Beyond Uber:
Instantiating Generic Groups via PGGs

Balthazar Bauer[1], Pooya Farshim[2], Patrick Harasser[3], and Adam O'Neill[4]

[1]IRIF, CNRS, France
[2]IOHK and Durham University, UK
[3]Technische Universität Darmstadt, Germany
[4]University of Massachusetts Amherst, USA

TCC 2022

November 10th, 2022

Background and Motivation

Two step process for building cryptographic schemes

- Design + proof in idealized model
- Heuristic instantiation

Background and Motivation

Two step process for building cryptographic schemes

- Design + proof in idealized model
- Heuristic instantiation

This paradigm is not sound [CGH98; MRH04; Den02]

Find standard-model assumptions which

- Can be satisfied by building blocks
- Yield interesting applications

[CGH98]: Canetti, Goldreich, Halevi. The Random Oracle Methodology, Revisited. *STOC 1998*.

[MRH04]: Maurer, Renner, Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. *TCC 2004*.

[Den02]: Dent. Adapting the Weaknesses of the Random Oracle Model to the Generic Group Model. *ASIACRYPT 2002*.

Idealized Models vs. Assumptions

Primitive	Idealized Model	Assumption
Hash function	ROM	CR, OW, Elf, UCE, ...

Idealized Models vs. Assumptions

Primitive	Idealized Model	Assumption
Hash function	ROM	CR, OW, Elf, UCE, ...
Permutation	RPM	psPRP [ST17]

[ST17]: Soni, Tessaro. Public-Seed Pseudorandom Permutations. *EUROCRYPT 2017*.

Idealized Models vs. Assumptions

Primitive	Idealized Model	Assumption
Hash function	ROM	CR, OW, Elf, UCE, ...
Permutation	RPM	psPRP [ST17]
Cryptographic group	GGM	$\underbrace{\text{DDH, } q\text{-DDH, DDHI, ...}}_{\text{Uber}}$, ...

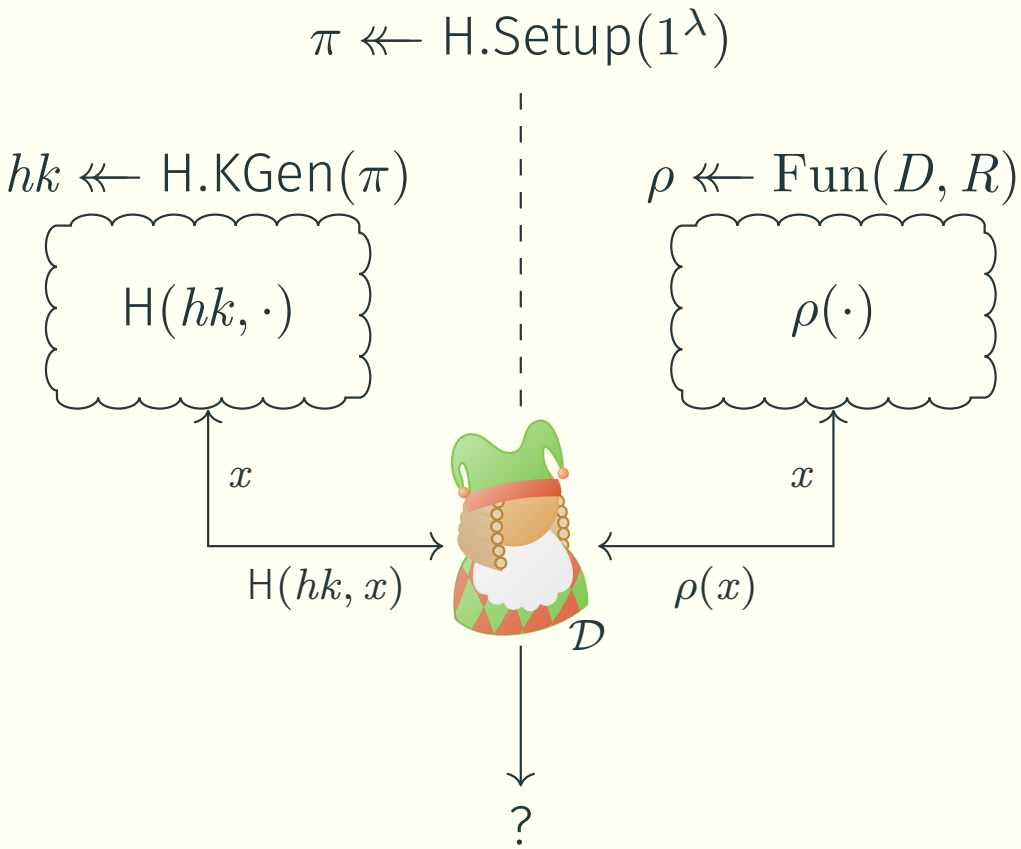
[ST17]: Soni, Tessaro. Public-Seed Pseudorandom Permutations. *EUROCRYPT 2017*.

Idealized Models vs. Assumptions

Primitive	Idealized Model	Assumption
Hash function	ROM	CR, OW, Elf, UCE, ...
Permutation	RPM	psPRP [ST17]
Cryptographic group	GGM	DDH, q-DDH, DDHI, ... (Uber), ... ?

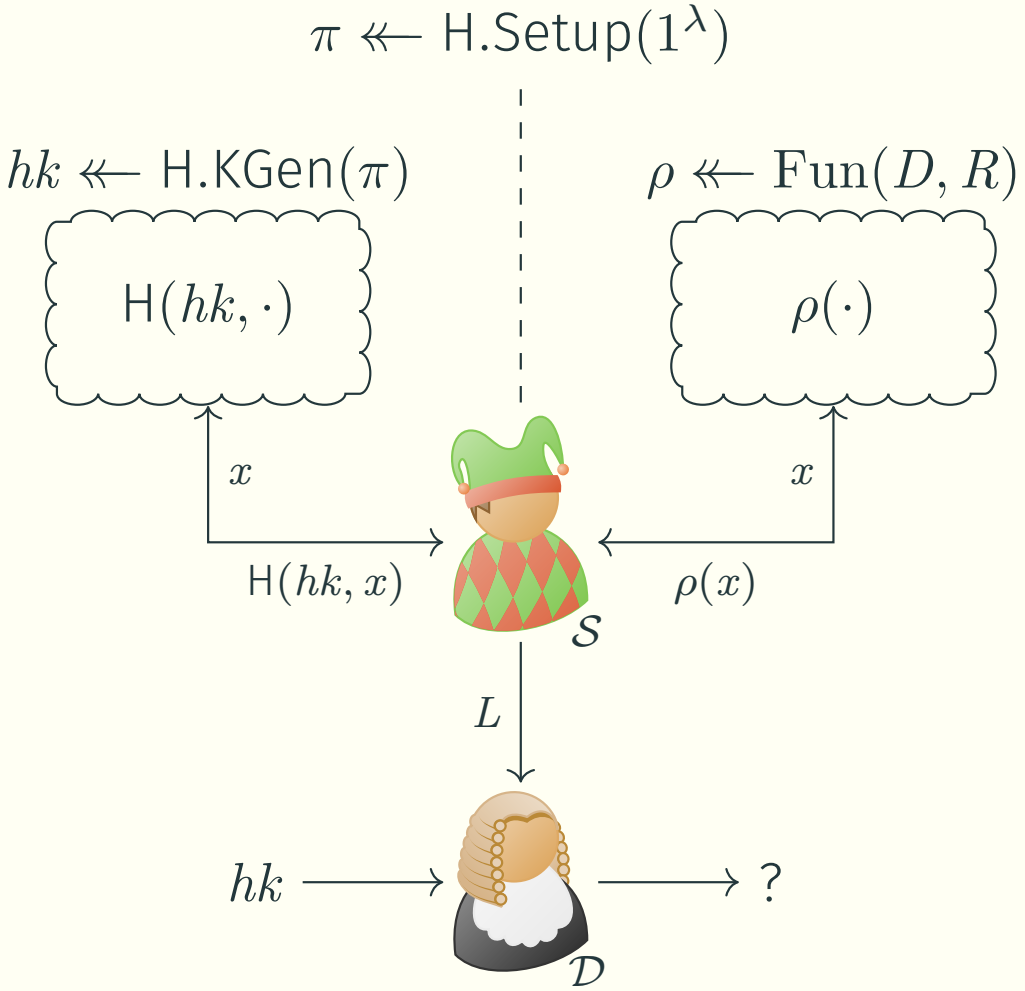
[ST17]: Soni, Tessaro. Public-Seed Pseudorandom Permutations. *EUROCRYPT 2017*.

UCE Security for Hash Functions [BHK13]



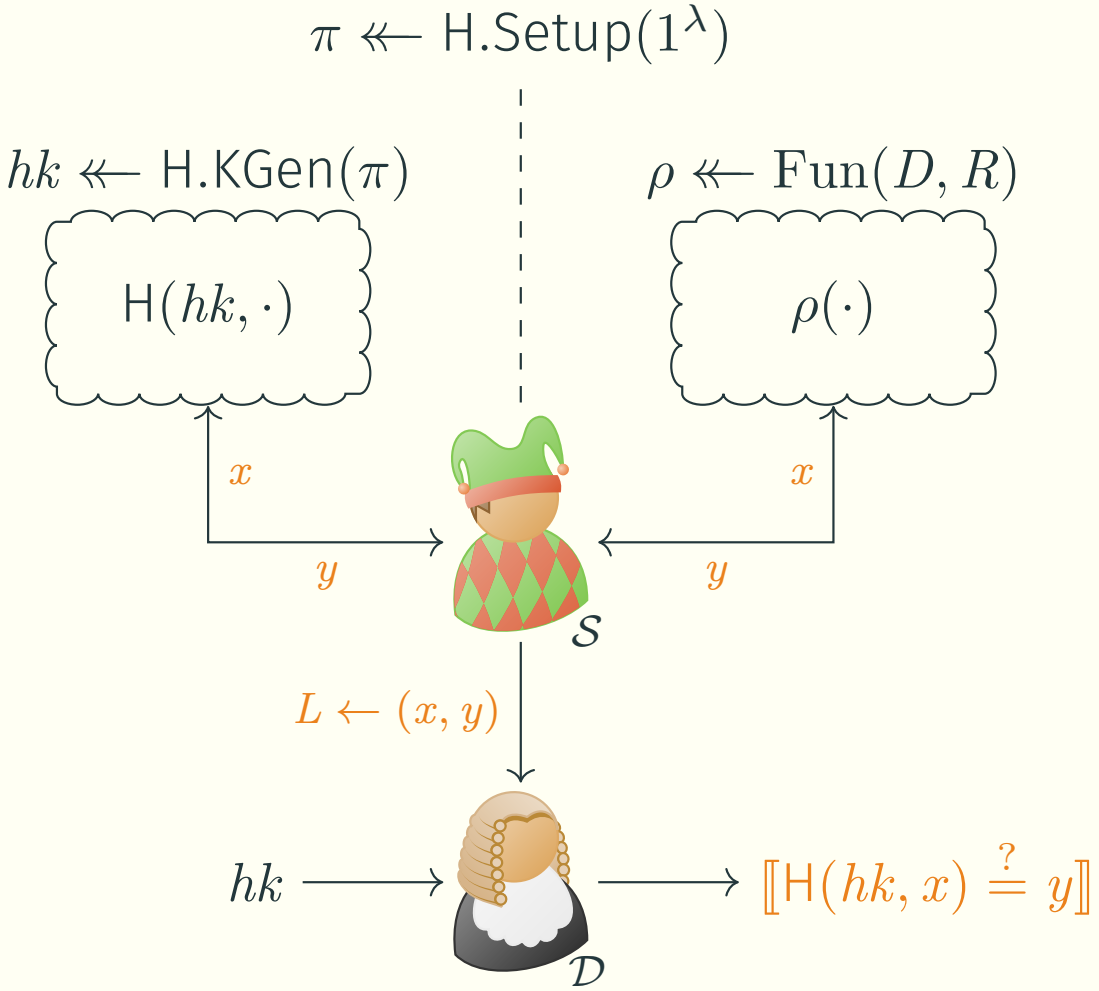
[BHK13]: Bellare, Hoang, Keelveedhi. Instantiating Random Oracles via UCEs. *CRYPTO 2013*.

UCE Security for Hash Functions [BHK13]



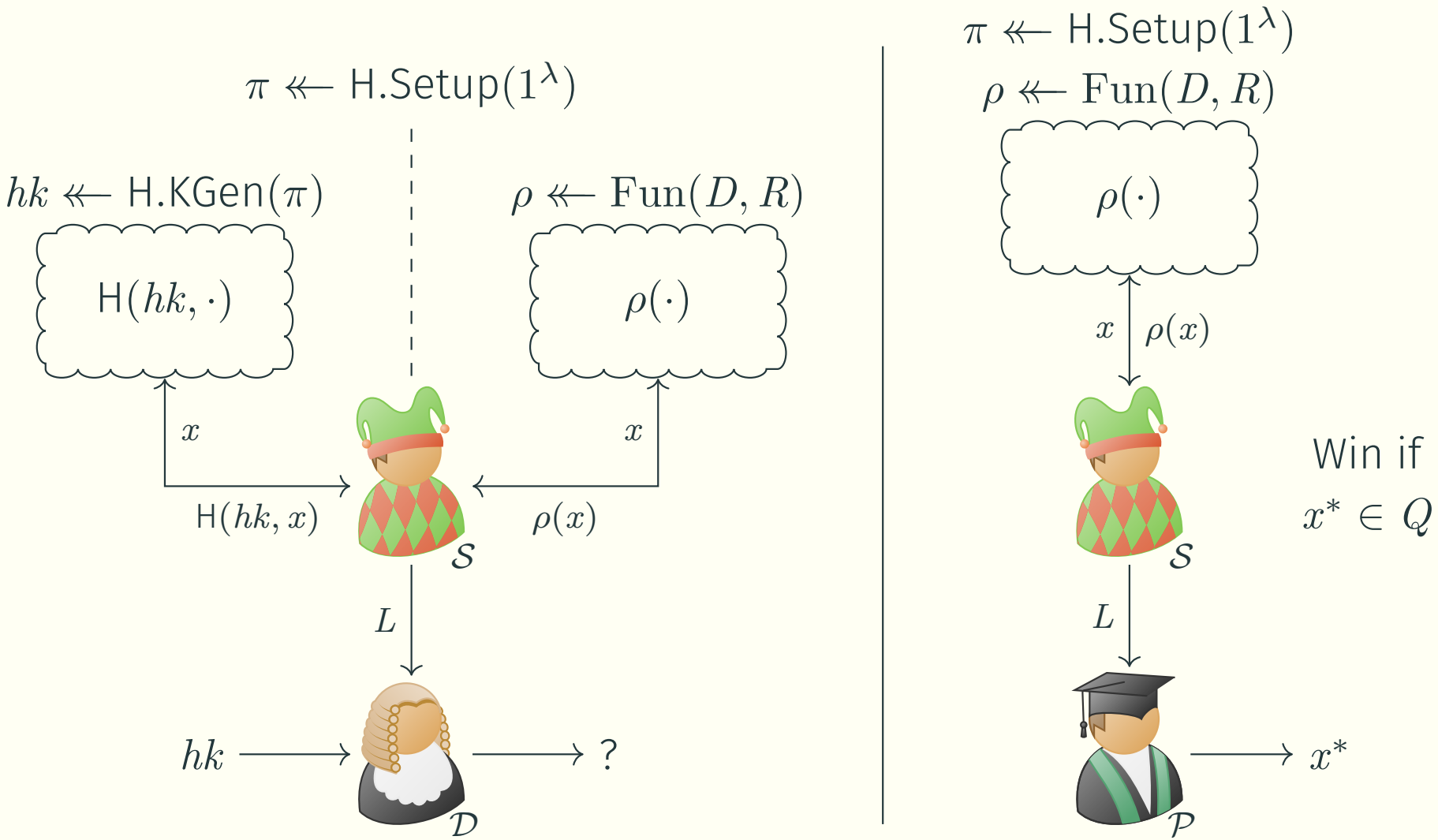
[BHK13]: Bellare, Hoang, Keelveedhi. Instantiating Random Oracles via UCEs. *CRYPTO 2013*.

UCE Security for Hash Functions [BHK13]



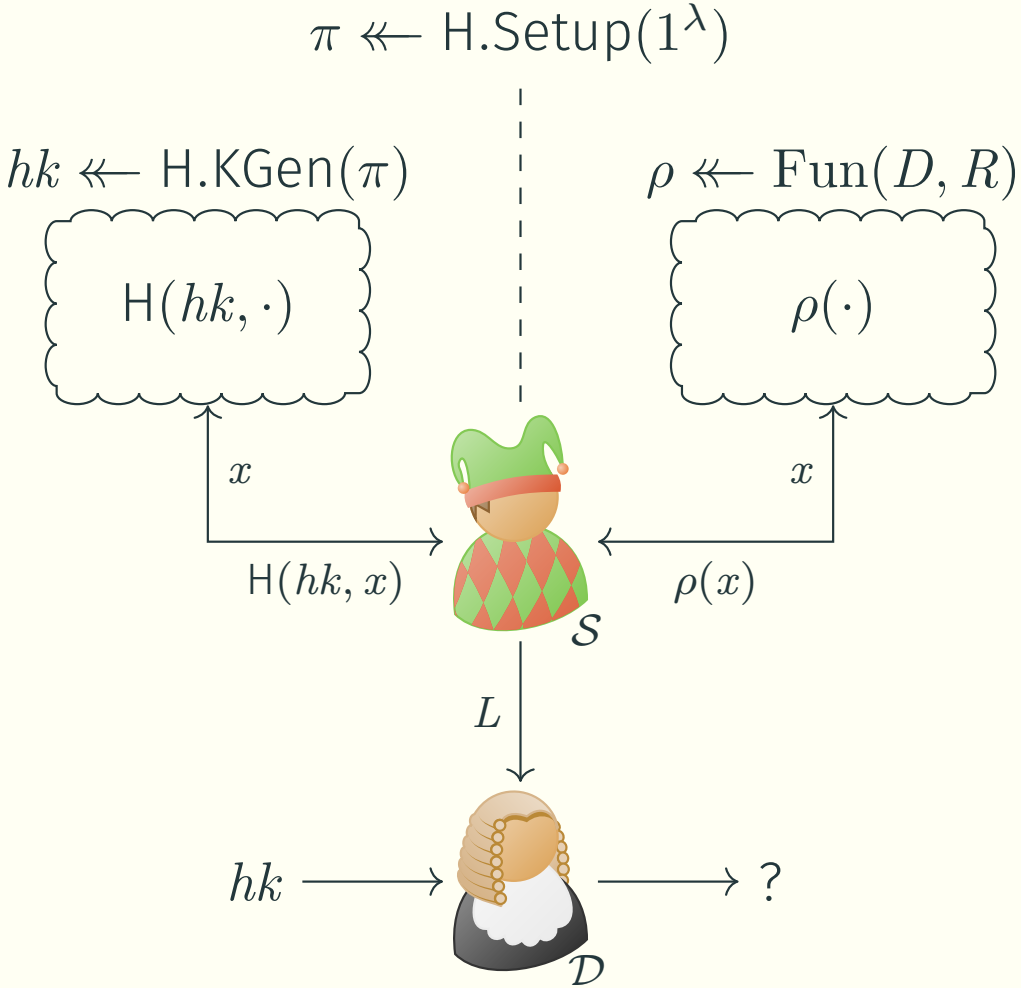
[BHK13]: Bellare, Hoang, Keelveedhi. Instantiating Random Oracles via UCEs. *CRYPTO 2013*.

UCE Security for Hash Functions [BHK13]

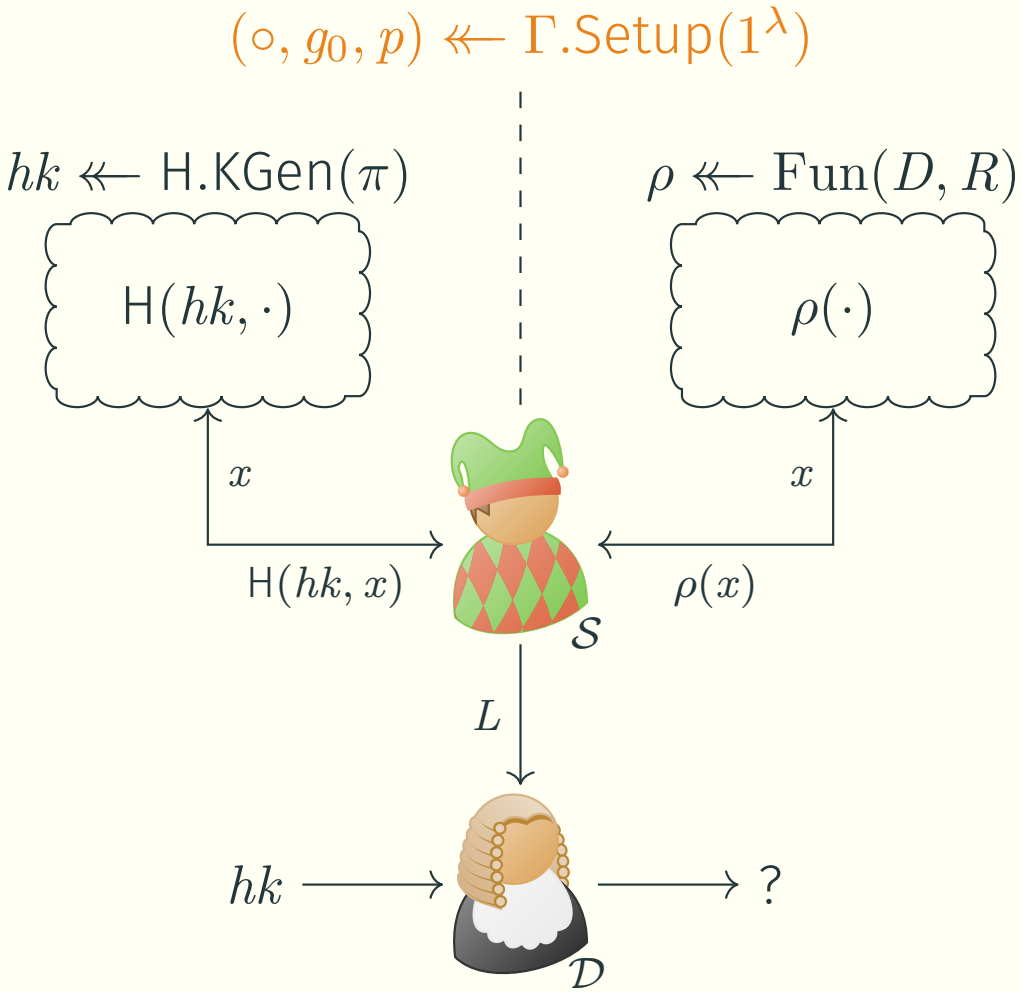


[BHK13]: Bellare, Hoang, Keelveedhi. Instantiating Random Oracles via UCEs. *CRYPTO 2013*.

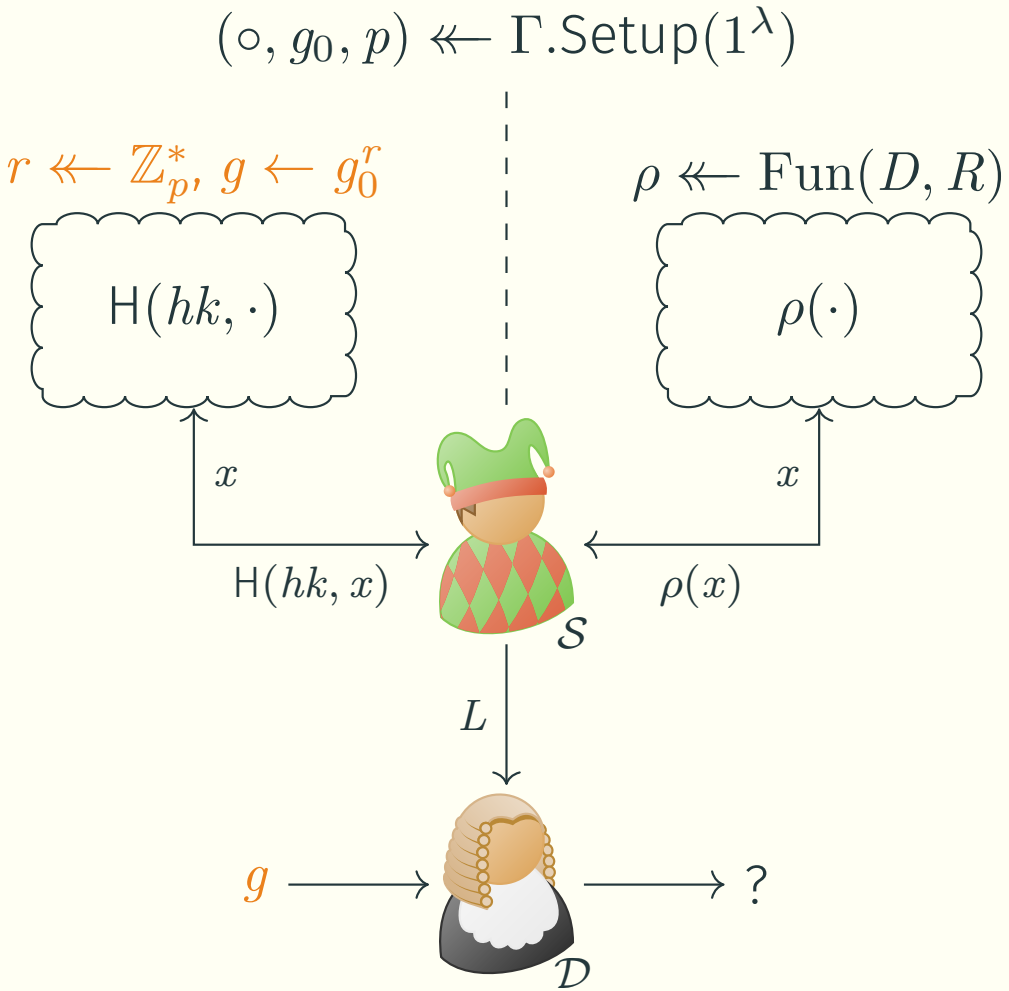
From Hash Functions to Groups



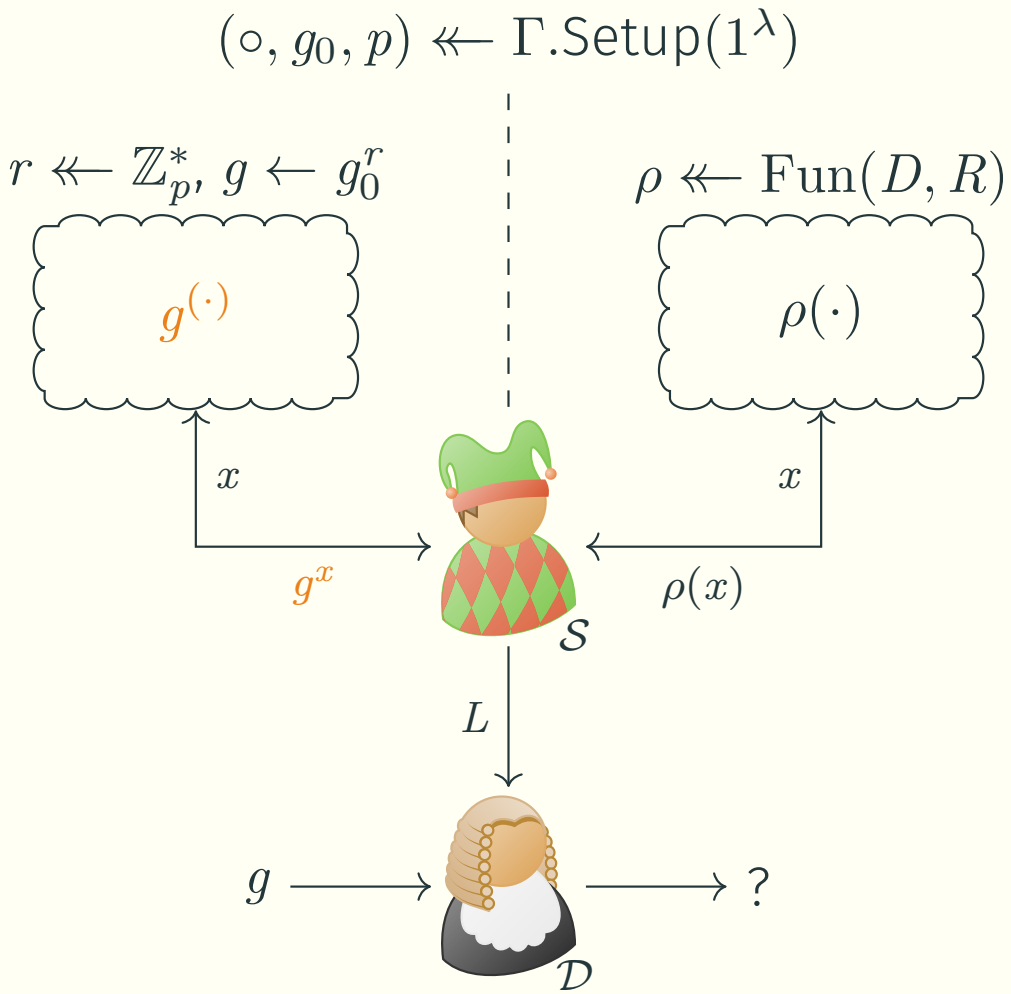
From Hash Functions to Groups



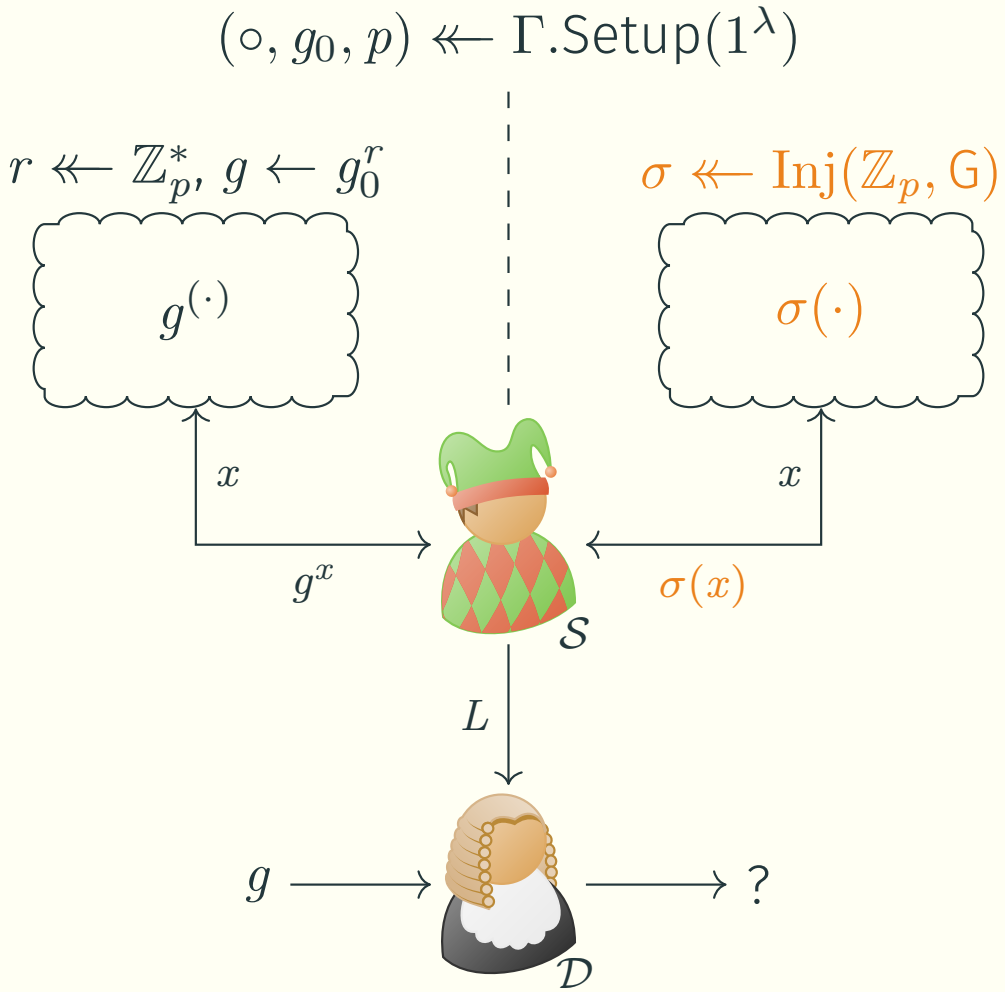
From Hash Functions to Groups



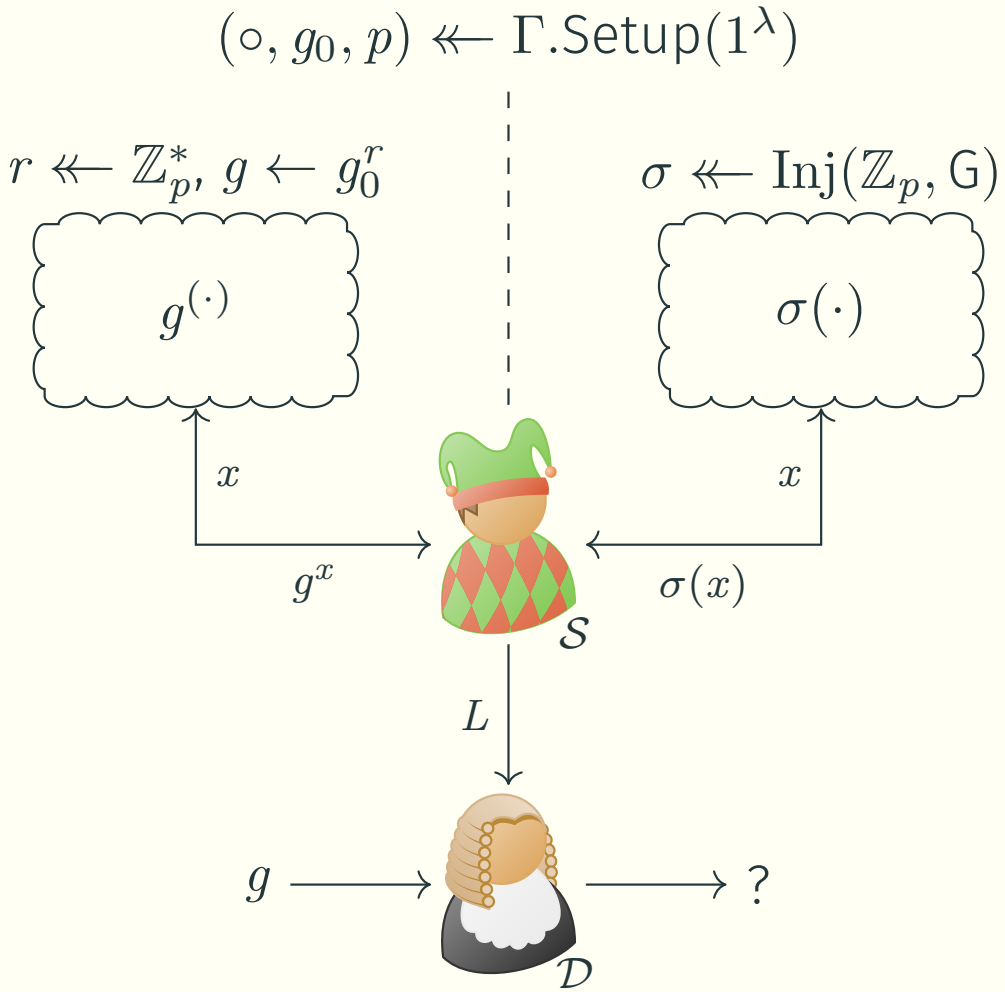
From Hash Functions to Groups



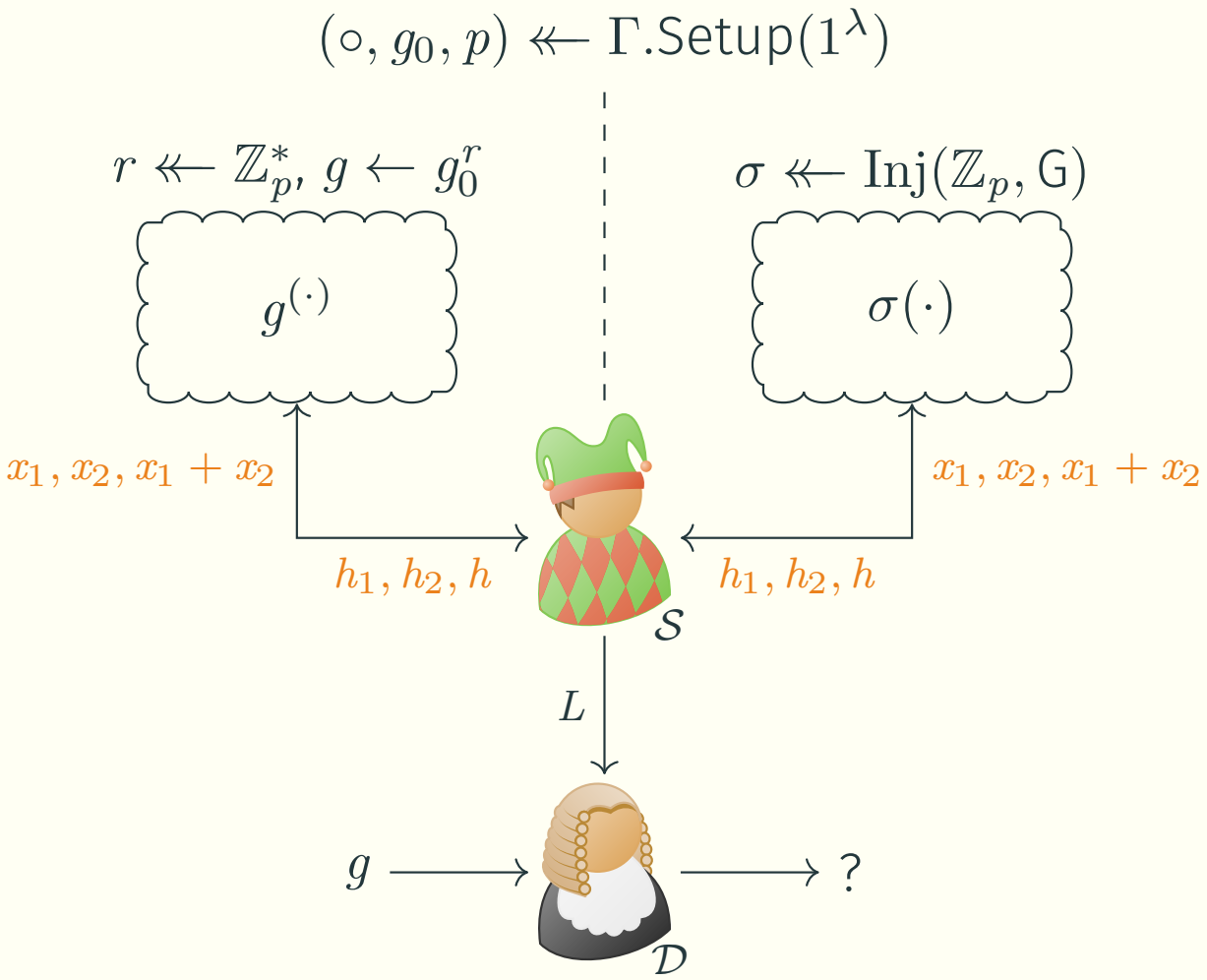
From Hash Functions to Groups



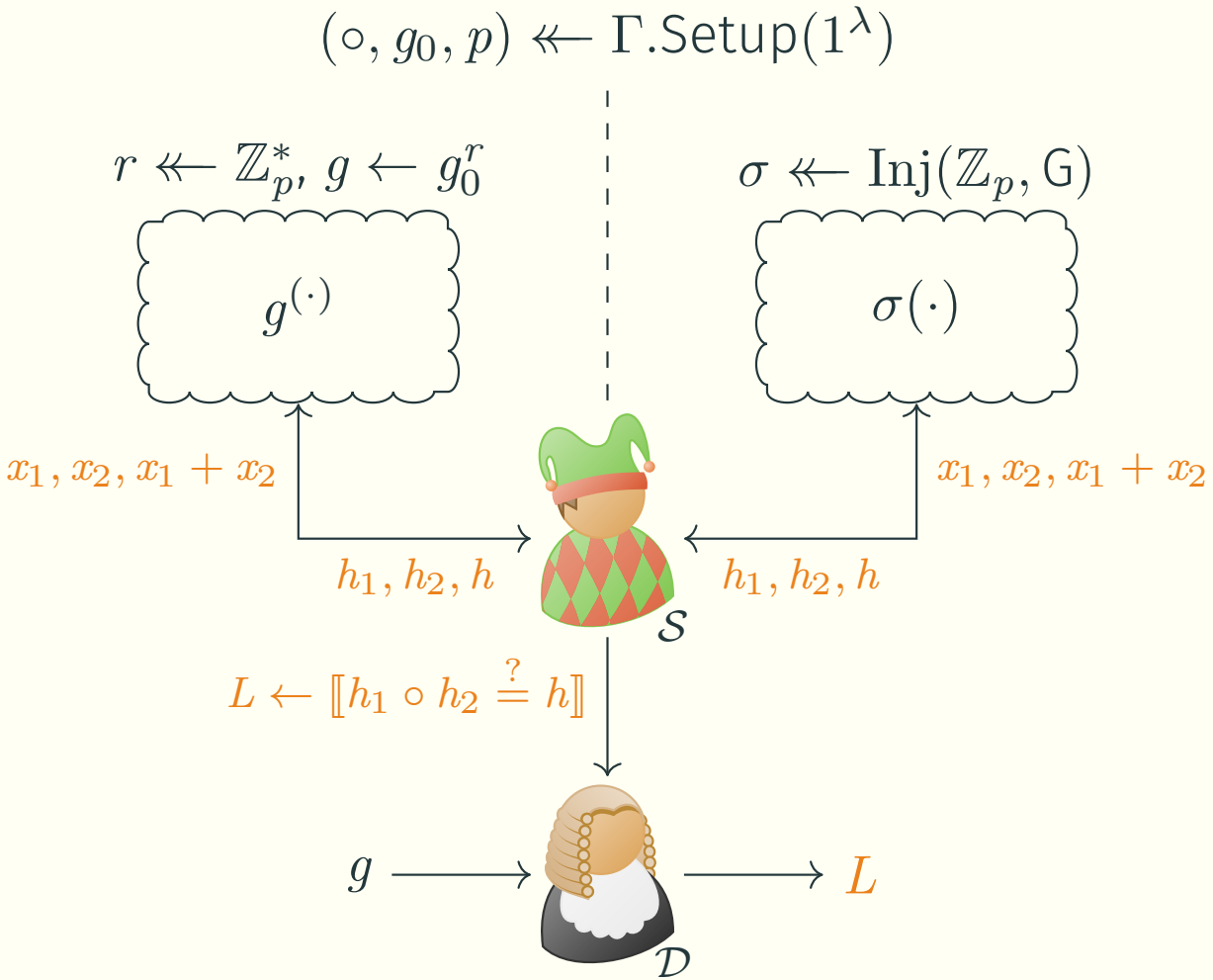
From Hash Functions to Groups



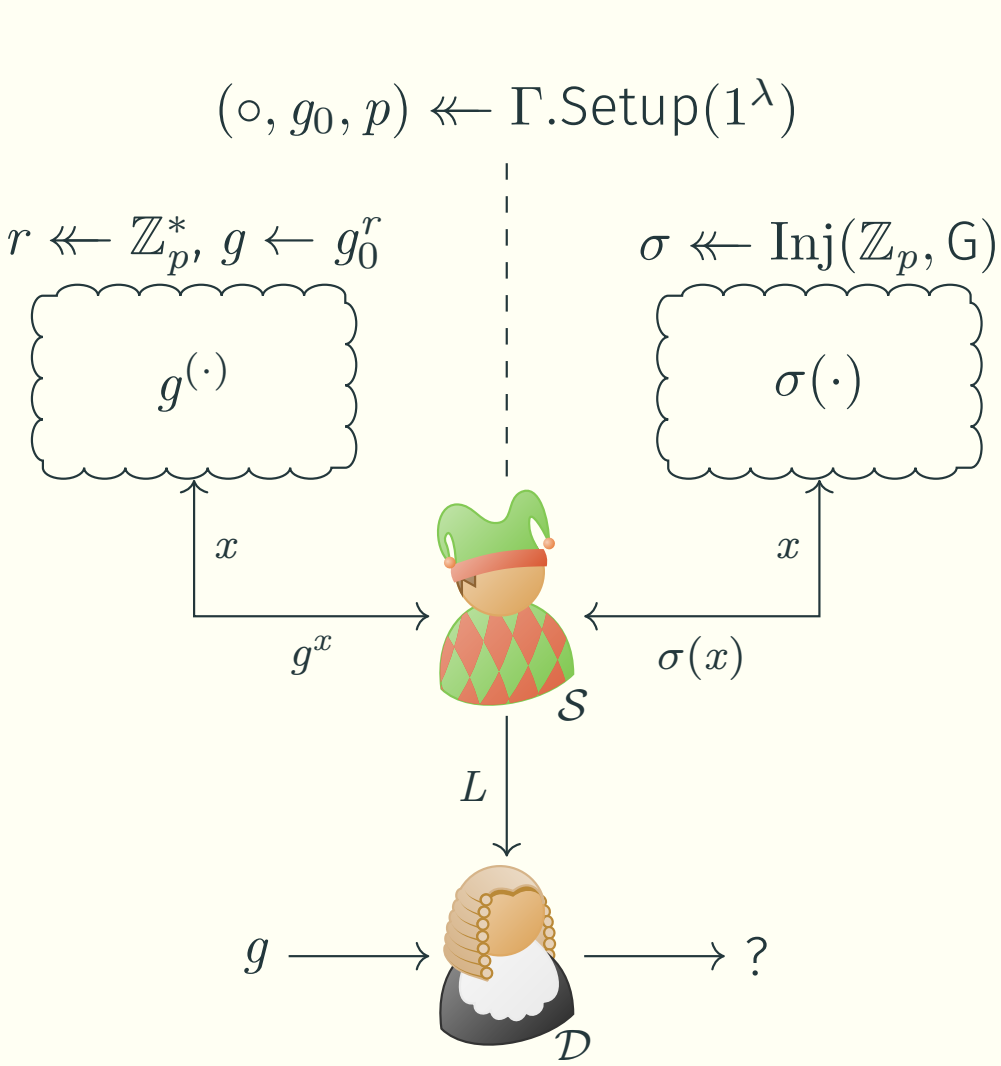
New Attacks

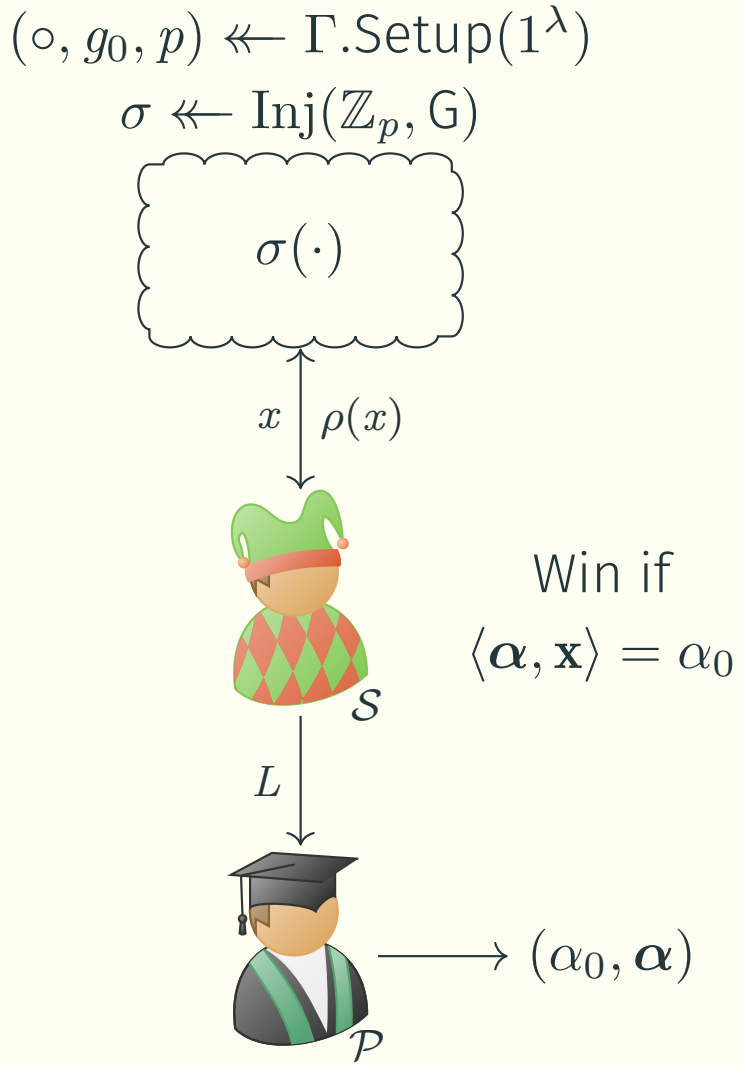

$(\circ, g_0, p) \leftarrow\!\!\!\!\leftarrow \Gamma.\mathsf{Setup}(1^\lambda)$
$r \leftarrow\!\!\!\!\leftarrow \mathbb{Z}_p^*,\ g \leftarrow g_0^r$
$\sigma \leftarrow\!\!\!\!\leftarrow \mathrm{Inj}(\mathbb{Z}_p, \mathsf{G})$
$g^{(\cdot)}$
$\sigma(\cdot)$
$x_1, x_2, x_1 + x_2$
h_1, h_2, h
h_1, h_2, h
$x_1, x_2, x_1 + x_2$
$\mathcal{S}$
L
g
$?$
$\mathcal{D}$

New Attacks

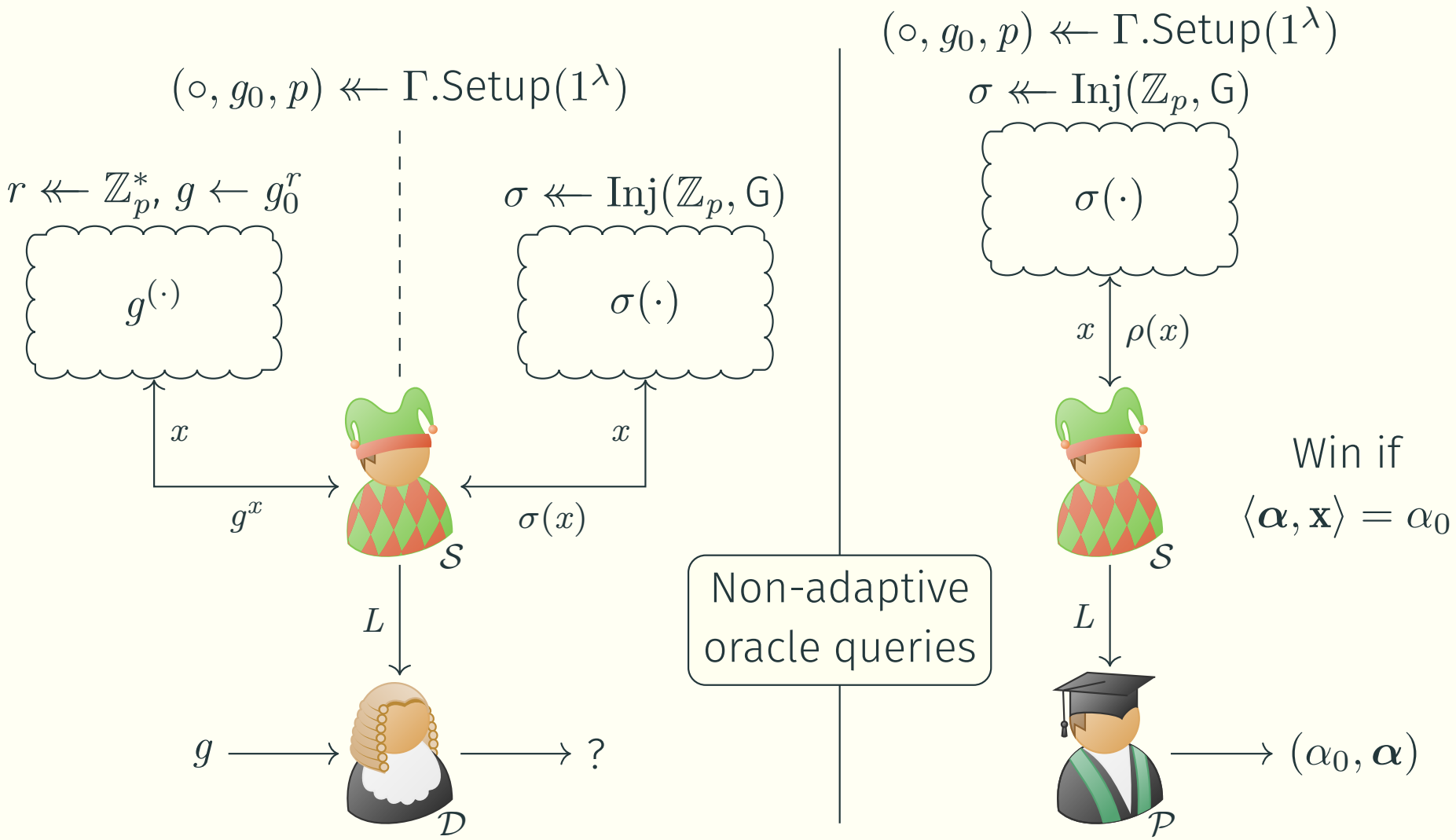

$(\circ, g_0, p) \leftarrow\!\!\!\!\leftarrow \Gamma.\mathsf{Setup}(1^\lambda)$
$r \leftarrow\!\!\!\!\leftarrow \mathbb{Z}_p^*,\ g \leftarrow g_0^r$
$\sigma \leftarrow\!\!\!\!\leftarrow \mathrm{Inj}(\mathbb{Z}_p, \mathsf{G})$
$g^{(\cdot)}$
$\sigma(\cdot)$
$x_1, x_2, x_1 + x_2$
$x_1, x_2, x_1 + x_2$
h_1, h_2, h
h_1, h_2, h
$\mathcal{S}$
$L \leftarrow [\![h_1 \circ h_2 \stackrel{?}{=} h]\!]$
g
L
$\mathcal{D}$

Algebraic Unpredictability





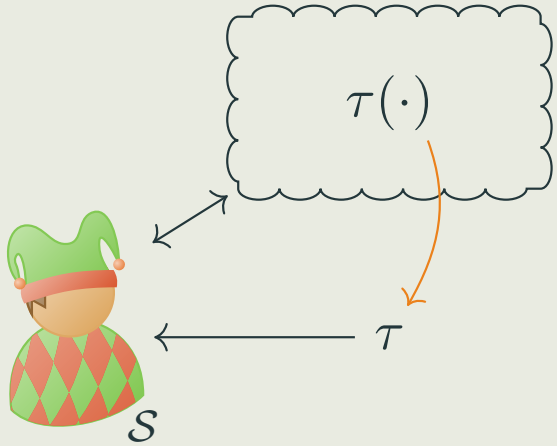
Algebraic Unpredictability



Soundness of the Definition: GGM Feasibility

Modeling of sources

- Sources are unbounded
- Receive τ in full, not only oracle access
- Capture more applications and pre-processing attacks
- Use bit-fixing [CDG18]

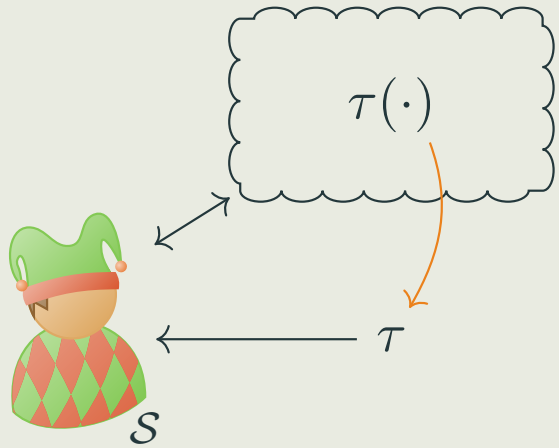


[CDG18]: Coretti, Dodis, Guo. Non-Uniform Bounds in the Random-Permutation, Ideal-Cipher, and Generic-Group Models. *CRYPTO 2018*.

Soundness of the Definition: GGM Feasibility

Modeling of sources

- Sources are unbounded
- Receive τ in full, not only oracle access
- Capture more applications and pre-processing attacks
- Use bit-fixing [CDG18]



Different proof strategy

- Schwartz–Zippel lemma $\rightsquigarrow$ Algebraic unpredictability
- Reinterpret Schwartz–Zippel as an assumption on sources

[CDG18]: Coretti, Dodis, Guo. Non-Uniform Bounds in the Random-Permutation, Ideal-Cipher, and Generic-Group Models. *CRYPTO 2018*.

Overview of Applications

Uber assumption

- Also generalizations thereof, e.g., [Can97]

[Can97]: Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. *CRYPTO 1997*.

Overview of Applications

Uber assumption

- Also generalizations thereof, e.g., [Can97]

UCEs for simple split sources

- Correlated input hashing
- Storage auditing protocols

[Can97]: Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. *CRYPTO 1997*.

Overview of Applications

Uber assumption

- Also generalizations thereof, e.g., [Can97]

UCEs for simple split sources

- Correlated input hashing
- Storage auditing protocols

Practical cryptosystems

- Variants of the ElGamal encryption scheme are KDM, DE, RKA secure

---

[Can97]: Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. *CRYPTO 1997*.

Overview of Applications

Uber assumption

- Also generalizations thereof, e.g., [Can97]

UCEs for simple split sources

- Correlated input hashing
- Storage auditing protocols

Practical cryptosystems

- Variants of the ElGamal encryption scheme are KDM, DE, RKA secure

In the GGM, security of all applications against pre-processing attacks

---

[Can97]: Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. *CRYPTO 1997*.

Overview of Applications

Uber assumption

- Also generalizations thereof, e.g., [Can97]

UCEs for simple split sources

- Correlated input hashing
- Storage auditing protocols

Practical cryptosystems

- Variants of the ElGamal encryption scheme are KDM, DE, RKA secure

In the GGM, security of all applications against pre-processing attacks

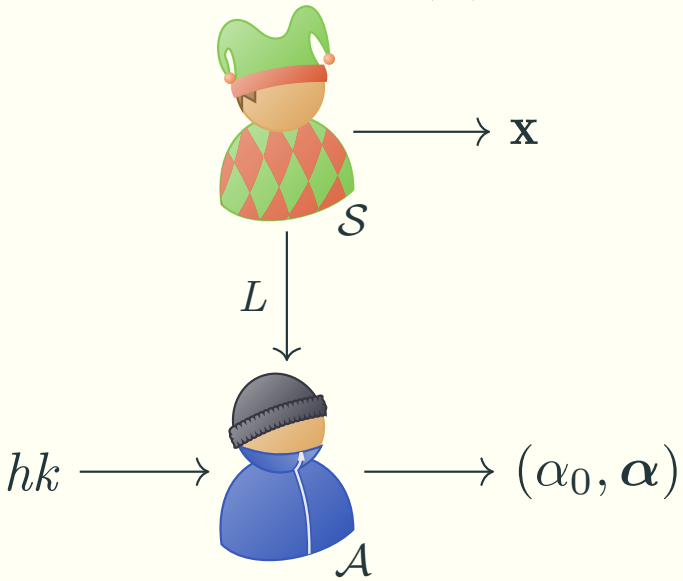
---

[Can97]: Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. *CRYPTO 1997*.

Linear Dependence Destroyers (LDDs)

$\pi \leftarrow\!\!\!\!\leftarrow \mathsf{H.Setup}(1^\lambda)$

$hk \leftarrow\!\!\!\!\leftarrow \mathsf{H.KGen}(\pi)$

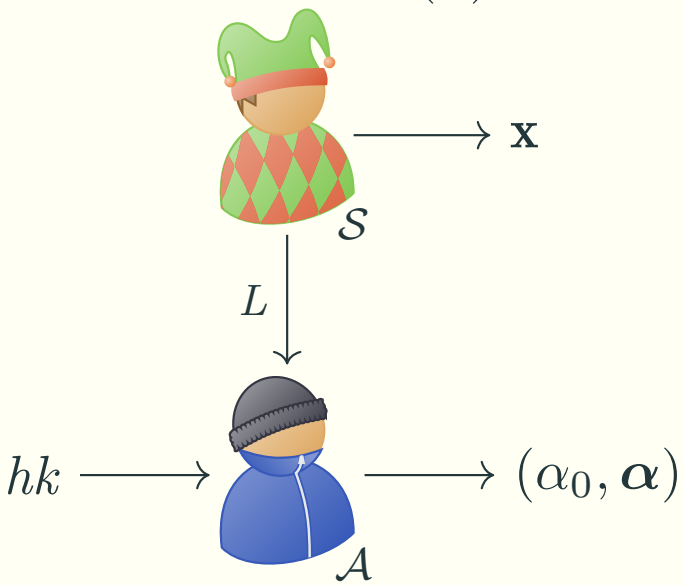


Win if $\sum \boldsymbol{\alpha}[i] \cdot \mathsf{H}(hk, \mathbf{x}[i]) = \alpha_0$

Linear Dependence Destroyers (LDDs)

$\pi \twoheadleftarrow \mathsf{H.Setup}(1^\lambda)$

$hk \twoheadleftarrow \mathsf{H.KGen}(\pi)$



Win if $\sum \boldsymbol{\alpha}[i] \cdot \mathsf{H}(hk, \mathbf{x}[i]) = \alpha_0$

Results on LDDs

- Provide instantiation for low-degree sources
- Show that a random function is an LDD in certain parameter ranges

Conclusion and Open Problems

Paper summary

- Provide a new definitional framework for assumptions on groups
- Prove that the definition is void of trivial attacks
- Show interesting applications

Conclusion and Open Problems

Paper summary

- Provide a new definitional framework for assumptions on groups
- Prove that the definition is void of trivial attacks
- Show interesting applications

Open questions

- Adaptivity, fixed generator, ...
- Do LDDs for all statistically unpredictable sources exist?

Conclusion and Open Problems

Paper summary

- Provide a new definitional framework for assumptions on groups
- Prove that the definition is void of trivial attacks
- Show interesting applications

Open questions

- Adaptivity, fixed generator, ...
- Do LDDs for all statistically unpredictable sources exist?
- How far can we push this "high-entropy approach" to connect the standard and idealized models?

Conclusion and Open Problems

Paper summary

- Provide a new definitional framework for assumptions on groups
- Prove that the definition is void of trivial attacks
- Show interesting applications

Open questions

- Adaptivity, fixed generator, ...
- Do LDDs for all statistically unpredictable sources exist?
- How far can we push this "high-entropy approach" to connect the standard and idealized models?

ia.cr/2022/1502