Combiners for Backdoored Random Oracles

Balthazar Bauer, Pooya Farshim, Sogol Mazaheri

ENS, Paris

TU Darmstadt
Backdoors

It makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact.

James Comey (former FBI director, Oct. 2014)
It makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact.

James Comey (former FBI director, Oct. 2014)
Hash Functions

Hash Functions are Everywhere:

KDFs
OWFs
MACs
FDH
PoW
Hash Functions

Hash Functions are Everywhere:

- KDFs
- OWFs
- FDH
- MACs
- PoW

security proofs are not always possible...
Random Oracles

The quick brown fox jumps over the lazy dog.

SHA

08bff1e0b0162
Random Oracles = Ideal Hash Functions

The quick brown fox jumps over the lazy dog.

ideal hash function

08bff1e0b0162
Random Oracles = Ideal Hash Functions

Random Oracles are Practical, enabling proofs of many practical schemes:

- RSA-OAEP
- TLS
- Identification protocols
  - FDH
  - DSA
  - PSS
Backdoored Random Oracles (BROs)
Backdoored Random Oracles (BROs)

\[ H(x) \]

\[ f(H(x)) \]
Backdoored Random Oracles (BROs)

random oracle $\xrightarrow{x} H \xrightarrow{H(x)}$
Backdoored Random Oracles (BROs)
Backdoored Random Oracles (BROs)

random oracle \( \xrightarrow{x} H \xrightarrow{H(x)} \)

backdoor oracle \( \xrightarrow{f} BD_H \xrightarrow{f(H)} \)

adaptive and unrestricted access to the backdoor oracle
Backdoor Capabilities

\[ BD_H \]
Backdoor Capabilities

\[ \text{BD}_H \]

\( (x, x') \)

collisions?

\[ H - (y) \]

starting with \( k \) zeros?

\[ 0^k \]

any \( f \) \( f(\text{BD}_H) \) no security is possible...
Backdoor Capabilities

BD$_H$ collisions? $H^-(y)?$ 

$x$, $x'$ starting with $k$ zeros?

no security is possible...

Backdoor Capabilities

**BD**


collisions? \(H^-(y)?\)

\[H^-(y)\] starting with \(k\) zeros?

\[0^k|x\]

\((x, x')\)

starting with \(k\) zeros?

no security is possible...

Backdoor Capabilities
Backdoor Capabilities

BDH

$H^-(y)$? $H^-(y)$ starting with $k$ zeros?

$H^-(y)$? collisions?

any $f$

$f(H)$

$x$

$(x, x')$

$0^k | x$
Backdoor Capabilities

$\text{BD}_H$

- $H^-(y)$?
- $H^-(y)$ starting with $k$ zeros?
- $f(H)$
- $0^k|x$
- $(x, x')$
- any $f$

no security is possible...
Combining BROs

Can we combine two independent but backdoored hash functions to build one that is secure against adversaries with access to backdoor oracles?
Combining BROs

Can we combine two independent but backdoored hash functions to build one that is secure against adversaries with access to both backdoor oracles?
Combining BROs

Can we combine two independent but backdoored hash functions to build one that is secure against adversaries with access to both backdoor oracles?
Combiners
Combiners

concatenation:

\[
G \quad H
\]

\[
\oplus
\]

cascade:

\[
G \quad H
\]

\[
\oplus
\]
Combiners

concatenation:

xor:

\[
\begin{align*}
\text{concatenation:} & \quad H \quad G \\
\text{xor:} & \quad H \oplus G
\end{align*}
\]
Combiners

concatenation:

xor:

cascade:
Combiners

concatenation:

xor:

cascade:
Concatenation in 2-BRO

H → BD_H

G → BD_G
Concatenation in 2-BRO

one-way security?
Concatenation in 2-BRO

one-way security? pseudorandomness?

collision-resistance?
Concatenation in 2-BRO

one-way security? pseudorandomness?
collision-resistance?

We need results from communication complexity...
Communication Complexity

$A$ $t(A, B)$ $B$

Theorem ([Babai, Frankl, Simon 86]): For independent random sets $A, B \subseteq [2^n]$ of size $2^n/2$, and protocols with 99% correctness, it holds that $CC(DISJ) \geq \Omega(2^n/2)$. 
Communication Complexity

Theorem ([Babai, Frankl, Simon 86]): For independent random sets $A, B \subseteq [2^n]$ of size $2^n/2$, and protocols with 99% correctness, it holds that $\text{CC}(\text{DISJ}) \geq \Omega(2^n/2)$. 

$\text{INT}$: find $x \in A \cap B$.

$\text{DISJ}$: decide $A \cap B = \emptyset$. 

A

\[ \begin{array}{c}
A \\
\cap \\
B
\end{array} \]

B
Communication Complexity

**INT**: find $x \in A \cap B$.

**DISJ**: decide $A \cap B = \emptyset$.

Theorem ([Babai, Frankl, Simon 86]): For independent random sets $A, B \subseteq \{2^n\}$ of size $2^n / 2$, and protocols with 99% correctness, it holds that $\text{CC}(\text{DISJ}) \geq \Omega(2^n / 2)$. 

9
Communication Complexity

\[ t(A, B) \]

**INT:** find \( x \in A \cap B \).

**DISJ:** decide \( A \cap B = \emptyset \)

**Theorem** ([Babai, Frankl, Simon 86]): For independent random sets \( A, B \subseteq [2^n] \) of size \( 2^{n/2} \), and protocols with 99% correctness, it holds that

\[ \text{CC}(\text{DISJ}) \geq \Omega(2^{n/2}). \]
**Communication Complexity - Generalized**

| $|A|, |B|$ | lower-bound | problem | by |
|---|---|---|---|
| $= 2^{n/2}$ | $\Omega(2^{n/2})$ | DISJ | [Babai, Frankl, Simon 86] |
| $\approx 2^{n/2}$ | $\Omega(2^{n/2})$ | DISJ | [Moshkovitz, Barak 12], [Guruswami, Cheraghchi 13] |
### Communication Complexity – Generalized

| $|A|, |B|$ | lower-bound | problem | by |
|---|---|---|---|
| $= 2^{n/2}$ | $\Omega(2^{n/2})$ | DISJ | [Babai, Frankl, Simon 86] |
| $\approx 2^{n/2}$ | $\Omega(2^{n/2})$ | DISJ | [Moshkovitz, Barak 12], [Guruswami, Cheraghchi 13] |

**Theorem:** For independent random sets $A, B \subseteq [2^n]$ of expected sizes $2^n(1-\alpha)$ and $2^n(1-\beta)$ respectively,

$$\text{CC}(\text{INT}) \geq \Omega(2^n(\min(\alpha,\beta)+\alpha+\beta-1)),$$

for $(\alpha, \beta)$ in the feasible region.
### Communication Complexity - Generalized

| $|A|$, $|B|$ | lower-bound | problem | by |
|---|---|---|---|
| $= 2^{n/2}$ | $\Omega(2^{n/2})$ | DISJ | [Babai, Frankl, Simon 86] |
| $\approx 2^{n/2}$ | $\Omega(2^{n/2})$ | DISJ | [Moshkovitz, Barak 12], [Guruswami, Cheraghchi 13] |

**Theorem:** For independent random sets $A, B \subseteq [2^n]$ of expected sizes $2^n(1-\alpha)$ and $2^n(1-\beta)$ respectively,

$$\text{CC(INT)} \geq \Omega(2^n (\min(\alpha, \beta) + \alpha + \beta - 1)),$$

for $(\alpha, \beta)$ in the feasible region.
**Theorem**: Inverting a random value $u|v$ under $H|G$ in the 2-BRO model is as hard as the set-intersection problem.
One-Way Security of Concatenation Combiner

**Theorem**: Inverting a random value $u|v$ under $H|G$ in the 2-BRO model is as hard as the set-intersection problem.

Let $A := H^-(u)$ and $B := G^-(v)$.

![Venn Diagram](image)
One-Way Security of Concatenation Combiner

**Theorem:** Inverting a random value $u|v$ under $H|G$ in the 2-BRO model is as hard as the set-intersection problem.

Let $A := H^-(u)$ and $B := G^-(v)$.

Then, for any pre-image $x$ of $u|v$:

$x \in H^-(u)$ and $x \in G^-(v)$
Theorem: Inverting a random value \( u|v \) under \( H|G \) in the 2-BRO model is as hard as the set-intersection problem.

Let \( A := H^-(u) \) and \( B := G^-(v) \).

Then, for any pre-image \( x \) of \( u|v \):

\[
\begin{align*}
  x &\in H^-(u) \quad \text{and} \quad x \in G^-(v) \\
  \text{Hence,} \quad x &\in A \cap B.
\end{align*}
\]
Security of Concatenation in 2-BRO

One-Way Security

Inverting a random value $u|v$ is as hard as the set-intersection problem.
Security of Concatenation in 2-BRO

One-Way Security

Inverting a random value $u|v$ is as hard as the set-intersection problem.

Pseudorandomness

Deciding whether a random value $u|v$ has a pre-image is as hard as the set-disjointness problem.
Security of Concatenation in 2-BRO

One-Way Security
Inverting a random value $u|v$ is as hard as the set-intersection problem.

Pseudorandomness
Deciding whether a random value $u|v$ has a pre-image is as hard as the set-disjointness problem.

Collision-Resistance
Finding a collision is as hard as ...
Collision-Resistance of Concatenation

**Theorem**: Finding a collision under $H|G$ in the 2-BRO model is as hard as finding 2 sets, given many, and 2 elements in their intersection.
Collision-Resistance of Concatenation

**Theorem:** Finding a collision under $H|G$ in the 2-BRO model is as hard as finding 2 sets, given many, and 2 elements in their intersection.
Collision-Resistance of Concatenation

**Theorem:** Finding a collision under $H|G$ in the 2-BRO model is as hard as finding 2 sets, given many, and 2 elements in their intersection.

Hardness of the above problem is open.
Combiners and Security Notions

<table>
<thead>
<tr>
<th>H ⊕ G</th>
<th>OW</th>
<th>PRG</th>
<th>CR</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>??</td>
<td></td>
</tr>
<tr>
<td>✓ ?</td>
<td></td>
<td>??</td>
<td></td>
</tr>
<tr>
<td>✓ ✓</td>
<td>✓</td>
<td>??</td>
<td></td>
</tr>
</tbody>
</table>
Open Problems

- lower bound for the multi-INT problem
- extend parameters for DISJ and INT
- combiners for other backdoored primitives
Thank You.

Thanks to Giorgia Marson for drawing Alice, Bob, and the sheet.
Thank You.

Thanks to Giorgia Marson for drawing Alice, Bob, and the sheet.