Combiners for Backdoored Random Oracles

Balthazar Bauer, Pooya Farshim, Sogol Mazaheri

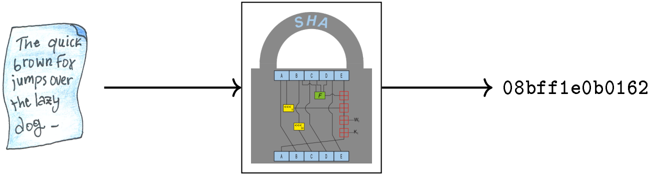
ENS, Paris TU Darmstadt

Backdoors

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)

Hash Functions



Hash Functions are Everywhere:

KDFs

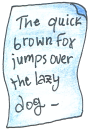
OWFs

FDH

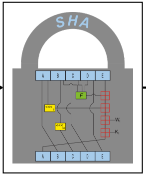
MACs

PoW

Hash Functions



→



→ `08bff1e0b0162`

Hash Functions are Everywhere:

KDFs

OWFs

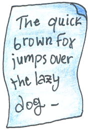
FDH

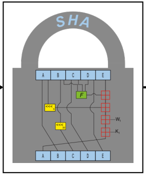
MACs

PoW

security proofs are not always possible...

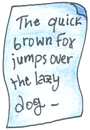
Random Oracles





08bff1e0b0162

Random Oracles = Ideal Hash Functions



→

ideal hash function

→ `08bff1e0b0162`

Random Oracles = Ideal Hash Functions

ideal hash function

Random Oracles are Practical,

enabling proofs of many practical schemes:

RSA-OAEP

TLS

Identification protocols

FDH

DSA

PSS

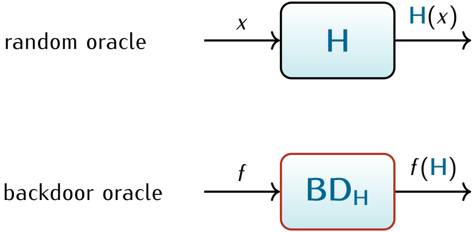
Backdoored Random Oracles (BROs)

Backdoored Random Oracles (BROs)

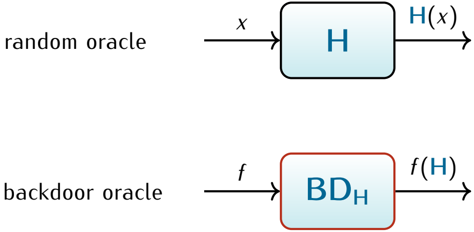
Backdoored Random Oracles (BROs)

random oracle

Backdoored Random Oracles (BROs)



Backdoored Random Oracles (BROs)

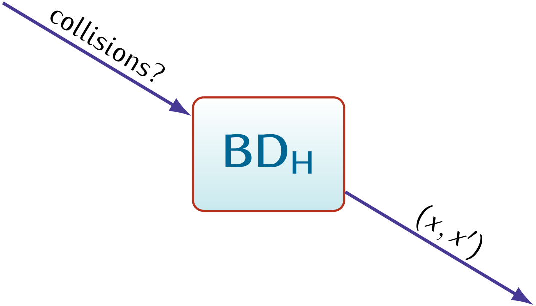


adaptive and unrestricted access to the backdoor oracle

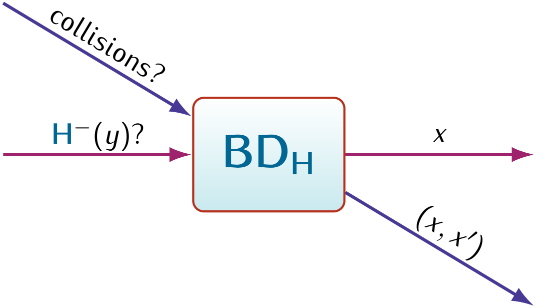
Backdoor Capabilities

BD_H

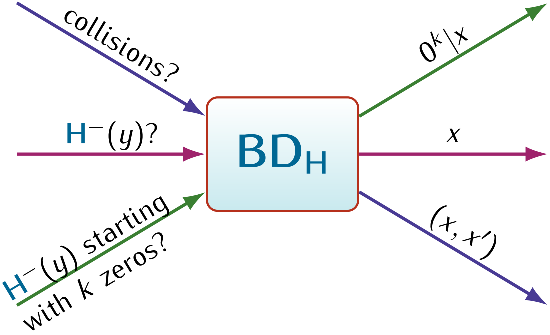
Backdoor Capabilities



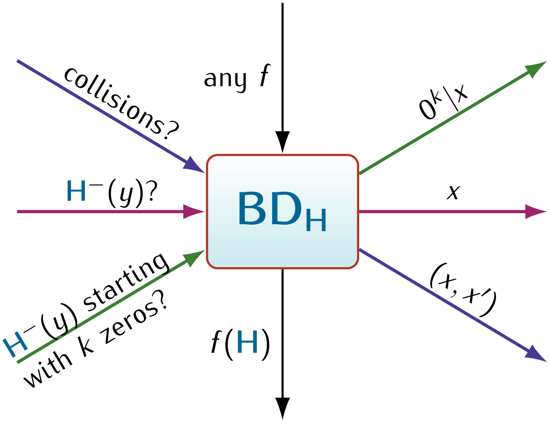
Backdoor Capabilities



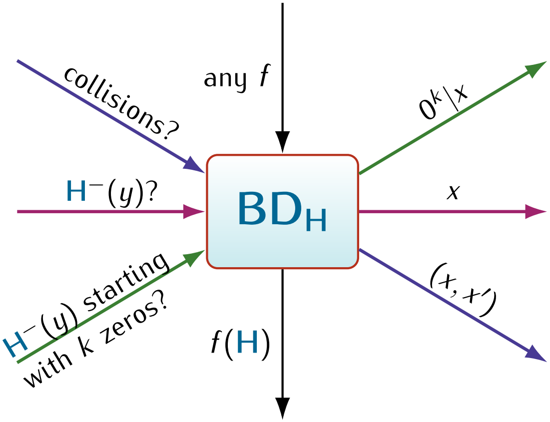
Backdoor Capabilities



Backdoor Capabilities

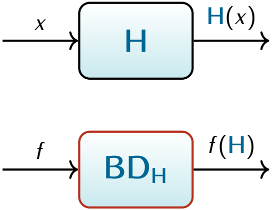


Backdoor Capabilities

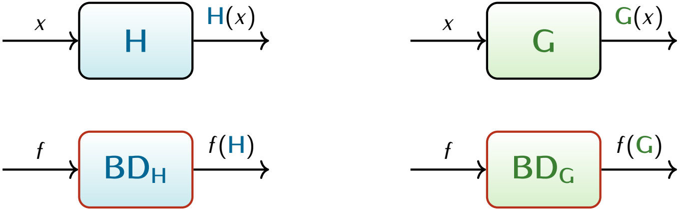


no security is possible...

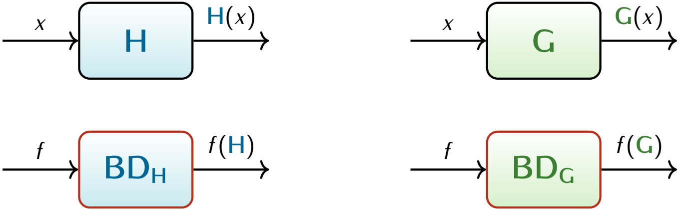
Combining BROs



Combining BROs



Combining BROs

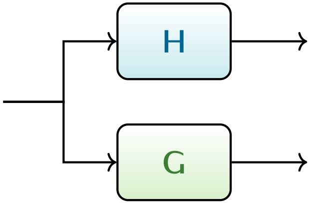


Can we combine two **independent** but **backdoored** hash functions to build one that is secure against adversaries with access to **both** backdoor oracles?

Combiners

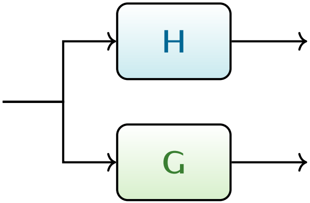
Combiners

concatenation:

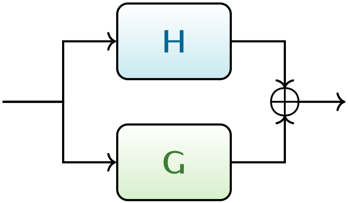


Combiners

concatenation:

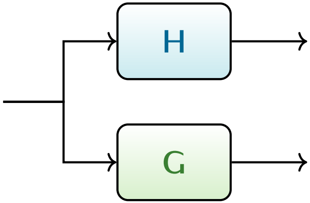


xor:

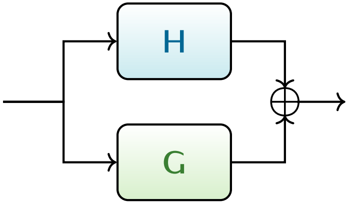


Combiners

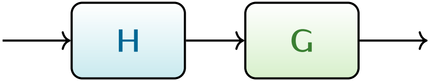
concatenation:



xor:

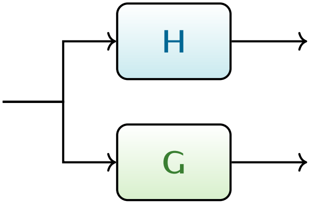


cascade:

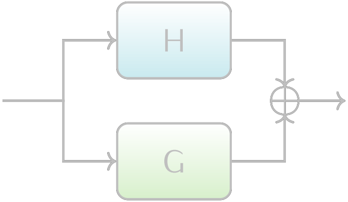


Combiners

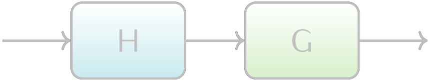
concatenation:



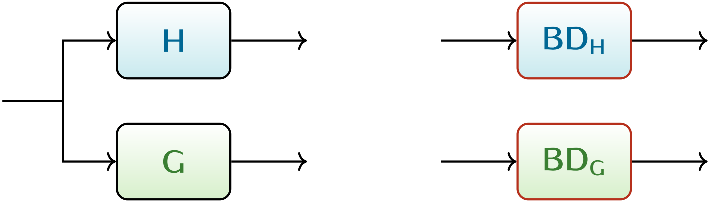
xor:



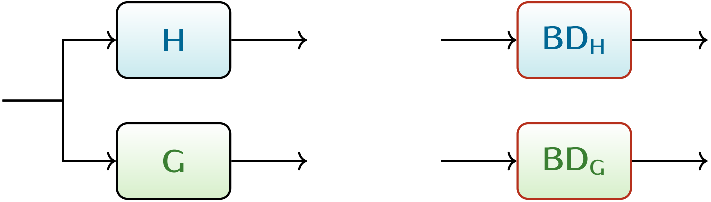
cascade:



Concatenation in 2-BRO

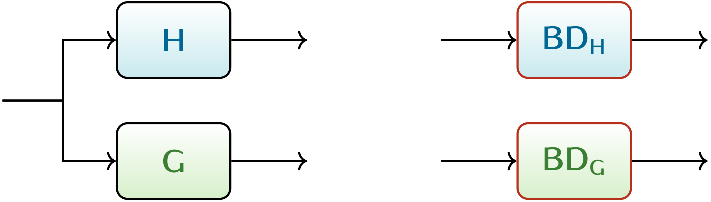


Concatenation in 2-BRO



one-way security?

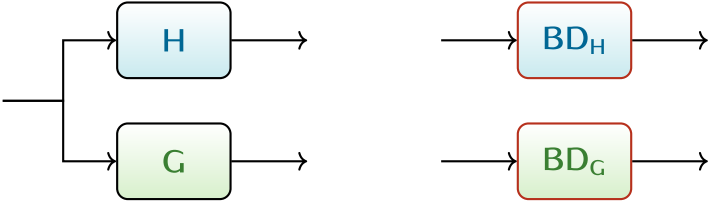
Concatenation in 2-BRO



one-way security? pseudorandomness?

collision-resistance?

Concatenation in 2-BRO

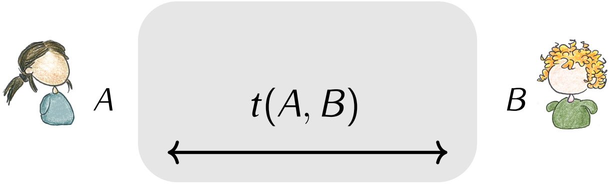


one-way security?   pseudorandomness?

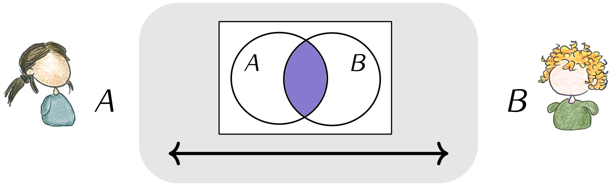
collision-resistance?

We need results from **communication complexity**...

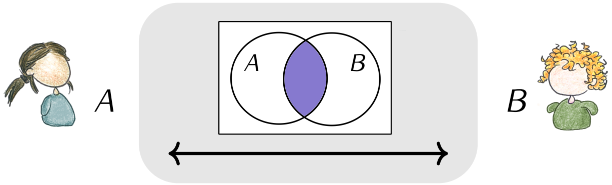
Communication Complexity



Communication Complexity



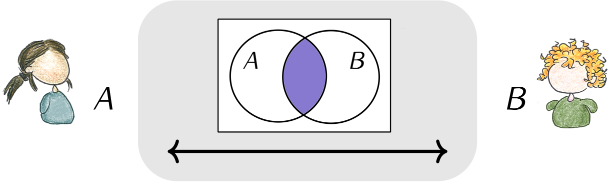
Communication Complexity



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

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

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

$$\mathsf{CC}(\mathsf{DISJ}) \geq \Omega(2^{n/2}).$$

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]

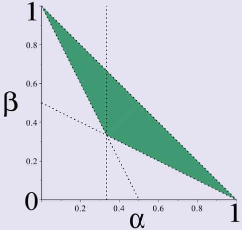
Communication Complexity - Generalized

$\|A\|, \|B\|$	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,

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

for (α, β) in the feasible region.



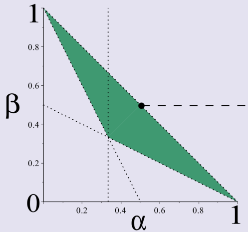
Communication Complexity – Generalized

$\|A\|, \|B\|$	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,

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

for (α, β) in the feasible region.



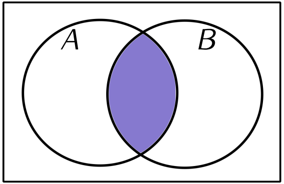
One-Way Security of Concatenation Combiner

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

One-Way Security of Concatenation Combiner

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

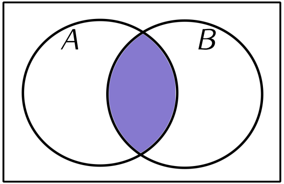
$$\text{Let } A := \mathsf{H}^{-}(\mathsf{u}) \quad \text{and} \quad B := \mathsf{G}^{-}(\mathsf{v}).$$



One-Way Security of Concatenation Combiner

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

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



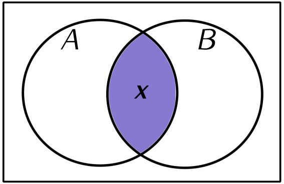
Then, for any pre-image x of $\mathsf{u}|\mathsf{v}$:

$$x \in \mathsf{H}^{-}(\mathsf{u}) \quad \text{and} \quad x \in \mathsf{G}^{-}(\mathsf{v})$$

One-Way Security of Concatenation Combiner

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

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



Then, for any pre-image x of $\mathsf{u}|\mathsf{v}$:

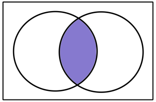
$x \in \mathsf{H}^{-}(\mathsf{u})$ and $x \in \mathsf{G}^{-}(\mathsf{v})$

Hence, $x \in A \cap B$.

Security of Concatenation in 2-BRO

One-Way Security

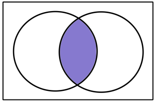
Inverting a random value u|v is as hard as the **set-intersection** problem.



Security of Concatenation in 2-BRO

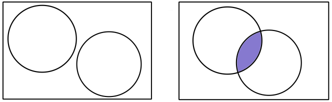
One-Way Security

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



Pseudorandomness

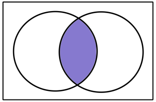
Deciding whether a random value u|v has a pre-image is as hard as the **set-disjointness** problem.



Security of Concatenation in 2-BRO

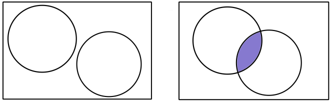
One-Way Security

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



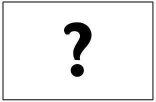
Pseudorandomness

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 ...

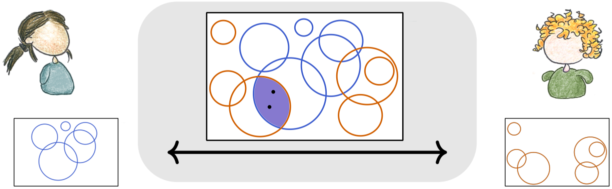


Collision-Resistance of Concatenation

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

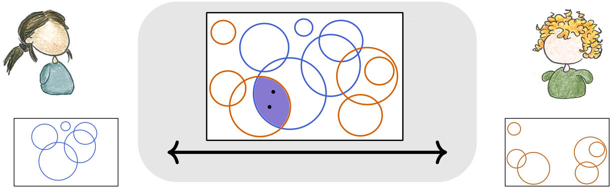
Collision-Resistance of Concatenation

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.



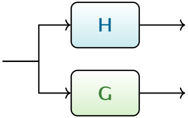
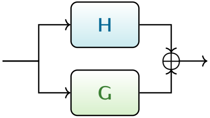
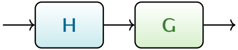
Collision-Resistance of Concatenation

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



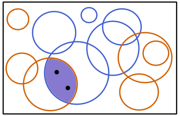
Hardness of the above problem is open.

Combiners and Security Notions

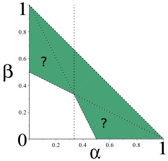
	OW	PRG	CR
	✓	✓	??
	✓	?	??
	✓	✓	??

Open Problems

- lower bound for the multi-INT problem



- extend parameters for DISJ and INT



- combiners for other backdoored primitives

π E

Thank You.

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