# Reset Indifferentiability and its Consequences

ASIACRYPT 2013

Paul Baecher, Christina Brzuska, Arno Mittelbach

Tel Aviv University & Darmstadt University of Technology; supported by DFG Heisenberg and Center For Advanced Security Research Darmstadt (CASED)

CASED

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Heisenberg-Programm
Deutsche Forschungsgemeinschaft

# Introduction

# Idealized Models

- problem: cannot prove scheme/protocol secure ☹

# Idealized Models

- problem: cannot prove scheme/protocol secure ☹
- solution
  - construction has oracle access to some primitive
  - probabilistic security statement over random choice of the primitive's implementation

# Idealized Models

- problem: cannot prove scheme/protocol secure ☹
- solution
  - construction has oracle access to some primitive
  - probabilistic security statement over random choice of the primitive's implementation

**random-oracle model** (ROM, [BR93])

- choice: set of functions
- example: $\{0,1\}^n \to \{0,1\}^n$

# Idealized Models

- problem: cannot prove scheme/protocol secure ☹
- solution
  - construction has oracle access to some primitive
  - probabilistic security statement over random choice of the primitive's implementation

**random-oracle model** (ROM, [BR93])

- choice: set of functions
- example: $\{0,1\}^n \to \{0,1\}^n$

**ideal-cipher model** (ICM, [Sha49])

- choice: set of keyed permutations
- example: $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

# Idealized Models

- problem: cannot prove scheme/protocol secure ☹
- solution (not really. . . )
  - construction has oracle access to some primitive
  - probabilistic security statement over random choice of the primitive's implementation

**random-oracle model** (ROM, [BR93])

- choice: set of functions
- example: $\{0,1\}^n \to \{0,1\}^n$

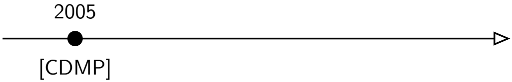
**ideal-cipher model** (ICM, [Sha49])

- choice: set of keyed permutations
- example: $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

# ROM $\stackrel{?}{\equiv}$ ICM

is the random-oracle model equivalent to the ideal-cipher model?

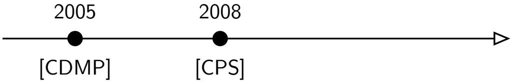
# ROM $\stackrel{?}{\equiv}$ ICM




is the random-oracle model equivalent to the ideal-cipher model?

- ideal cipher $\Rightarrow$ random oracle [CDMP05]

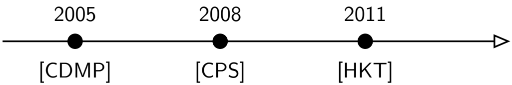
# ROM $\stackrel{?}{\equiv}$ ICM




is the random-oracle model equivalent to the ideal-cipher model?

- ideal cipher $\Rightarrow$ random oracle [CDMP05]
- random oracle $\Rightarrow^*$ ideal cipher [CPS08]

# ROM $\stackrel{?}{\equiv}$ ICM

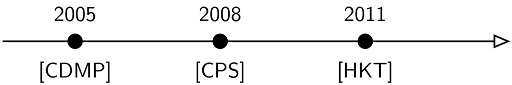



is the random-oracle model equivalent to the ideal-cipher model?

- ideal cipher $\Rightarrow$ random oracle [CDMP05]
- random oracle $\Rightarrow^*$ ideal cipher [CPS08]
- random oracle $\Rightarrow$ ideal cipher [HKT11]

thus, ROM $\equiv$ ICM

# ROM $\overset{?}{\equiv}$ ICM



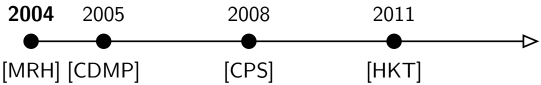

is the random-oracle model equivalent to the ideal-cipher model?

- ideal cipher $\Rightarrow$ random oracle [CDMP05]
- random oracle $\Rightarrow^*$ ideal cipher [CPS08]
- random oracle $\Rightarrow$ ideal cipher [HKT11]

thus, ROM $\equiv$ ICM

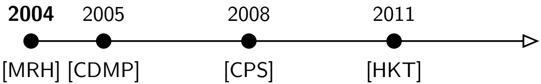
but what is "$\equiv$"?

# Equivalence Through Indifferentiability

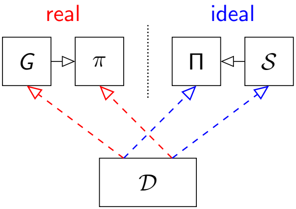



- composition theorem by Maurer, Renner, and Holenstein [MRH04]
- proof in $\Pi$ model $\rightsquigarrow$ proof in $\pi$ model, given indiff. construction $G^{\pi}$

# Equivalence Through Indifferentiability

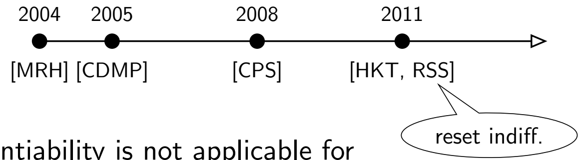



- composition theorem by Maurer, Renner, and Holenstein [MRH04]
- proof in $\Pi$ model $\rightsquigarrow$ proof in $\pi$ model, given indiff. construction $G^{\pi}$



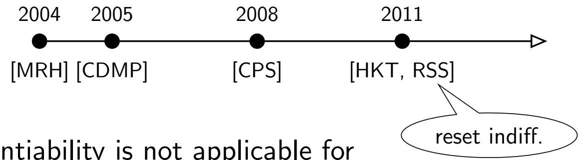

- e.g., $G$: constructed "random oracle"; $\pi$: ideal cipher; $\Pi$: real random oracle
- ask for simulator $\mathcal{S}$ such that $(G^{\pi}, \pi) \stackrel{c}{\approx} (\Pi, \mathcal{S}^{\Pi})$

# Limitations of Indifferentiability




- indifferentiability is not applicable for multi-stage games with ideal primitives [RSS11]
- $\ldots, x \leftarrow \mathcal{A}_1, \ldots, y \leftarrow \mathcal{A}_2, \ldots$

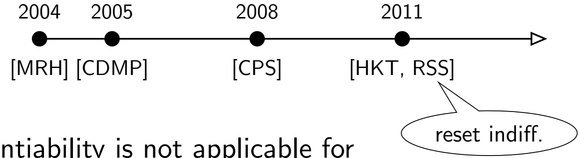
# Limitations of Indifferentiability




- indifferentiability is not applicable for multi-stage games with ideal primitives [RSS11]
- $\ldots, x \leftarrow \mathcal{A}_1, \ldots, y \leftarrow \mathcal{A}_2, \ldots$

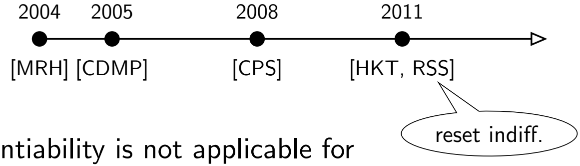
no shared state

# Limitations of Indifferentiability




- indifferentiability is not applicable for multi-stage games with ideal primitives [RSS11]
- $\ldots, x \leftarrow \mathcal{A}_1, \ldots, y \leftarrow \mathcal{A}_2, \ldots$
  - e.g. deterministic/hedged/efficiently-searchable/public-key encryption, KDM/RKA security, non-malleable hashing, proof-of-storage security, anything with leakage...

# Limitations of Indifferentiability




- indifferentiability is not applicable for multi-stage games with ideal primitives [RSS11]
- $\ldots, x \leftarrow \mathcal{A}_1, \ldots, y \leftarrow \mathcal{A}_2, \ldots$
  - e.g. deterministic/hedged/efficiently-searchable/public-key encryption, KDM/RKA security, non-malleable hashing, proof-of-storage security, anything with leakage...
- problem (roughly): distinct stages result in distinct simulators, distinct simulators are inconsistent
- allow the distinguisher to reset the simulator, reset indifferentiability [RSS11]

$$\text{ROM} \stackrel{?}{\equiv} \text{ICM}$$

# ROM $\stackrel{?}{\equiv}$ ICM, Revisited

- ROM $\equiv$ ICM for single-stage games
- constructions in [CDMP05, CPS08, HKT11] are not reset indifferentiable
  - i.e., do not apply to multi-stage games

# ROM $\stackrel{?}{\equiv}$ ICM, Revisited

- ROM $\equiv$ ICM for single-stage games
- constructions in [CDMP05, CPS08, HKT11] are not reset indifferentiable
    - i.e., do not apply to multi-stage games
- reset-indifferentiable constructions cannot be domain extending [LAMP12, DGHM13]
    - assuming that ROs have infinite domain, ICM $\not\Rightarrow$ ROM

# In This Work

- a different notion to characterize reset indifferentiability — multi-stage indifferentiability

# In This Work

- a different notion to characterize reset indifferentiability — multi-stage indifferentiability

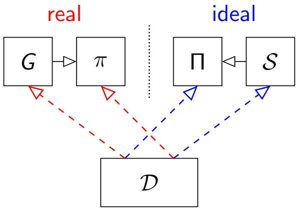
1. under reset indifferentiability, ROM $\not\equiv$ ICM
   - i.e., ICM $\not\Rightarrow$ ROM and ROM $\not\Rightarrow$ ICM
2. "Duality Lemma": two primitives are either equivalent or incomparable
3. $n$-reset indifferentiability $\equiv$ 1-reset indifferentiability

# In This Work

- a different notion to characterize reset indifferentiability — multi-stage indifferentiability

1. under reset indifferentiability, ROM $\not\equiv$ ICM
   - i.e., ICM $\not\Rightarrow$ ROM and ROM $\not\Rightarrow$ ICM
   - (no result for length-preserving constructions)
2. "Duality Lemma": two primitives are either equivalent or incomparable
3. $n$-reset indifferentiability $\equiv$ 1-reset indifferentiability

# Multi-Stage Indifferentiability



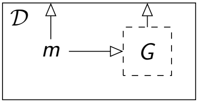

- instead of resettable simulators, consider stateless ones
- think "reset after each query"
- equivalent to reset indifferentiability
- simulators are *pseudo deterministic*—why?

# No Domain Extension

- there is no domain-extending construction of a RO from an IC

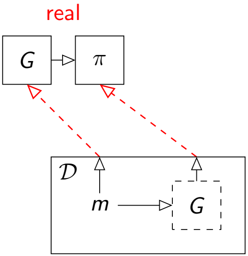
# No Domain Extension

- there is no domain-extending construction of a RO from an IC
- consider a length-doubling construction $G^{\pi}$
- let distinguisher $\mathcal{D}$ sample $m \leftarrow \{0,1\}^{\ell}$ and locally evaluate $G^{(\cdot)}(m)$, then query $m$ on left-hand side interface



# No Domain Extension

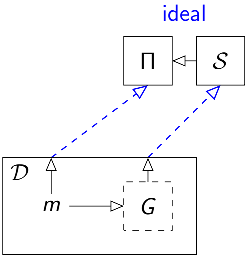
- there is no domain-extending construction of a RO from an IC
- consider a length-doubling construction $G^{\pi}$
- let distinguisher $\mathcal{D}$ sample $m \leftarrow \{0,1\}^{\ell}$ and locally evaluate $G^{(\cdot)}(m)$, then query $m$ on left-hand side interface




- real world: identical results

# No Domain Extension

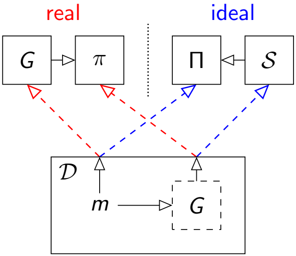
- there is no domain-extending construction of a RO from an IC
- consider a length-doubling construction $G^\pi$
- let distinguisher $\mathcal{D}$ sample $m \leftarrow \{0,1\}^\ell$ and locally evaluate $G^{(\cdot)}(m)$, then query $m$ on left-hand side interface




- real world: identical results
- ideal world
  - $\mathcal{S}$ needs to query $\Pi$ on $m$
  - gets $k$ inputs of size $\frac{\ell}{2} < \ell = |\Pi(m)|$
  - but $k \cdot 2^{\ell/2} \ll 2^\ell$
  - $\Rightarrow$ very unlikely to "hit" $m$ reliably

# No Domain Extension

- there is no domain-extending construction of a RO from an IC
- consider a length-doubling construction $G^\pi$
- let distinguisher $\mathcal{D}$ sample $m \leftarrow \{0,1\}^\ell$ and locally evaluate $G^{(\cdot)}(m)$, then query $m$ on left-hand side interface




- real world: identical results
- ideal world
  - $\mathcal{S}$ needs to query $\Pi$ on $m$
  - gets $k$ inputs of size $\frac{\ell}{2} < \ell = |\Pi(m)|$
  - but $k \cdot 2^{\ell/2} \ll 2^\ell$
  - $\Rightarrow$ very unlikely to "hit" $m$ reliably

- note: choice of primitives arbitrary

# No Domain Extension (cont'd)

- ICM $\not\Rightarrow$ ROM (also shown by [LAMP12, DGHM13] for one-bit extension)
- ROM $\not\Rightarrow$ ICM
  - typical Feistel constructions are length doubling

# No Domain Extension (cont'd)

- ICM $\not\Rightarrow$ ROM (also shown by [LAMP12, DGHM13] for one-bit extension)
- ROM $\not\Rightarrow$ ICM
  - typical Feistel constructions are length doubling
- what about domain shrinking?

# The Duality Lemma

- what about domain shrinking?

**observation:**

- simulators are pseudo deterministic
- constructions are typically (pseudo) deterministic, e.g. hash function, block cipher, ...

# The Duality Lemma

- what about domain shrinking?

**observation:**

- simulators are pseudo deterministic
- constructions are typically (pseudo) deterministic, e.g. hash function, block cipher, ...

- can switch roles!

# The Duality Lemma (cont'd)

given two ideal primitives $\pi_1$ and $\pi_2$, one of the following holds

1. $\pi_1$ and $\pi_2$ are equivalent

2. $\pi_1$ and $\pi_2$ are incomparable

# The Duality Lemma (cont'd)

given two ideal primitives $\pi_1$ and $\pi_2$, one of the following holds

1. $\pi_1$ and $\pi_2$ are equivalent
   - there exist constructions $G_1$ and $G_2$ such that $G_1^{\pi_2}$ (resp. $G_2^{\pi_1}$) is multi stage indifferentiable from $\pi_1$ (resp. $\pi_2$); i.e., $\pi_1 \Rightarrow \pi_2$ and $\pi_2 \Rightarrow \pi_1$
2. $\pi_1$ and $\pi_2$ are incomparable
   - no multi-stage indifferentiable constructions from each other exist; i.e., $\pi_1 \not\Rightarrow \pi_2$ <ins>and</ins> $\pi_2 \not\Rightarrow \pi_1$

# The Duality Lemma (cont'd)

given two ideal primitives $\pi_1$ and $\pi_2$, one of the following holds

1. $\pi_1$ and $\pi_2$ are equivalent
   - there exist constructions $G_1$ and $G_2$ such that $G_1^{\pi_2}$ (resp. $G_2^{\pi_1}$) is multi stage indifferentiable from $\pi_1$ (resp. $\pi_2$); i.e., $\pi_1 \Rightarrow \pi_2$ and $\pi_2 \Rightarrow \pi_1$
2. $\pi_1$ and $\pi_2$ are incomparable
   - no multi-stage indifferentiable constructions from each other exist; i.e., $\pi_1 \not\Rightarrow \pi_2$ <u>and</u> $\pi_2 \not\Rightarrow \pi_1$

- positive (resp. negative) result in one direction translates to other direction
- no domain-extending constructions $\Rightarrow$ no domain-shrinking constructions; ROM and ICM are incomparable

# Do Weaker Notions Help?

- reset indifferentiability permits poly. many resets
- Luykx et al. [LAMP12] consider $n$-reset indifferentiability
    - $n$ resets compose with $n$ stages

# Do Weaker Notions Help?

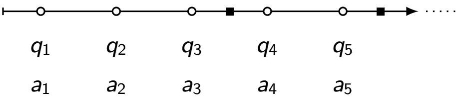
- reset indifferentiability permits poly. many resets
- Luykx et al. [LAMP12] consider $n$-reset indifferentiability
  - $n$ resets compose with $n$ stages

- turns out $n$-reset $=$ $n'$-reset $=$ 1-reset
- idea: at least one reset must be "critical", find it

# Eliminating Resets

consider the distinguisher $\mathcal{D}_n$ on randomness $r$ (max. $n$ resets)

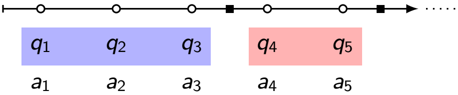
$\mathcal{D}_n(r)$



# Eliminating Resets

consider the distinguisher $\mathcal{D}_n$ on randomness $r$ (max. $n$ resets)

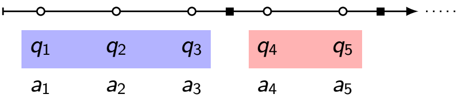
$\mathcal{D}_n(r)$



# Eliminating Resets

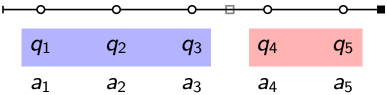
consider the distinguisher $\mathcal{D}_n$ on randomness $r$ (max. $n$ resets)

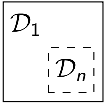
$\mathcal{D}_n(r)$




construct $\mathcal{D}_1$

$\mathcal{D}_1(r)$

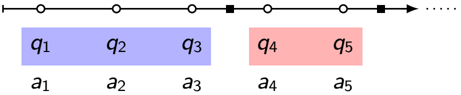


# Eliminating Resets

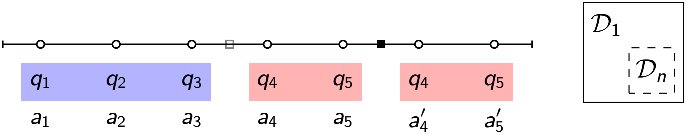
consider the distinguisher $\mathcal{D}_n$ on randomness $r$ (max. $n$ resets)

$\mathcal{D}_n(r)$




construct $\mathcal{D}_1$

$\mathcal{D}_1(r)$




let $\mathcal{D}_1$'s output be $(a_4, a_5) \stackrel{?}{=} (a'_4, a'_5)$

next, consider $\mathcal{D}_{n-1}$

# Summary

**take-home message**

- is the ROM equivalent to the ICM?
- answer—depends on "equivalent"
  - for composing single-stage games: ✓
  - multi stage / non length preserving: ✗
  - multi stage / length preserving:

**open question**

# Summary

**take-home message**

- is the ROM equivalent to the ICM?
- answer—depends on "equivalent"
  - for composing single-stage games: ✓
  - multi stage / non length preserving: ✗
  - multi stage / length preserving: ???

**open question**

# The End

Thank you!

?

# References I


Mihir Bellare and Phillip Rogaway.
Random oracles are practical: A paradigm for designing efficient protocols.
In V. Ashby, editor, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya.
Merkle-Damgård revisited: How to construct a hash function.
In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 430–448. Springer, August 2005.

Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin.
The random oracle model and the ideal cipher model are equivalent.
In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 1–20. Springer, August 2008.

Gregory Demay, Peter Gazi, Martin Hirt, and Ueli Maurer.
Resource-restricted indifferentiability.
In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 664–683. Springer, May 2013.

Thomas Holenstein, Robin Künzler, and Stefano Tessaro.
The equivalence of the random oracle model and the ideal cipher model, revisited.
In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 89–98. ACM Press, June 2011.

Atul Luykx, Elena Andreeva, Bart Mennink, and Bart Preneel.
Impossibility results for indifferentiability with resets.
Cryptology ePrint Archive, Report 2012/644, 2012.
http://eprint.iacr.org/.

Ueli M. Maurer, Renato Renner, and Clemens Holenstein.
Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology.
In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 21–39. Springer, February 2004.

# References II

Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton.
Careful with composition: Limitations of the indifferentiability framework.
In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 487–506. Springer, May 2011.

Claude E. Shannon.
Communication theory of secrecy systems.
*Bell Systems Technical Journal*, 28(4):656–715, 1949.