• Follow up works
  • STB conjecture proven for $ST^2 \leq N$ [AGL22]
  • similar question studied for sponge [FGK22]

Open problem:
Prove the STB conjecture or give better attacks for $ST^2 > N$

Paper: [https://eprint.iacr.org/2022/309](https://eprint.iacr.org/2022/309)