ON DISTRIBUTIONAL COLLISION RESISTANT HASHING

Eylon Yogev
Technion

Joint Work with Ilan Komargodski (Cornell Tech)

CRYPTO 2018

ASK LESS OF A HASH FUNCTION AND IT IS LESS LIKELY TO DISAPPOINT!

Bellare-Rogaway ‘97

What is the “right” notion of hardness of finding collisions in a cryptographic hash function?

Depends on the application!

- Universal One-Way Hash Functions (UOWHF)
- Multiple Collision Resistant Hashing (MCRH)
- Collision Resistant Hashing (CRH)

- Storing passwords
- Delegation of computation
- Signatures
- POW/ Blockchains

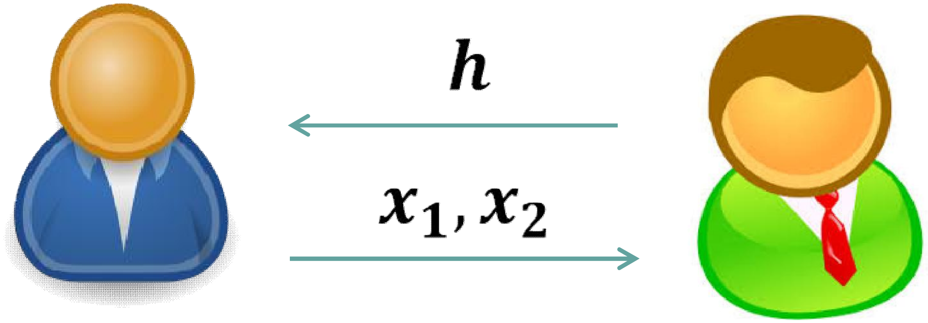
COLLISION RESISTANT HASHING (CRH)

A family H of functions such that:

1. Efficient: easy to sample $h \in H$ and compute $h(x)$
2. Compressing: $h: \{0,1\}^{2n} \rightarrow \{0,1\}^n$
3. Security:

CRH

Adv wins if
$\boldsymbol{h(x_1) = h(x_2)}$



UNIVERSAL ONE-WAY HASH FUNCTION (UOWHF)

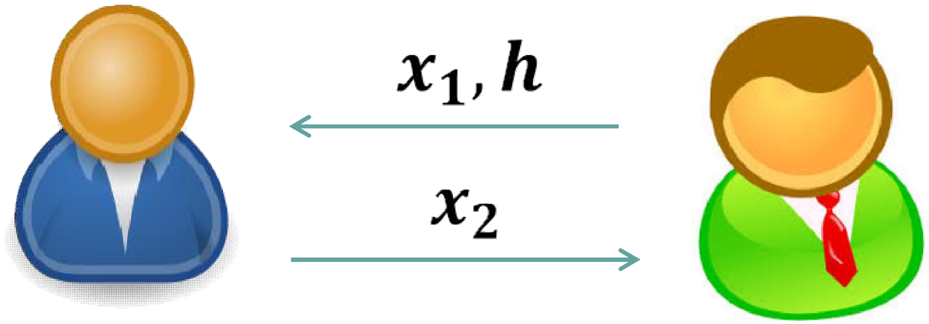
[Naor-Yung89]

A family H of functions such that:

1. Efficient: easy to sample $h \in H$ and compute $h(x)$
2. Compressing: $h: \{0,1\}^{2n} \to \{0,1\}^n$
3. Security:

UOWHF

Adv wins if
$\boldsymbol{h(x_1) = h(x_2)}$



MULTI COLLISION RESISTANT HASH (MCRH)

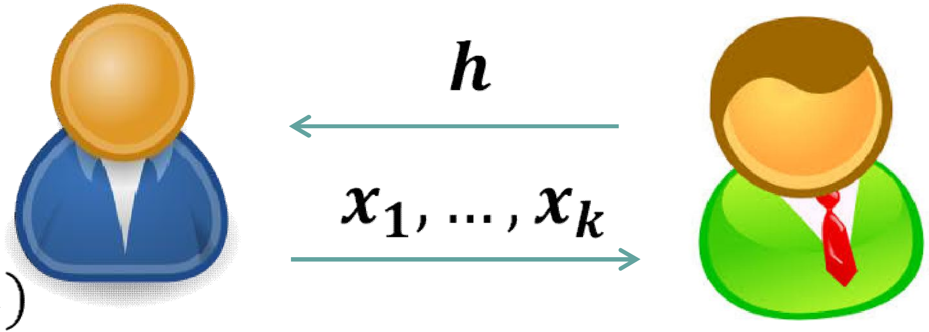
[Komargodski-Naor-Y17]

A family H of functions such that:

1. Efficient: easy to sample $h \in H$ and compute $h(x)$
2. Compressing: $h: \{0,1\}^{2n} \to \{0,1\}^n$
3. Security:

MCRH

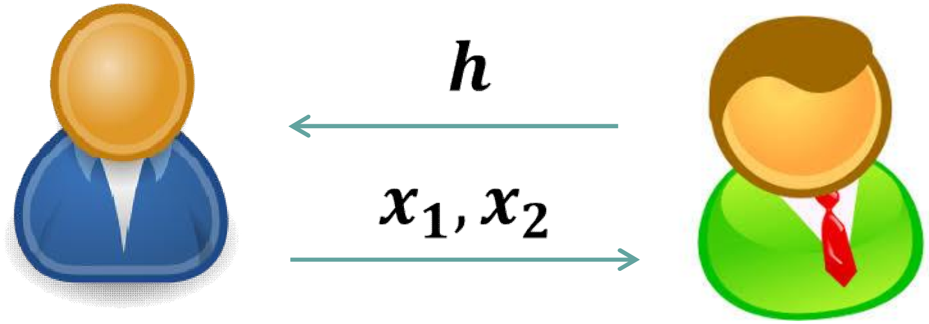
Adv wins if
$h(x_1) = \cdots = h(x_k)$



LWE, DL, Factoring…

CRH

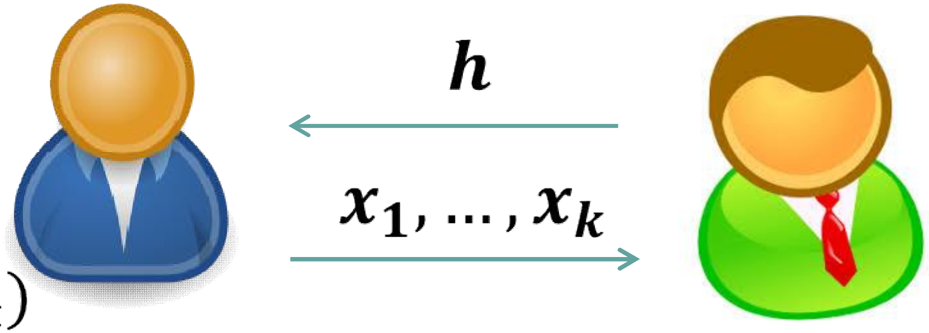
Adv wins if
$h(x_1) = h(x_2)$



EA*,Ramsey
[KNY17], [BDRV18], [BKP18], [KNY18]

MCRH

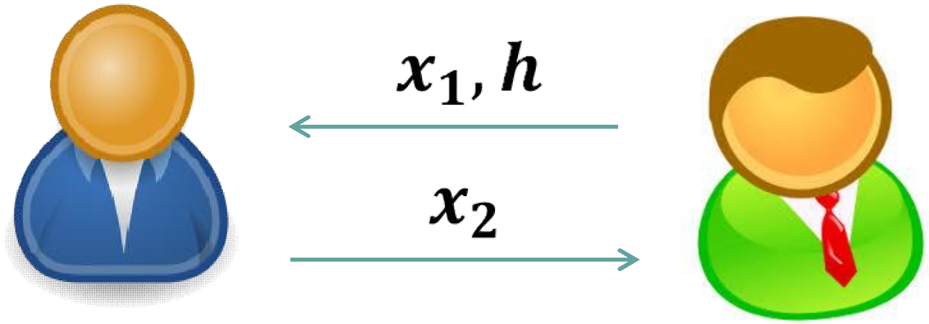
Adv wins if
$h(x_1) = \cdots = h(x_k)$



Any One-way function
[Naor-Yung89], [Rompel90], [Katz-Koo05]

UOWHF

Adv wins if
$h(x_1) = h(x_2)$



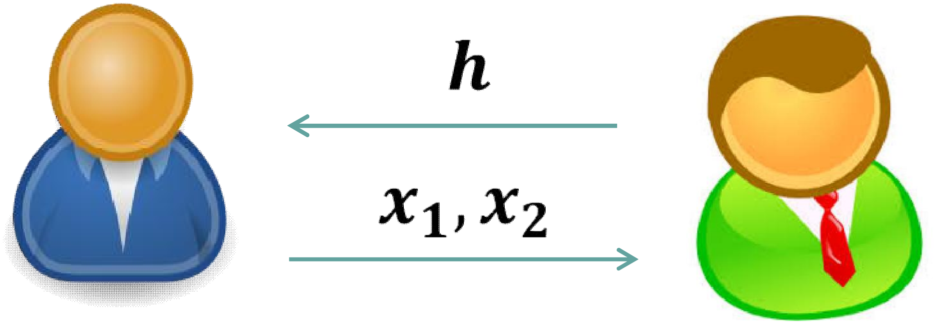
DISTRIBUTIONAL CRH [Dubrov-Ishai06]

A family H of functions such that:

1. Efficient: easy to sample $h \in H$ and compute $h(x)$
2. Compressing: $h: \{0,1\}^{2n} \rightarrow \{0,1\}^n$
3. Security:

dCRH

Adv wins if (x_1, x_2) "is a random collision"



DISTRIBUTIONAL CRH [Dubrov-Ishai06]

$\mathbf{COL}_h$:

1. Sample a random $x_1 \in \{0,1\}^{2n}$
2. Sample a random pre-image $x_2 \in h^{-1}(x_1)$
3. Output (x_1, x_2)

Negligible function

H is a dCRH if:

$$\Pr_{\mathrm{h}}[\Delta(\mathrm{A}(\mathrm{h}), \mathrm{COL}_{\mathrm{h}}) \leq \epsilon] \leq 1 - \epsilon$$

Statistical Distance

$$\Delta(X, Y) = \frac{1}{2} \sum_{x \in \Omega} |\Pr[X = x] - \Pr[Y = x]|$$

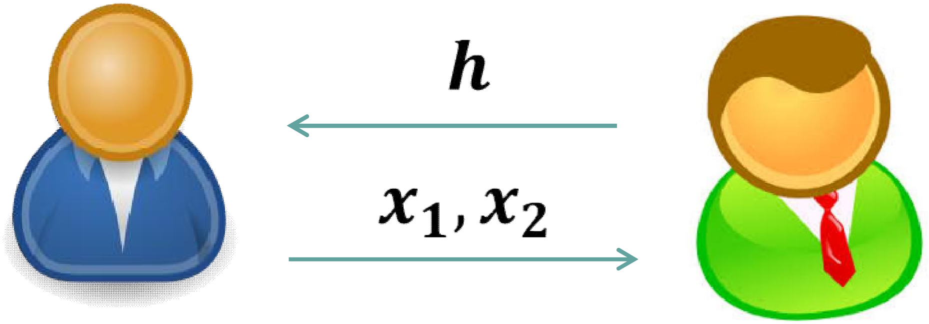
DISTRIBUTIONAL CRH [Dubrov-Ishai06]

A family H of functions such that:

1. Efficient: easy to sample $h \in H$ and compute $h(x)$
2. Compressing: $h: \{0,1\}^{2n} \rightarrow \{0,1\}^{n}$
3. Security:

dCRH

Adv wins if
$(x_1, x_2) \equiv COL_h$



FUN FACTS ABOUT DCRH

1. Introduced by Dubrov-Ishai06 in the context of randomness complexity in efficient sampling (win-win result)
2. A weak primitive:
   An adversary that commits to $h(x)$ might still be able to find all x': $h(x') = h(x)$ only with a skewed distribution!
3. Are analogous to distributional one-way functions; the adversary must find a random inverse.
   Impagliazzo-Luby89: distributional OWF $\leftrightarrow$ OWF
4. Black-box separated from one-way permutations (even with iO)

OUR RESULTS

We give 2 constructions of dCRH from different assumptions

One is black-box – one is not

One is efficient – one is not

One is explicit – one is not

MCRH ⇒ DCRH

Theorem: A non-black-box construction of a dCRH from any k-MCRH (for any constant k)

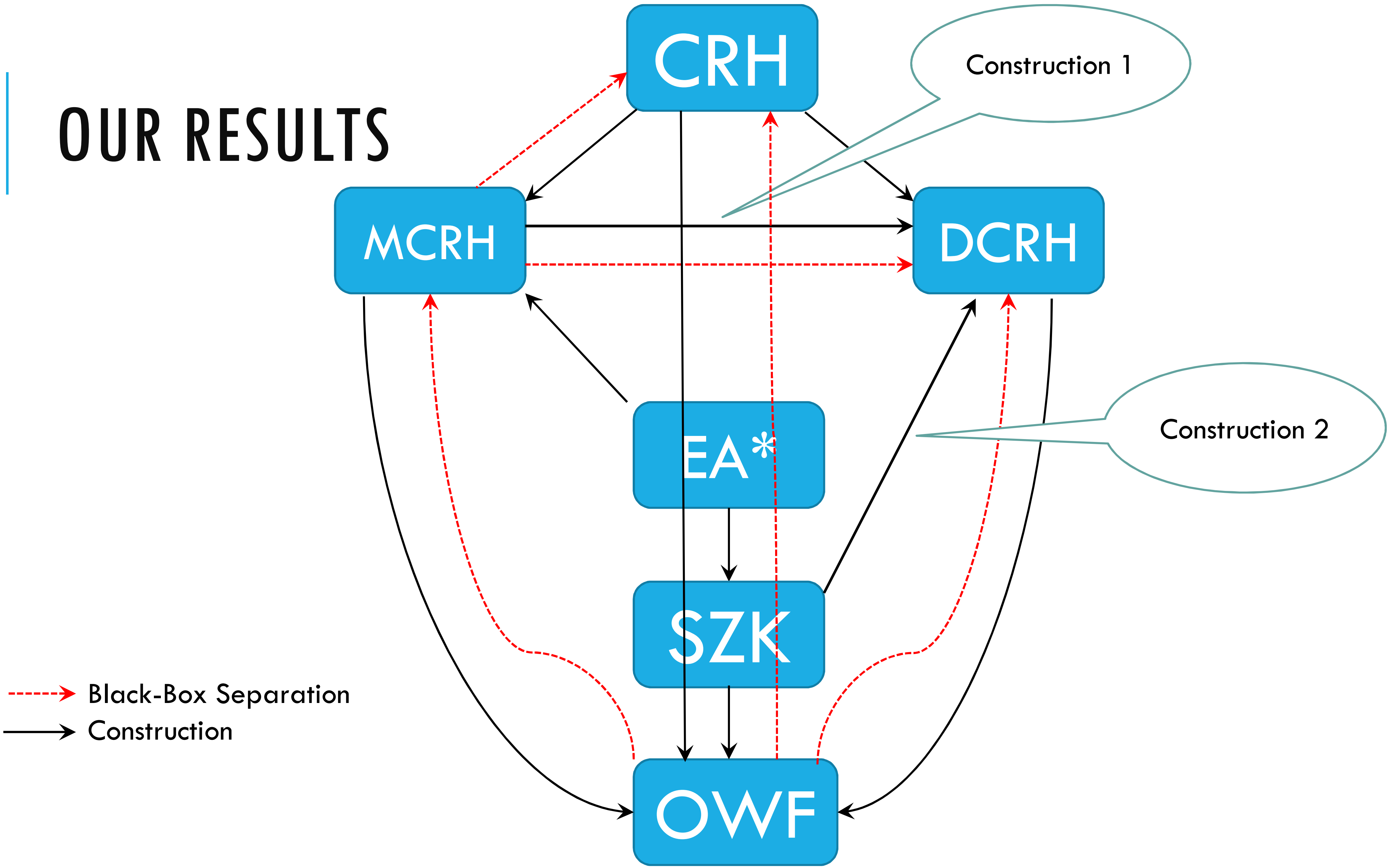
1. Proof is non-constructive: uses an adversary in a non-black-box way
2. Yields an infinitely-often dCRH
   (should merely serve as evidence of a construction)
3. Partially resolves an open question of [Berman-Degwekar-Rothblum-Vasudevan18]

SZK $\Rightarrow$ DCRH

Theorem: A construction of a dCRH from average-case hardness of SZK

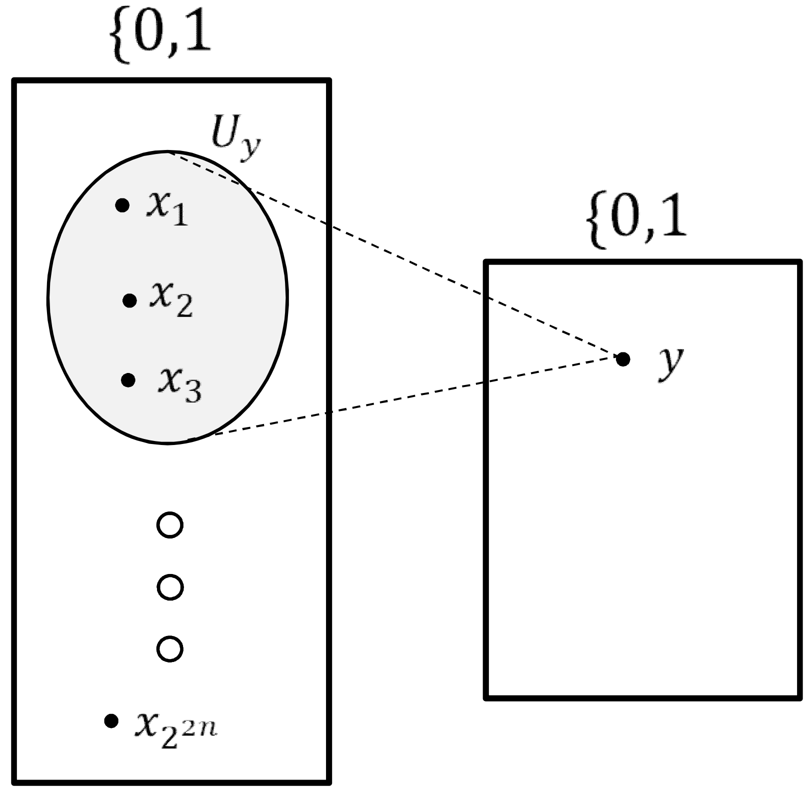
1. Previously SZK was not known to imply any form of hashing (except UOWHFs)
2. Since we know that:
   iO + OWP $\not\Rightarrow$ CRH [Asharov-Segev16]
   we get the corollary: iO + OWP $\not\Rightarrow$ SZK
   (previously shown by [Bitansky-Degwekar-Vaikuntanathan17])

OUR RESULTS


CRH
Construction 1
MCRH
DCRH
EA*
Construction 2
SZK
OWF
Black-Box Separation
Construction

PROOF 3-MCRH $\Rightarrow$ DCRH

1. Let $H = \{h: \{0,1\}^{2n} \rightarrow \{0,1\}^n\}$ be an 3-MCRH
2. Assume that dCRH **do not exist.**
3. There is an adversary A that can find a random collision in H
4. Fact: w.h.p. $h^{-1}(x)$ is exponentially large (over a random x)



PROOF

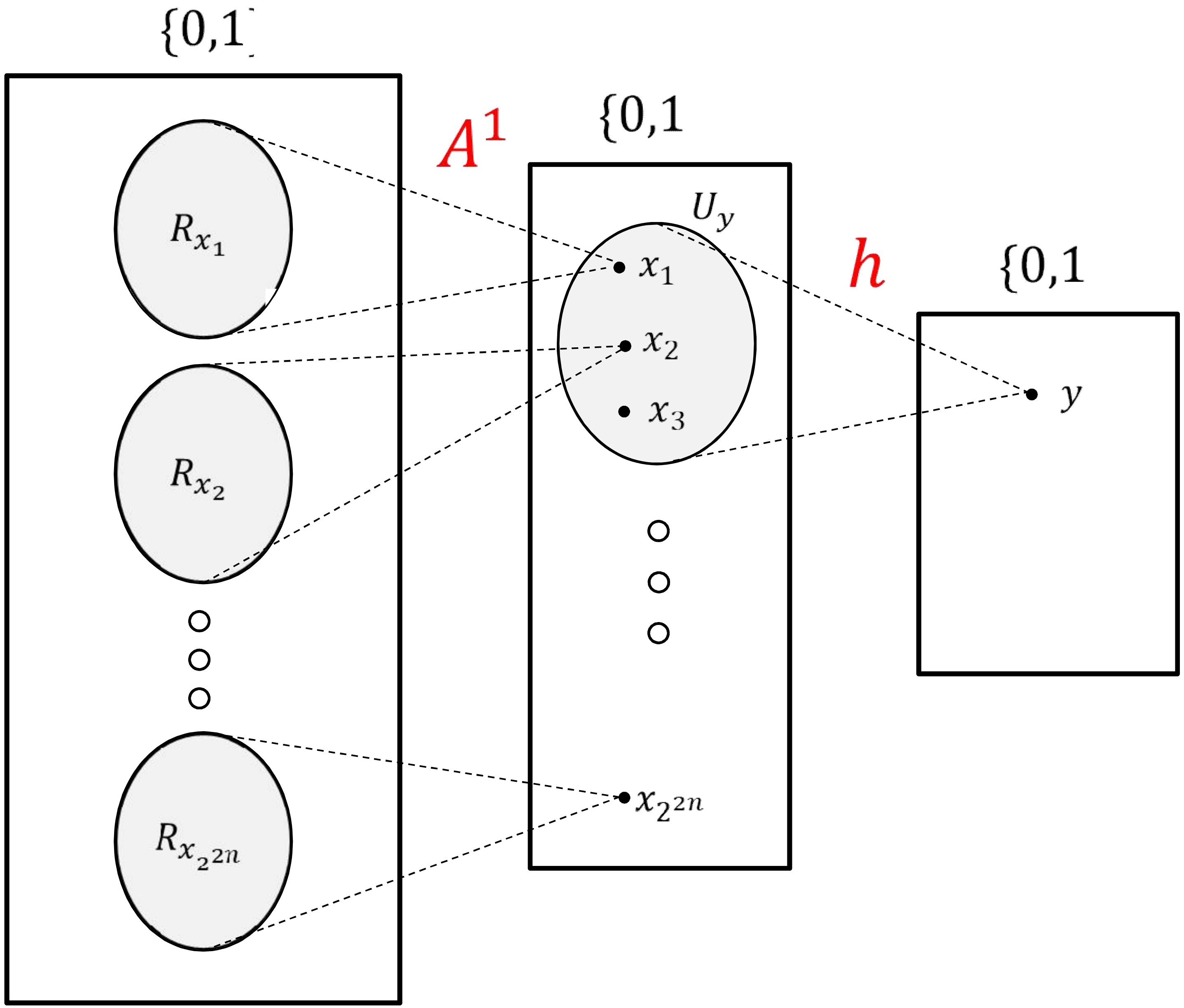
1. Define H' which depends on H **and on the adversary** A
2. $h' \in H'$ uses the input x as **random coins** to run A
3. Let $A^1(h;r) = x_1$ where $(x_1, x_2) \leftarrow A(h;r)$
4. Define:

$$h'(r) = h\big(A^1(h;r)\big)$$

CONSTRUCTION

<u>$h'(r)$:</u>

1. $(x_1, x_2) \leftarrow A(h; r)$
2. $y \leftarrow h(x_1)$
3. Output y



PROOF

1. Since H' is not a dCRH $\rightarrow \exists\, A'$ that breaks H'
2. We use A' and A to break H as a 3-MCRH

Break(h):

1. Define h': $h'(r) = h\left(A^1(h; r)\right)$
2. $(r_1, r_2) \leftarrow A'(h')$
3. $(x_1, x_2) \leftarrow A(h; r_1)$
4. $(x_3, x_4) \leftarrow A(h; r_2)$
5. Output (x_1, x_2, x_3)

PROOF

Claim 1: $h(x_1) = h(x_2) = h(x_3)$

Proof: r_1 is uniform $\rightarrow$

$A(h; r_1)$ succeeds w.h.p.

(r_1, r_2) are a collision $\rightarrow$

$h\left(A^1(h; r_1)\right) = h\left(A^1(h; r_2)\right) \rightarrow$

$h(x_1) = h(x_3)$

Break(h):

1. Define h': $h'(r) = h\left(A^1(h; r)\right)$
2. $(r_1, r_2) \leftarrow A'(h')$
3. $(x_1, x_2) \leftarrow A(h; r_1)$
4. $(x_3, x_4) \leftarrow A(h; r_2)$
5. Output (x_1, x_2, x_3)

PROOF

Claim 2: x_1, x_2, x_3 are distinct

Proof: r_1 is uniform $\rightarrow$

$x_2 \in_R h^{-1}(x_1) \rightarrow$

w.h.p. $x_2 \neq x_1$

Why would x_3 be distinct?

Break(h):

1. Define h': $h'(r) = h\big(A^1(h; r)\big)$
2. $(r_1, r_2) \leftarrow A'(h')$
3. $(x_1, x_2) \leftarrow A(h; r_1)$
4. $(x_3, x_4) \leftarrow A(h; r_2)$
5. Output (x_1, x_2, x_3)

PROOF

Why would x_3 be distinct?

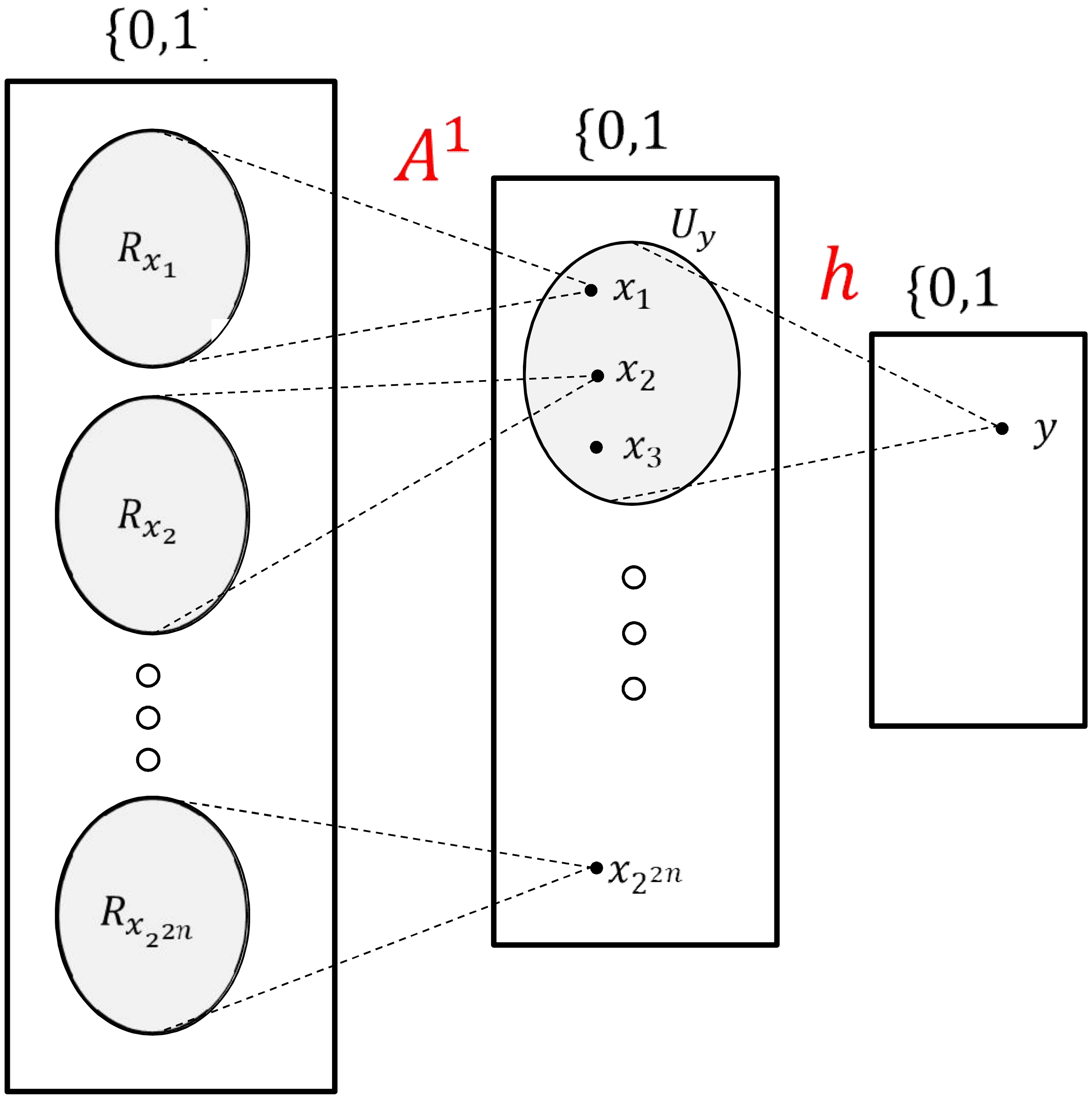
$\Pr[x_3 = x_1] = \Pr[r_2 \in R_{x_1}]$.

Since A is an dCRH adversary →

$|R_{x_1}| \approx |R_{x_2}|$.

r_2 is random s.t. $h'(r_1) = h'(r_2)$ →

$\Pr[r_2 \in R_{x_1}] \approx \Pr[r_2 \in R_{x_i}]$



GOING BEYOND 3-MCRH

Can we hope to find more than a 3-way collision?

Recall that it might hold that $h(x_4) \neq h(x_3)$.

A finds a random collision $\rightarrow$ Break(h) finds a 3-way collision

GOING BEYOND 3-MCRH

Can we hope to find more than a 3-way collision?

Recall that it might hold that $h(x_4) \neq h(x_3)$.

A finds a random collision $\rightarrow$ Break(h) finds a random 3-collision

GOING BEYOND 3-MCRH

Can we hope to find more than a 3-way collision?

Recall that it might hold that $h(x_4) \neq h(x_3)$.

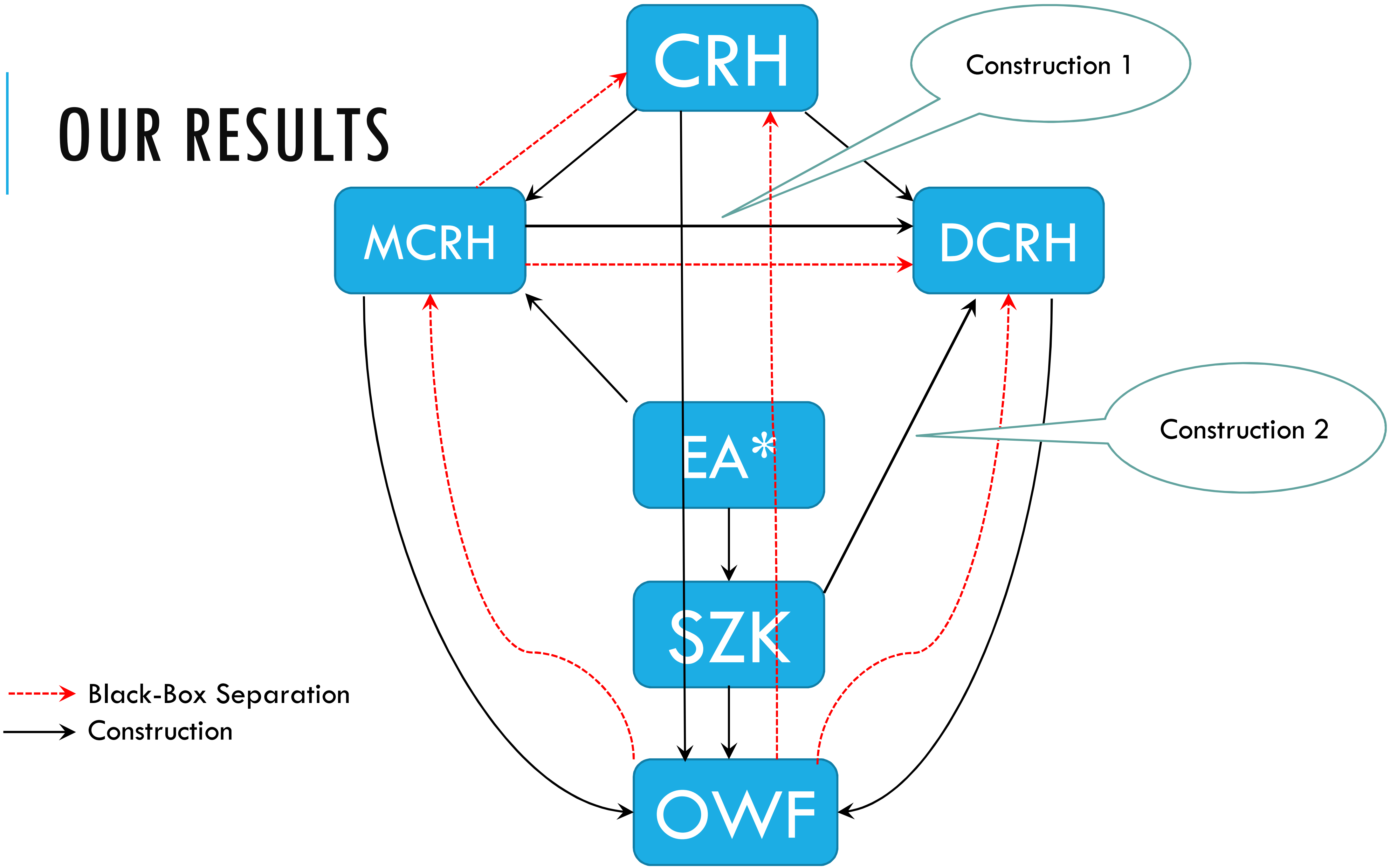
A finds a random collision→ Break(h) finds a random 3-collision

Break(h) finds a random 3-collision → Break'(h) finds a random 4-collision

Break(h) finds a random k-collision → Break'(h) finds a random (k+1)-collision

Works for any constant k.

OUR RESULTS


CRH
MCRH
DCRH
EA*
SZK
OWF
Construction 1
Construction 2
Black-Box Separation
Construction

OPEN PROBLEMS