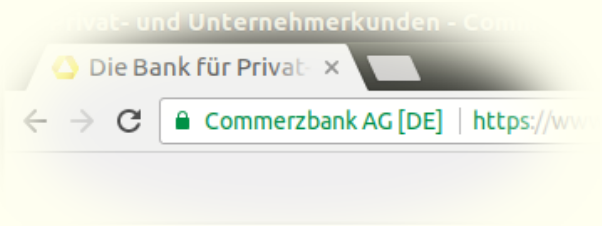
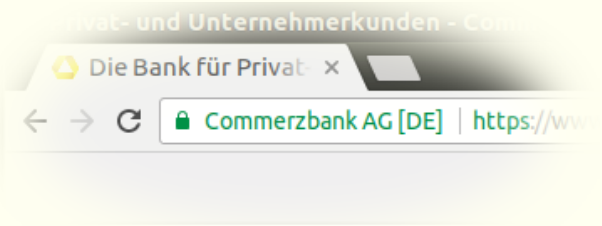
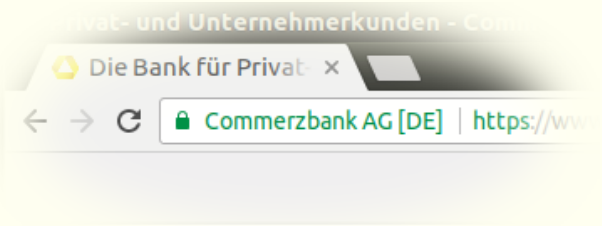
On Assumptions and the Limits of Cryptography

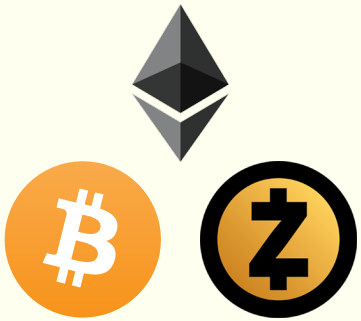
Nils Fleischhacker

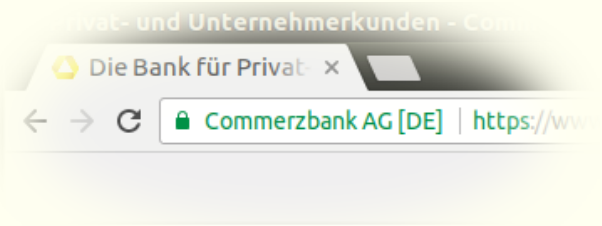
Bochum, January 24, 2018


Die Bank für Privat
Commerzbank AG [DE]

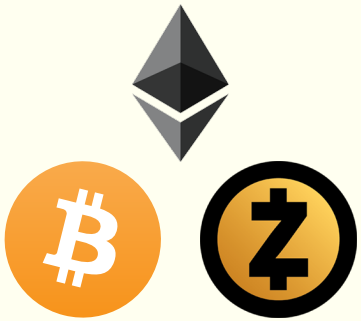

Die Bank für Privat
Commerzbank AG [DE]

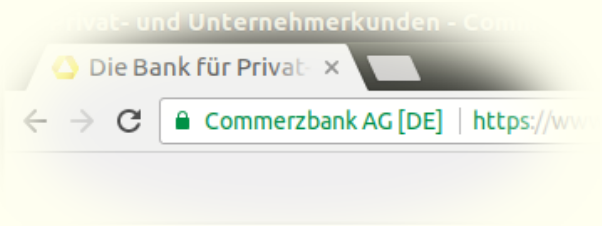

Die Bank für Privat
Commerzbank AG [DE]



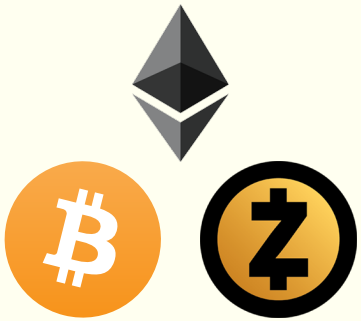


So, how do we know all of this is secure?

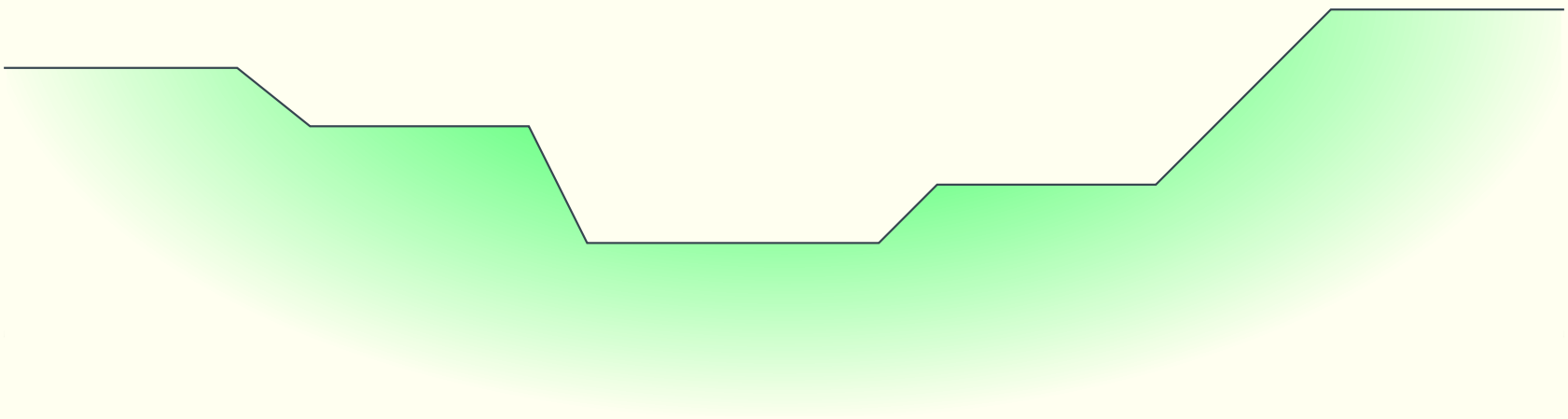




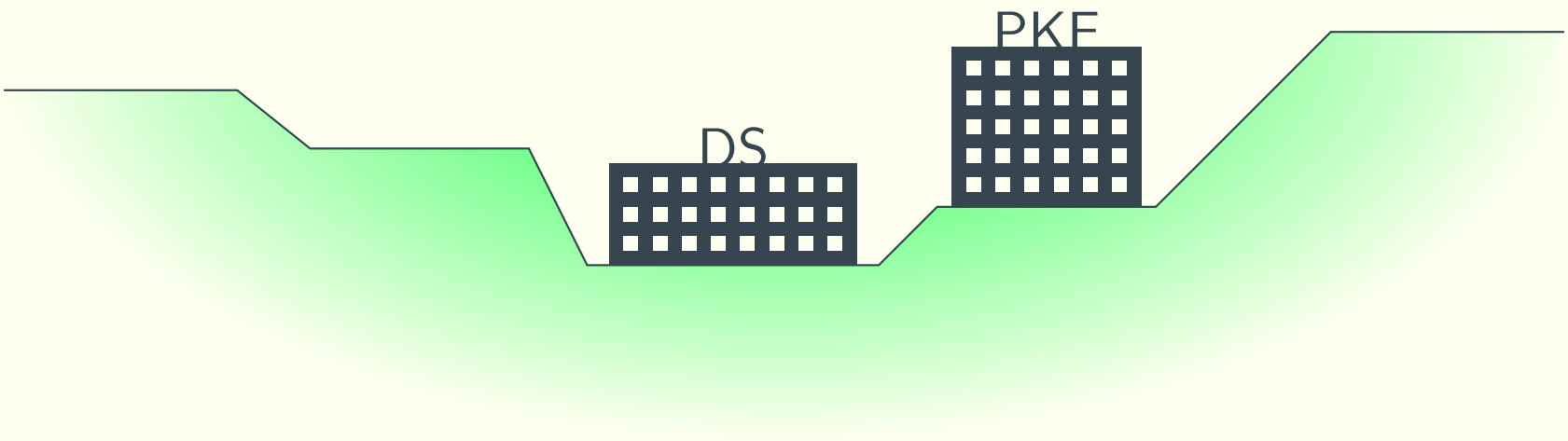
The sad truth is: We don't! Not really.



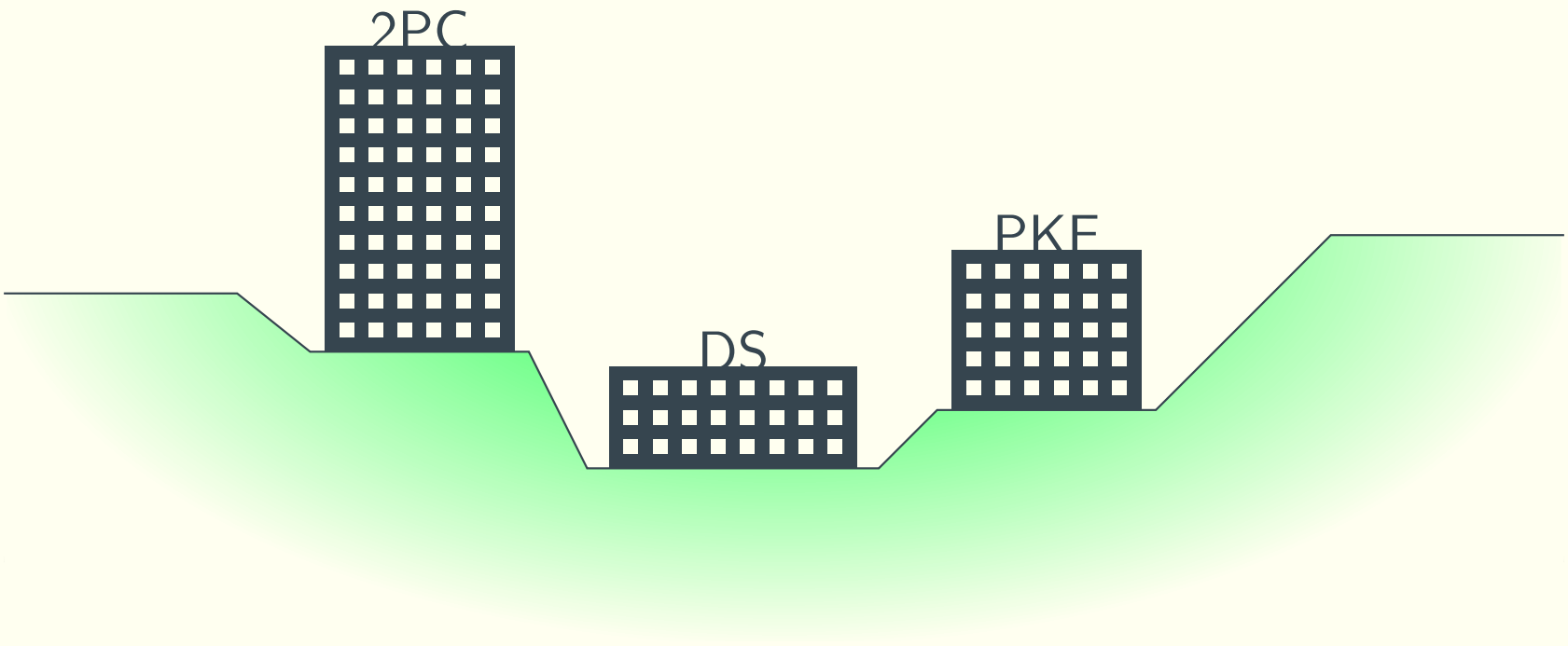
The Cryptographic Landscape



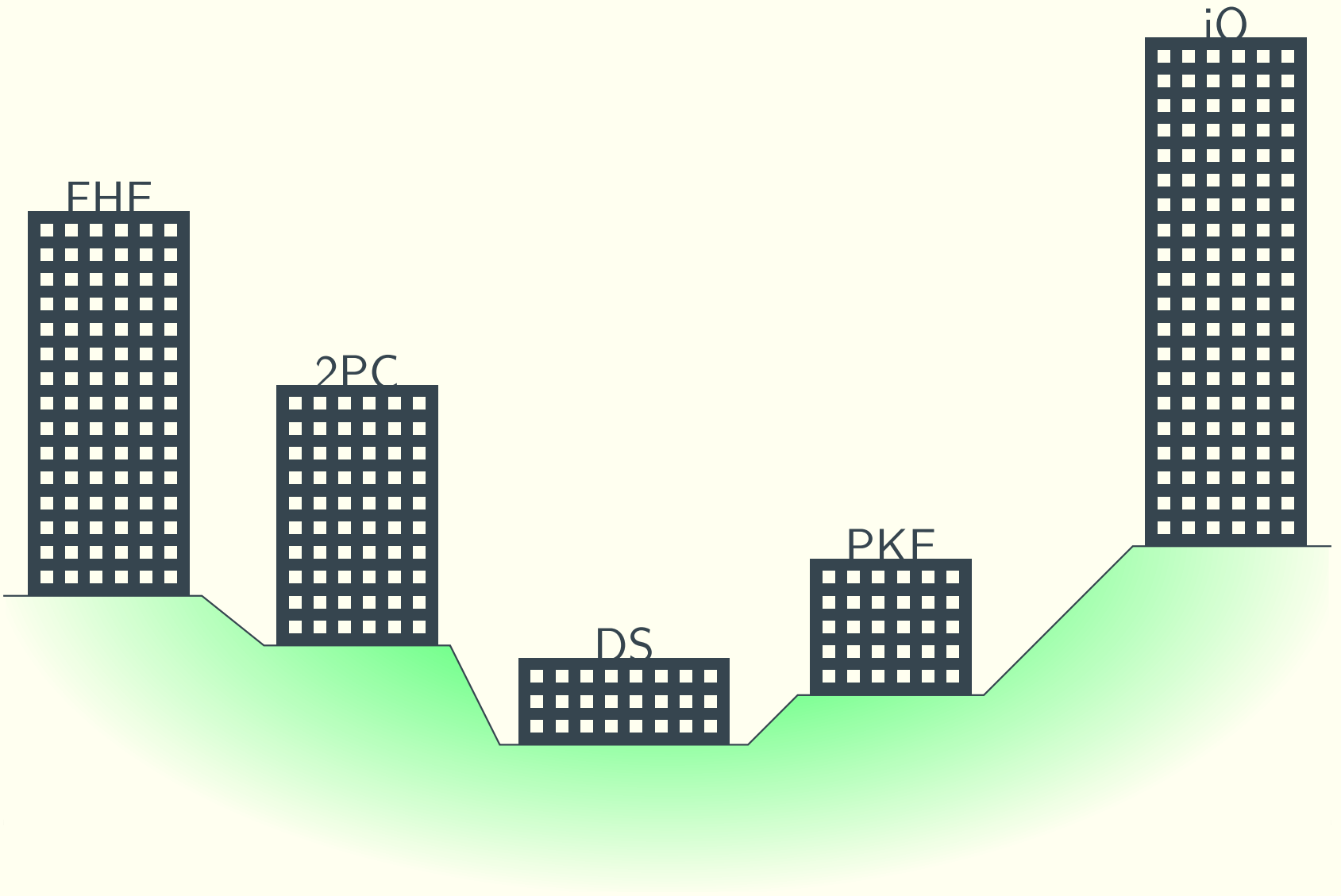
The Cryptographic Landscape



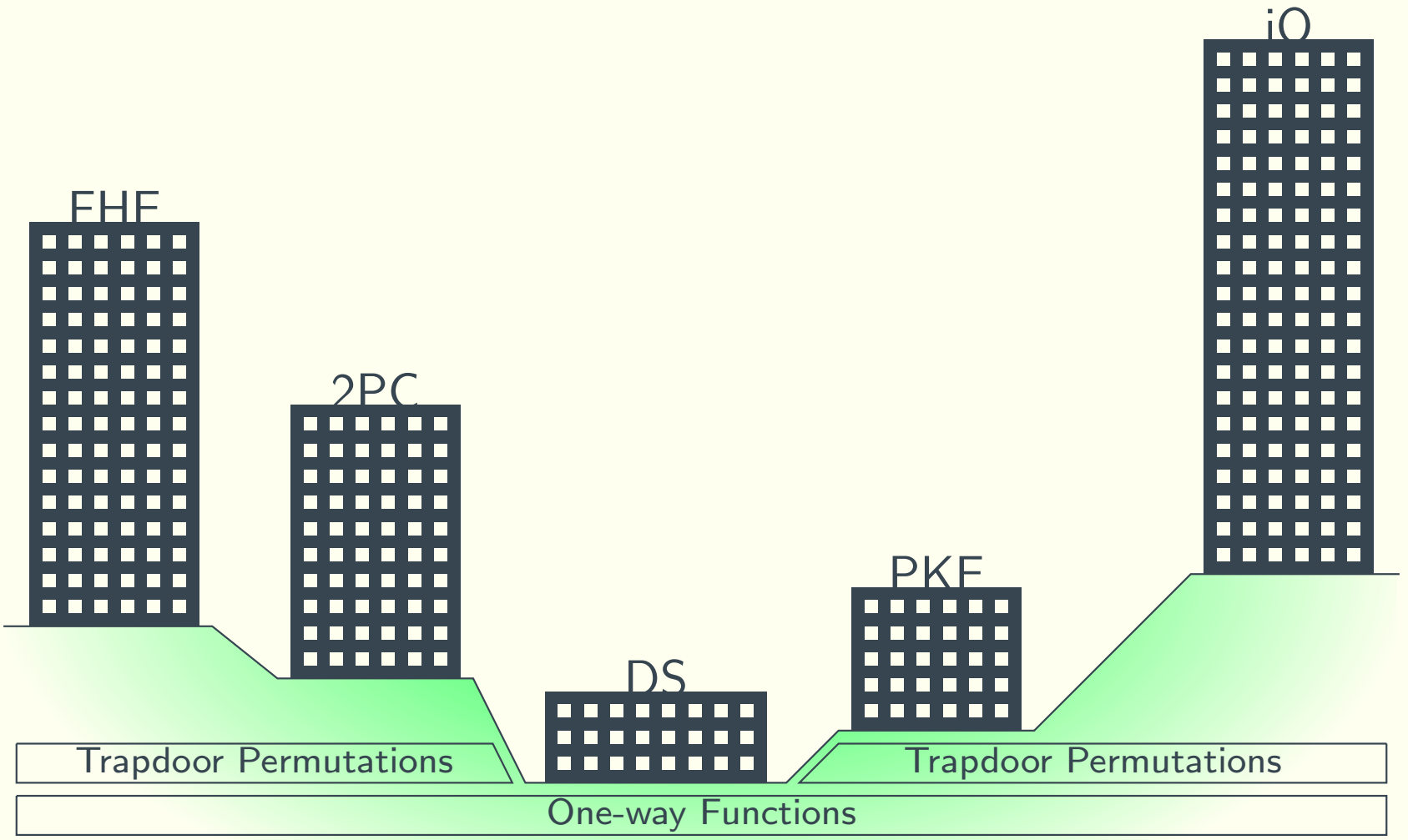
The Cryptographic Landscape



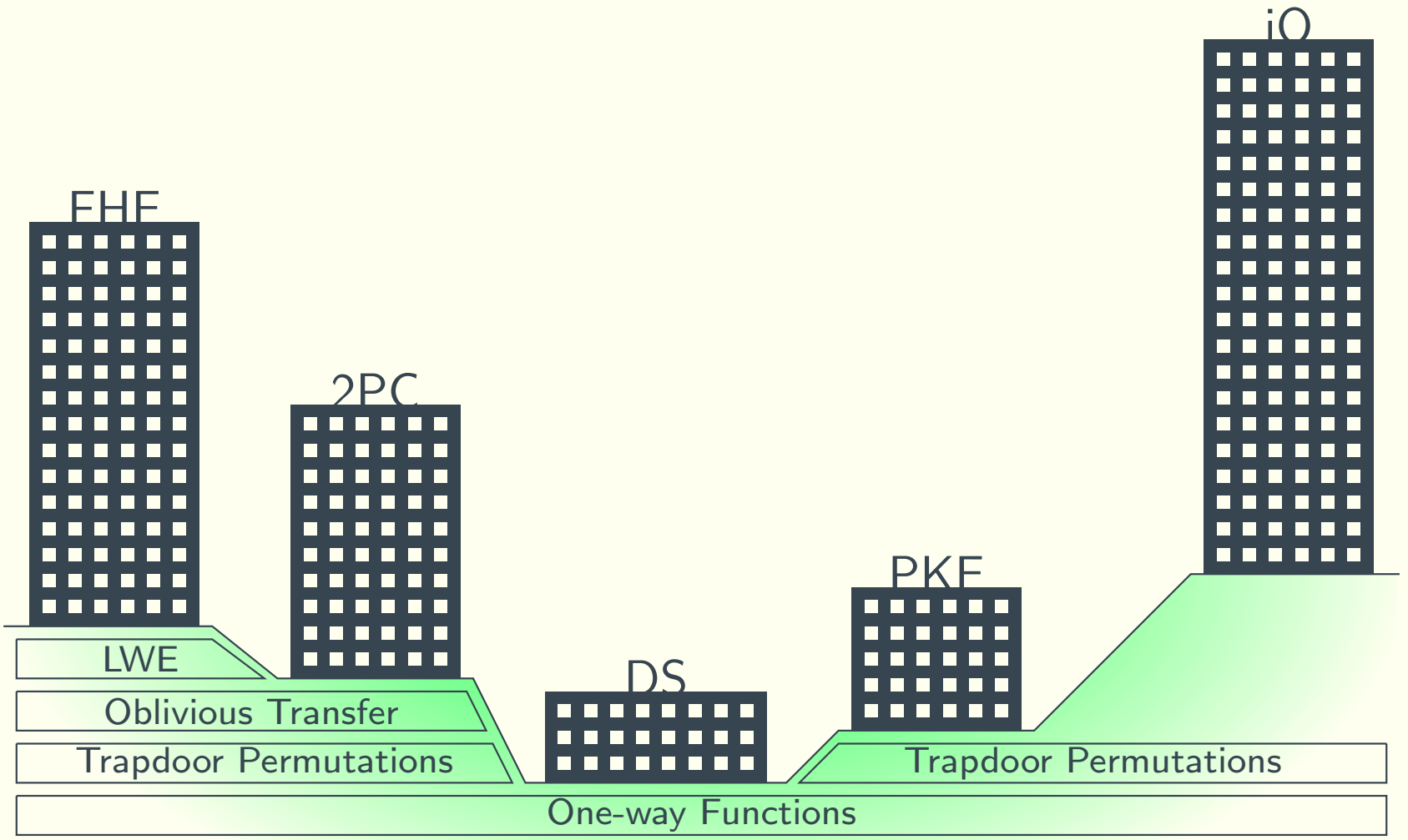
The Cryptographic Landscape



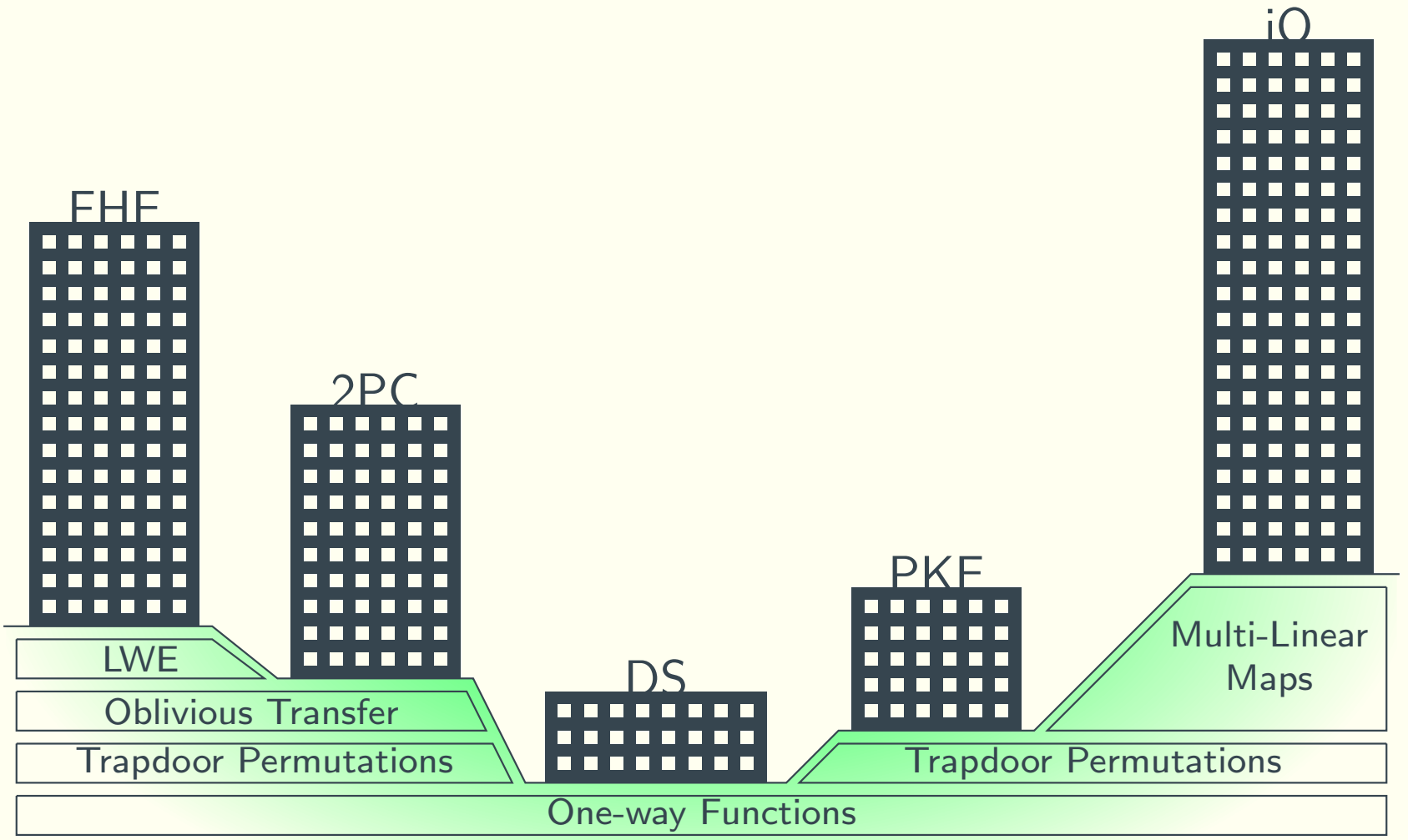
The Cryptographic Landscape



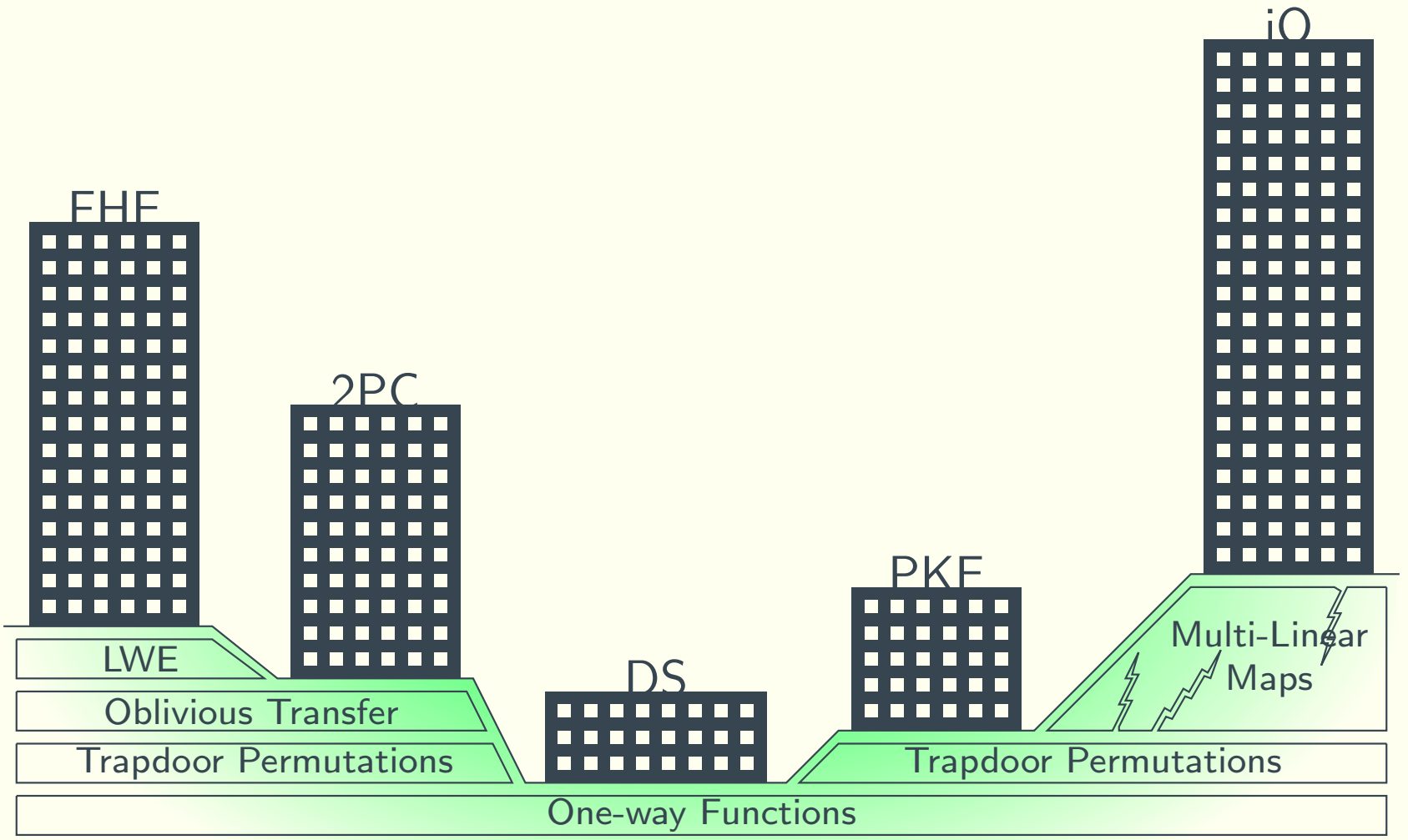
The Cryptographic Landscape



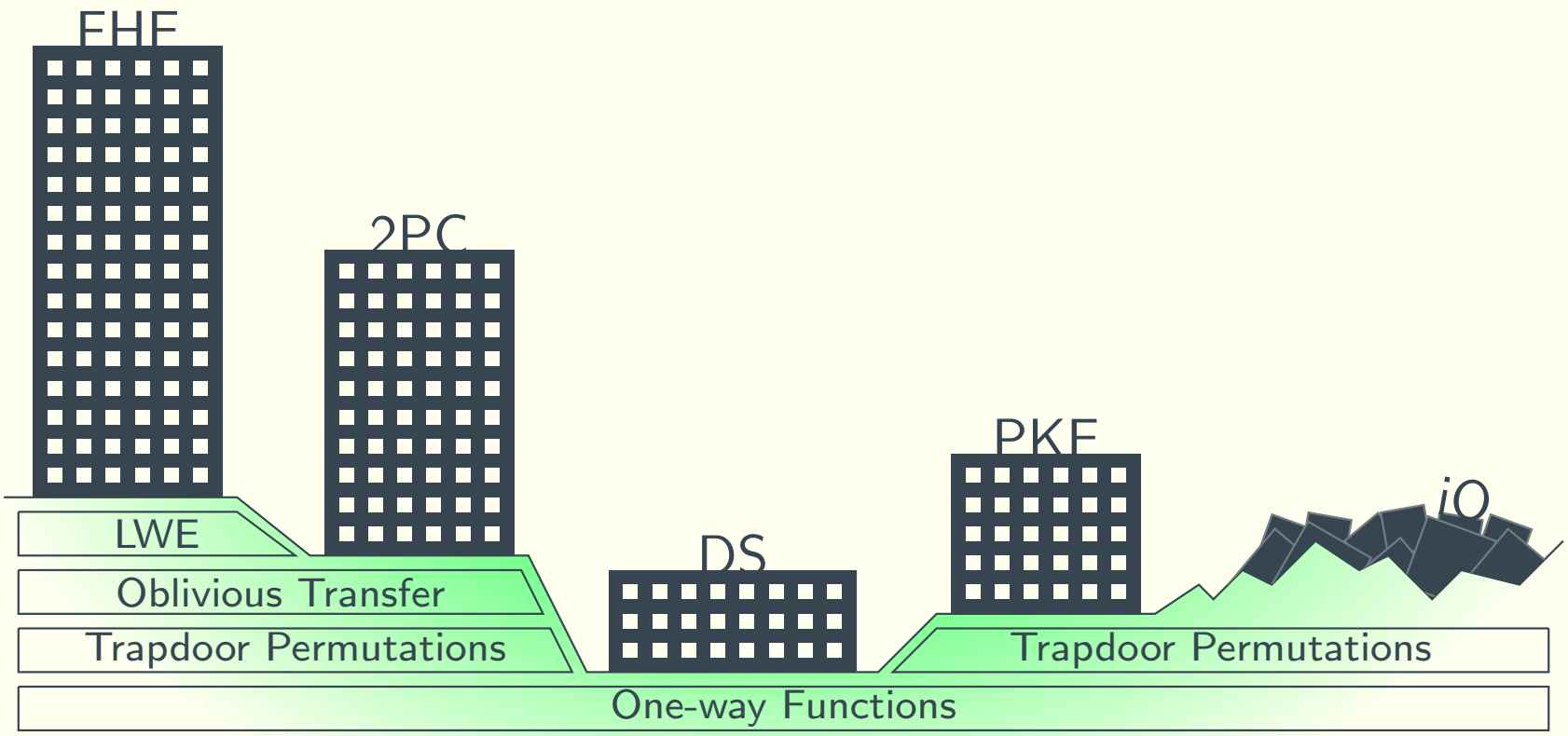
The Cryptographic Landscape



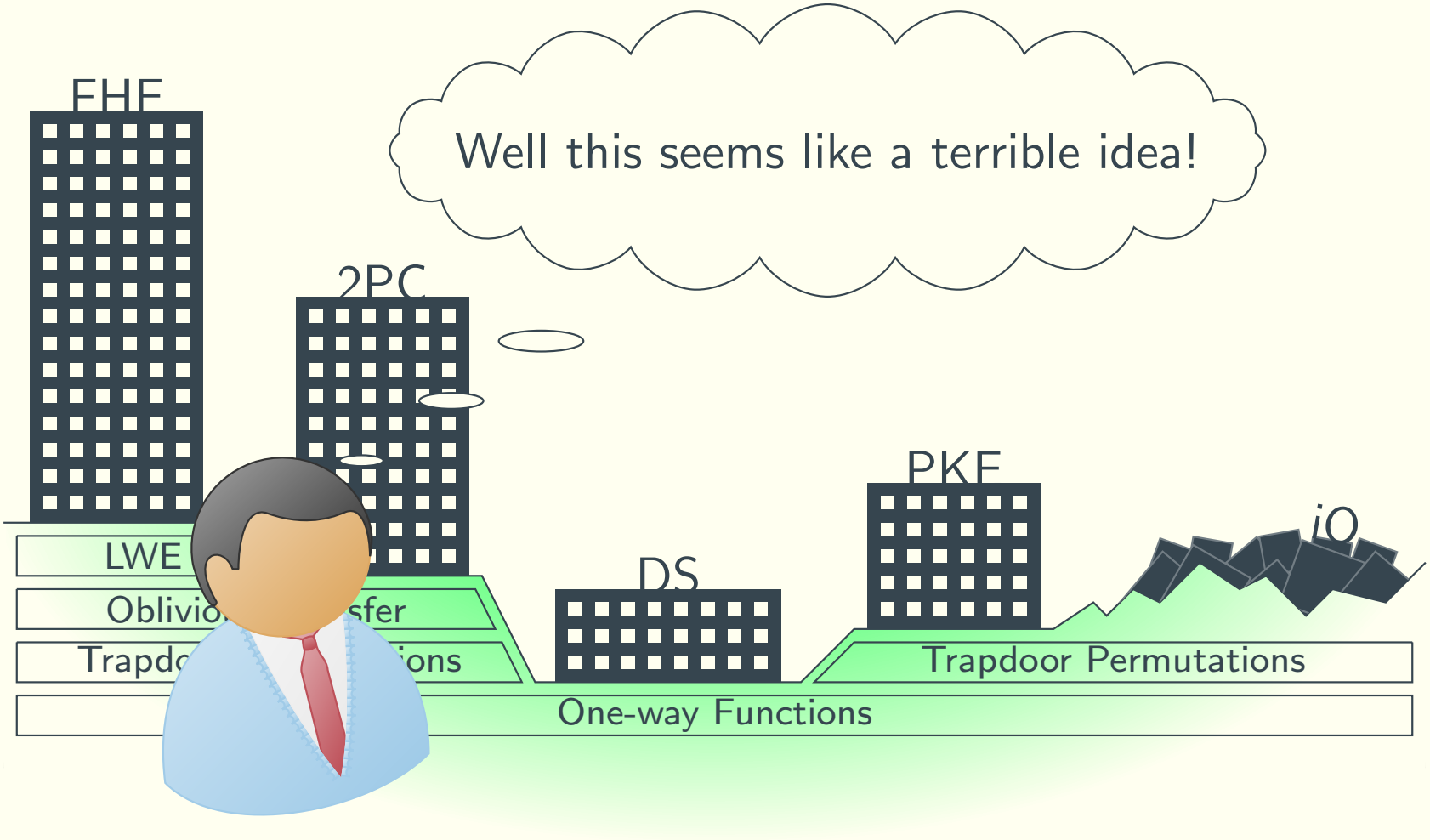
The Cryptographic Landscape



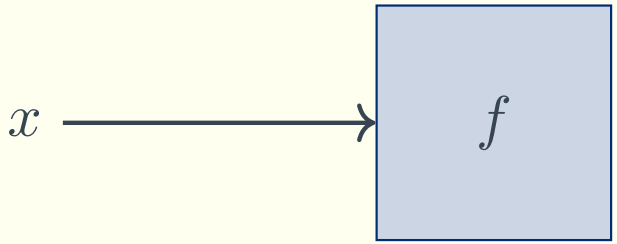
The Cryptographic Landscape



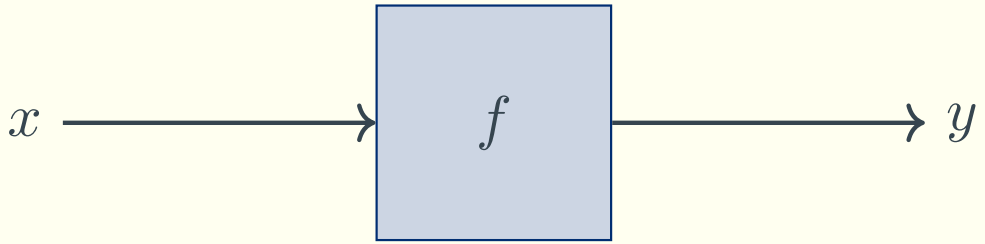
The Cryptographic Landscape



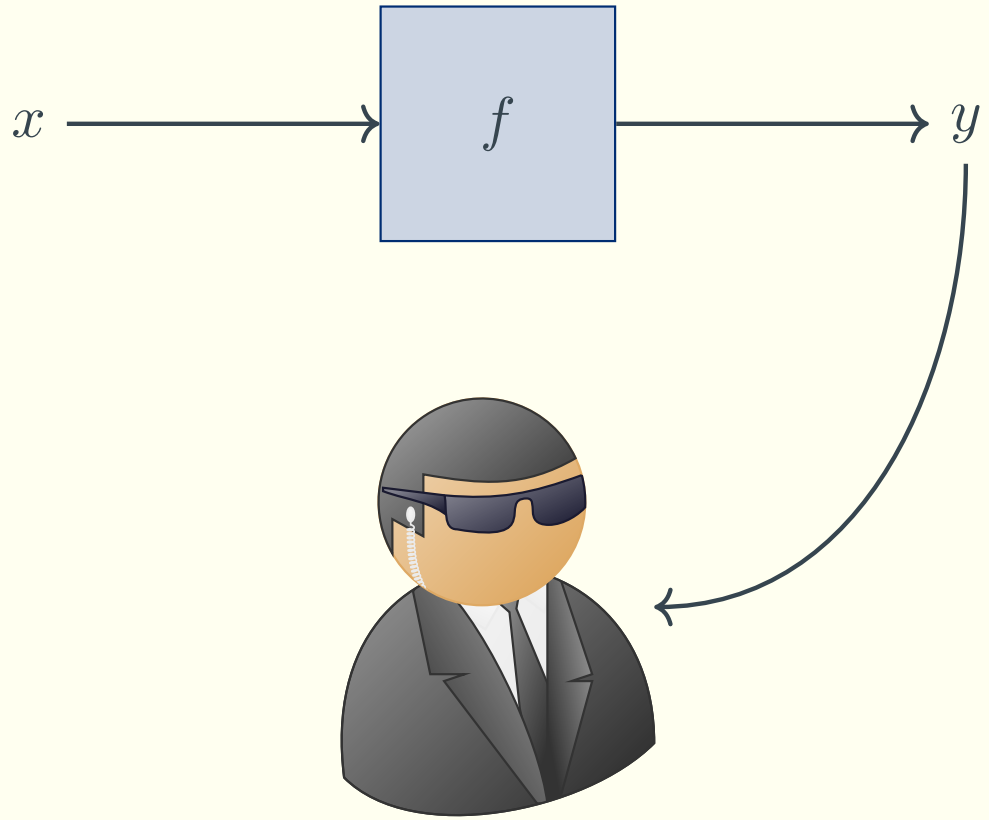
One-Way Functions



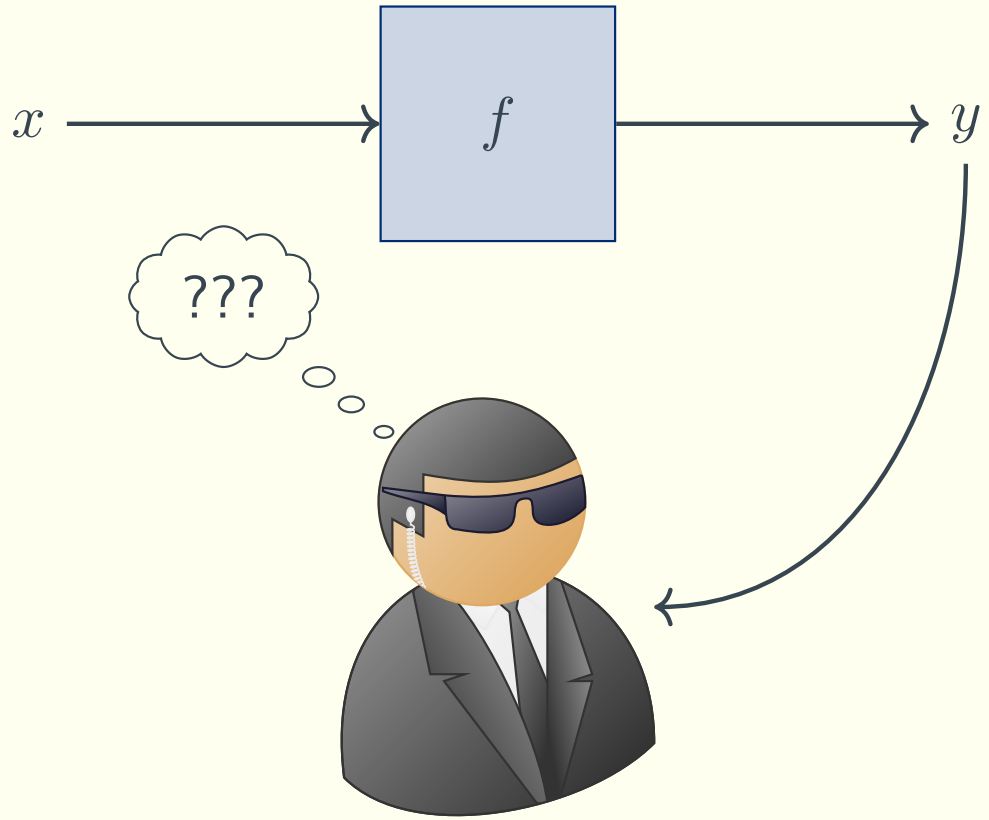
One-Way Functions



One-Way Functions

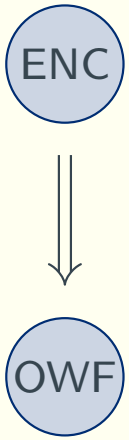


One-Way Functions

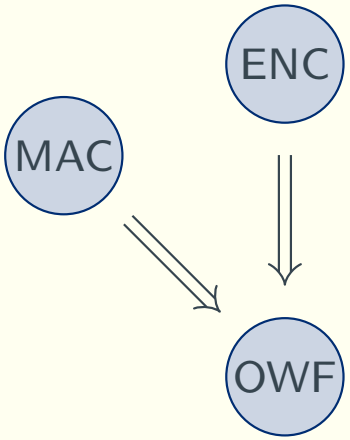


Why We Need to Make Assumptions

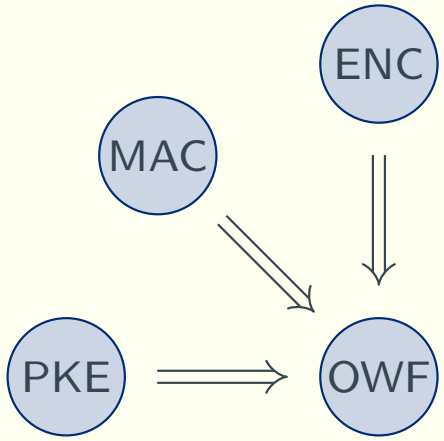
Why We Need to Make Assumptions



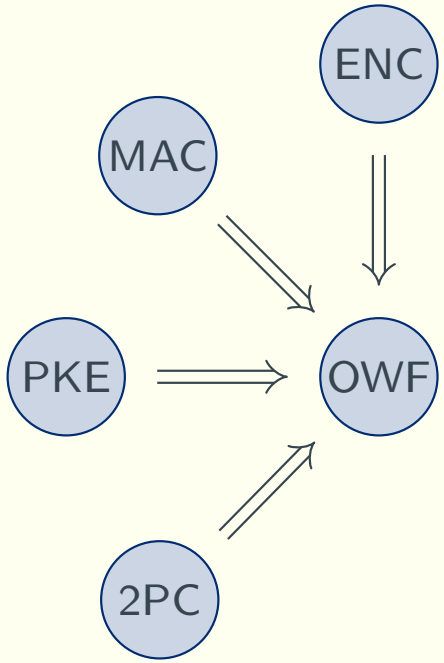
Why We Need to Make Assumptions



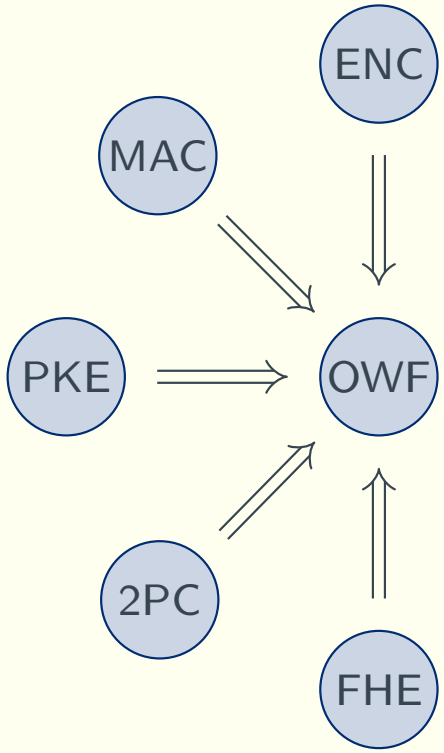
Why We Need to Make Assumptions



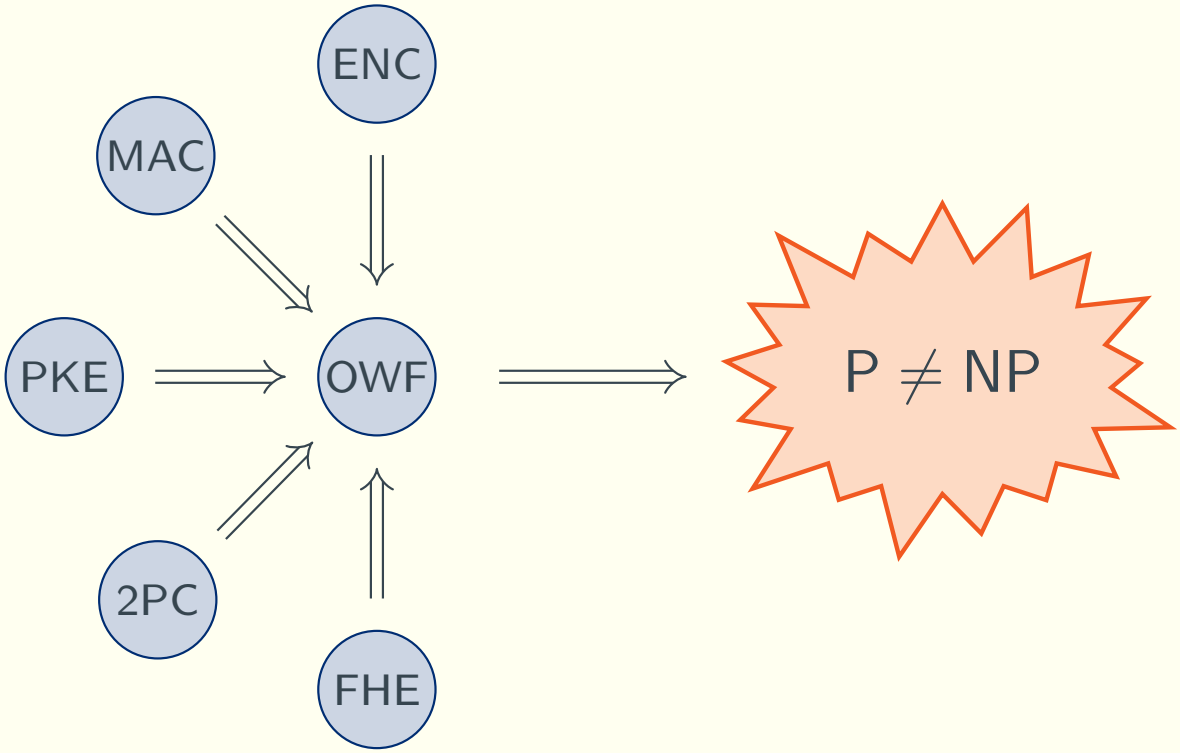
Why We Need to Make Assumptions



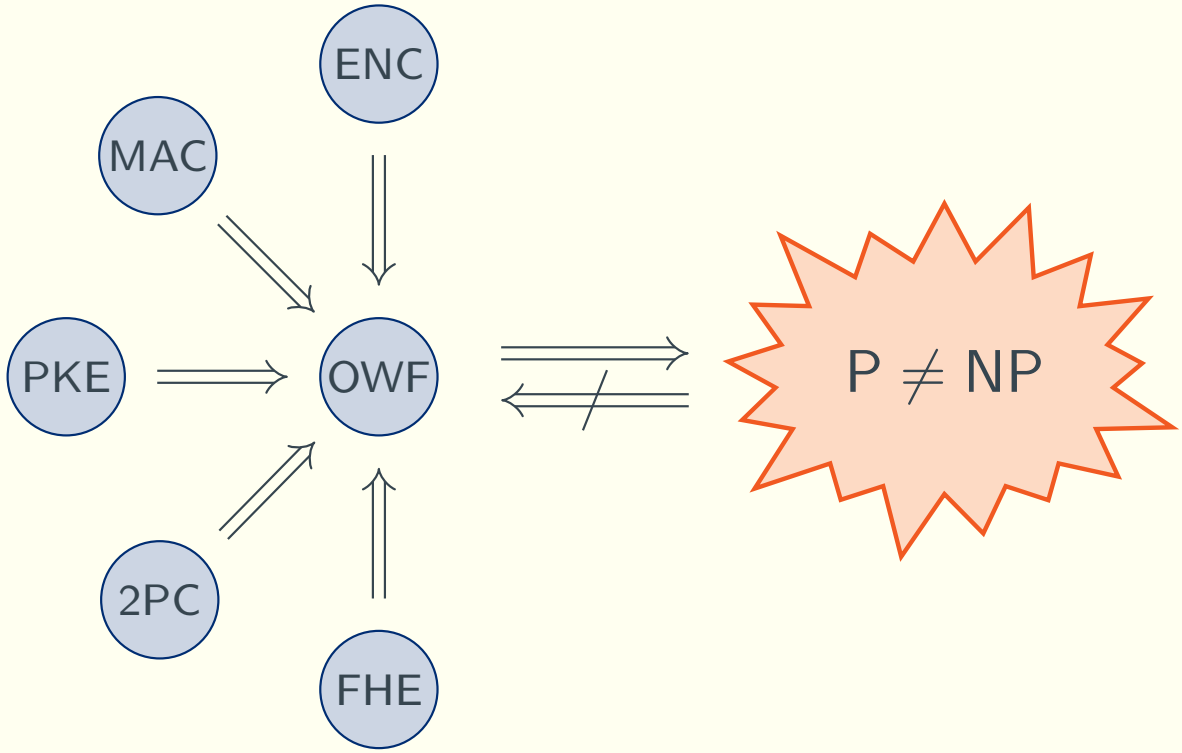
Why We Need to Make Assumptions



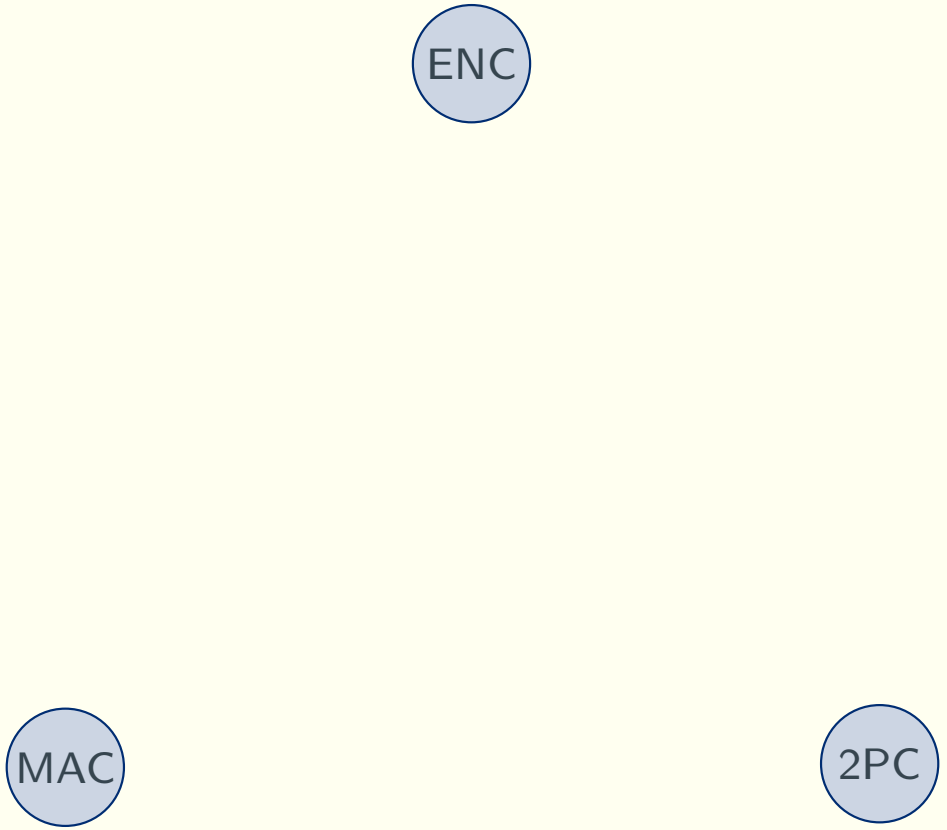
Why We Need to Make Assumptions



Why We Need to Make Assumptions



Idea Behind Provable Security



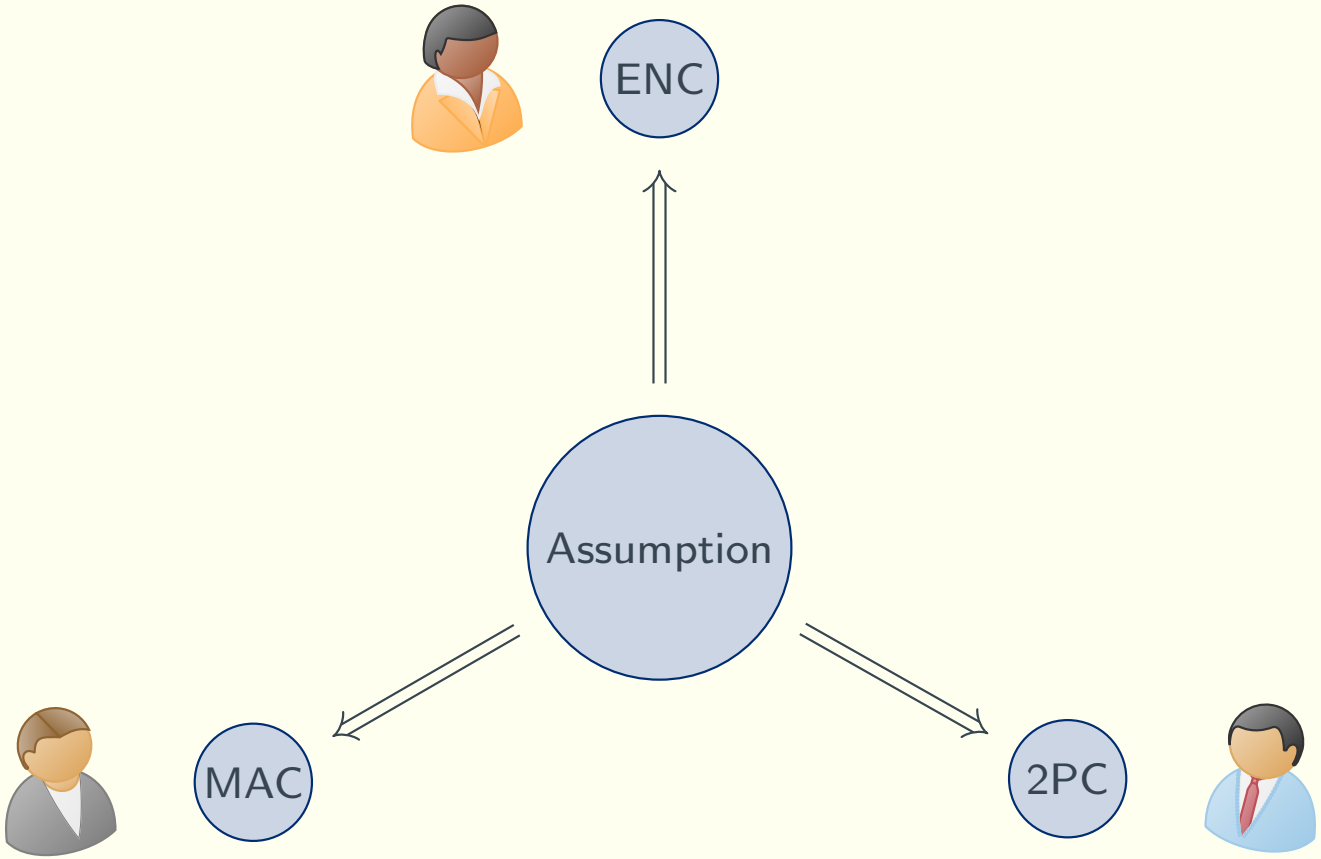
Idea Behind Provable Security

ENC

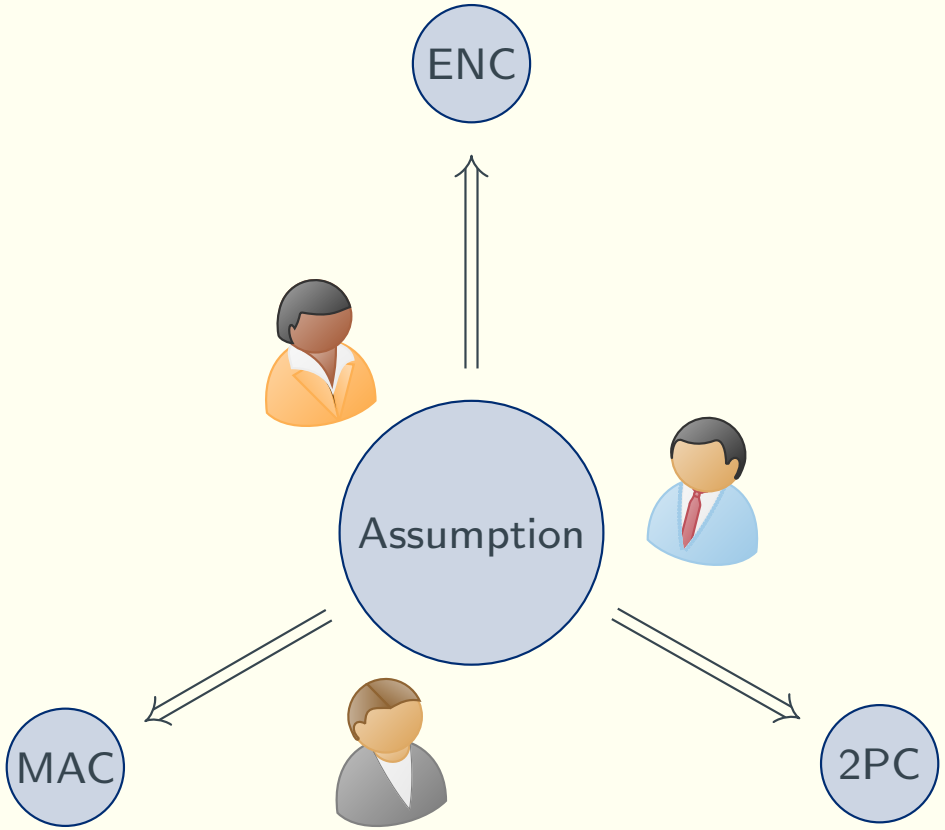
MAC

2PC

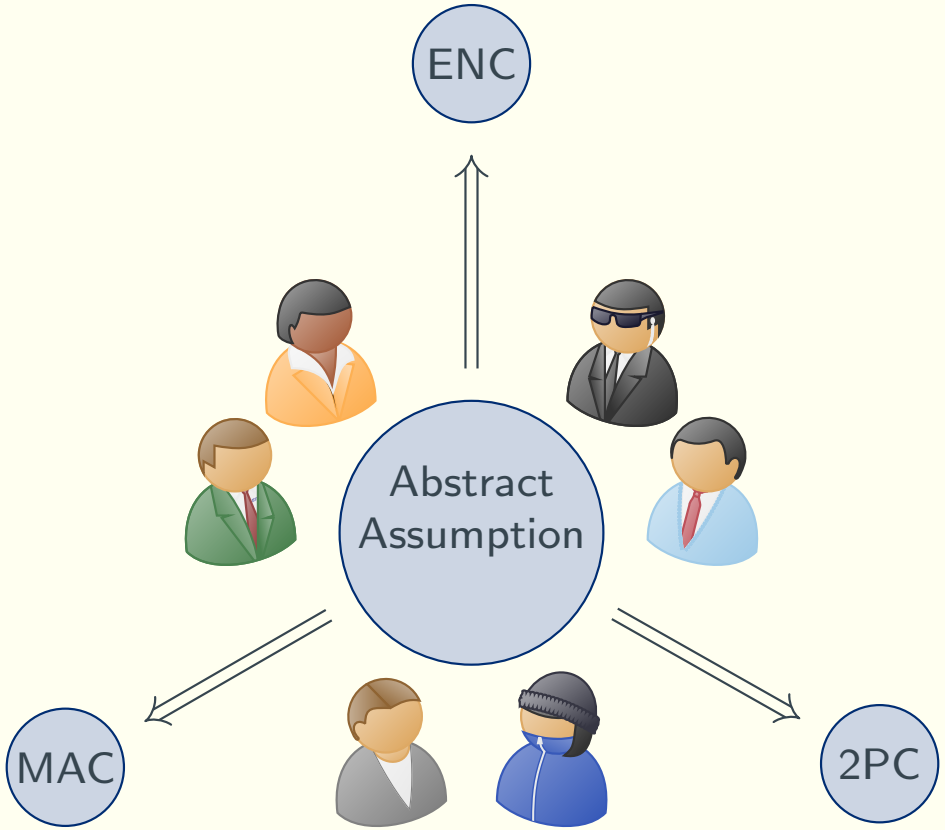
Idea Behind Provable Security



Idea Behind Provable Security



Idea Behind Provable Security



Determining Minimal Assumptions

Determining Minimal Assumptions

One-Way Functions

Statistical Security

Determining Minimal Assumptions

Trapdoor Permutations

One-Way Functions

Statistical Security

Determining Minimal Assumptions

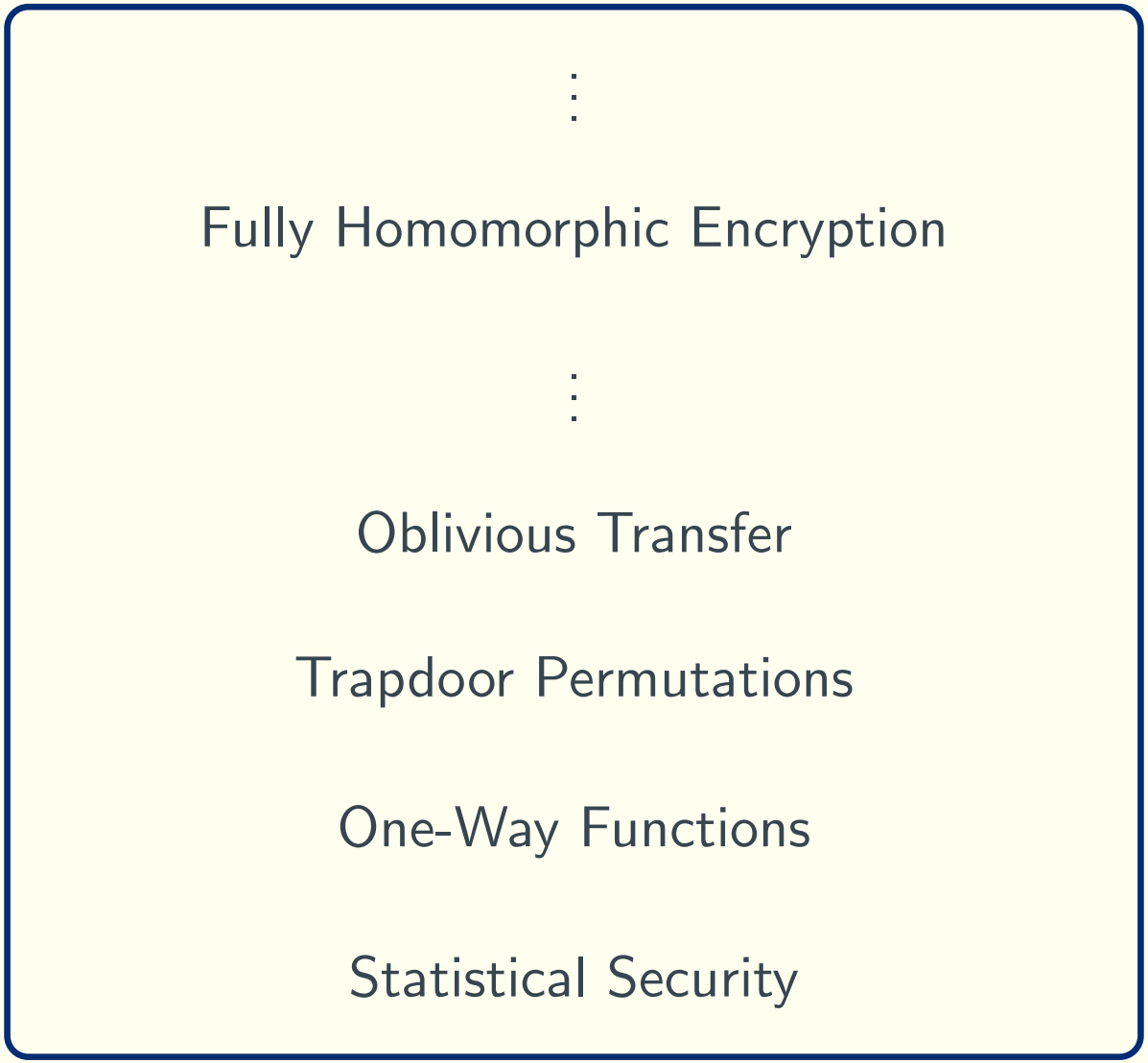
Oblivious Transfer

Trapdoor Permutations

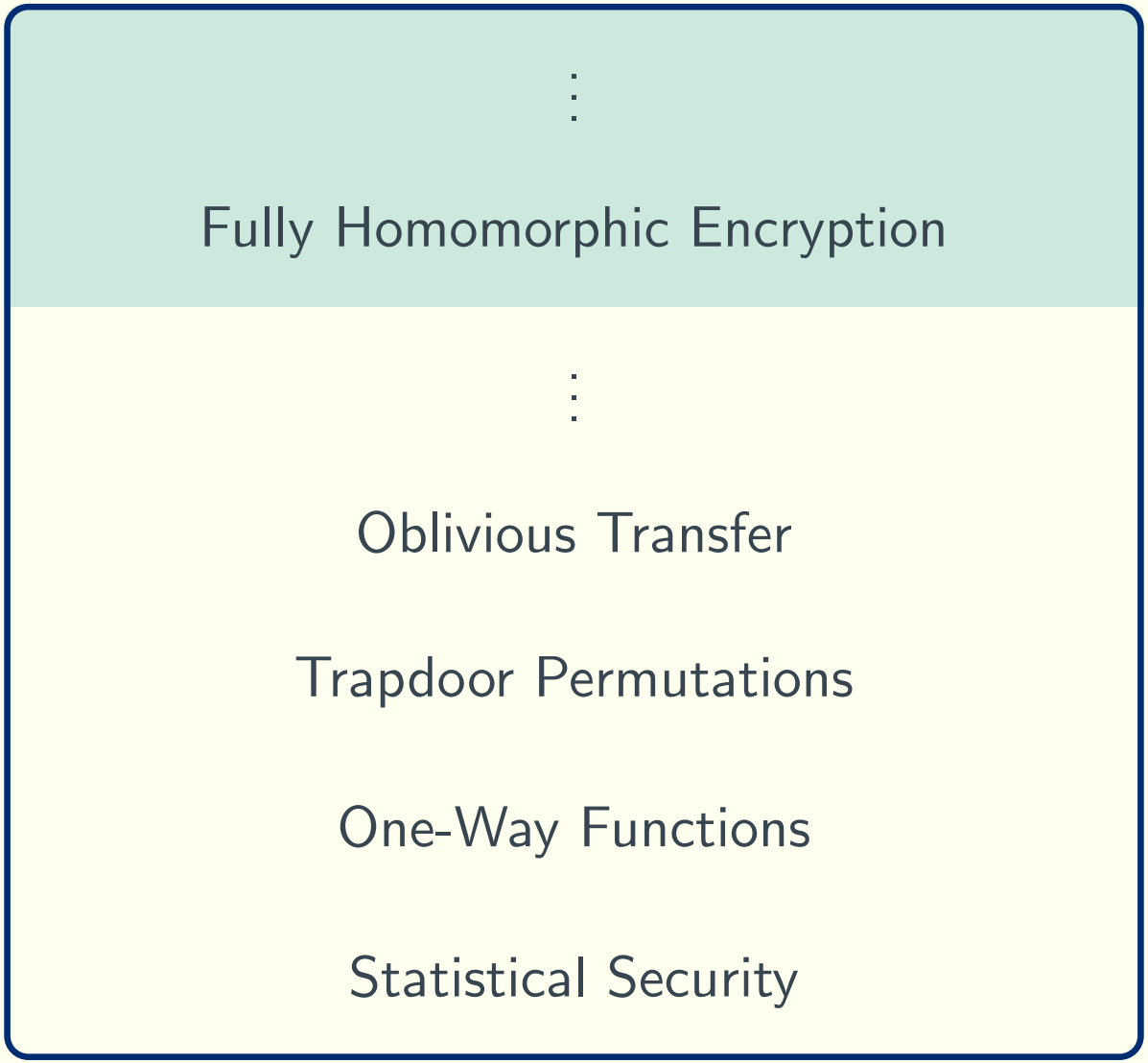
One-Way Functions

Statistical Security

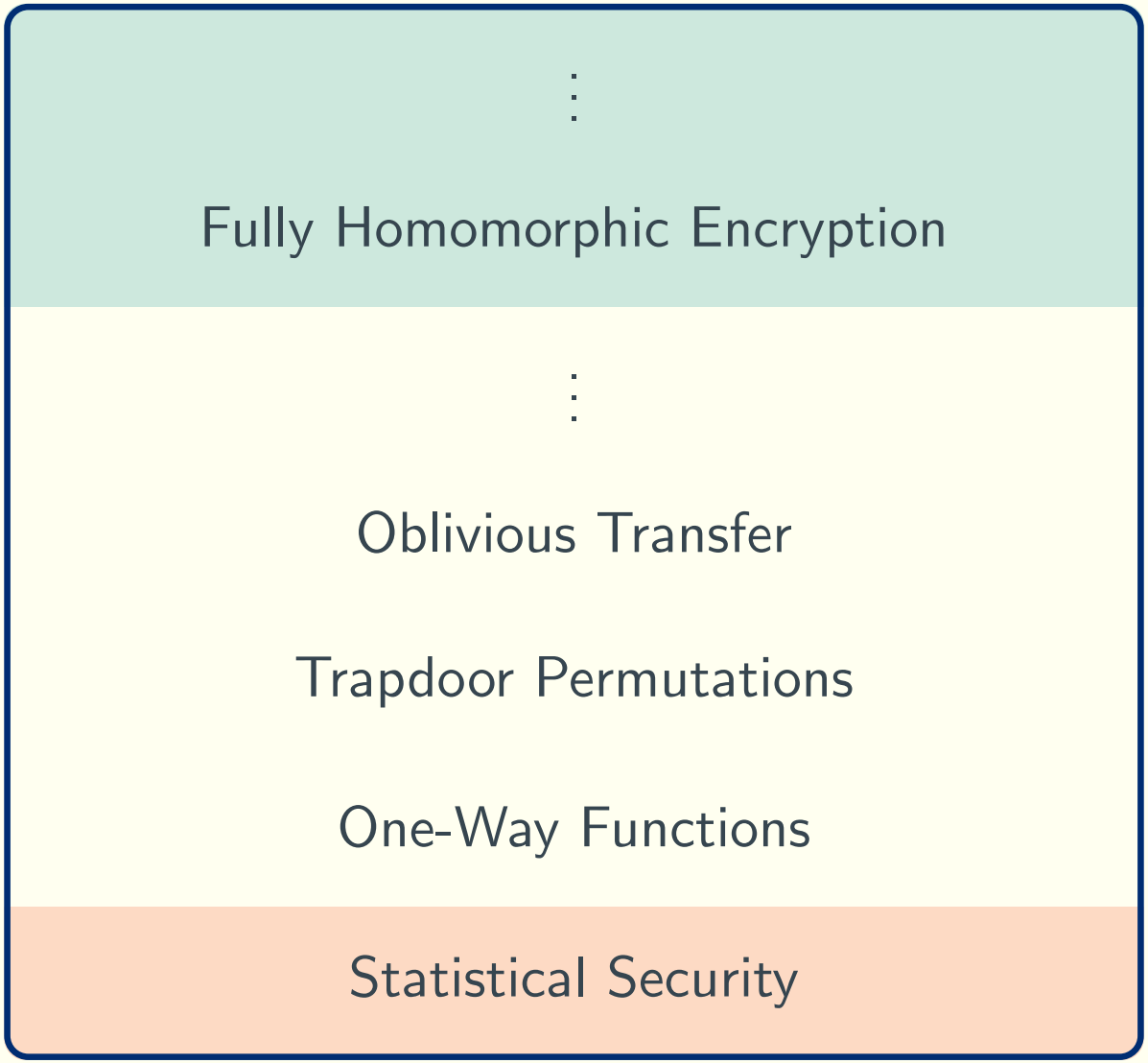
Determining Minimal Assumptions



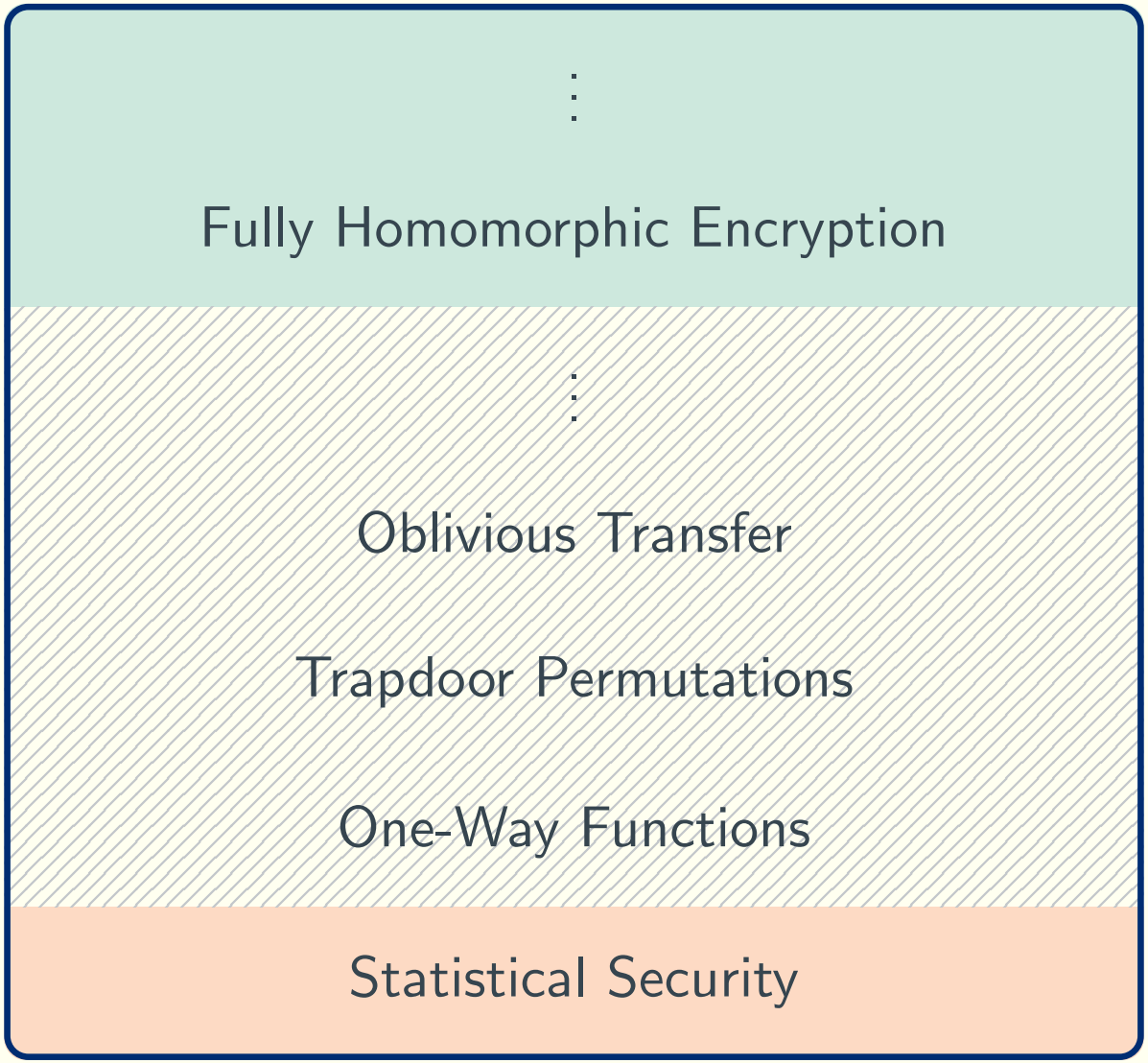
Determining Minimal Assumptions



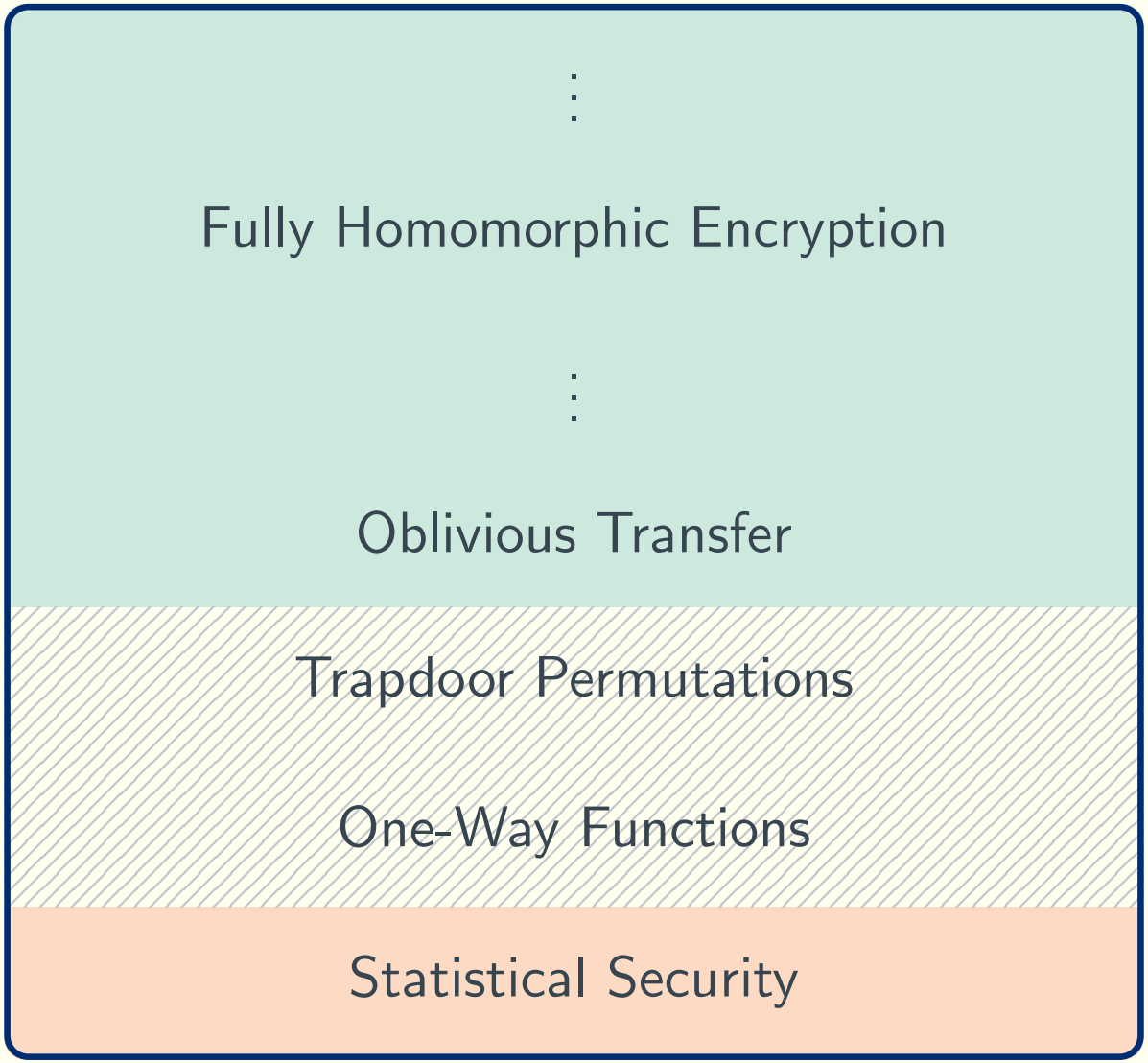
Determining Minimal Assumptions



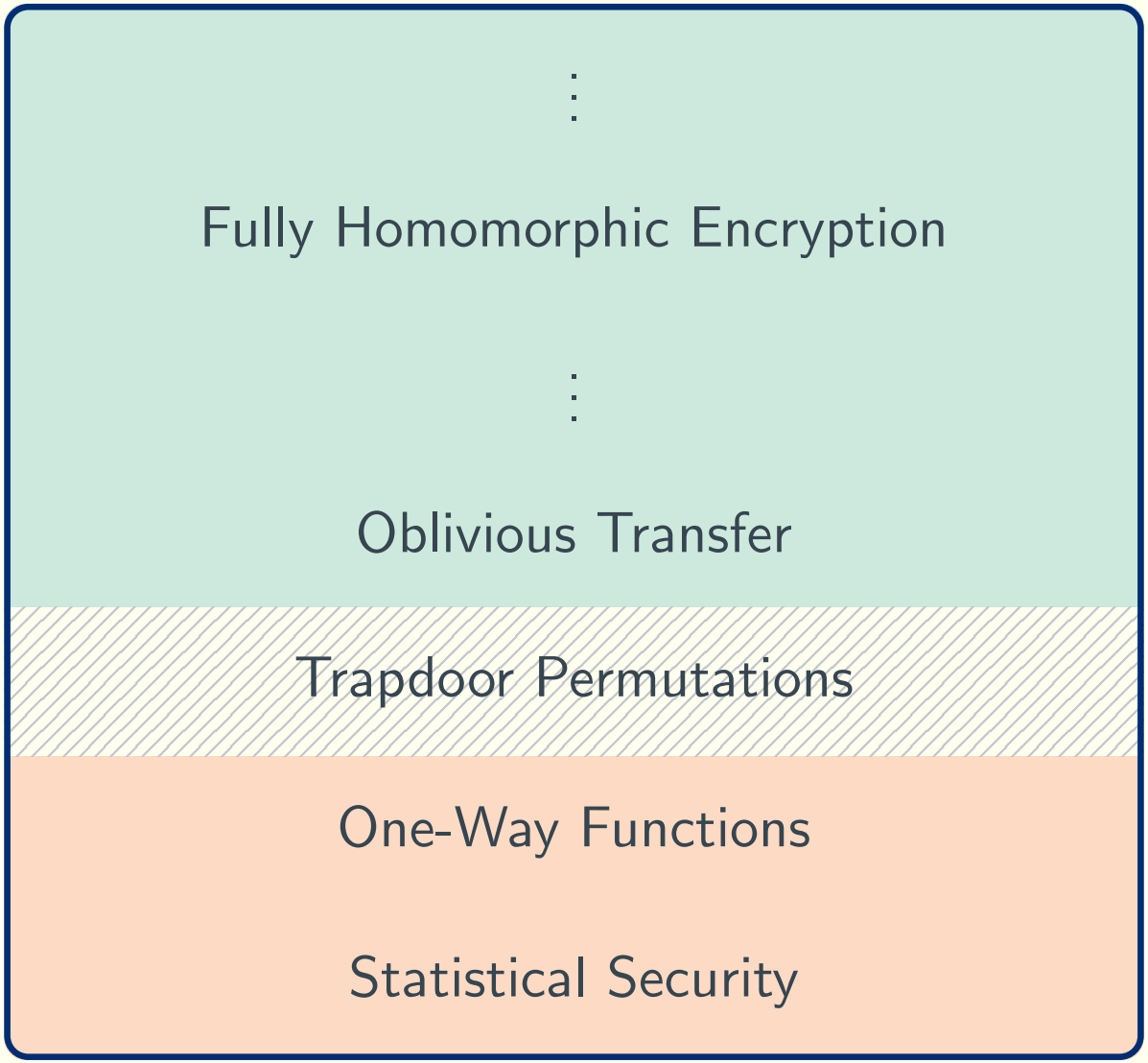
Determining Minimal Assumptions



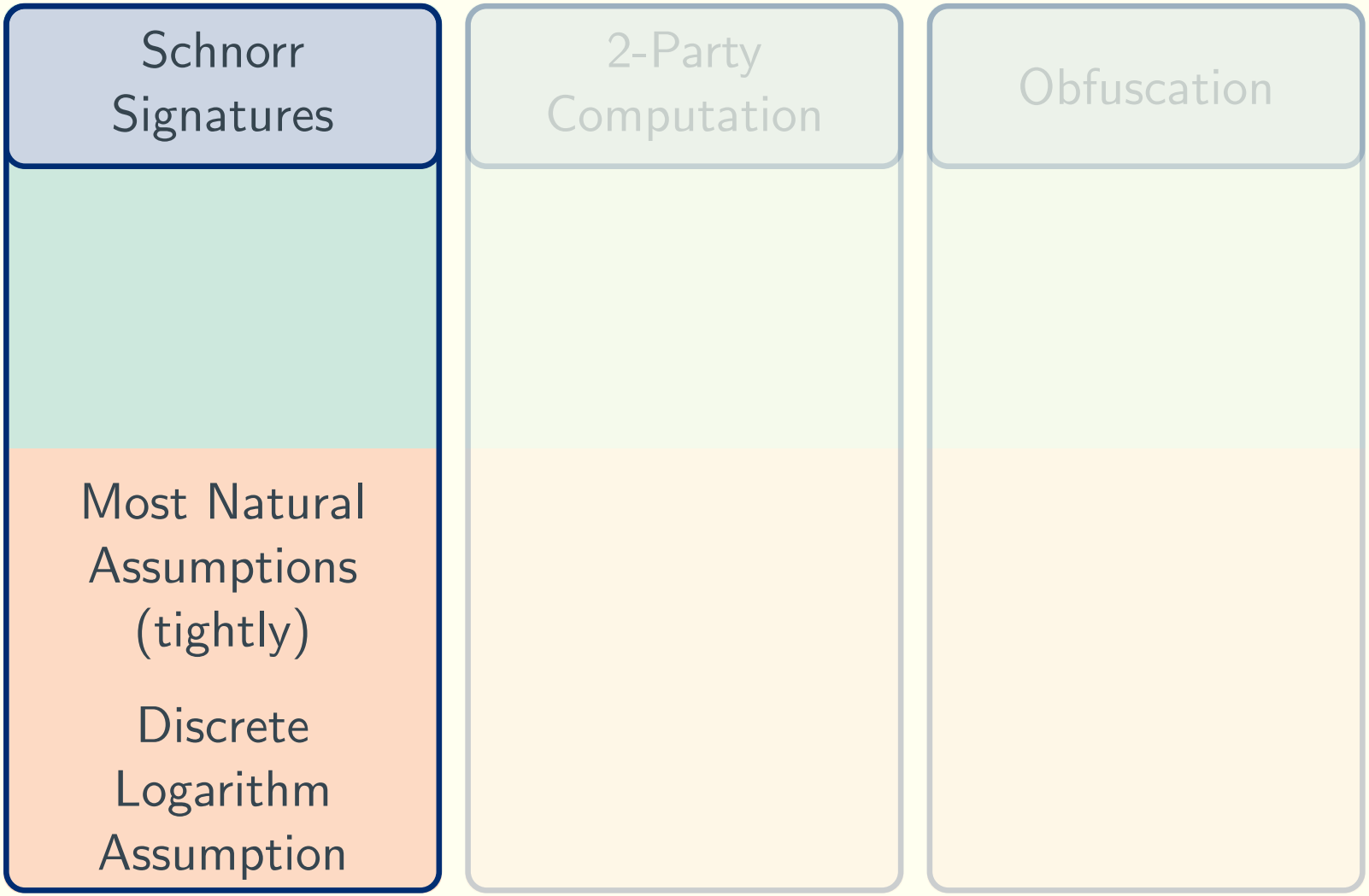
Determining Minimal Assumptions



Determining Minimal Assumptions



Schnorr Signatures	2-Party Computation	Obfuscation


Schnorr Signatures
2-Party Computation
Obfuscation
Most Natural Assumptions (tightly)
Discrete Logarithm Assumption

[FF13,FJS14]

Schnorr Signatures

- Very simple, very efficient!

Schnorr Signatures

- Very simple, very efficient!
- Proven secure under the discrete log assumption. [PS96] But

Schnorr Signatures

- Very simple, very efficient!
- Proven secure under the discrete log assumption. [PS96] But
  - Proof in the Random Oracle Model

Schnorr Signatures

- Very simple, very efficient!
- Proven secure under the discrete log assumption. [PS96] But
  - Proof in the Random Oracle Model
  - Proof is extremely loose.

Schnorr Signatures

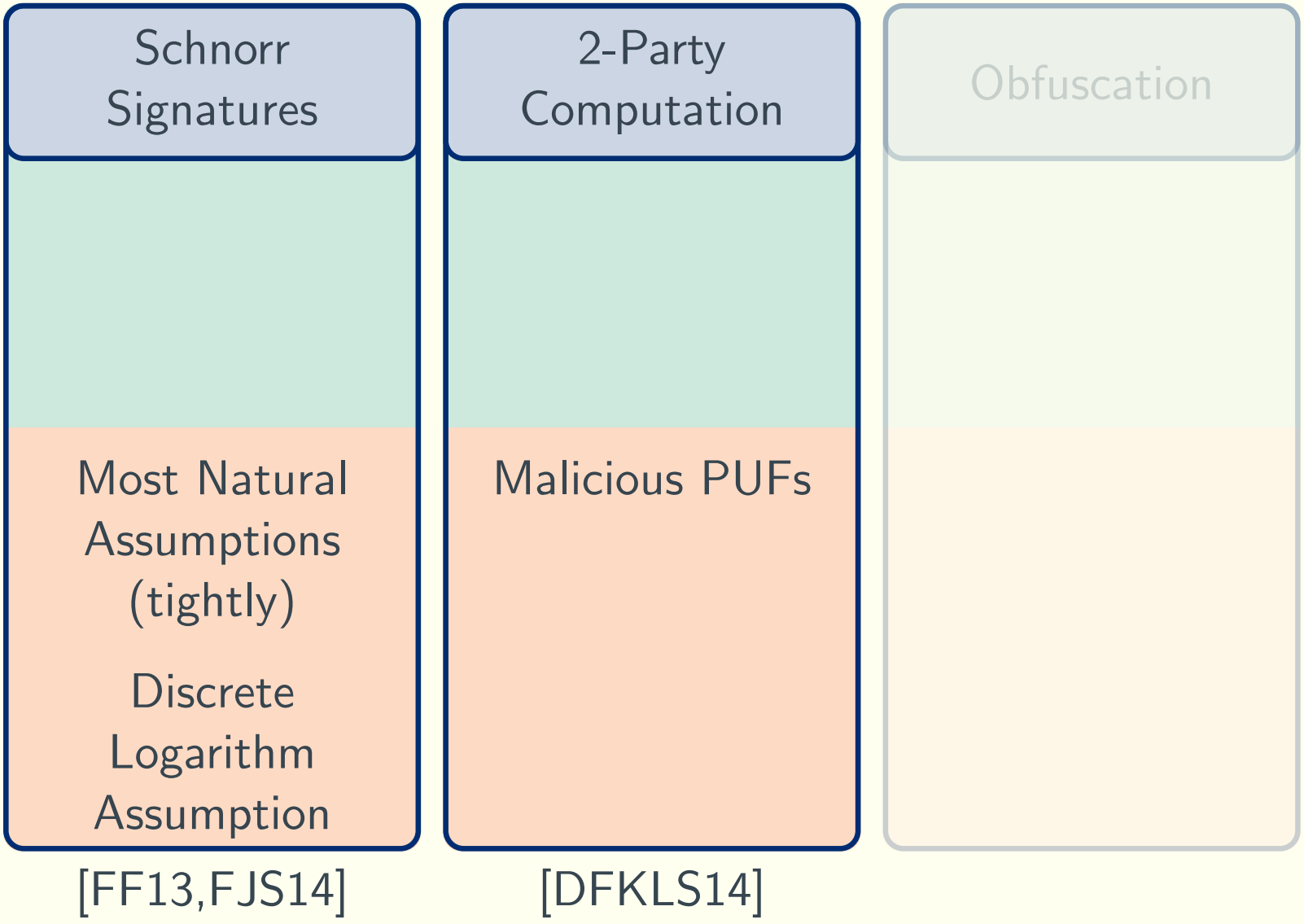
The security of Schnorr signatures cannot be reduced to the discrete logarithm assumption using a naturally restricted reduction in a less idealized model (NPROM).

The result holds under the slightly stronger one-more discrete logarithm assumption.

Schnorr Signatures

The security of Schnorr signatures cannot be tightly reduced to any natural non-interactive assumption using a generic reduction.

The result holds unconditionally.


Schnorr Signatures
2-Party Computation
Obfuscation
Most Natural Assumptions (tightly)
Discrete Logarithm Assumption
Malicious PUFs
[FF13,FJS14]
[DFKLS14]

Secure Two-Party Computation from PUFs

- The idea: Use secure hardware to overcome impossibility of information theoretically secure 2-PC.

Secure Two-Party Computation from PUFs

- The idea: Use secure hardware to overcome impossibility of information theoretically secure 2-PC.
- Use Physically Uncloneable Functions

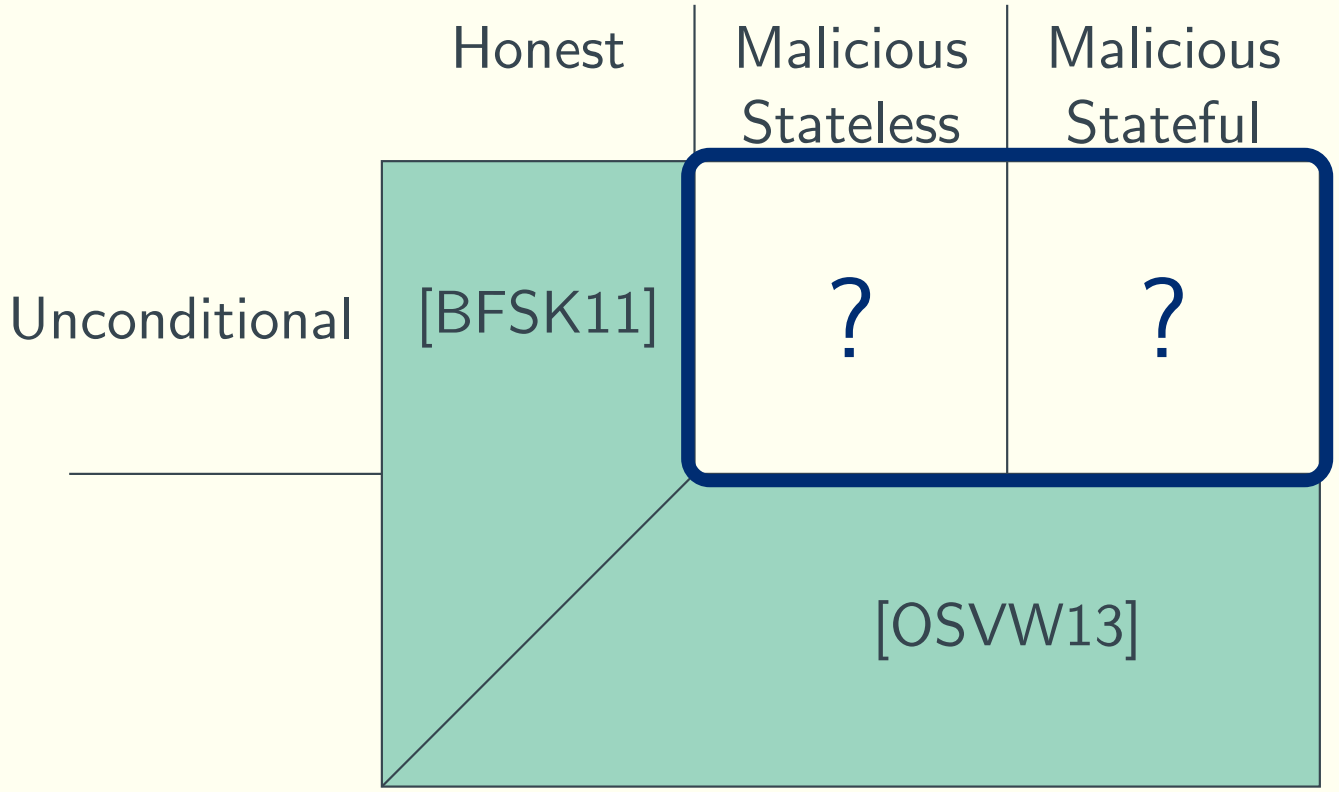
Secure Two-Party Computation from PUFs

- The idea: Use secure hardware to overcome impossibility of information theoretically secure 2-PC.
- Use Physically Uncloneable Functions
  - Behave like random functions.

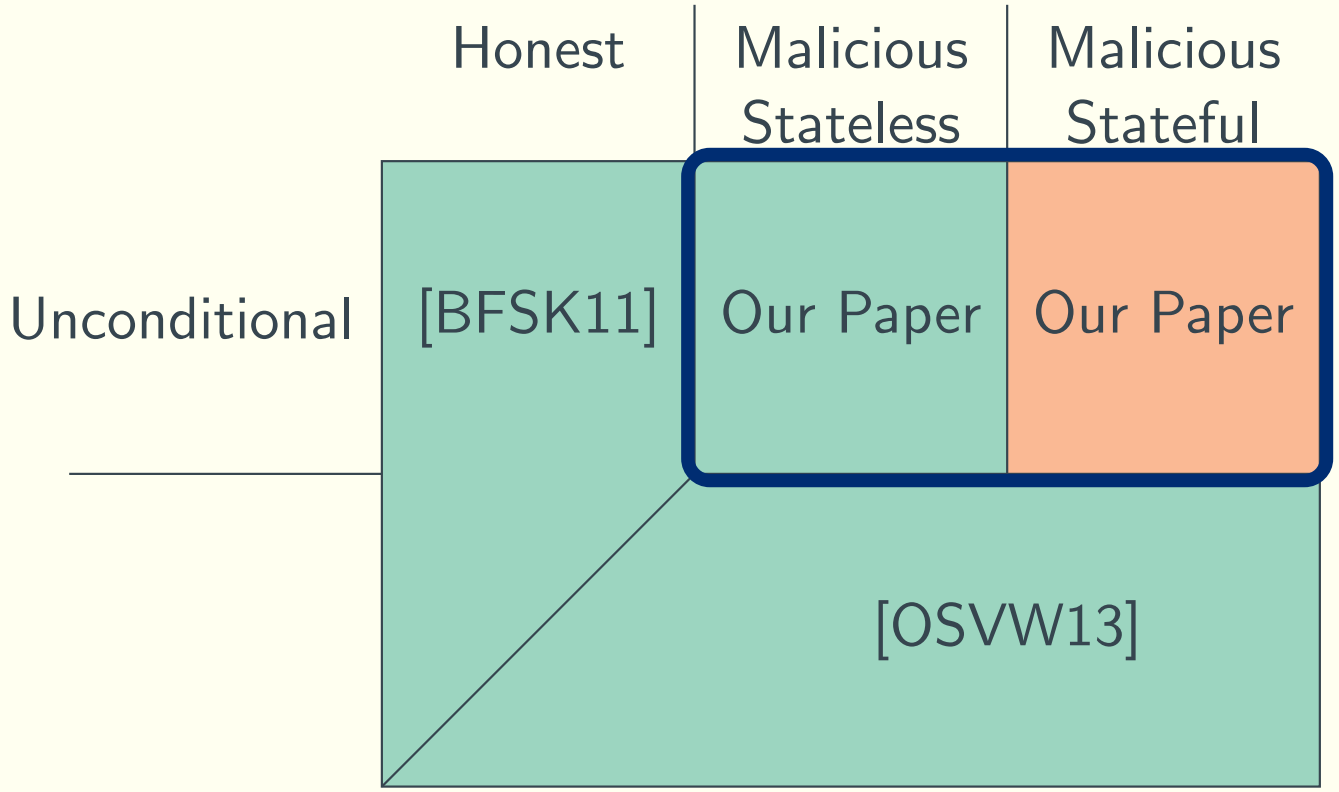
Secure Two-Party Computation from PUFs

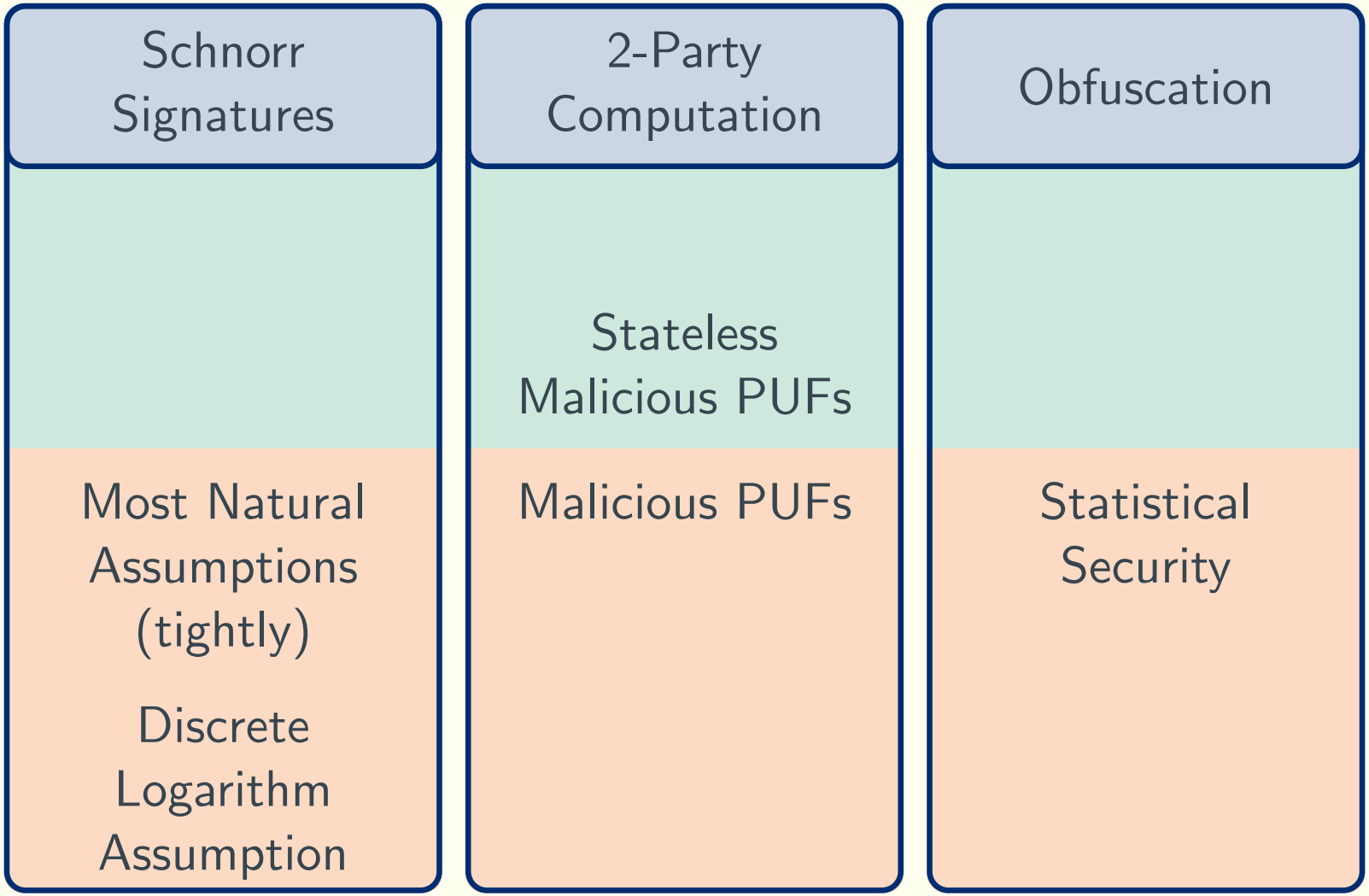
- The idea: Use secure hardware to overcome impossibility of information theoretically secure 2-PC.
- Use Physically Uncloneable Functions
  - Behave like random functions.
  - Cannot be copied.

Secure Computation from PUFs

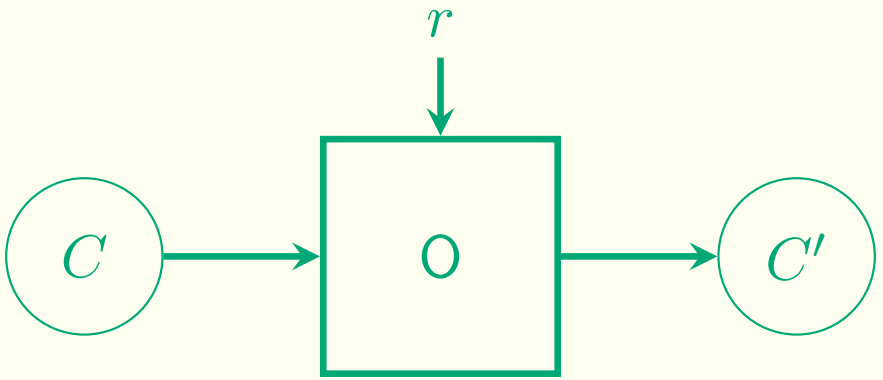


Secure Computation from PUFs

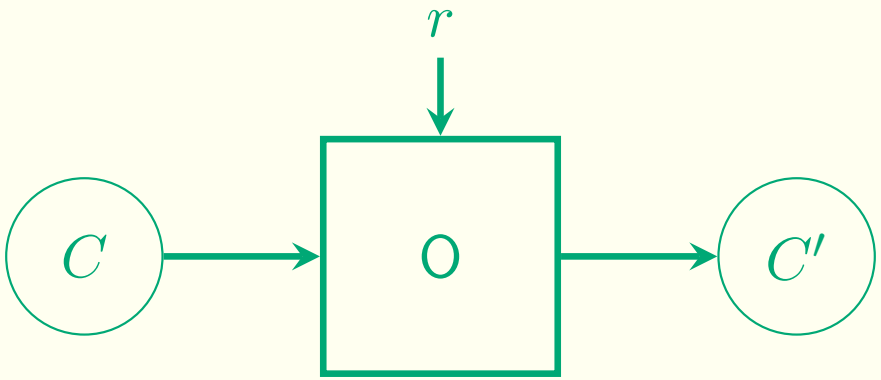



Schnorr Signatures
2-Party Computation
Obfuscation
Stateless Malicious PUFs
Most Natural Assumptions (tightly)
Discrete Logarithm Assumption
Malicious PUFs
Statistical Security
[FF13,FJS14]
[DFKLS14]
[BBF16]

Statistically Secure Obfuscation



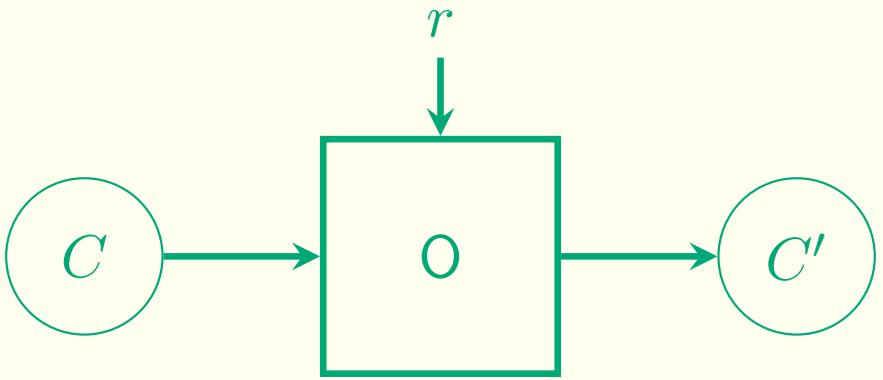
Statistically Secure Obfuscation



- **Perfect Correctness:** For any circuit C

$$\forall x : C'(x) = C(x)$$

Statistically Secure Obfuscation



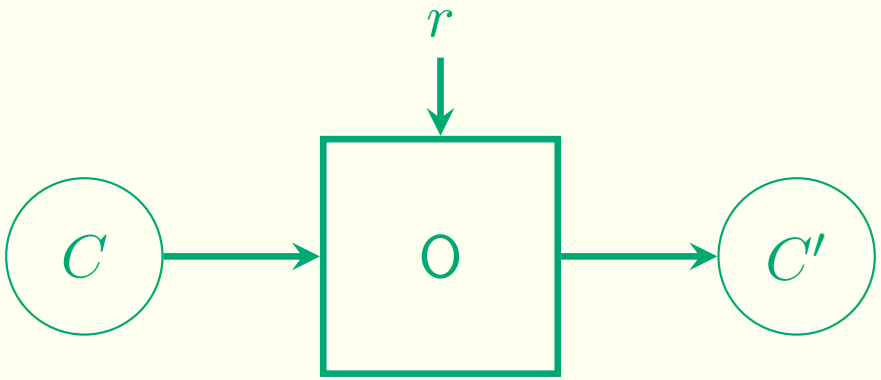
- ~~**Perfect Correctness:** For any circuit C~~

$$\forall x : C'(x) = C(x)$$

- $(1-\epsilon)$-**Approximate Correctness:** For any circuit C,

$$\Pr_{r,x}\left[C'(x) = C(x)\right] \geq 1 - \epsilon(n)$$

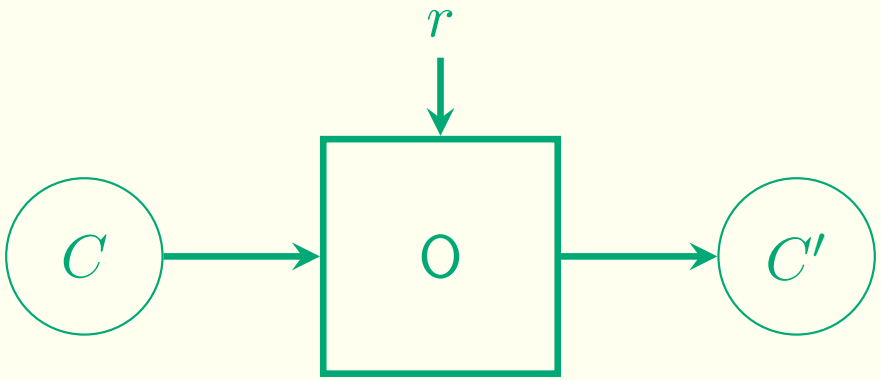
Statistically Secure Obfuscation



- **Indistinguishability Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \mathsf{negl}(n)$$

Statistically Secure Obfuscation



- **Indistinguishability Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

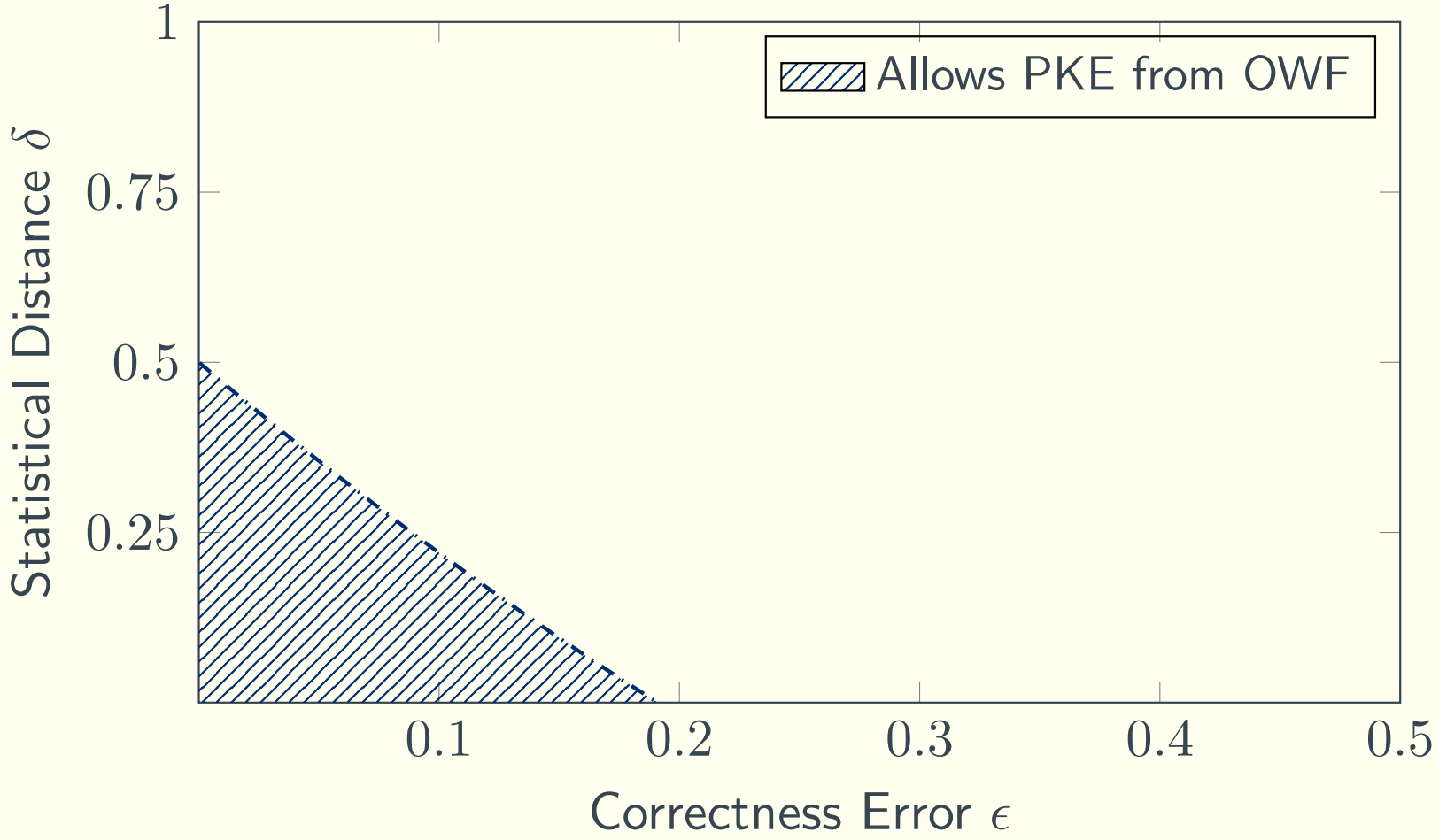
$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \mathsf{negl}(n)$$

- $(1-\delta)$-**Correlation Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \delta(n)$$

Why Do We Even Care About Approximate Correctness?

Because approximate obfuscation is useful!
[MMNPs16,SW14,Hol06]



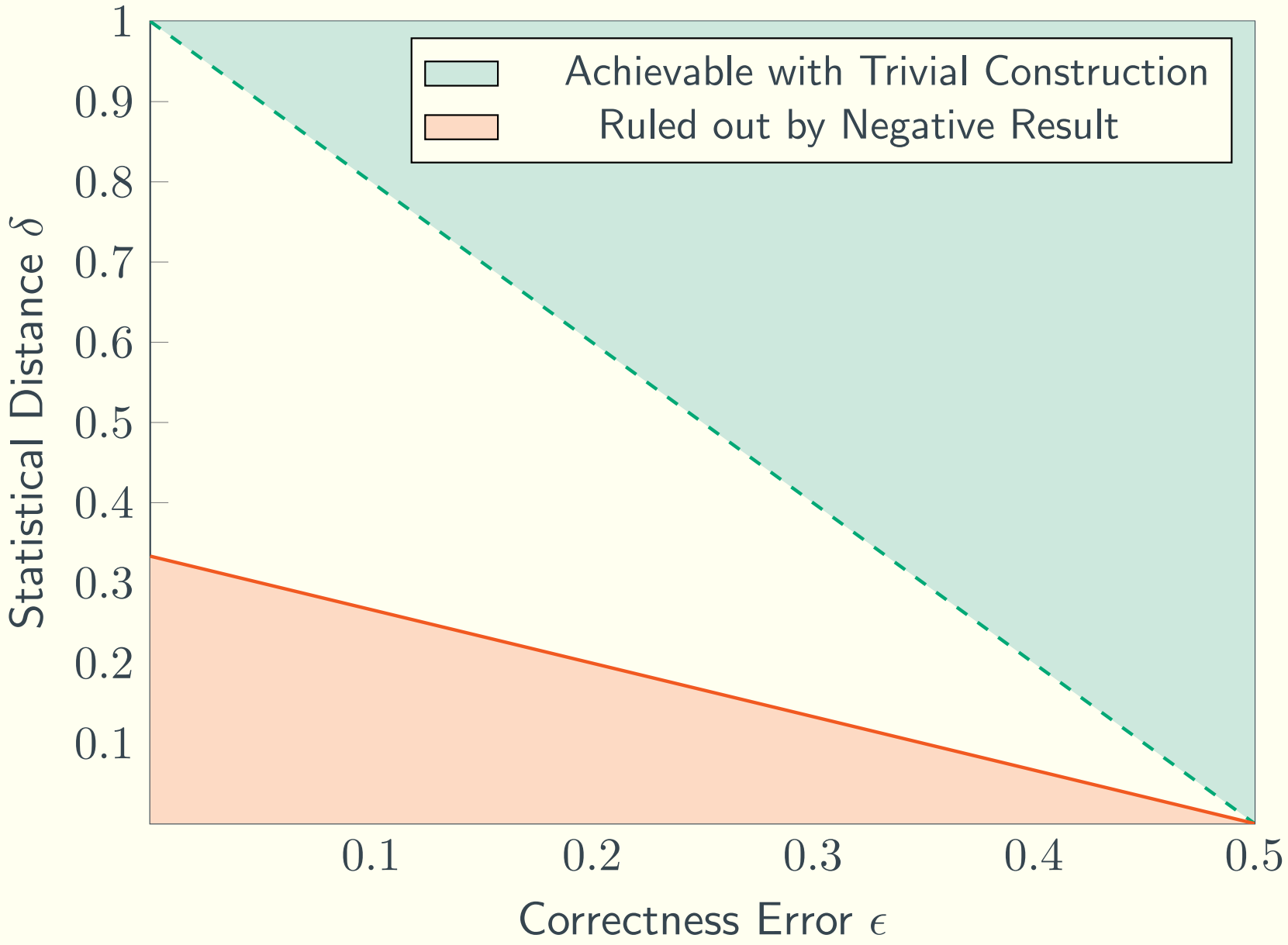
Main Result

- If statistically secure, approximately correct iO (saiO) exists, then either one-way functions do not exist, or $\mathsf{NP} \subseteq \mathsf{AM} \cap \mathsf{coAM}$.

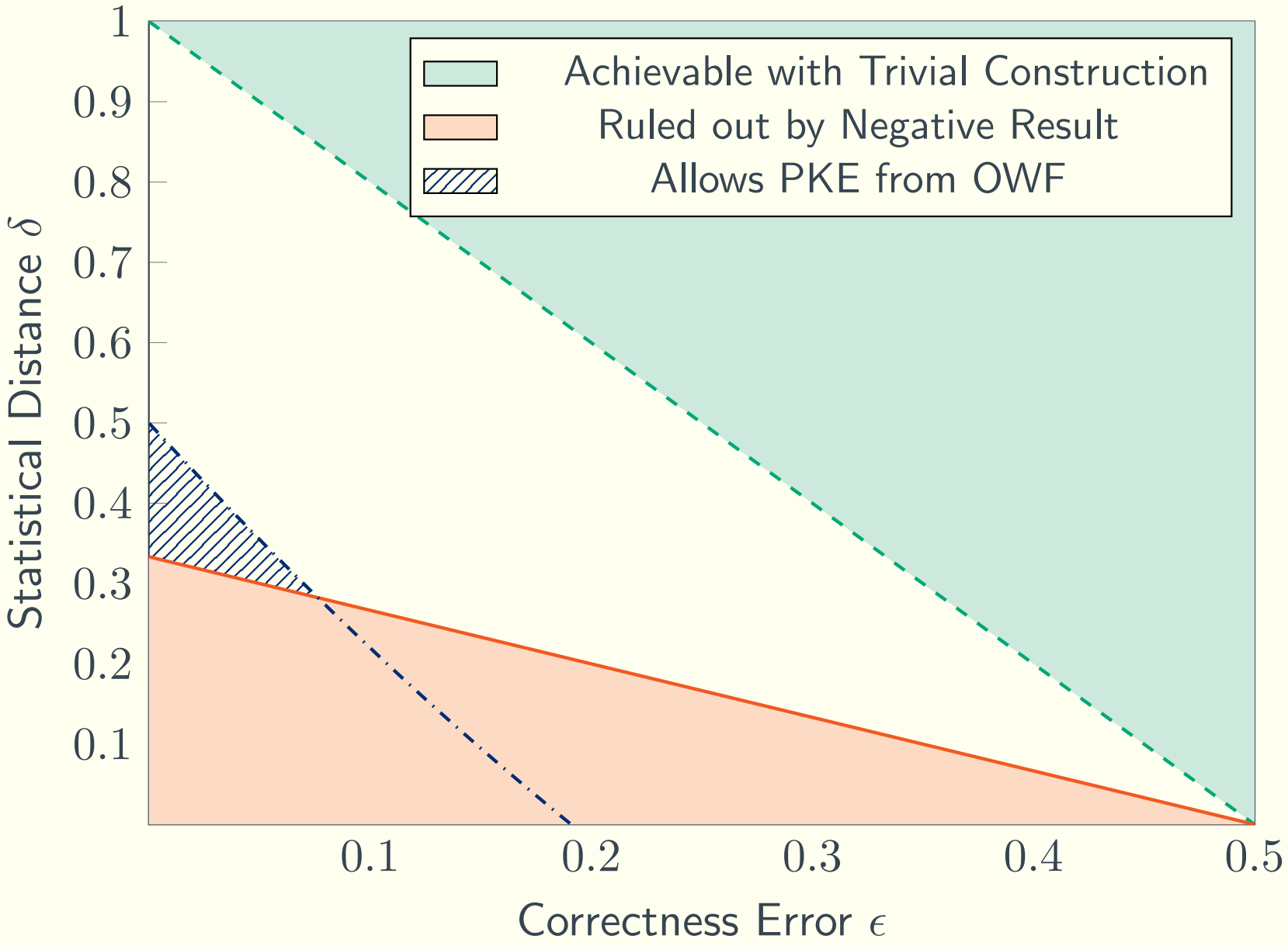
- **More Generally:** If $(1-\delta)$-statistically secure, $(1-\epsilon)$-approximately correct correlation obfuscation (sacO) exists with $\delta(n) \leq \frac{1}{3} - \frac{2}{3}\epsilon(n) - \frac{1}{\mathsf{poly}(n)}$, then either one-way functions do not exist, or $\mathsf{NP} \subseteq \mathsf{AM} \cap \mathsf{coAM}$.

- For very weak parameters, a trivial construction of sacO exists with $\delta(n) = 2\epsilon(n)$.

The Landscape of Correlation Obfuscation



The Landscape of Correlation Obfuscation



Publications

On the Existence of Three Round Zero-Knowledge Proofs (EUROCRYPT 2018)
Nils Fleischhacker, Vipul Goyal, Abhishek Jain

Efficient Cryptographic Password Hardening Services From Partially Oblivious Commitments (CCS 2016)
Jonas Schneider, Nils Fleischhacker, Dominique Schröder, Michael Backes

On Statistically Secure Obfuscation with Approximate Correctness (CRYPTO 2016)
Zvika Brakerski, Chris Brzuska, Nils Fleischhacker

Two Message Oblivious Evaluation of Cryptographic Functionalities (CRYPTO 2016)
Nico Doettling, Nils Fleischhacker, Johannes Krupp, Dominique Schröder

Efficient Unlinkable Sanitizable Signatures from Signatures with Re-Randomizable Keys (PKC 2016)
Nils Fleischhacker, Johannes Krupp, Giulio Malavolta, Jonas Schneider, Dominique Schröder, Mark Simkin

On Tight Security Proofs for Schnorr Signatures (ASIACRYPT 2014)
Nils Fleischhacker, Tibor Jager, Dominique Schröder

Feasibility and Infeasibility of Secure Computation with Malicious PUFs (CRYPTO 2014)
Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, Dominique Schröder

Limitations of the Meta-Reduction Technique: The Case of Schnorr Signatures (EUROCRYPT 2013)
Marc Fischlin, Nils Fleischhacker

Thank You!