Lifting Standard Model Reductions to Common Setup Assumptions

Ngoc Khanh Nguyen[1] **Eftychios Theodorakis**[2] Bogdan Warinschi[3,4]

IBM Research Europe – Zurich and ETH Zurich

Dicrypt

Dfinity

University of Bristol

March 8/7, 10:30-11:00 JST/1:30-2:00 UTC

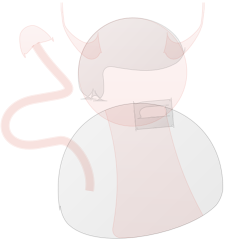
PKC 2022

Outline: In this Talk...

1. High level Abstract Definitions: Reductions
2. How to lift the BB reduction?
3. Claim
4. Well Defined Setup Assumptions
5. Intuition over Technical Points
6. Summary

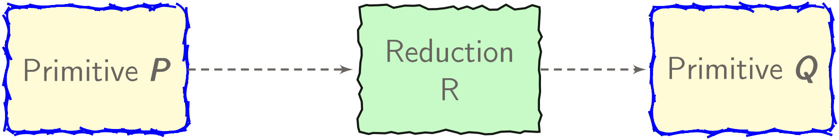
A Black Box Construction

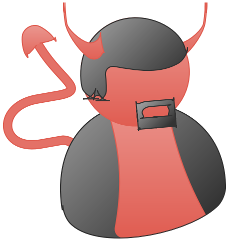
Primitive $\boldsymbol{P}$ $\xrightarrow{\text{Based on}}$ Primitive $\boldsymbol{Q}$



$Pr[R_P^{Q,A}]$

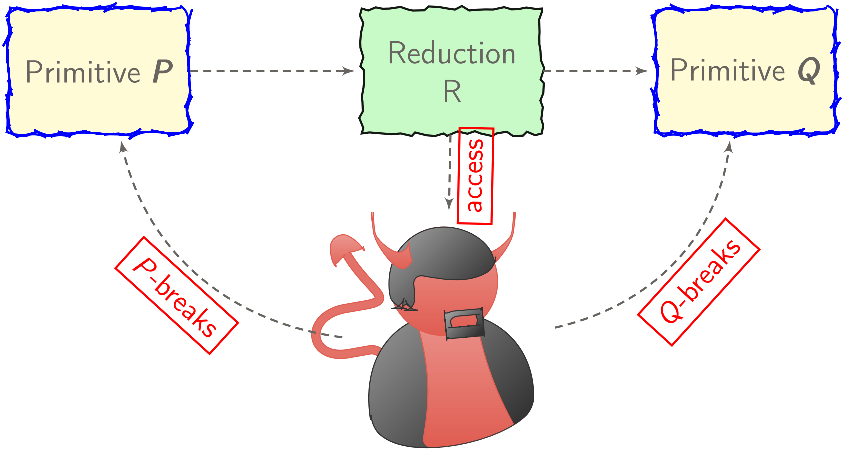
A Black Box Construction





$$Pr[R_P^{Q,A}]$$

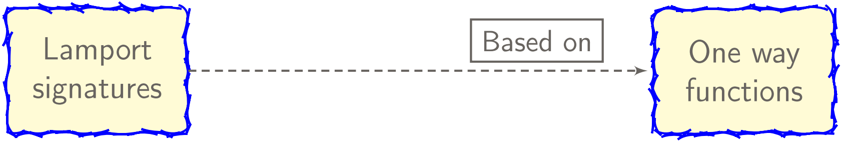
A Black Box Construction



$Pr[R_P^{Q,A}]$

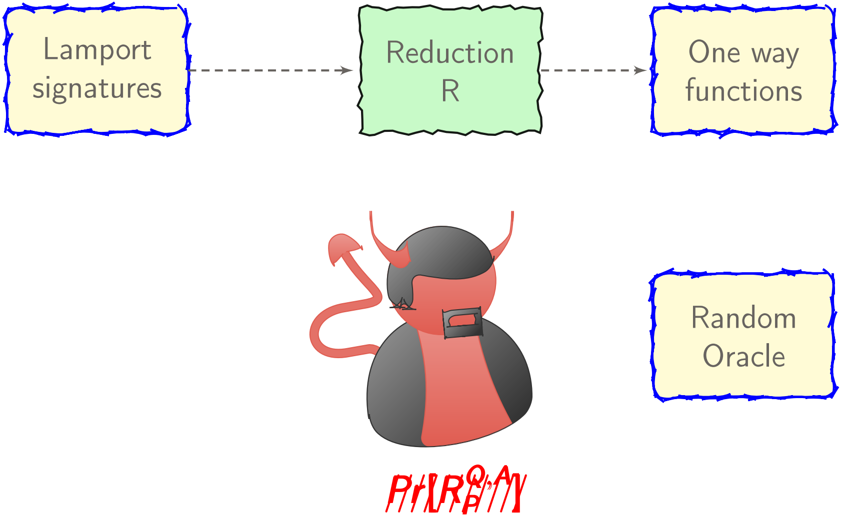
Example: Lamport one time signatures

For concreteness: let's use ... lamport one time signature.



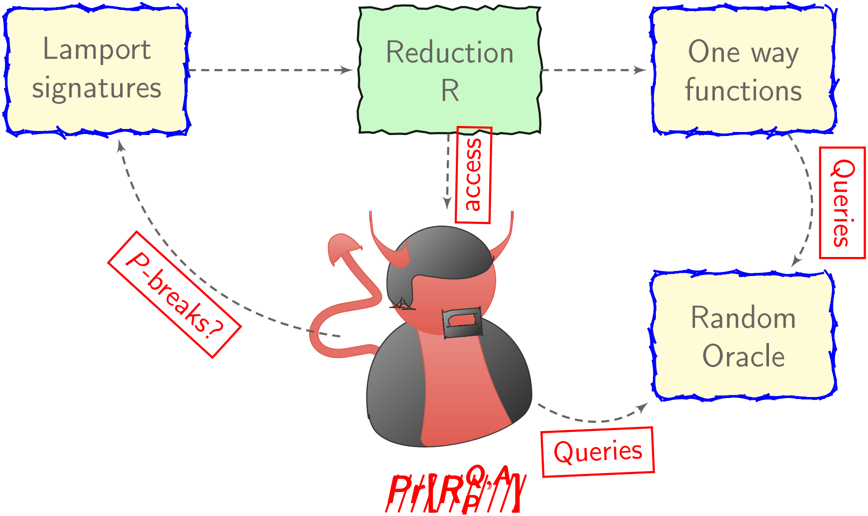
Example: Lamport one time signatures

For concreteness: let's use ... lamport one time signature.



Example: Lamport one time signatures

For concreteness: let's use ... lamport one time signature.



Striking out the problems

- How to make the Reduction[1,2,3] work?
- Establish Correctness?
- Sampling over Oracle Machines?
- Sampling over an Infinite (Countable) Spaces (example: Random Oracle)?

---

[1] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Notions of Reducibility between Cryptographic Primitives". In: 2004, pp. 1–20. DOI: 10.1007/978-3-540-24638-1_1.

[2] Paul Baecher, Christina Brzuska, and Marc Fischlin. "Notions of Black-Box Reductions, Revisited". In: 2013, pp. 296–315. DOI: 10.1007/978-3-642-42033-7_16.

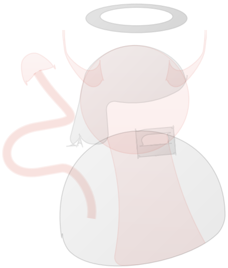
[3] Dennis Hofheinz and Ngoc Khanh Nguyen. "On Tightly Secure Primitives in the Multi-instance Setting". In: 2019, pp. 581–611. DOI: 10.1007/978-3-030-17253-4_20.

Setup Assumptions

- Random Oracle model
- Ideal Cipher model
- Common Random String (CRS)
- Random Beacon

Example: Lamport One Time signatures via Random Oracle

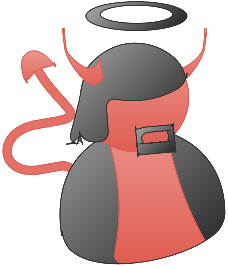
$$\text{Lamport signatures} \xrightarrow{\boxed{\text{Based on}}} \text{One way functions}$$



$Pr[R_P^{f^O, A^O}]$

Example: Lamport One Time signatures via Random Oracle

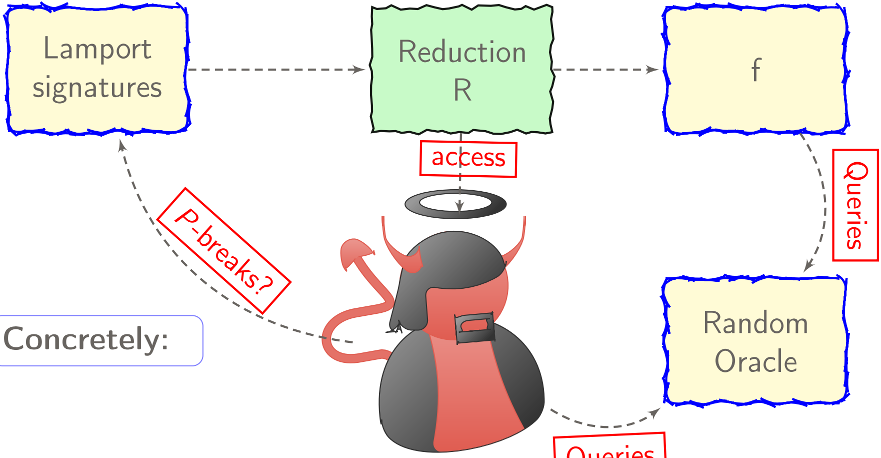
Lamport signatures → Reduction R → f



Random Oracle

$Pr[R_P^{f^O, A^O}]$

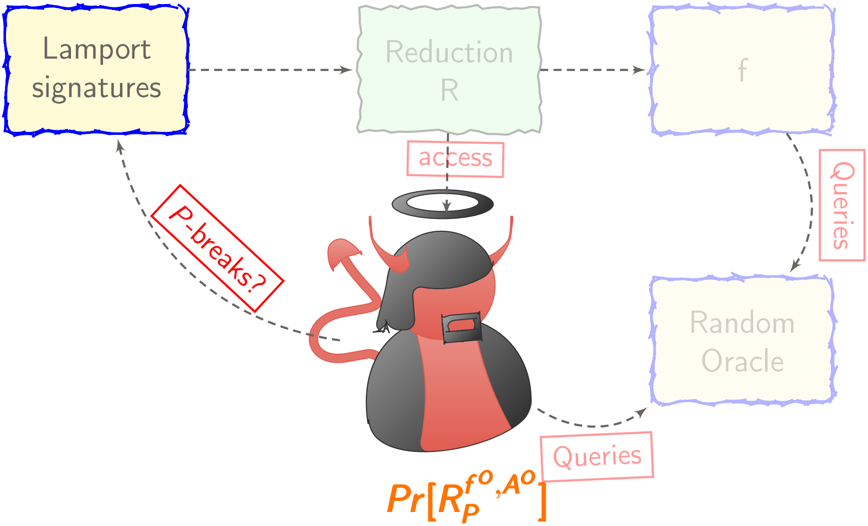
Example: Lamport One Time signatures via Random Oracle



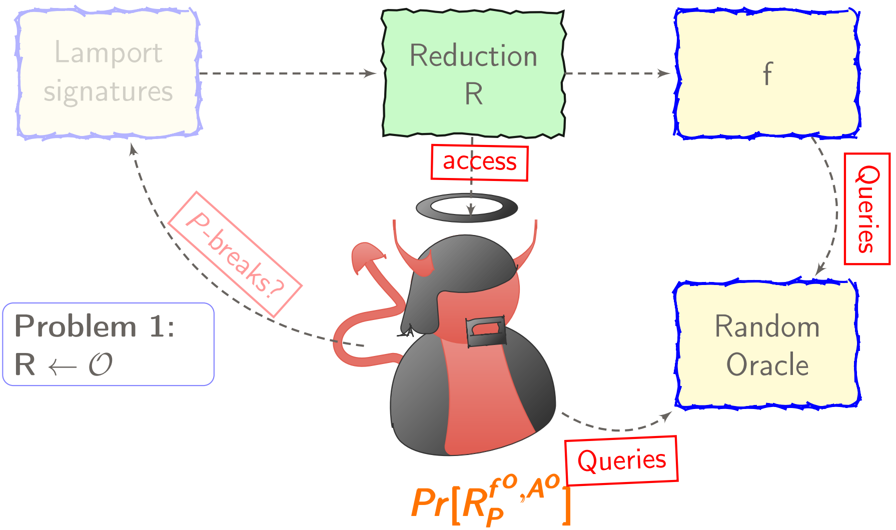
Concretely:

$Pr[R_P^{f^O, A^O}]$

The Problems

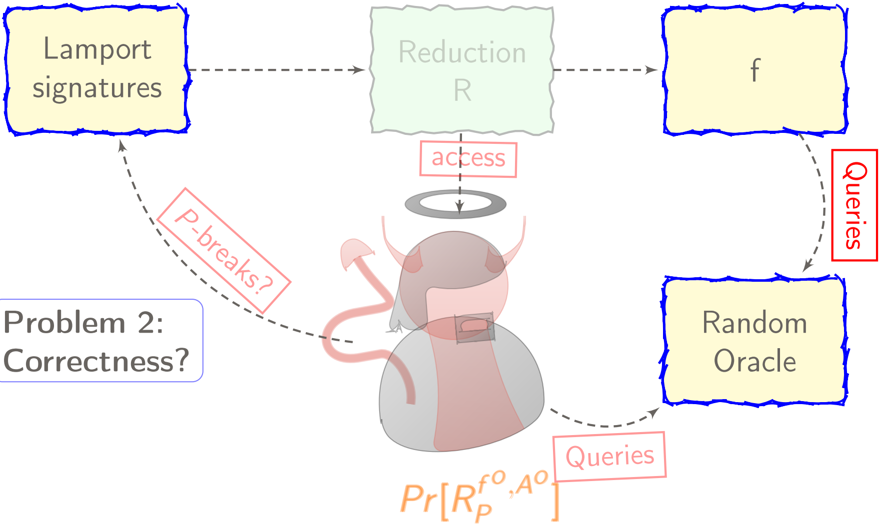


The Problems



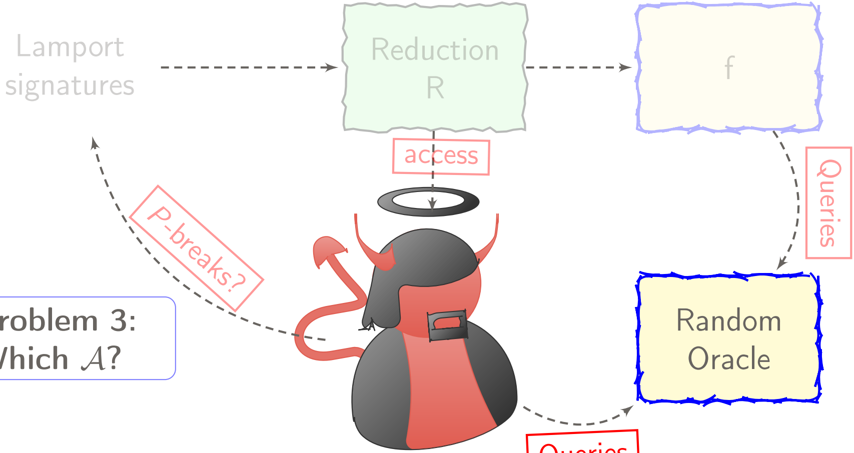
Problem 1:
R $\leftarrow \mathcal{O}$

The Problems



Problem 2: Correctness?

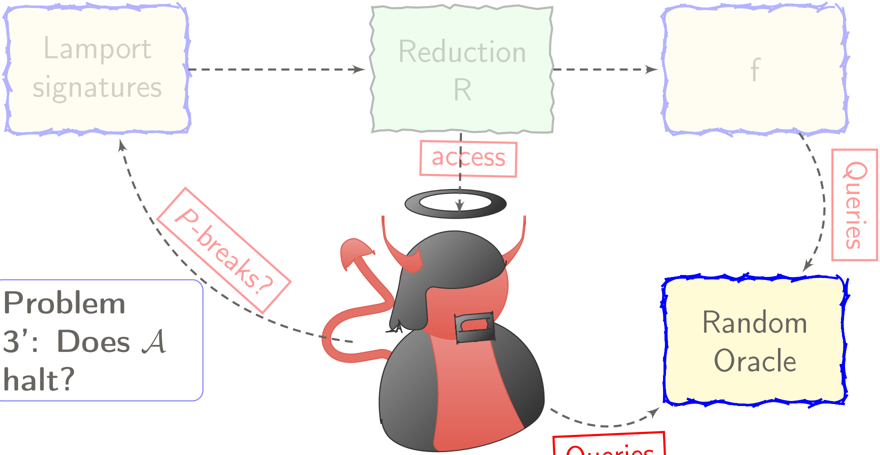
The Problems



Problem 3: Which $\mathcal{A}$?

$Pr[R_P^{f^O, A^O}]$

The Problems



Problem 3': Does $\mathcal{A}$ halt?

$Pr[R_P^{f^O, A^O}]$

Sketched Result

$$
\begin{tikzcd}
\mathcal{A}\ P-\text{breaks}\ G^{f} \arrow[r, hook, "R"] \arrow[d] & \mathcal{S}^{f,\mathcal{A}}\ Q-\text{breaks}\ f \arrow[d] \\
\mathcal{B}^{\mathcal{O}}\ P-\text{breaks}\ G^{f^{\mathcal{O}}} \arrow[r, hook, "R"] & \mathcal{S}^{f^{\mathcal{O}},\mathcal{B}^{\mathcal{O}}}\ Q-\text{breaks}\ f^{\mathcal{O}}
\end{tikzcd}
$$

Informal Theorem

$$
\begin{tikzcd}
 & P - \text{breaks } G^f \arrow[d, color=orange] \arrow[r, hook, "R"] & \mathcal{S}^{f,\mathcal{A}} & Q - \text{breaks } f \arrow[d, color=orange] \\
\mathcal{B}^{\mathcal{O}} & P - \text{breaks } G^{f^{\mathcal{O}}} \arrow[r, hook, "R"] & \mathcal{S}^{f^{\mathcal{O}},\mathcal{B}^{\mathcal{O}}} & Q - \text{breaks } f^{\mathcal{O}}
\end{tikzcd}
$$

Theorem

[4] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Notions of Reducibility between Cryptographic Primitives". In: 2004, pp. 1–20. DOI: 10.1007/978-3-540-24638-1_1.

Informal Theorem

$$\begin{tikzcd}
P - \text{breaks } G^f \arrow[d] \arrow[r, hook, "R" description] & \mathcal{S}^{f,\mathcal{A}} \ Q - \text{breaks } f \arrow[d] \\
\mathcal{B}^{\mathcal{O}} \ P - \text{breaks } G^{f^{\mathcal{O}}} \arrow[r, hook, "R" description] & \mathcal{S}^{f^{\mathcal{O}},\mathcal{B}^{\mathcal{O}}} \ Q - \text{breaks } f^{\mathcal{O}}
\end{tikzcd}$$

Theorem

1. *Primitives P, Q, and setup assumption M*

[4] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Notions of Reducibility between Cryptographic Primitives". In: 2004, pp. 1–20. DOI: 10.1007/978-3-540-24638-1_1.

Informal Theorem

$$\begin{array}{ccc} P-\text{breaks } G^f & \hookleftarrow R \longrightarrow & \mathcal{S}^{f,\mathcal{A}}\ Q-\text{breaks } f \\ \downarrow & & \downarrow \\ \mathcal{B}^{\mathcal{O}}\ P-\text{breaks } G^{f^{\mathcal{O}}} & \hookleftarrow R \rightarrow & \mathcal{S}^{f^{\mathcal{O}},\mathcal{B}^{\mathcal{O}}}\ Q-\text{breaks } f^{\mathcal{O}} \end{array}$$

Theorem

1. *Primitives P, Q, and setup assumption M*
2. *Fully Black-Box reduction from P to Q (Standard Model)*

---

[4] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Notions of Reducibility between Cryptographic Primitives". In: 2004, pp. 1–20. DOI: 10.1007/978-3-540-24638-1_1.

Informal Theorem

$$
\begin{tikzcd}
P-\text{breaks } G^{f} \arrow[d] & \hookleftarrow R \longrightarrow & \mathcal{S}^{f,\mathcal{A}}\ Q-\text{breaks } f \arrow[d] \\
\mathcal{B}^{\mathcal{O}}\ P-\text{breaks } G^{f^{\mathcal{O}}} & \hookleftarrow R \rightarrow & \mathcal{S}^{f^{\mathcal{O}},\mathcal{B}^{\mathcal{O}}}\ Q-\text{breaks } f^{\mathcal{O}}
\end{tikzcd}
$$

Theorem

1. *Primitives P, Q, and setup assumption M*
2. *Fully Black-Box reduction from P to Q (Standard Model)*
3. $\Longrightarrow$ *reduction from P to Q in setup assumption M*

[4] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Notions of Reducibility between Cryptographic Primitives". In: 2004, pp. 1–20. DOI: 10.1007/978-3-540-24638-1_1.

Informal Theorem

We extend RTV[4]!

$$
\begin{tikzcd}
P-\text{breaks } G^{f} \arrow[r, hook', "R"] \arrow[d] & \mathcal{S}^{f,\mathcal{A}} \; Q-\text{breaks } f \arrow[d] \\
\mathcal{B}^{\mathcal{O}} \; P-\text{breaks } G^{f^{\mathcal{O}}} \arrow[r, hook', "R"] & \mathcal{S}^{f^{\mathcal{O}},\mathcal{B}^{\mathcal{O}}} \; Q-\text{breaks } f^{\mathcal{O}}
\end{tikzcd}
$$

Theorem

1. *Primitives P, Q, and setup assumption M*
2. *Fully Black-Box reduction from P to Q (Standard Model)*
3. $\Longrightarrow$ *reduction from P to Q in setup assumption M*

[4] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Notions of Reducibility between Cryptographic Primitives". In: 2004, pp. 1–20. DOI: 10.1007/978-3-540-24638-1_1.

Beyond BBB[5]

Where do we stand in Baecher, Brzuska, and Fischlin?

[5] Paul Baecher, Christina Brzuska, and Marc Fischlin. "Notions of Black-Box Reductions, Revisited". In: 2013, pp. 296–315. DOI: 10.1007/978-3-642-42033-7_16.

Beyond BBB[5]

Kind	Definition				Implication
BBB	$\exists G$	$\exists \mathcal{S}$	$\forall f$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
BNB	$\exists G$	$\forall \mathcal{A}$	$\exists \mathcal{S}$	$\forall f$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
BBN	$\exists G$	$\forall f$	$\exists \mathcal{S}$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
BNN	$\exists G$	$\forall f$	$\forall \mathcal{A}$	$\exists \mathcal{S}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
NBB	$\exists \mathcal{S}$	$\forall f$	$\exists G$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
NBN	$\forall f$	$\exists G$	$\exists \mathcal{S}$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
NNN	$\forall f$	$\exists G$	$\forall \mathcal{A}$	$\exists \mathcal{S}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$

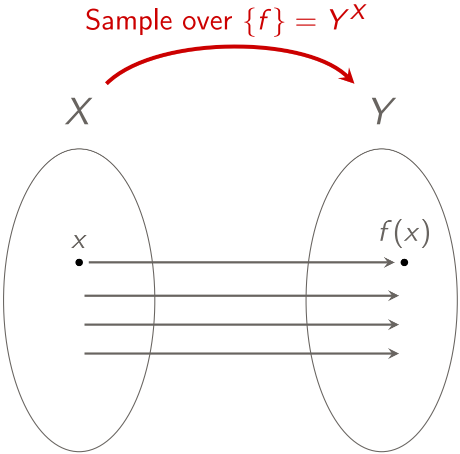
[5] Paul Baecher, Christina Brzuska, and Marc Fischlin. "Notions of Black-Box Reductions, Revisited". In: 2013, pp. 296–315. DOI: 10.1007/978-3-642-42033-7_16.

Instantiating a new Setup Assumption

1. Can write concretely
2. Consistent Sampling

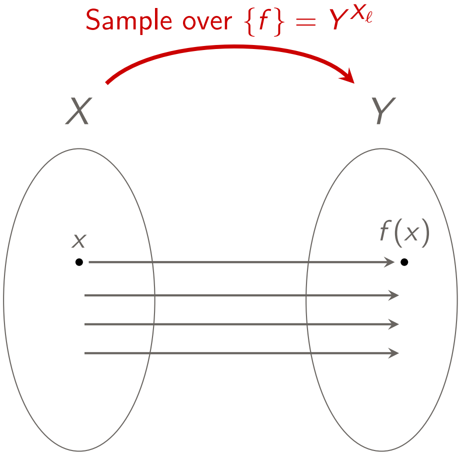
Instantiating a new Setup Assumption

1. Can write concretely
2. Consistent Sampling



Instantiating a new Setup Assumption

1. Can write concretely
2. Consistent Sampling (parametric sampling $\ell + 1$ "agrees" with previous samplings)



Sketching the Intuition

Primitive P

Primitive f

Primitive P

Primitive f^{O}

$\forall$ 

$\Pr[R_P^{f^{\mathcal{O}}, \mathcal{A}^{\mathcal{O}}}]$

Sketching the Intuition

Primitive P

Primitive f

Oracle $\mathcal{O}$ Inst

Primitive P

Primitive $f^{\mathcal{O}}$

$\forall$

$$\Pr[R_P^{f^{\mathcal{O}}, \mathcal{A}^{\mathcal{O}}}]$$

Sketching the Intuition

Primitive P

Primitive f

Oracle $\mathcal{O}$ Inst

Primitive P

Primitive $f^{\mathcal{O}}$

$\forall$

$$\Pr_{\mathcal{A}\in OA}\left[R_P^{f^{\mathcal{O}},\, \mathcal{A}^{\mathcal{O}}}\right]$$

Sketching the Intuition

Primitive $\boldsymbol{P}$

Primitive $\boldsymbol{f}_{\boldsymbol{k}}$

Oracle $\mathcal{O}$ Inst

Primitive $\boldsymbol{P}$

Primitive $\boldsymbol{f}^{\boldsymbol{O}}{}_{\boldsymbol{k}}$

$\forall$

$$\Pr_{\mathcal{A}\in OA}\left[R_P^{f_k^{\mathcal{O}},\ \mathcal{A}^{\mathcal{O}}}\right]$$

Sketching the Intuition

Primitive P

Primitive f_k

$\forall$

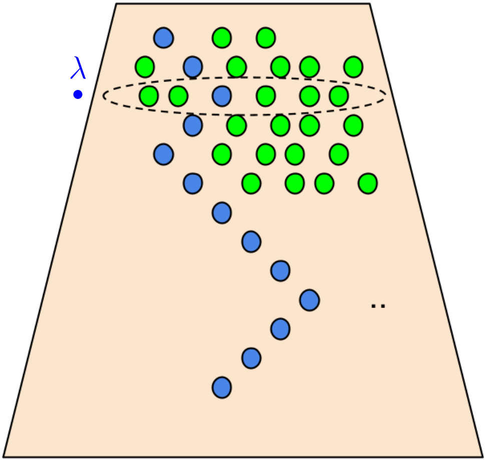
Oracle $\mathcal{O}$ Inst

$$\Pr_{\mathcal{A} \in OA}[R_P^{f_k^{\mathcal{O}},\ \mathcal{A}^{\mathcal{O}}{}_{\ell}}]$$

Primitive P

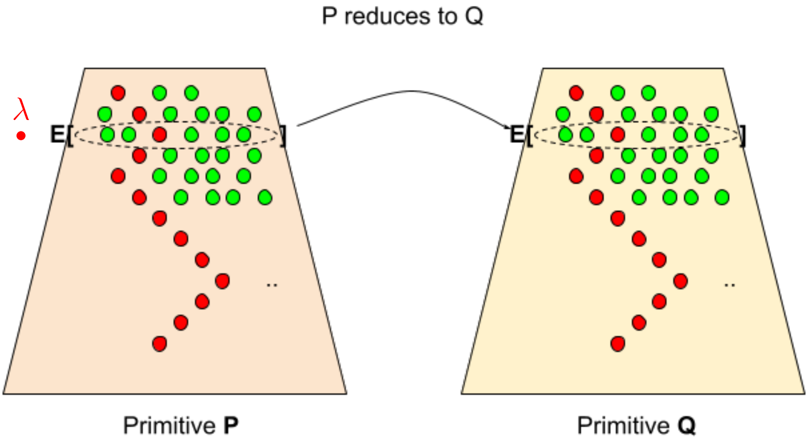
Primitive $f^{O}{}_{k}$

Oracle Instantiations



Primitive **P**

Oracle Instantiations (cont'd)



Future Work & Summary

Summary:

- Standard model reductions lift to setup assumptions even with unbounded adversaries

Questions:

- rest of the hierarchy Baecher, Brzuska, and Fischlin

Contact:

Shoot us an email/contact us to grab some (virtual) coffee and chat!

- nkn@zurich.ibm.com – Ngoc Khanh Nguyen
- crypto@eftychis.org – **Eftychios Theodorakis**
- csxbw@bristol.ac.uk – Bogdan Warinschi