Radbound University

Indifferentiability of the Sponge Construction with a Restricted Number of Message Blocks

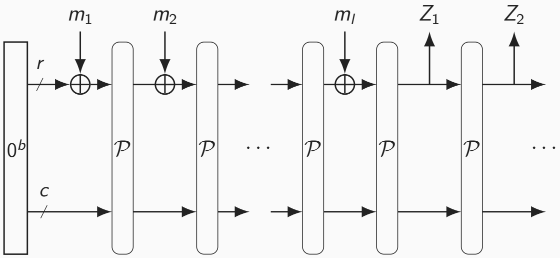
Charlotte Lefevre
Radboud University (The Netherlands)

FSE

20 March 2023

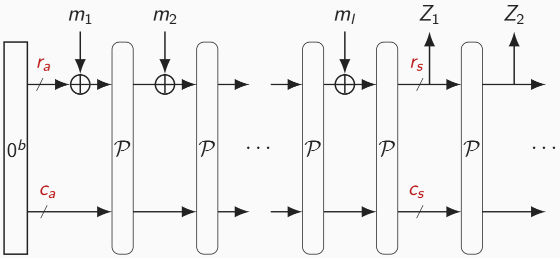
ESCADA

The Sponge Construction [Bertoni et al., 2007]



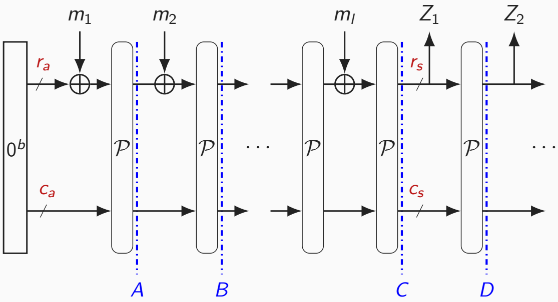
- Extendable output function
- $m_1 \| \cdots \| m_l$ is the message padded into r-bit blocks

The Sponge Construction [Bertoni et al., 2007]



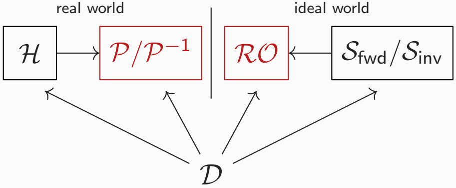
- Extendable output function
- $m_1 \| \cdots \| m_l$ is the message padded into r_a-bit blocks
- Absorb rate and squeeze rate different [Guo et al., 2011, Naito and Ohta, 2014]

The Sponge Construction [Bertoni et al., 2007]

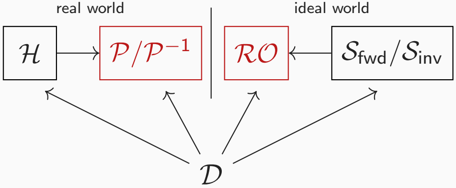


- Extendable output function
- $m_1 \| \cdots \| m_l$ is the message padded into -bit blocks
- Absorb rate and squeeze rate different [Guo et al., 2011, Naito and Ohta, 2014]
- Graph notation: $0^b \xrightarrow{m_1} A \xrightarrow{m_2} B \longrightarrow \cdots \xrightarrow{m_l} C \longrightarrow D$

Indifferentiability [Maurer et al., 2004, Coron et al., 2005]



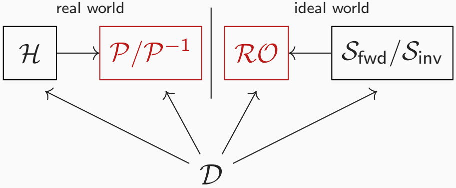
- $(\mathcal{H}^{\mathcal{P}}, \mathcal{P})$ for a random primitive $\mathcal{P}$ should behave like a random oracle $\mathcal{RO}$ paired with a simulator $\mathcal{S}$ that maintains construction-primitive consistency
- $\mathcal{H}$ is indifferentiable from $\mathcal{RO}$ for some simulator $\mathcal{S}$ whenever any $\mathcal{D}$ can distinguish the two worlds only with a negligible probability
- This probability is usually expressed as a function of the number of queries made



- Indifferentiability advantage:

$$\mathbf{Adv}^{\mathrm{iff}}_{\mathsf{Sponge}}(q) = \max_{\mathcal{D} \text{ with } q \text{ queries}} \left| \mathbf{Pr}\left(\mathcal{D}^{\mathsf{Real}} = 1\right) - \mathbf{Pr}\left(\mathcal{D}^{\mathsf{Ideal}} = 1\right) \right|$$

Indifferentiability [Maurer et al., 2004, Coron et al., 2005]



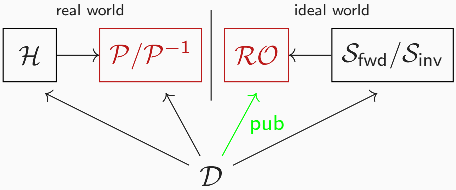
- Indifferentiability advantage:

$$\mathbf{Adv}^{\mathrm{iff}}_{\mathsf{Sponge}}(q) = \max_{\mathcal{D} \text{ with } q \text{ queries}} \left| \mathbf{Pr}\left(\mathcal{D}^{\mathsf{Real}} = 1\right) - \mathbf{Pr}\left(\mathcal{D}^{\mathsf{Ideal}} = 1\right) \right|$$

- Consider the following restriction:

$$\mathbf{Adv}^{\mathrm{R\text{-}iff}}_{\mathsf{Sponge}}(q, \ell) = \max_{\substack{\mathcal{D} \text{ with } q \text{ queries}, \\ \mathsf{pad}(M) \leq r_a \times \ell}} \left| \mathbf{Pr}\left(\mathcal{D}^{\mathsf{Real}} = 1\right) - \mathbf{Pr}\left(\mathcal{D}^{\mathsf{Ideal}} = 1\right) \right|$$

Public Indifferentiability [Yoneyama et al., 2009, Dodis et al., 2009]



- All construction queries are public $\implies$ helps the simulator to keep $\mathcal{RO}$-consistency
- Weaker model than (plain) indifferentiability: e.g., (plain) Merkle-Damgård is not indifferentiable but publicly indifferentiable [Dodis et al., 2009]
- Useful in practice, e.g., digital signature schemes

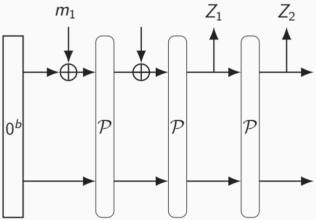
Sponge Indifferentiability

- Sponge indifferentiable with bound $\mathcal{O}\left(\frac{q^2}{2^c}\right)$ [Bertoni et al., 2008]
- Generalized sponge indifferentiable with bound $\mathcal{O}\left(\frac{q}{2^{c_a/2}}\right)$ as long as $c_s \geq c_a/2 + \log_2(c_a)$ [Naito and Ohta, 2014]

$\Longrightarrow$ At least $2^{c_a/2}$ queries to differentiate with high probability

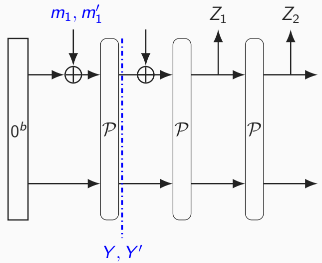
- Tight bound: inner collisions while absorbing allow to differentiate

Collision Attack with $q \approx 2^{c_a/2}$ queries [Bertoni et al., 2011]



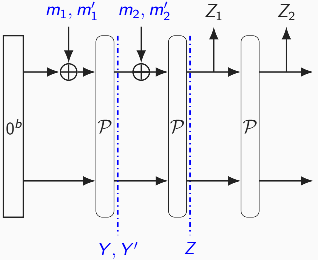
- Query $\mathcal{P}(m_1 \| 0^{c_a})$ for $2^{c_a/2}$ different m_1's and store them in a list L

Collision Attack with $q \approx 2^{c_a/2}$ queries [Bertoni et al., 2011]



- Query $\mathcal{P}(m_1 \| 0^{c_a})$ for $2^{c_a/2}$ different m_1's and store them in a list L
- With high probability there exist $Y \neq Y' \in L$ s.t., $\text{inner}_{c_a}(Y) = \text{inner}_{c_a}(Y')$

Collision Attack with $q \approx 2^{c_a/2}$ queries [Bertoni et al., 2011]

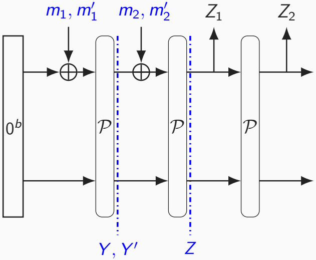


- Query $\mathcal{P}(m_1 \| 0^{c_a})$ for $2^{c_a/2}$ different m_1's and store them in a list L
- With high probability there exist $Y \neq Y' \in L$ s.t., $\text{inner}_{c_a}(Y) = \text{inner}_{c_a}(Y')$

$\Longrightarrow$ Take $m_2 = \text{outer}_{r_a}(Y)$ and $m_2' = \text{outer}_{r_a}(Y')$

$\Longrightarrow$ It gives $0^b \xrightarrow[m_1 \| m_2]{m_1' \| m_2'} Z$

Collision Attack with $q \approx 2^{c_a/2}$ queries [Bertoni et al., 2011]



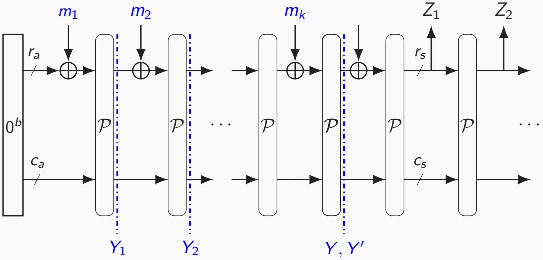
- Query $\mathcal{P}(m_1 \| 0^{c_a})$ for $2^{c_a/2}$ different m_1's and store them in a list L
- With high probability there exist $Y \neq Y' \in L$ s.t., $\text{inner}_{c_a}(Y) = \text{inner}_{c_a}(Y')$

$\implies$ Take $m_2 = \text{outer}_{r_a}(Y)$ and $m_2' = \text{outer}_{r_a}(Y')$

$\implies$ It gives $0^b \xrightarrow[m_1 \| m_2]{m_1' \| m_2'} Z$

- Requires $r_a \geq c_a/2$ and two absorb calls

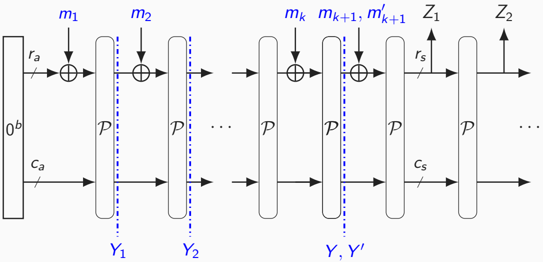
Collision Attack with $q \approx 2^{c_a/2}$ queries [Bertoni et al., 2011]



General case:

- Let $k = \lceil \frac{c_a}{2r_a} \rceil$
- One absorb round gives 2^{r_a} different states: not enough for an inner collision
- To have $2^{c_a/2}$ states (thus an inner collision w.h.p.,) need k absorb calls

Collision Attack with $q \approx 2^{c_a/2}$ queries [Bertoni et al., 2011]



General case:

- Let $k = \lceil \frac{c_a}{2r_a} \rceil$
- One absorb round gives 2^{r_a} different states: not enough for an inner collision
- To have $2^{c_a/2}$ states (thus an inner collision w.h.p.,) need k absorb calls
- Need also the compensation absorb call to have a full-state collision

$\Longrightarrow$ Requires $k+1$ absorb calls

Restricted Sponge

- Consider a sponge where at most ℓ absorb calls are allowed (but an arbitrary number of blocks can be squeezed)
  - Restrictive setting
  - Useful in e.g., password hashing, Fiat-Shamir transform

Restricted Sponge

- Consider a sponge where at most ℓ absorb calls are allowed (but an arbitrary number of blocks can be squeezed)
  - Restrictive setting
  - Useful in e.g., password hashing, Fiat-Shamir transform
- When $\ell < k+1$, the collision (thus differentiability) attack on the sponge does not apply anymore

Restricted Sponge

- Consider a sponge where at most ℓ absorb calls are allowed (but an arbitrary number of blocks can be squeezed)
  - Restrictive setting
  - Useful in e.g., password hashing, Fiat-Shamir transform
- When $\ell < k + 1$, the collision (thus differentiability) attack on the sponge does not apply anymore
- One full-state collision attack in $2^{b-\ell \times r_a}$ queries:
  1. Make all $\ell - 1$ first absorb call queries to obtain $\left(0^b \xrightarrow{M_i} Y_i\right)_i$
  2. Compute with primitive queries $0^b \xrightarrow{M_1} Y_1 \to N_1 \cdots \to N_{2^{b-\ell \times r_a}}$
  3. $2^{(\ell-1) \times r_a}$ Y_i states and $2^{b-\ell \times r_a}$ N_i states $\implies$ inner collision between some Y_i and N_j happens with high probability
  4. Use the last absorb call on Y_i to obtain a full state collision

Tightness of Indifferentiability With a Restricted Sponge

- Attack has a cost of $2^{b-\ell\times r_a}$ while indifferentiability of the sponge guarantees security up to $\approx 2^{c_a/2}$ queries

$\Longrightarrow$ There is a gap when $\ell < k+1$

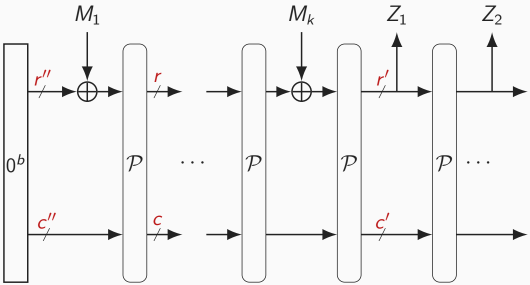
- Attack has a cost of $2^{b-\ell\times r_a}$ while indifferentiability of the sponge guarantees security up to $\approx 2^{c_a/2}$ queries

$\Longrightarrow$ There is a gap when $\ell < k+1$

- Contribution of this work:

$$\mathbf{Adv}^{\text{R-iff}}_{\mathsf{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

$$\mathbf{Adv}^{\text{R-pubiff}}_{\mathsf{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$



- When $\ell = 1$ the bound is already captured by an indifferentiability result from Naito and Ohta: set $r = 0, r' = r_s, r'' = r_a$
- New results whenever $1 < \ell < \lceil \frac{c_a}{2r_a} \rceil + 1$

Notation

- Define `AbsorbPath` as

$$\texttt{AbsorbPath} = \left\{0^b\right\} \cup \left\{ Y \mid \exists 0^b \xrightarrow{m_1\|\cdots\|m_l} Y \text{ with } l < \ell \right\}$$

$\Longrightarrow$ `AbsorbPath` contains the rooted nodes where absorption of a message block is still possible

- Remark: $|\texttt{AbsorbPath}| \le \min\left\{q+1, 2 \times 2^{(\ell-1)\times r_a}\right\}$

Notation

- Define `AbsorbPath` as

$$\texttt{AbsorbPath} = \left\{0^b\right\} \cup \left\{ Y \mid \exists 0^b \xrightarrow{m_1\|\cdots\|m_l} Y \text{ with } l < \ell \right\}$$

$\Longrightarrow$ `AbsorbPath` contains the rooted nodes where absorption of a message block is still possible

- Remark: $|\texttt{AbsorbPath}| \leq \min\left\{q+1, 2 \times 2^{(\ell-1)\times r_a}\right\}$
- $0^b \xrightarrow{m_1} A_1 \xrightarrow{m_2} \cdots \xrightarrow{m_l} A_l \longrightarrow S_1 \longrightarrow \cdots \longrightarrow S_n$ is a valid path whenever $l \leq \ell$

The Simulator Used

$\mathcal{S} = (\mathcal{S}_{\mathsf{fwd}}, \mathcal{S}_{\mathsf{inv}})$, similar to the one used in indifferentiability of sponge proof [Bertoni et al., 2008]:

- $\mathcal{S}$ keeps track of the graph construction
- $\mathcal{S}_{\mathsf{inv}}$ returns random elements
- On query with input X, $\mathcal{S}_{\mathsf{fwd}}$ keeps $\mathcal{RO}$-consistency whenever X appears in a valid path
- $\mathcal{S}$ behaves like a two-sided RF

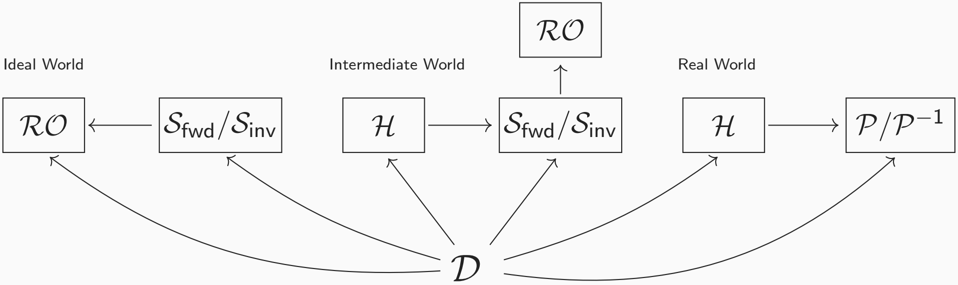
$\mathcal{S} = (\mathcal{S}_{\mathsf{fwd}}, \mathcal{S}_{\mathsf{inv}})$, similar to the one used in indifferentiability of sponge proof [Bertoni et al., 2008]:

- $\mathcal{S}$ keeps track of the graph construction
- $\mathcal{S}_{\mathsf{inv}}$ returns random elements
- On query with input X, $\mathcal{S}_{\mathsf{fwd}}$ keeps $\mathcal{RO}$-consistency whenever X appears in a valid path
- $\mathcal{S}$ behaves like a two-sided RF
- For public indifferentiability: build $\mathcal{S}'$ which additionally relays to $\mathcal{S}$ all primitive queries associated to the construction queries

World Decomposition

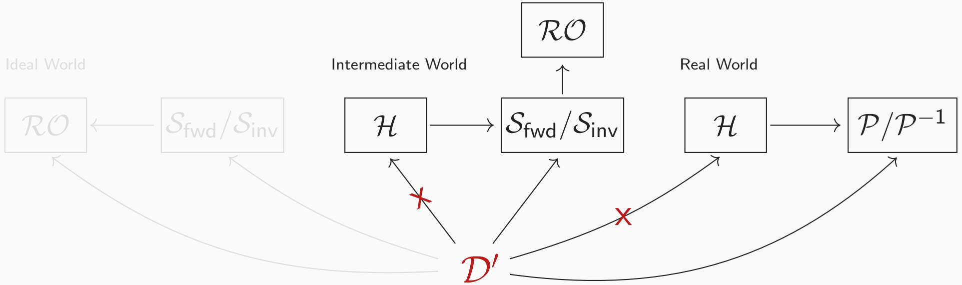
$$
\begin{tikzcd}
\text{Ideal World} & & & \text{Real World} & \\
\boxed{\mathcal{RO}} & \boxed{\mathcal{S}_{\mathsf{fwd}}/\mathcal{S}_{\mathsf{inv}}} \arrow[l] & & \boxed{\mathcal{H}} \arrow[r] & \boxed{\mathcal{P}/\mathcal{P}^{-1}} \\
& & \mathcal{D} \arrow[ull, bend left] \arrow[ul, bend left] \arrow[ur, bend right] \arrow[urr, bend right] & &
\end{tikzcd}
$$

World Decomposition

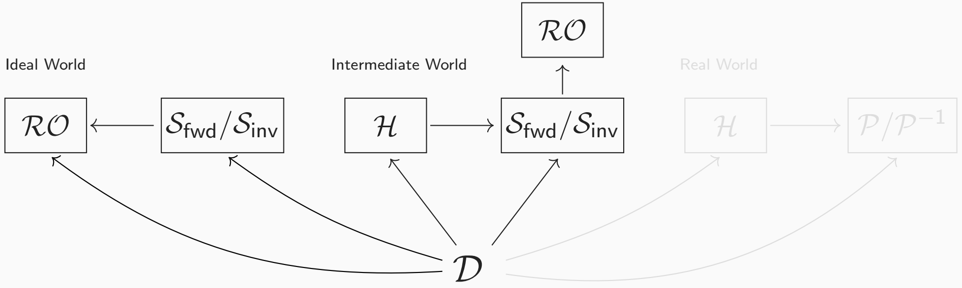


- One Intermediate World is introduced to facilitate the analysis

World Decomposition



- One Intermediate World is introduced to facilitate the analysis
- Intermediate versus Real: construction queries can be transformed into primitive queries $\implies$ PRP/PRF switching lemma



- One Intermediate World is introduced to facilitate the analysis
- Intermediate versus Real: construction queries can be transformed into primitive queries $\implies$ PRP/PRF switching lemma
- Ideal versus Intermediate: consistency of the simulator with respect to $\mathcal{RO}$ and extra queries to $\mathcal{S}$ in Intermediate World $\implies$ identical until **BAD**

Ideal versus Intermediate: Bad Events

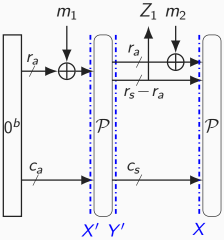
$$\mathbf{Adv}^{\text{R-iff}}_{\text{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

- **GUESS**: (only in Intermediate World) adversary guesses an intermediate state generated from construction queries without having made the primitive queries

  To do that, it can guess:

  1. Either the full state of any rooted node
  2. Either the inner part of a node in `AbsorbPath`

  GUESS does not apply in public indifferentiability



Ideal versus Intermediate: Bad Events

$$\mathbf{Adv}^{\text{R-iff}}_{\mathsf{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

- **GUESS**: (only in Intermediate World) adversary guesses an intermediate state generated from construction queries without having made the primitive queries
  To do that, it can guess:
  1. Either the full state of any rooted node
  2. Either the inner part of a node in `AbsorbPath`

  GUESS does not apply in public indifferentiability
- **INNER**: inner collisions with `AbsorbPath`

$$\mathbf{Adv}^{\text{R-iff}}_{\text{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

- **GUESS**: (only in Intermediate World) adversary guesses an intermediate state generated from construction queries without having made the primitive queries

  To do that, it can guess:

  1. Either the full state of any rooted node
  2. Either the inner part of a node in `AbsorbPath`

  GUESS does not apply in public indifferentiability
- **INNER**: inner collisions with `AbsorbPath`
- **COL**: $X_i = X_j$ or $Y_i = Y_j$ for some $j < i$

Ideal versus Intermediate: Bad Events

$$\mathbf{Adv}^{\text{R-iff}}_{\text{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

- **GUESS**: (only in Intermediate World) adversary guesses an intermediate state generated from construction queries without having made the primitive queries
  To do that, it can guess:
  1. Either the full state of any rooted node
  2. Either the inner part of a node in `AbsorbPath`

  GUESS does not apply in public indifferentiability
- **INNER**: inner collisions with `AbsorbPath`
- **COL**: $X_i = X_j$ or $Y_i = Y_j$ for some $j < i$
- **CONNECT**: $Y_i = X_j$ or $X_i = Y_j$ for some $j < i$

Tightness of the bound

- Remember that

$$\mathbf{Adv}^{\text{R-iff}}_{\text{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

- Inner collision attack has a cost of $\approx \max\left\{2^{c_a/2}; 2^{b-\ell\times r_a}\right\}$ queries
- What about the others terms?

Tightness of the bound

- Remember that

$$\textbf{Adv}^{\text{R-iff}}_{\text{Sponge}}(q,\ell) = \mathcal{O}\left(\frac{q}{2^{c_s}} + \frac{q^2}{2^b} + \min\left\{\frac{q^2}{2^{c_a}}, \frac{q}{2^{b-\ell\times r_a}}\right\}\right)$$

- Inner collision attack has a cost of $\approx \max\left\{2^{c_a/2}; 2^{b-\ell\times r_a}\right\}$ queries
- What about the others terms?
  - 2^{c_s} queries: adversary can try all inner parts
  - $2^{b/2}$ queries: adversary can set **CONNECT**

Application

- Ascon-hash
  - $b = 320, c = 256, r = 64$
  - Unrestricted sponge: 128 bits of security
  - Sponge with input messages of at most 127 bits: 160 bits of security
- Photon Beetle-Hash or T-Quark
  - $b = 256, c = 224, r = 32$
  - Unrestricted sponge: 112 bits of security
  - Sponge with input messages of at most 127 bits: 128 bits of security
- To maximize security and absorbing rate, the best parameter choice is $\ell = 1, c_a = r_a = b/2$

Conclusion

- Proved a tight indifferentiability bound for the sponge construction when the number of message blocks is restricted
- It gives a better security bound when less than $\lceil \frac{c_a}{2r_a} \rceil + 1$ blocks are absorbed

Thank you for your attention!

Bertoni, G., Daemen, J., Peeters, M., and Van Assche, G. (2007).
Sponge functions.
Ecrypt Hash Workshop 2007.

Bertoni, G., Daemen, J., Peeters, M., and Van Assche, G. (2008).
On the Indifferentiability of the Sponge Construction.
In Smart, N. P., editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer.

Bertoni, G., Daemen, J., Peeters, M., and Van Assche, G. (2011).
Cryptographic sponge functions.
`https://keccak.team/files/CSF-0.1.pdf`.

Coron, J., Dodis, Y., Malinaud, C., and Puniya, P. (2005).
Merkle-Damgård Revisited: How to Construct a Hash Function.
In Shoup, V., editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 430–448. Springer.

Dodis, Y., Ristenpart, T., and Shrimpton, T. (2009).
Salvaging merkle-damgård for practical applications.
In Joux, A., editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 371–388. Springer.

Guo, J., Peyrin, T., and Poschmann, A. (2011).
The PHOTON family of lightweight hash functions.
In Rogaway, P., editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer.

Maurer, U. M., Renner, R., and Holenstein, C. (2004).
Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology.
In Naor, M., editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer.

Naito, Y. and Ohta, K. (2014).
Improved indifferentiable security analysis of PHOTON.
In Abdalla, M. and Prisco, R. D., editors, *Security and Cryptography for Networks - 9th International Conference, SCN 2014, Amalfi, Italy, September 3-5, 2014. Proceedings*, volume 8642 of *Lecture Notes in Computer Science*, pages 340–357. Springer.

Yoneyama, K., Miyagawa, S., and Ohta, K. (2009).
Leaky random oracle.
IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 92-A(8):1795–1807.