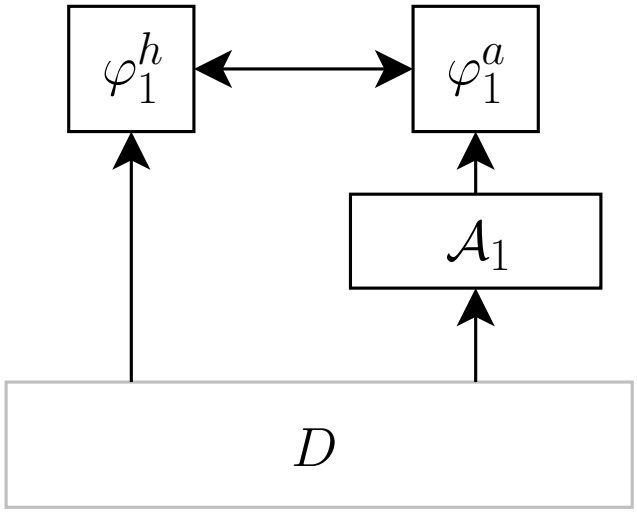
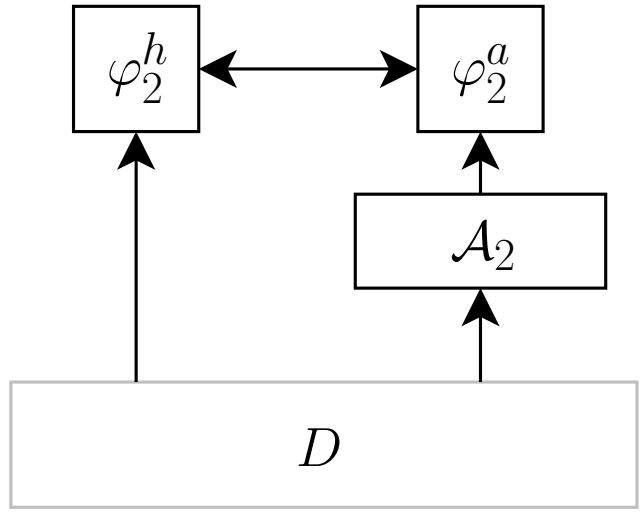
Impossibility Results for Indifferentiability with Resets

Atul Luykx, Elena Andreeva, Bart Mennink, and Bart Preneel
KU Leuven

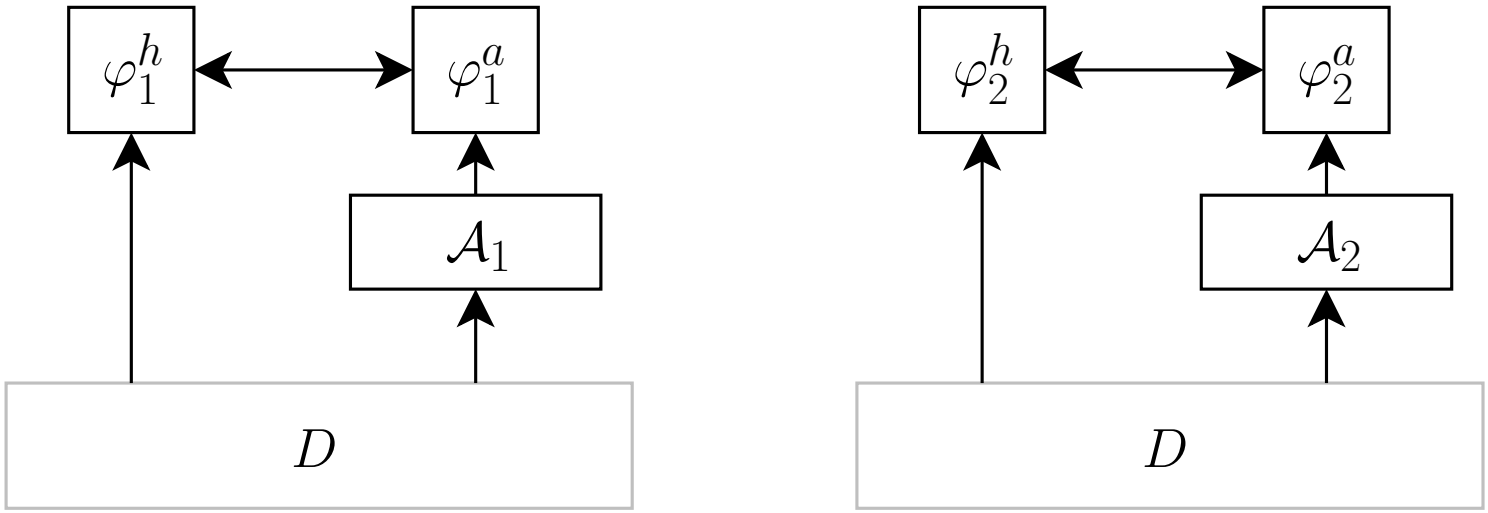
ESC 2013 — January 18, 2012

Indifferentiability





Indifferentiability

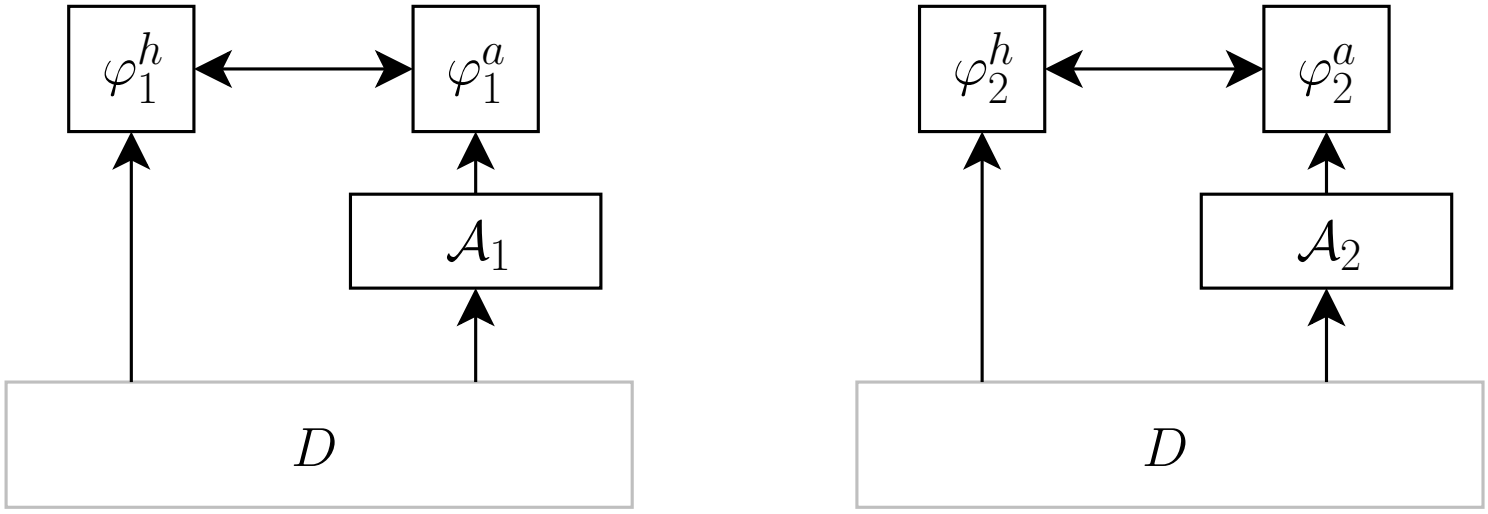


Definition

Functionality φ_1 is at least as secure as φ_2 if for any distinguisher D and adversary $\mathcal{A}_1$ there exist adversary $\mathcal{A}_2$ such that

$$\left|\mathbf{Pr}\left(D_{\varphi_1}^{\mathcal{A}_1} \to 1\right) - \mathbf{Pr}\left(D_{\varphi_2}^{\mathcal{A}_2} \to 1\right)\right| \text{ is small}$$

Indifferentiability



Definition

Functionality φ_1 is at least as secure as φ_2 if for any distinguisher D and adversary $\mathcal{A}_1$ there exist adversary $\mathcal{A}_2$ such that

$$\left|\mathbf{Pr}\left(D_{\varphi_1}^{\mathcal{A}_1} \to 1\right) - \mathbf{Pr}\left(D_{\varphi_2}^{\mathcal{A}_2} \to 1\right)\right| \text{ is small}$$

- Original framework of Maurer et al. (MRH, TCC'04)
- Popularized for domain extenders by Coron et al. (CDMP, Crypto'05)

Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

- Ristenpart et al. (RSS, Eurocrypt'11) revealed surprising result

Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

- Ristenpart et al. (RSS, Eurocrypt'11) revealed surprising result
- Proof-of-storage challenge-response protocol:

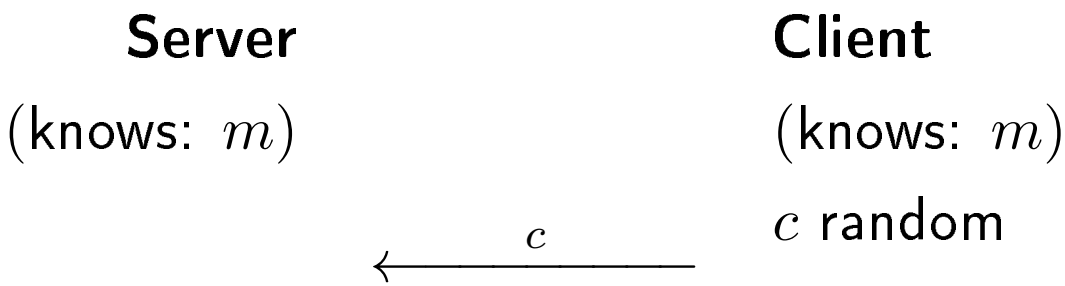
Server	**Client**
(knows: m)	(knows: m)

Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

- Ristenpart et al. (RSS, Eurocrypt'11) revealed surprising result
- Proof-of-storage challenge-response protocol:

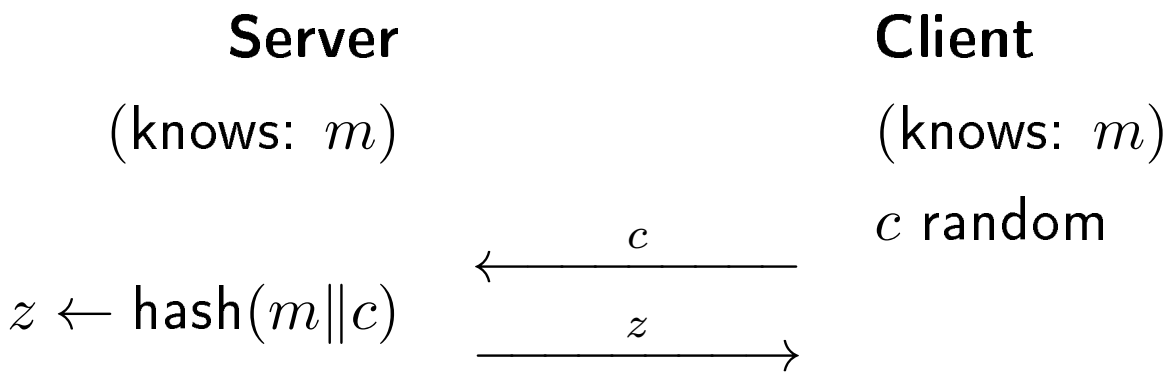


Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

- Ristenpart et al. (RSS, Eurocrypt'11) revealed surprising result
- Proof-of-storage challenge-response protocol:

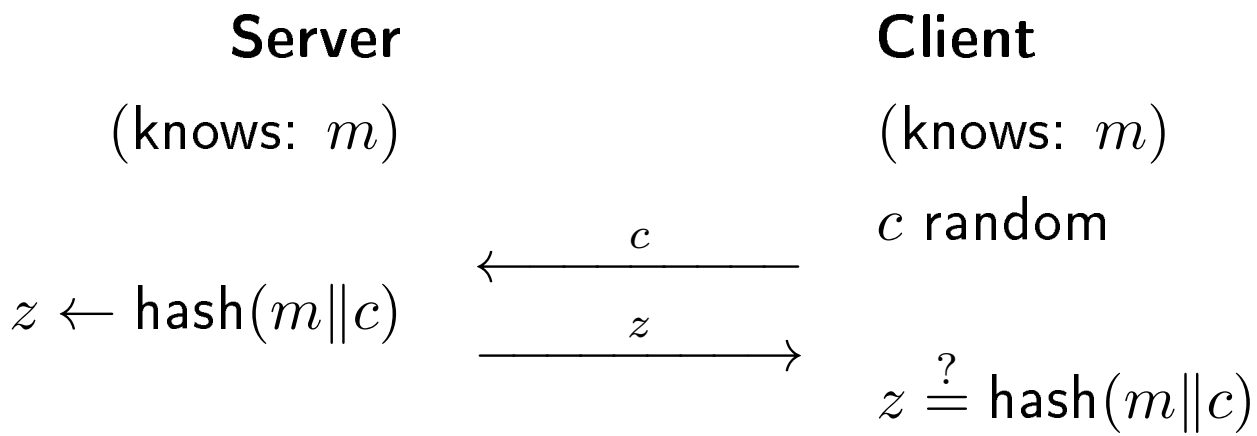


Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

- Ristenpart et al. (RSS, Eurocrypt'11) revealed surprising result
- Proof-of-storage challenge-response protocol:

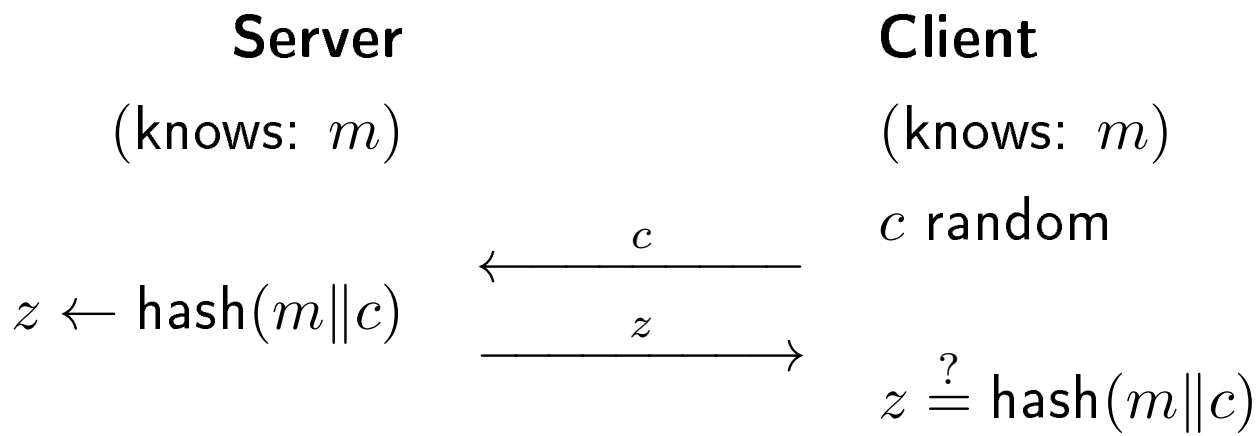


Indifferentiability

"security against all generic attacks"

"hash function can replace RO in any RO-secure scheme"

- Ristenpart et al. (RSS, Eurocrypt'11) revealed surprising result
- Proof-of-storage challenge-response protocol:



- Secure in ROM, but insecure for some indifferentiable hash functions

Remarks

- The attack of RSS does not mean there is a fault in the indifferentiability framework!

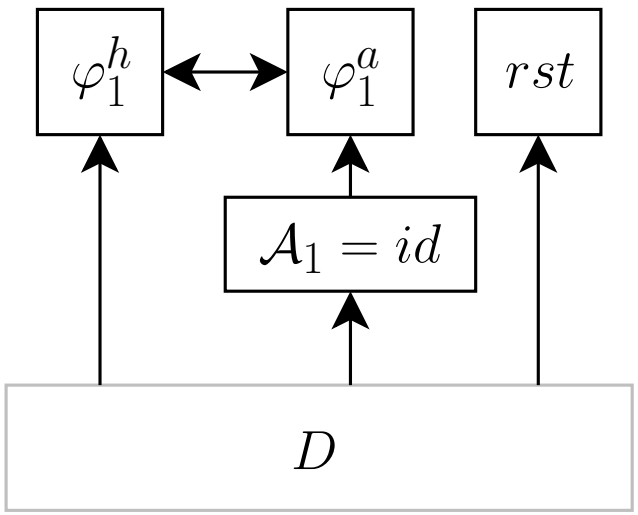
- Indifferentiability is general enough due to MRH's random systems

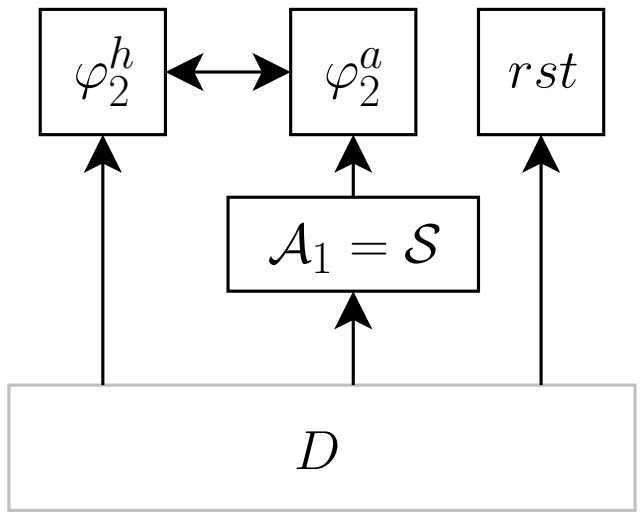
Remarks

- The attack of RSS does not mean there is a fault in the indifferentiability framework!
- Indifferentiability is general enough due to MRH's random systems
- Issue comes from CDMP's definition that does not allow distinguishers to manipulate states
- All indifferentiability proofs following CDMP's model limit types of distinguishers (their power) that are covered

Reset-Indifferentiability

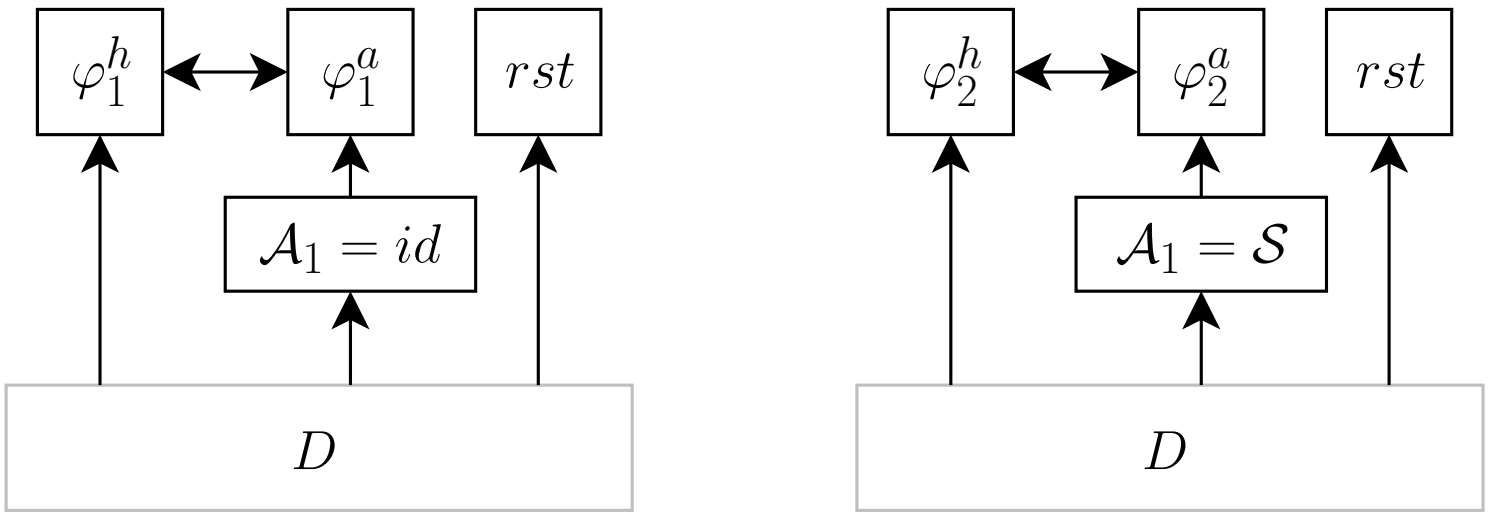
- RSS introduce reset-indifferentiability
- Additional procedure rst that when called initializes all of $\mathcal{A}$'s variables





Reset-Indifferentiability

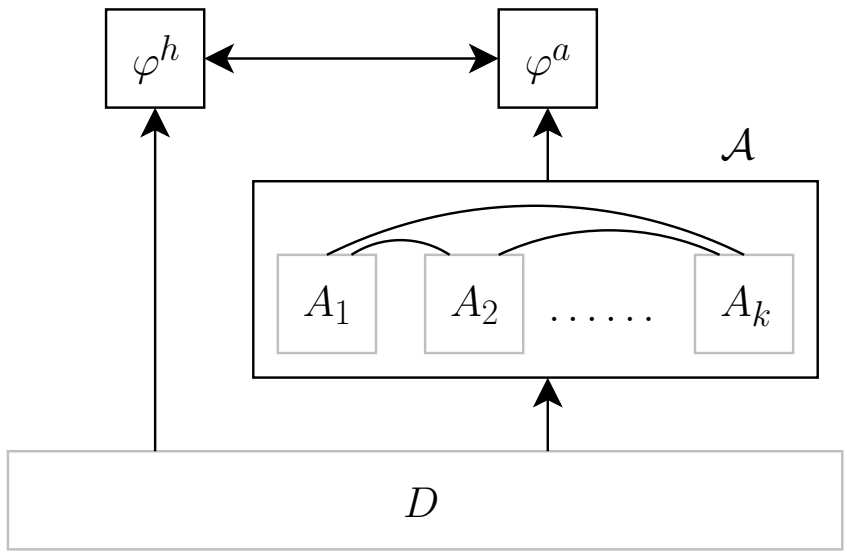
- RSS introduce reset-indifferentiability
- Additional procedure rst that when called initializes all of $\mathcal{A}$'s variables



- RSS: impossibility of reset-indifferentiable one-pass domain extenders
  - Applies to MD, chopMD, pfMD, EMD, Sponge, ...
- Model is too strong

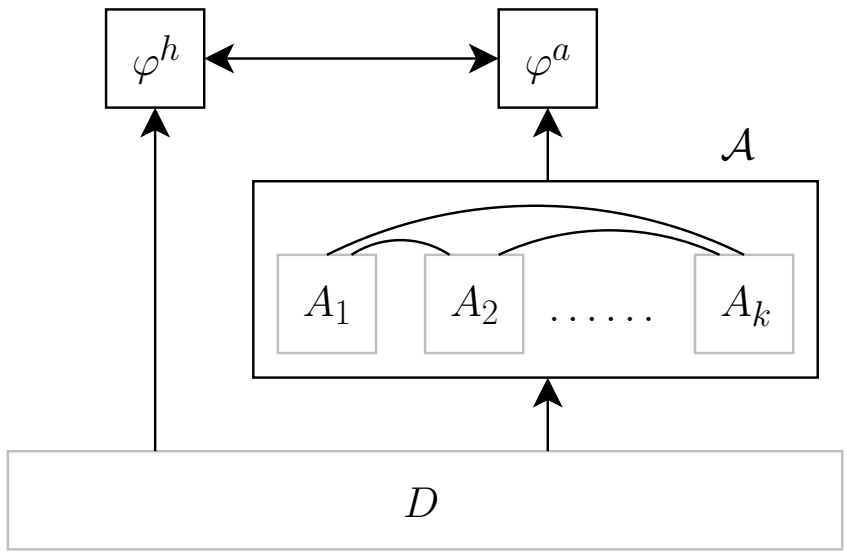
Formalizing Reset-Indifferentiability

- Our approach: explicitly model communication between adversaries
  - Storage procedures for any pair of adversaries
  - Reset corresponds to change of adversary



Formalizing Reset-Indifferentiability

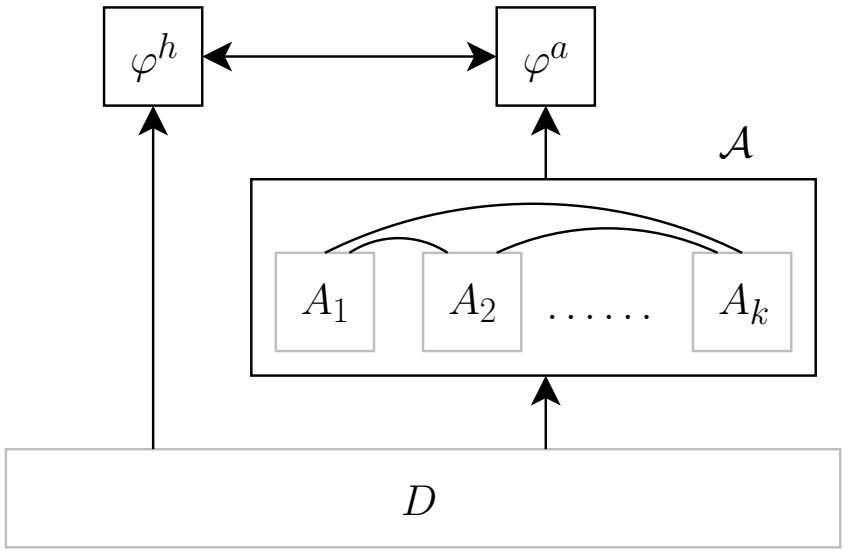
- Our approach: explicitly model communication between adversaries
  - Storage procedures for any pair of adversaries
  - Reset corresponds to change of adversary



- Model allows for whole spectrum of indifferentiability notions

Formalizing Reset-Indifferentiability

- Our approach: explicitly model communication between adversaries
  - Storage procedures for any pair of adversaries
  - Reset corresponds to change of adversary



- Model allows for whole spectrum of indifferentiability notions
- k-stage distinguishers
  - 1-stage: regular indifferentiability
  - CRP is 2-stage

$\mathcal{G}$-Indifferentiability

- Let $\mathcal{G}$ be a class of distinguishers
- E.g.: 1-stage, 1-stage $+$ CRP, 2-stage, $\ldots$
- $\mathcal{G}$-indifferentiability: indifferentiability for every distinguisher in $\mathcal{G}$

$\mathcal{G}$-Indifferentiability

- Let $\mathcal{G}$ be a class of distinguishers
- E.g.: 1-stage, 1-stage + CRP, 2-stage, ...
- $\mathcal{G}$-indifferentiability: indifferentiability for every distinguisher in $\mathcal{G}$

$\mathcal{G}$-**indifferentiability**	**security against**
(regular) indifferentiability	1-stage distinguishers
...	...
...	...
reset-indifferentiability	multi-stage distinguishers

$\mathcal{G}$-Indifferentiability

- Let $\mathcal{G}$ be a class of distinguishers
- E.g.: 1-stage, 1-stage + CRP, 2-stage, ...
- $\mathcal{G}$-indifferentiability: indifferentiability for every distinguisher in $\mathcal{G}$

$\mathcal{G}$-**indifferentiability**	**security against**
(regular) indifferentiability	1-stage distinguishers
single-reset-indifferentiability	...
...	...
reset-indifferentiability	multi-stage distinguishers

$\mathcal{G}$-Indifferentiability

- Let $\mathcal{G}$ be a class of distinguishers
- E.g.: 1-stage, 1-stage + CRP, 2-stage, ...
- $\mathcal{G}$-indifferentiability: indifferentiability for every distinguisher in $\mathcal{G}$

$\mathcal{G}$-**indifferentiability**	**security against**
(regular) indifferentiability	1-stage distinguishers
single-reset-indifferentiability	(almost all) 2-stage distinguishers
...	...
reset-indifferentiability	multi-stage distinguishers

Impossibility of Reset-Indifferentiability

- RSS: impossibility of reset-indifferentiable one-pass domain extenders
- We generalize to any domain extender

Impossibility of Reset-Indifferentiability

- RSS: impossibility of reset-indifferentiable one-pass domain extenders
- We generalize to any domain extender
- In this talk, simplified version:

consider $F : \{0,1\}^M \to \{0,1\}^H$ using $\pi : \{0,1\}^a \to \{0,1\}^b$

Impossibility of Reset-Indifferentiability

- RSS: impossibility of reset-indifferentiable one-pass domain extenders
- We generalize to any domain extender
- In this talk, simplified version:

$$\text{consider } F : \{0,1\}^M \to \{0,1\}^H \text{ using } \pi : \{0,1\}^a \to \{0,1\}^b$$

Theorem

There exists n-stage distinguisher D such that $\forall\ \mathcal{A}$:

$$\left|\mathbf{Pr}\left(D_{(F,\pi)} \to 1\right) - \mathbf{Pr}\left(D^{\mathcal{A}}_{RO} \to 1\right)\right| \geq 1 - \left(\frac{q}{2^{M-a}} + \frac{1}{2^H}\right)$$

where $\mathcal{A}$ makes q RO-queries, D makes one message evaluation

- Can be made arbitrarily close to $1 - 1/2^H$

Impossibility of Reset-Indifferentiability: Proof Idea

Theorem

There exists n-stage distinguisher D such that $\forall\ \mathcal{A}$:

$$\left|\mathbf{Pr}\left(D_{(F,\pi)} \to 1\right) - \mathbf{Pr}\left(D^{\mathcal{A}}_{RO} \to 1\right)\right| \geq 1 - \left(\frac{q}{2^{M-a}} + \frac{1}{2^{H}}\right)$$

where $\mathcal{A}$ makes q RO-queries, D makes one message evaluation

Proof Idea

- Distinguisher evaluates oracles for some $m \in \{0,1\}^M$
- Resets before every $\mathcal{A}$-call
- At last $\mathcal{A}$-call: learns at most $a \ll M$ bits of m

Impossibility of Single-Reset-Indifferentiability

- No "meaningful" domain extender can be single-reset-indifferentiable:
  - Modifying input bit results in different digest w.p. $\geq 1 - \varepsilon$ ("avalanche effect")

Impossibility of Single-Reset-Indifferentiability

- No "meaningful" domain extender can be single-reset-indifferentiable:
  - Modifying input bit results in different digest w.p. $\geq 1 - \varepsilon$ ("avalanche effect")
- In this talk, simplified version:

  consider $F : \{0,1\}^M \to \{0,1\}^H$ using $\pi : \{0,1\}^a \to \{0,1\}^b$
- Attack works if $M \geq \max\{8N, 8a\}$
  - N is maximal internal state size of F in bits

Impossibility of Single-Reset-Indifferentiability

- No "meaningful" domain extender can be single-reset-indifferentiable:
  - Modifying input bit results in different digest w.p. $\geq 1 - \varepsilon$ ("avalanche effect")
- In this talk, simplified version:

  consider $F : \{0,1\}^M \to \{0,1\}^H$ using $\pi : \{0,1\}^a \to \{0,1\}^b$
- Attack works if $M \geq \max\{8N, 8a\}$
  - N is maximal internal state size of F in bits

Theorem

There exists single-reset distinguisher D such that $\forall\ \mathcal{A}$:

$$\left|\mathbf{Pr}\left(D_{(F,\pi)} \to 1\right) - \mathbf{Pr}\left(D^{\mathcal{A}}_{RO} \to 1\right)\right| \geq \min\left\{1 - \frac{1}{2^H} - \frac{q}{2^{M/4-2}}, \frac{3}{8} - \frac{3}{M} - \frac{\varepsilon}{2}\right\}$$

where $\mathcal{A}$ makes q RO-queries, D makes one message evaluation

Impossibility of Single-Reset-Indifferentiability: Proof Idea

Theorem

There exists single-reset distinguisher D such that $\forall\ \mathcal{A}$:

$$\left|\mathbf{Pr}\left(D_{(F,\pi)} \to 1\right) - \mathbf{Pr}\left(D^{\mathcal{A}}_{RO} \to 1\right)\right| \geq \min\left\{1 - \frac{1}{2^H} - \frac{q}{2^{M/4-2}}, \frac{3}{8} - \frac{3}{M} - \frac{\varepsilon}{2}\right\}$$

where $\mathcal{A}$ makes q RO-queries, D makes one message evaluation

Proof Idea

- Distinguisher D is a combination of two distinguishers P and Q
  - If F is "roughly" one-pass: previous distinguisher (call it P) works
  - Otherwise, new distinguisher Q: manipulates m in a sophisticated way
- Distinguisher D chooses m runs either P or Q (depending on m)

Comparison with Resource-Restricted Indifferentiability

- Independent paper of Demay et al. (DGHM, ePrint 2012/613)
- Based on restricting memory of simulator

Comparison with Resource-Restricted Indifferentiability

- Independent paper of Demay et al. (DGHM, ePrint 2012/613)
- Based on restricting memory of simulator
- Maybe simpler generalization of indifferentiability, but: too strong
- For instance, single-reset-indifferentiability models the CRP distinguisher more closely than memory-restricted indifferentiability

Comparison with Resource-Restricted Indifferentiability

- Independent paper of Demay et al. (DGHM, ePrint 2012/613)
- Based on restricting memory of simulator
- Maybe simpler generalization of indifferentiability, but: too strong
- For instance, single-reset-indifferentiability models the CRP distinguisher more closely than memory-restricted indifferentiability

- DGHM's work:
  - Focus on reductions between "resources"
  - Target impossibility results
- Our work:
  - Focus on indifferentiability as way to guarantee security against a variety of attacks
  - More suitable to discover possibilities for composition
  - It shows that there are many different notions to consider

Conclusions

- Indifferentiability framework comes with a range of subtleties
- Reset-indifferentiability as remedy, but model is too strong
- There does not exist any meaningful domain extender that is single-reset-indifferentiability

Conclusions

- Indifferentiability framework comes with a range of subtleties
- Reset-indifferentiability as remedy, but model is too strong
- There does not exist any meaningful domain extender that is single-reset-indifferentiability

End of indifferentiability?

Conclusions

- Indifferentiability framework comes with a range of subtleties
- Reset-indifferentiability as remedy, but model is too strong
- There does not exist any meaningful domain extender that is single-reset-indifferentiability

End of indifferentiability?

- What lies between (regular) indifferentiability and single-reset indifferentiability?

  $\longrightarrow$ More natural classes $\mathcal{G}$?
- Applicability of our results to UC framework?

Conclusions

- Indifferentiability framework comes with a range of subtleties
- Reset-indifferentiability as remedy, but model is too strong
- There does not exist any meaningful domain extender that is single-reset-indifferentiability

End of indifferentiability?

- What lies between (regular) indifferentiability and single-reset indifferentiability?

  $\longrightarrow$ More natural classes $\mathcal{G}$?
- Applicability of our results to UC framework?

Thank you for your attention!