The Indifferentiability of the Duplex and its Practical Applications

TECHNISCHE UNIVERSITÄT DARMSTADT

Jean Paul Degabriele Marc Fischlin **Jérôme Govinden**

Technology Innovation Institute

TECHNISCHE UNIVERSITÄT DARMSTADT

Asiacrypt 2023

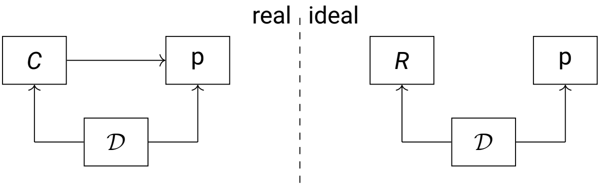
Outline

TECHNISCHE UNIVERSITÄT DARMSTADT

Background

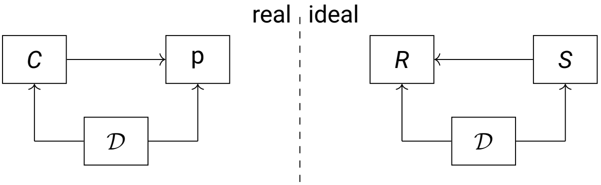
Indistinguishability vs. Indifferentiability

Indistinguishability



- Focused on a specific property
- Requires keyed constructions

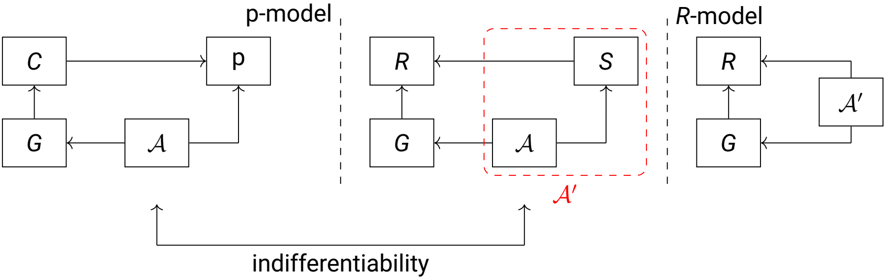
Indifferentiability [MRH04]



- Used to build an ideal primitive *R*
- For (un)keyed constructions
- Covers multiple security properties

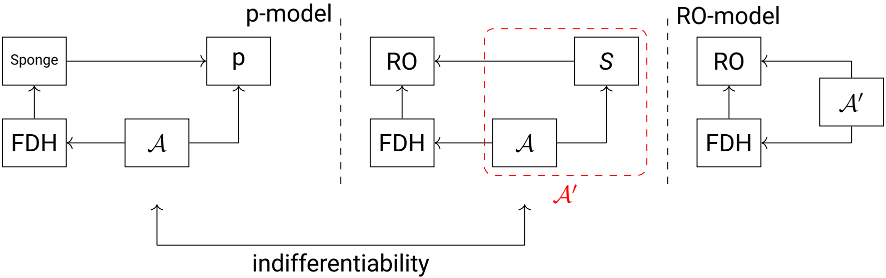
Composability [MRH04]

If C **is indifferentiable from** R,
then, in the p-model, it **has the same security properties** as R.



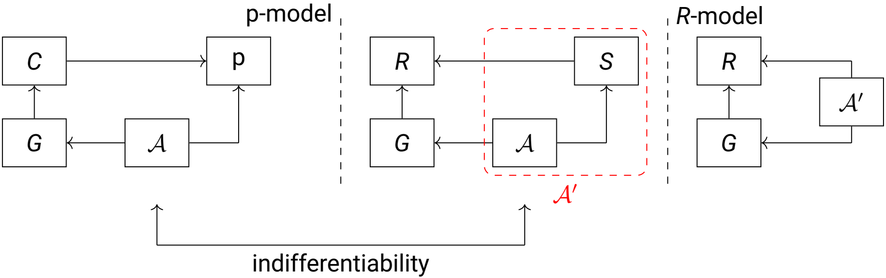
Composability [MRH04]
Full Domain Hash (FDH) Example

If C **is indifferentiable from** R,
then, in the p-model, it **has the same security properties** as R.



Composability [MRH04]

If C **is indifferentiable from** R,
then, in the p-model, it **has the same security properties** as R.



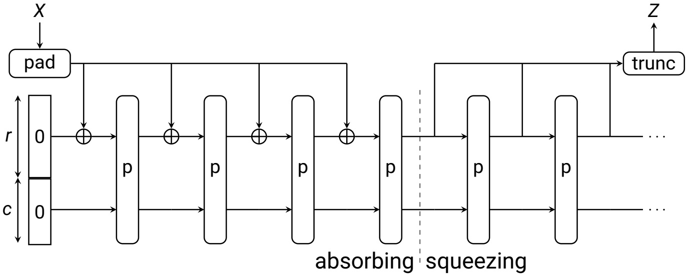
→ *C* and *R* need to share the **same interface**

Indifferentiability from Idealized Model

Primitive *C*	**Idealized Model** *R*
Hash Function	Random Oracle [Bellare and Rogaway, *ACM CCS 93*]
Block Cipher	Ideal Cipher [Holenstein, Künzler, and Tessaro, *43rd ACM STOC*] [Andreeva et al., *CRYPTO 2013, Part I*]
Authenticated Encryption	Random Injection [Barbosa and Farshim, *CRYPTO 2018, Part I*]
Duplex	??

The Sponge Construction [Ber+08]

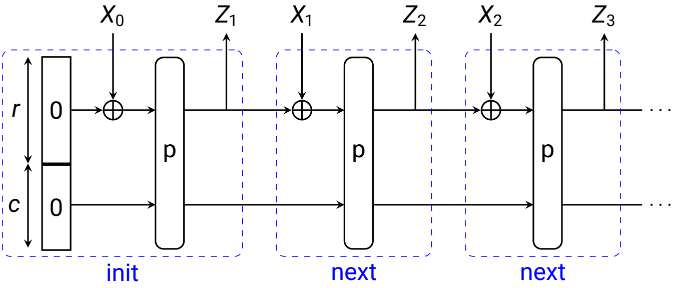
TECHNISCHE UNIVERSITÄT DARMSTADT



- Basis of multiple NIST standards:
  - SHA-3, cSHAKE, KMAC, TupleHash, ParallelHash
- Based on a public random permutation p
- Indifferentiable from a Random Oracle with bound $\mathcal{O}\left(\frac{q^2}{2^c}\right)$ [Ber+08]

The Duplex Construction [Ber+12]

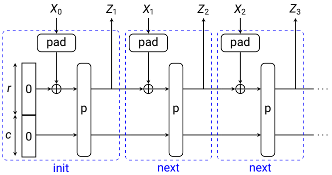
TECHNISCHE UNIVERSITÄT DARMSTADT

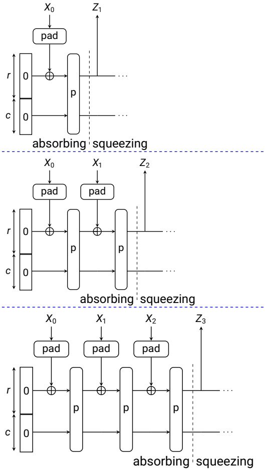


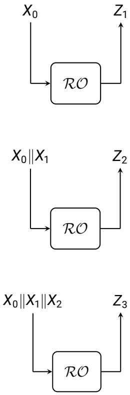
- Allows the construction of one-pass AEAD schemes
- Basis of multiple AEAD candidates of the CAESAR & NIST competitions
- Stateful construction that supersedes the Sponge

[Ber+12] Security Analysis

→ Reduces an instance of the Duplex to a sequence of Sponge calls

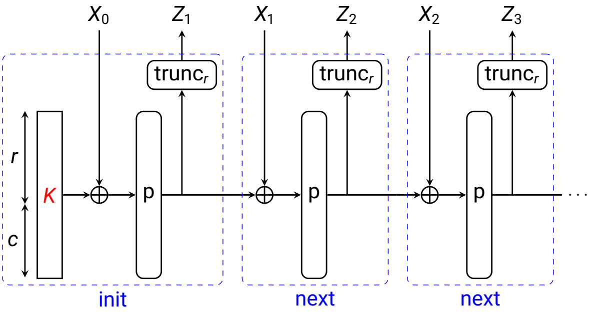






The Full-State Keyed Duplex [MRV15]

TECHNISCHE UNIVERSITÄT DARMSTADT



- Newer work focuses on the indistinguishability of the keyed Duplex
- Better bounds
- Improved absorption performance

The Duplex as a General-Purpose Primitive

Used for:

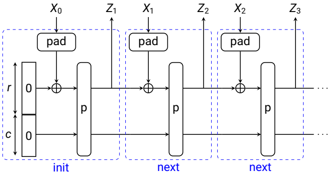
- **Authenticated Encryption/AEAD**
- **Online Hash**
  → Stateful Hash Object (SHO) within the Noise Protocol framework
- **MAC, Symmetric Ratcheting** and **Pseudorandomness Generation**
  → STROBE protocol framework (lib based only on the Duplex)

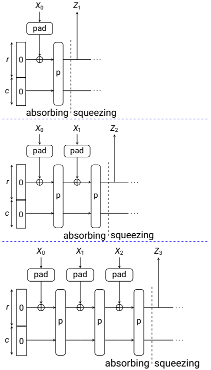
→ Prior security analyses focused on specific usage, and not as a general-purpose primitive (keyed or unkeyed)

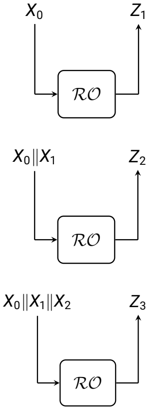
→ Need an idealized model for the Duplex

Indifferentiability of the Duplex from the Online Random Oracle

Limitations of [Ber+12] Security Analysis







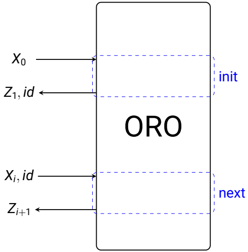
- Mismatching interface $\rightarrow$ cannot directly apply composition thm
- Needs an extra step
- Needs sponge-compliant padding in every call to p within the Duplex

Indifferentiability from Idealized Model

TECHNISCHE UNIVERSITÄT DARMSTADT

Primitive C	**Idealized Model** R
Hash Function	Random Oracle [Bellare and Rogaway, *ACM CCS 93*]
Block Cipher	Ideal Cipher [Holenstein, Künzler, and Tessaro, *43rd ACM STOC*] [Andreeva et al., *CRYPTO 2013, Part I*]
Authenticated Encryption	Random Injection [Barbosa and Farshim, *CRYPTO 2018, Part I*]
Duplex	Online Random Oracle (ORO) [This work]

The Online Random Oracle (ORO)



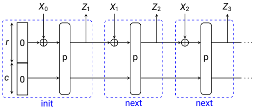
- Stateful & Online primitive

- To each query, we associate a path and we keep a table for mapping paths to answers
- The path corresponding to init is X_0
- The path corresponding to next is $X_0 \| X_1 \| \cdots \| X_i$
- The answer associated with a path is sampled at random once

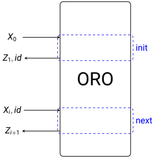
- We updated the syntax to supports multiple concurrent sessions

The Duplex is Indifferentiable from the ORO

The Duplex



The ORO

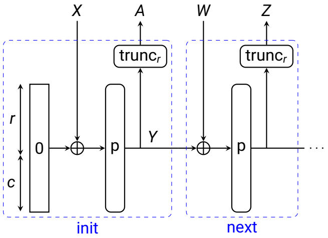


- We show that **the Duplex is indifferentiable from the ORO** with bound $\mathcal{O}\left(\frac{q^2}{2^c}\right)$
- We give a **proof using the code-based framework** from Bellare–Rogaway
- We obtain an **efficient simulator**
- No padding required

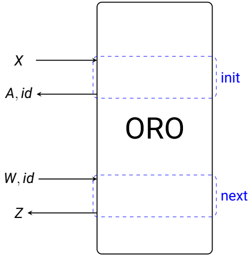
Full-State Duplex is Differentiable from the ORO

TECHNISCHE UNIVERSITÄT DARMSTADT

The Full-State Duplex



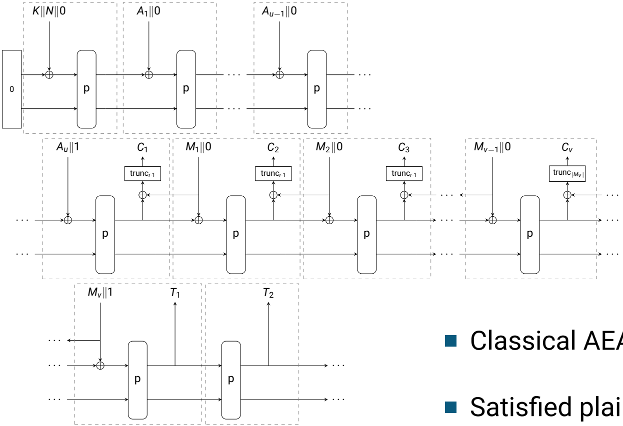
The ORO



- The full string Y is recoverable in the real world through the access to p
- It is possible to mount a collision $Y \oplus W = Y' \oplus W'$ in the real world
- In the ideal world, the input path to the ORO will be different

Applications of the Indifferentiability of the Duplex

A Nonce-Based Variant of SpongeWrap



- Classical AEAD template
- Satisfied plain AEAD security

KDM-AEAD, RKA-AEAD and CMT-AEAD Security

TECHNISCHE UNIVERSITÄT DARMSTADT

We prove the following **stronger security** for SpongeWrap in the **ORO model**:

- KDM-AEAD: **key-dependent message** security, i.e., when $M = \Phi(K)$
  $\rightarrow$ useful for disk encryption, HSM, KMS
- RKA-AEAD: **related-key attacks** security, i.e., when $K' = \Phi(K)$
  $\rightarrow$ models fault-injection attacks
- CMT-AEAD: **commitment** security
  $\rightarrow$ useful for message franking, key rotation

Benefits of the ORO Model

- The ORO model makes the proof **simpler** and **more intuitive**
- We use **composability** to translate the results in the random-permutation model
- Allow us to **bypass a complex analysis** in the random-permutation model
- We obtain the **first one-pass** AEAD scheme to **achieve KDM-AEAD, RKA-AEAD and CMT-AEAD** security

Future Work

TECHNISCHE UNIVERSITÄT DARMSTADT

- Prove **KDM**, **RKA** and **CMT** security **for other primitives** based on the Duplex such as PRF and MAC

- Use the ORO model to **prove** more easily security for upcoming **stronger security notions**

- **Prove the security of protocols** built from multiple instances of the Duplex (keyed and unkeyed)

Full version available soon on IACR ePrint

References I

[And+13] Elena Andreeva et al. “On the Indifferentiability of Key-Alternating Ciphers”. In: *CRYPTO 2013, Part I*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8042. LNCS. Springer, Heidelberg, Aug. 2013, pp. 531–550. DOI: 10.1007/978-3-642-40041-4_29.

[Ber+08] Guido Bertoni et al. “On the Indifferentiability of the Sponge Construction”. In: *EUROCRYPT 2008*. Ed. by Nigel P. Smart. Vol. 4965. LNCS. Springer, Heidelberg, Apr. 2008, pp. 181–197. DOI: 10.1007/978-3-540-78967-3_11.

[Ber+12] Guido Bertoni et al. “Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications”. In: *SAC 2011*. Ed. by Ali Miri and Serge Vaudenay. Vol. 7118. LNCS. Springer, Heidelberg, Aug. 2012, pp. 320–337. DOI: 10.1007/978-3-642-28496-0_19.

References II

[BF18] Manuel Barbosa and Pooya Farshim. "Indifferentiable Authenticated Encryption". In: *CRYPTO 2018, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10991. LNCS. Springer, Heidelberg, Aug. 2018, pp. 187–220. DOI: 10.1007/978-3-319-96884-1_7.

[BR93] Mihir Bellare and Phillip Rogaway. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols". In: *ACM CCS 93*. Ed. by Dorothy E. Denning et al. ACM Press, Nov. 1993, pp. 62–73. DOI: 10.1145/168588.168596.

References III

[HKT11] Thomas Holenstein, Robin Künzler, and Stefano Tessaro. "The equivalence of the random oracle model and the ideal cipher model, revisited". In: *43rd ACM STOC*. Ed. by Lance Fortnow and Salil P. Vadhan. ACM Press, June 2011, pp. 89–98. DOI: 10.1145/1993636.1993650.

[MRH04] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. "Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology". In: *TCC 2004*. Ed. by Moni Naor. Vol. 2951. LNCS. Springer, Heidelberg, Feb. 2004, pp. 21–39. DOI: 10.1007/978-3-540-24638-1_2.

References IV

[MRV15] Bart Mennink, Reza Reyhanitabar, and Damian Vizár. "Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption". In: *ASIACRYPT 2015, Part II*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9453. LNCS. Springer, Heidelberg, Nov. 2015, pp. 465–489. DOI: 10.1007/978-3-662-48800-3_19.