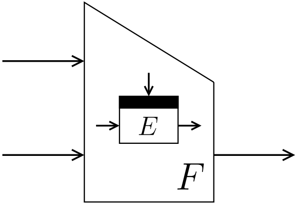
Indifferentiability of Double Length Compression Functions

Bart Mennink
KU Leuven

IMA Cryptography and Coding
December 18, 2013

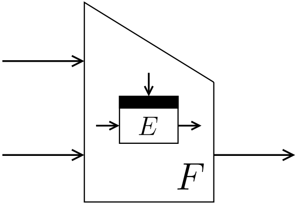
Block Cipher Based Hashing



$2n$-to-n-bit F using n-bit cipher E

- Davies-Meyer ('84), PGV ('93), ...
- MD5 ('92), SHA-1 ('95), SHA-2 ('01), ...

Block Cipher Based Hashing



$2n$-to-n-bit F using n-bit cipher E

- Davies-Meyer ('84), PGV ('93), ...
- MD5 ('92), SHA-1 ('95), SHA-2 ('01), ...

Same underlying primitive but larger compression function?

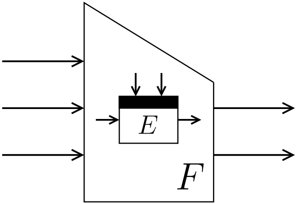
Double Block Length Hashing

$3n$-to-$2n$-bit F still using n-bit cipher E

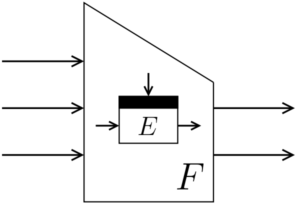
Double Block Length Hashing

$3n$-to-$2n$-bit F still using n-bit cipher E

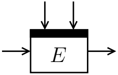
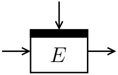
E with $2n$-bit Key
(since '92)



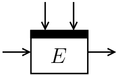
E with n-bit Key
(since '88)

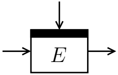


State of the Art

compression function	E-calls	collision security	preimage security	underlying cipher
				 $2n$-bit key
				 n-bit key

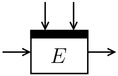
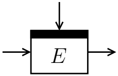
State of the Art

compression function	E-calls	collision security	preimage security	underlying cipher
Stam's ('08 -'10)	1	2^n	2^n	
Tandem-DM ('92)	2	2^n	2^{2n}	
Abreast-DM ('92)	2	2^n	2^{2n}	
Hirose's ('06)	2	2^n	2^{2n}	$2n$-bit key
Hirose-class ('04)	2	2^n	2^n	
Özen-Stam-class ('09)	2	2^n	2^n	

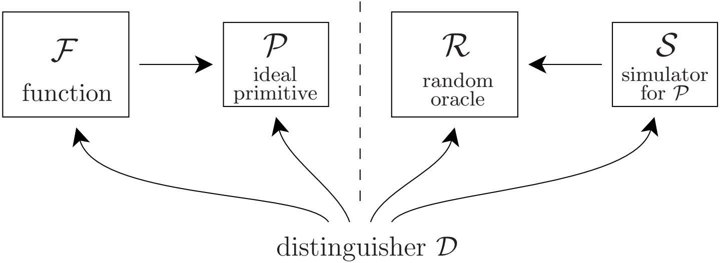


n-bit key

State of the Art

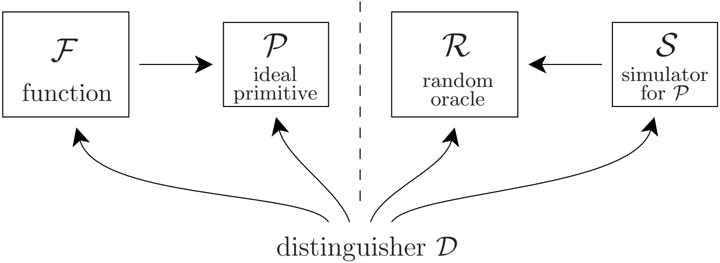
compression function	E-calls	collision security	preimage security	underlying cipher
Stam's ('08 -'10)	1	2^n	2^n	
Tandem-DM ('92)	2	2^n	2^{2n}	
Abreast-DM ('92)	2	2^n	2^{2n}	
Hirose's ('06)	2	2^n	2^{2n}	
Hirose-class ('04)	2	2^n	2^n	$2n$-bit key
Özen-Stam-class ('09)	2	2^n	2^n	
MDC-2 ('88)	2	$2^{n/2}$	2^n	
MJH ('11)	2	$2^{n/2}$	2^n	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	
Ours ('12)	3	2^n	$2^{3n/2}$	n-bit key
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$	

Indifferentiability



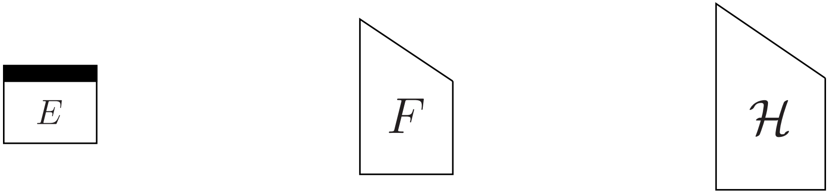
- Indifferentiability of function $\mathcal{F}$ from a random oracle
- $\mathcal{F}^{\mathcal{P}}$ is indifferentiable from $\mathcal{R}$ if $\exists$ simulator $\mathcal{S}$ such that $(\mathcal{F}, \mathcal{P})$ and $(\mathcal{R}, \mathcal{S})$ indistinguishable

Indifferentiability

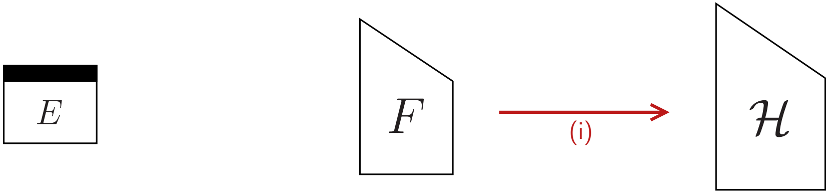


- Indifferentiability of function $\mathcal{F}$ from a random oracle
- $\mathcal{F}^{\mathcal{P}}$ is indifferentiable from $\mathcal{R}$ if $\exists$ simulator $\mathcal{S}$ such that $(\mathcal{F}, \mathcal{P})$ and $(\mathcal{R}, \mathcal{S})$ indistinguishable
- No structural design flaws
- Well-suited for composition

Composition



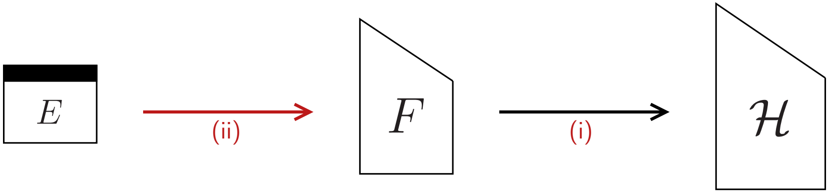
Composition



(i) First hash-function indifferentiability results

- Chop-MD with ideal $F \longrightarrow$ indifferentiable

Composition



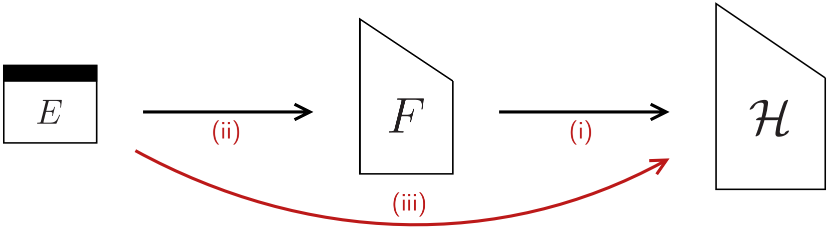
(i) First hash-function indifferentiability results

- Chop-MD with ideal $F \longrightarrow$ indifferentiable

(ii) Most obvious second step (composition)

- But Davies-Meyer with ideal $E \longrightarrow$ differentiable

Composition



(i) First hash-function indifferentiability results

- Chop-MD with ideal F $\longrightarrow$ indifferentiable

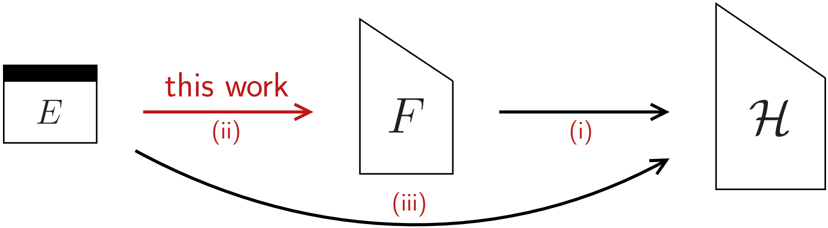
(ii) Most obvious second step (composition)

- But Davies-Meyer with ideal E $\longrightarrow$ differentiable

(iii) Researchers focus on direct proofs

- Chop-MD with Davies-Meyer and ideal E $\longrightarrow$ indifferentiable

Composition

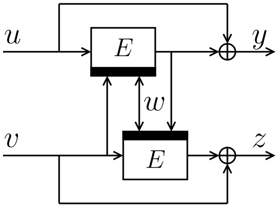


(i) First hash-function indifferentiability results
  - Chop-MD with ideal $F \longrightarrow$ indifferentiable

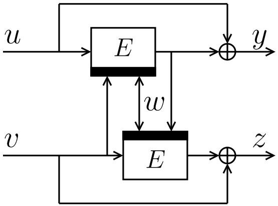
(ii) Most obvious second step (composition)
  - But Davies-Meyer with ideal $E \longrightarrow$ differentiable

(iii) Researchers focus on direct proofs
  - Chop-MD with Davies-Meyer and ideal $E \longrightarrow$ indifferentiable

Many Constructions Differentiable: Tandem-DM



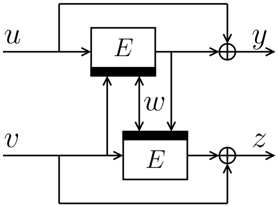
Many Constructions Differentiable: Tandem-DM



Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

- Differentiability: construct a distinguisher that tricks any simulator

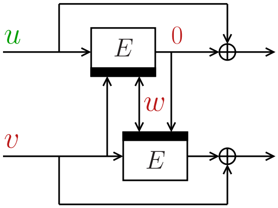
Many Constructions Differentiable: Tandem-DM



Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

- Differentiability: construct a distinguisher that tricks any simulator
- Focus on $\mathrm{TDM}(u, v, w) = (u, z)$ for some u, v, w, z

Many Constructions Differentiable: Tandem-DM

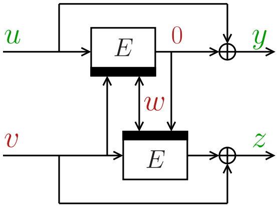


Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

- Differentiability: construct a distinguisher that tricks any simulator
- Focus on $\mathrm{TDM}(u, v, w) = (u, z)$ for some u, v, w, z

Real world (TDM, E)
$\mathcal{D}$ queries $E^{-1}(v \| w, 0) \to u$

Many Constructions Differentiable: Tandem-DM

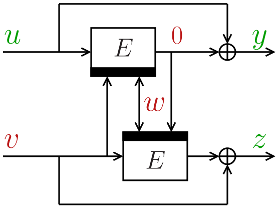


Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

- Differentiability: construct a distinguisher that tricks any simulator
- Focus on $\mathrm{TDM}(u, v, w) = (u, z)$ for some u, v, w, z

Real world (TDM, E)
$\mathcal{D}$ queries $E^{-1}(v \| w, 0) \to u$ $\mathcal{D}$ queries $\mathrm{TDM}(u, v, w) \to (y, z)$

Many Constructions Differentiable: Tandem-DM

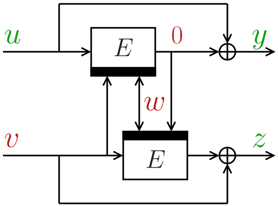


Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

- Differentiability: construct a distinguisher that tricks any simulator
- Focus on $\mathrm{TDM}(u, v, w) = (u, z)$ for some u, v, w, z

Real world (TDM, E)
$\mathcal{D}$ queries $E^{-1}(v \| w, 0) \to u$ $\mathcal{D}$ queries $\mathrm{TDM}(u, v, w) \to (y, z)$ $u = y$ with probability 1

Many Constructions Differentiable: Tandem-DM



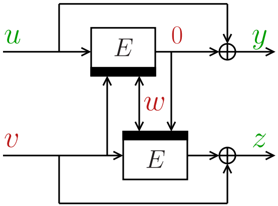
Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

- Differentiability: construct a distinguisher that tricks any simulator
- Focus on $\mathrm{TDM}(u, v, w) = (u, z)$ for some u, v, w, z

Real world (TDM, E)
$\mathcal{D}$ queries $E^{-1}(v \| w, 0) \to u$
$\mathcal{D}$ queries $\mathrm{TDM}(u, v, w) \to (y, z)$
$u = y$ with probability 1

Simulated world $(\mathcal{R}, \mathcal{S})$
$\mathcal{D}$ queries $\mathcal{S}^{-1}(v \| w, 0) \to u$
$\mathcal{D}$ queries $\mathcal{R}(u, v, w) \to (y, z)$

Many Constructions Differentiable: Tandem-DM

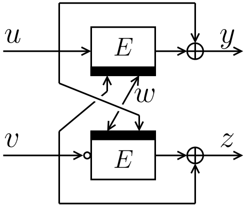


Tandem-DM differentiable from $\mathcal{R}$ in 2 queries

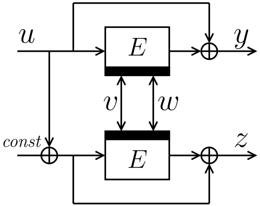
- Differentiability: construct a distinguisher that tricks any simulator
- Focus on $\mathrm{TDM}(u, v, w) = (u, z)$ for some u, v, w, z

Real world (TDM, E)	Simulated world $(\mathcal{R}, \mathcal{S})$
$\mathcal{D}$ queries $E^{-1}(v\|w, 0) \to u$	$\mathcal{D}$ queries $\mathcal{S}^{-1}(v\|w, 0) \to u$
$\mathcal{D}$ queries $\mathrm{TDM}(u, v, w) \to (y, z)$	$\mathcal{D}$ queries $\mathcal{R}(u, v, w) \to (y, z)$
$u = y$ with probability 1	$u = y$ with probability $O(1/2^n)$

Many Constructions Differentiable: Other Schemes (1)



Abreast-DM

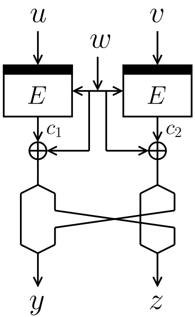


Hirose's

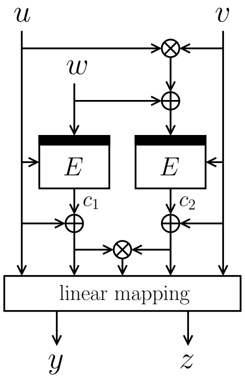
. . .

. . .

Many Constructions Differentiable: Other Schemes (2)



MDC-2

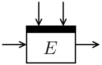
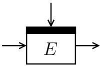


Jetchev-Özen-Stam's

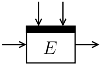
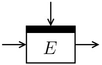
. . .

. . .

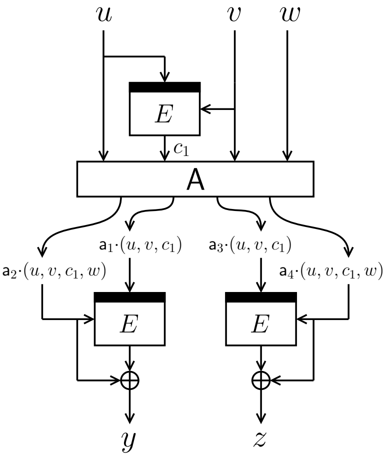
State of the Art

compression function	E-calls	collision security	preimage security	indifferen-tiability	underlying cipher
Stam's ('08 - '10)	1	2^n	2^n	**2**	
Tandem-DM ('92)	2	2^n	2^{2n}	**2**	
Abreast-DM ('92)	2	2^n	2^{2n}	**2**	
Hirose's ('06)	2	2^n	2^{2n}	**2**	$2n$-bit key
Hirose-class ('04)	2	2^n	2^n	**2**	
Özen-Stam-class ('09)	2	2^n	2^n	**2**	
MDC-2 ('88)	2	$2^{n/2}$	2^n	**2**	
MJH ('11)	2	$2^{n/2}$	2^n	**2**	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	**2**	
Ours ('12)	3	2^n	$2^{3n/2}$		n-bit key
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$		

State of the Art

compression function	E-calls	collision security	preimage security	indifferen-tiability	underlying cipher
Stam's ('08 - '10)	1	2^n	2^n	**2**	
Tandem-DM ('92)	2	2^n	2^{2n}	**2**	
Abreast-DM ('92)	2	2^n	2^{2n}	**2**	
Hirose's ('06)	2	2^n	2^{2n}	**2**	$2n$-bit key
Hirose-class ('04)	2	2^n	2^n	**2**	
Özen-Stam-class ('09)	2	2^n	2^n	**2**	
MDC-2 ('88)	2	$2^{n/2}$	2^n	**2**	
MJH ('11)	2	$2^{n/2}$	2^n	**2**	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	**2**	
Ours ('12)	3	2^n	$2^{3n/2}$	**??**	n-bit key
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$	**??**	

Our Construction

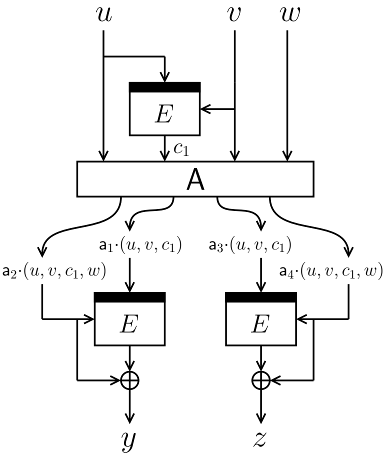


- F^3_{A} indexed by matrix A:

$$\mathsf{A} = \begin{pmatrix} \mathsf{a}_1 \\ \mathsf{a}_2 \\ \mathsf{a}_3 \\ \mathsf{a}_4 \end{pmatrix} = \begin{pmatrix} \mathsf{a}_{11} & \mathsf{a}_{12} & \mathsf{a}_{13} & 0 \\ \mathsf{a}_{21} & \mathsf{a}_{22} & \mathsf{a}_{23} & \mathsf{a}_{24} \\ \mathsf{a}_{31} & \mathsf{a}_{32} & \mathsf{a}_{33} & 0 \\ \mathsf{a}_{41} & \mathsf{a}_{42} & \mathsf{a}_{43} & \mathsf{a}_{44} \end{pmatrix}$$

- Math over finite field $GF(2^n)$

Our Construction

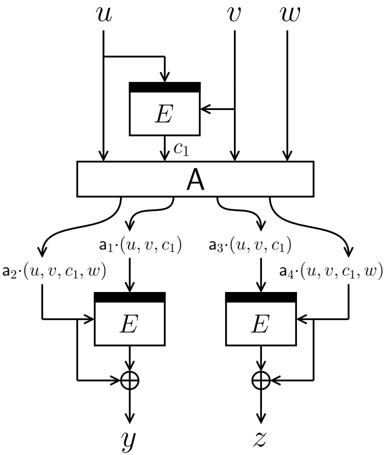


- F^3_{A} indexed by matrix A:

$$\mathsf{A} = \begin{pmatrix} \mathsf{a}_1 \\ \mathsf{a}_2 \\ \mathsf{a}_3 \\ \mathsf{a}_4 \end{pmatrix} = \begin{pmatrix} \mathsf{a}_{11} & \mathsf{a}_{12} & \mathsf{a}_{13} & 0 \\ \mathsf{a}_{21} & \mathsf{a}_{22} & \mathsf{a}_{23} & \mathsf{a}_{24} \\ \mathsf{a}_{31} & \mathsf{a}_{32} & \mathsf{a}_{33} & 0 \\ \mathsf{a}_{41} & \mathsf{a}_{42} & \mathsf{a}_{43} & \mathsf{a}_{44} \end{pmatrix}$$

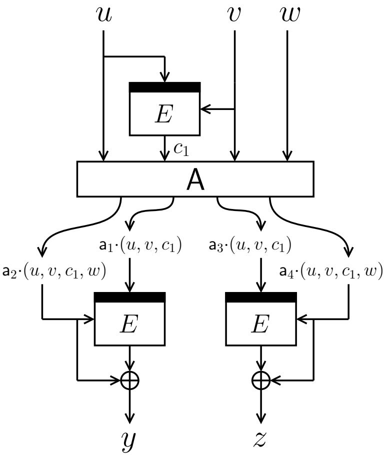
- Math over finite field $GF(2^n)$
- If A invertible and $\mathsf{a}_{24}, \mathsf{a}_{44} \neq 0$, any two E evaluations define (inputs to) third one

Indifferentiability



$$\mathbf{adv}^{\mathrm{iff}}_{F^3_{\mathsf{A}},\mathcal{S}}(q) = \Theta\left(\frac{q^2}{2^n}\right)$$

Indifferentiability

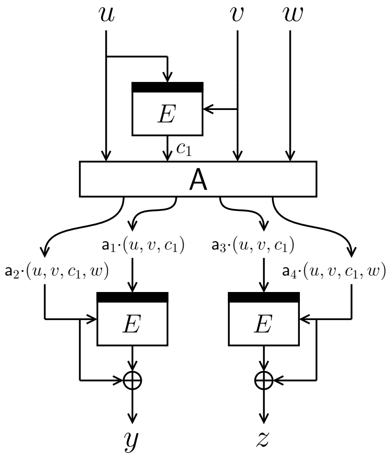


$$\mathbf{adv}^{\text{iff}}_{F^3_{\mathsf{A}}, \mathcal{S}}(q) = \Theta\left(\frac{q^2}{2^n}\right)$$

Simulator $\mathcal{S}$:

- "Look like E but comply with $\mathcal{R}$"

Indifferentiability

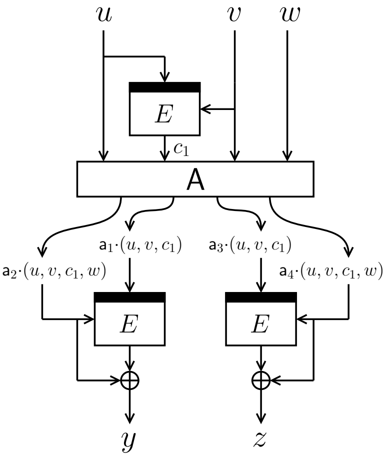


$$\mathbf{adv}^{\mathrm{iff}}_{F^3_{\mathsf{A}},\mathcal{S}}(q) = \Theta\left(\frac{q^2}{2^n}\right)$$

Simulator $\mathcal{S}$:

- "Look like E but comply with $\mathcal{R}$"
- If query at bottom for existing top query: consult $\mathcal{R}$
- Otherwise: behave like ideal E

Indifferentiability



$$\mathbf{adv}^{\mathrm{iff}}_{F^3_{\mathsf{A}}, \mathcal{S}}(q) = \Theta\left(\frac{q^2}{2^n}\right)$$

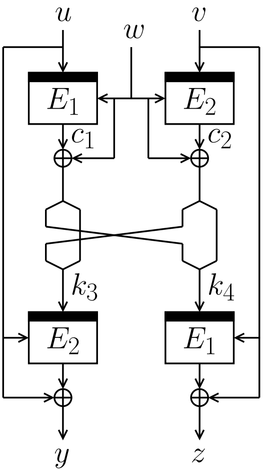
Simulator $\mathcal{S}$:

- "Look like E but comply with $\mathcal{R}$"
- If query at bottom for existing top query: consult $\mathcal{R}$
- Otherwise: behave like ideal E

$\mathcal{S}$ fails if:

1) Top query hits bottom query
2) Top query hits other top query (in a_1 or a_3)

MDC-4

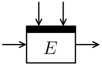
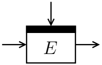


$$\mathbf{adv}^{\mathrm{iff}}_{\text{MDC-4},\mathcal{S}}(q) = \Theta\left(\frac{q^2}{2^{n/2}}\right)$$

Simulator $\mathcal{S}$:

- Based on same principles

Conclusions

compression function	E-calls	collision security	preimage security	indifferen-tiability	underlying cipher
Stam's ('08 - '10)	1	2^n	2^n	$\mathbf{2}$	
Tandem-DM ('92)	2	2^n	2^{2n}	$\mathbf{2}$	
Abreast-DM ('92)	2	2^n	2^{2n}	$\mathbf{2}$	
Hirose's ('06)	2	2^n	2^{2n}	$\mathbf{2}$	$2n$-bit key
Hirose-class ('04)	2	2^n	2^n	$\mathbf{2}$	
Özen-Stam-class ('09)	2	2^n	2^n	$\mathbf{2}$	
MDC-2 ('88)	2	$2^{n/2}$	2^n	$\mathbf{2}$	
MJH ('11)	2	$2^{n/2}$	2^n	$\mathbf{2}$	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	$\mathbf{2}$	
Ours ('12)	3	2^n	$2^{3n/2}$	$\mathbf{2^{n/2}}$	n-bit key
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$	$\mathbf{2^{n/4}}$	

Research Directions

- 2-call scheme with comparable security?
- Impossibility results?
- Indifferentiability beyond $2^{n/2}$?
- Iteration?

Thank you for your attention!