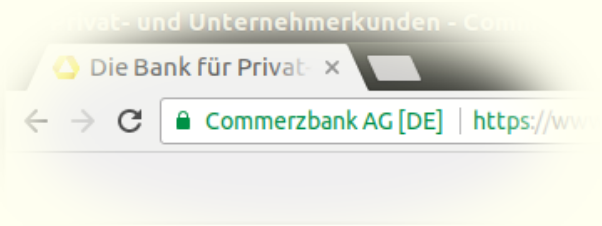
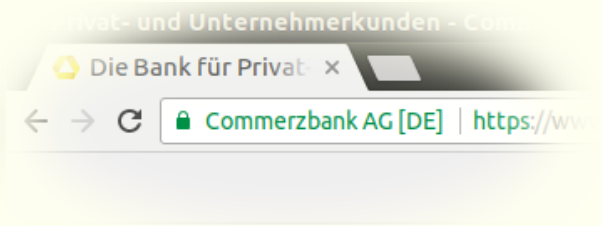
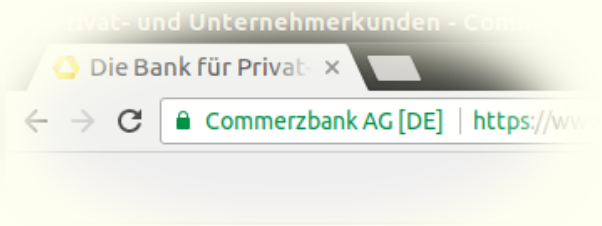
On Assumptions and the Limits of Cryptography

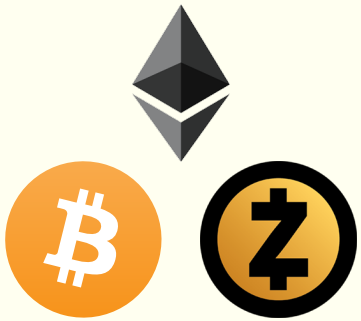
Nils Fleischhacker

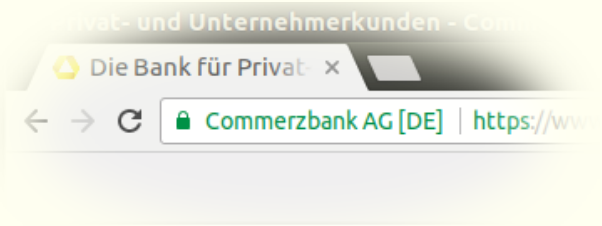
Bochum, January 23, 2019


Die Bank für Privat
Commerzbank AG [DE]

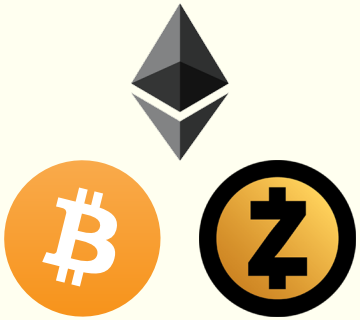

Die Bank für Privat
Commerzbank AG [DE]

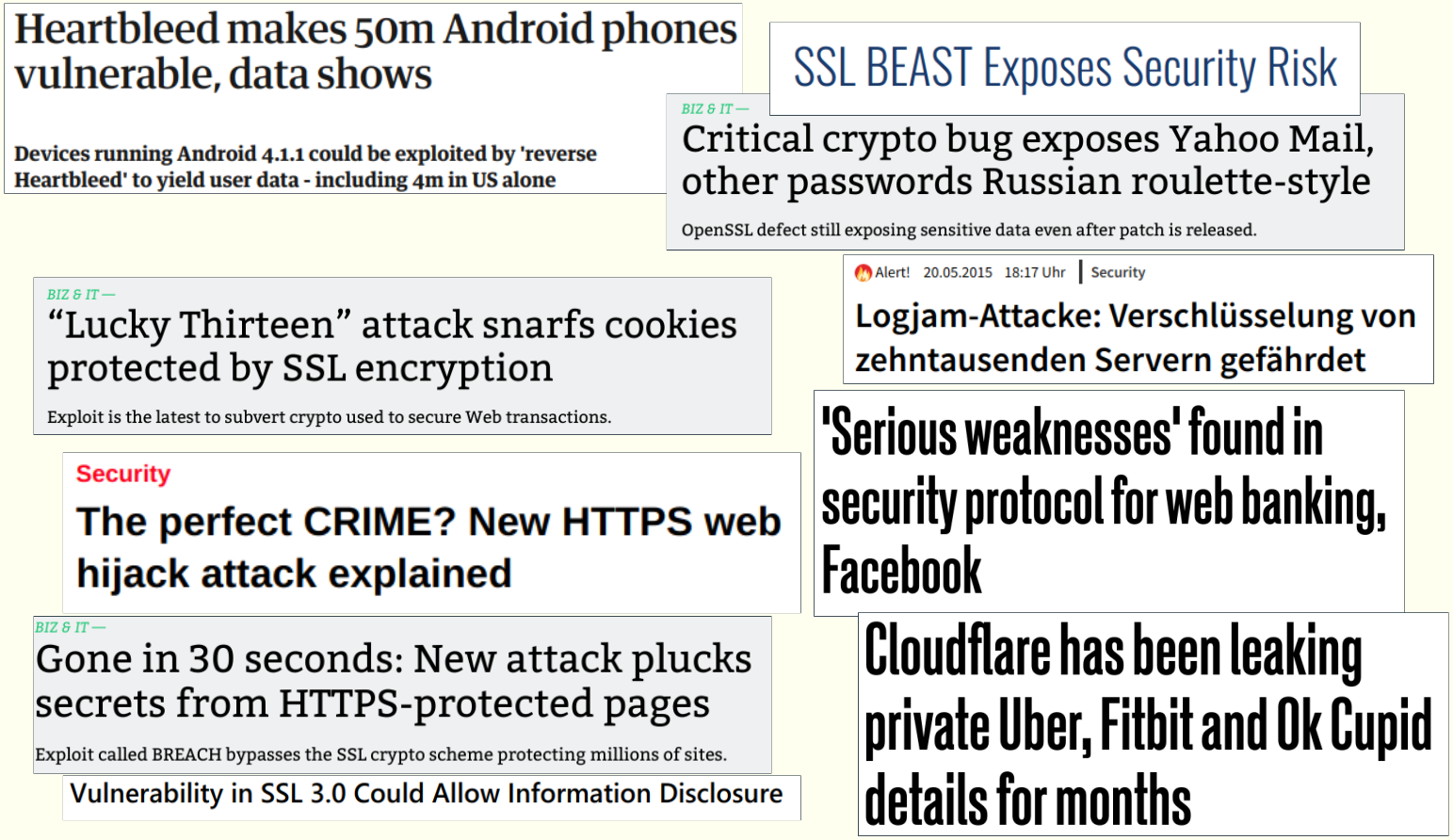

Die Bank für Privat
Commerzbank AG [DE]

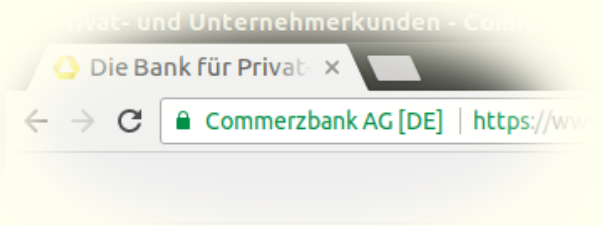




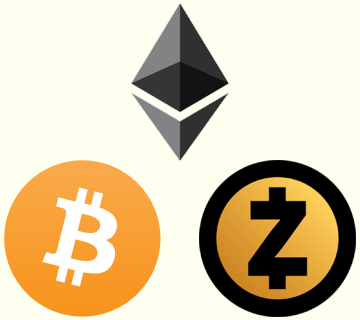
So, how do we know all of this is secure?

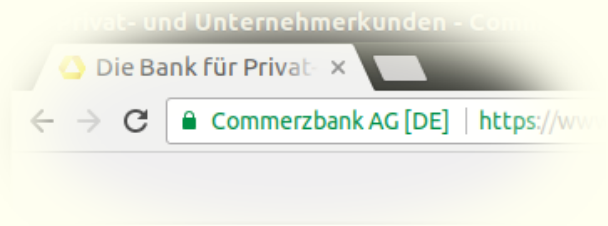



Heartbleed makes 50m Android phones vulnerable, data shows
Devices running Android 4.1.1 could be exploited by 'reverse Heartbleed' to yield user data - including 4m in US alone
SSL BEAST Exposes Security Risk
BIZ & IT —
Critical crypto bug exposes Yahoo Mail, other passwords Russian roulette-style
OpenSSL defect still exposing sensitive data even after patch is released.
BIZ & IT —
"Lucky Thirteen" attack snarfs cookies protected by SSL encryption
Exploit is the latest to subvert crypto used to secure Web transactions.
Alert! 20.05.2015 18:17 Uhr | Security
Logjam-Attacke: Verschlüsselung von zehntausenden Servern gefährdet
Security
The perfect CRIME? New HTTPS web hijack attack explained
'Serious weaknesses' found in security protocol for web banking, Facebook
BIZ & IT —
Gone in 30 seconds: New attack plucks secrets from HTTPS-protected pages
Exploit called BREACH bypasses the SSL crypto scheme protecting millions of sites.
Vulnerability in SSL 3.0 Could Allow Information Disclosure
Cloudflare has been leaking private Uber, Fitbit and Ok Cupid details for months

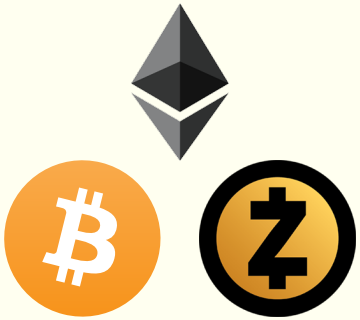


Can we know whether all of this is secure?

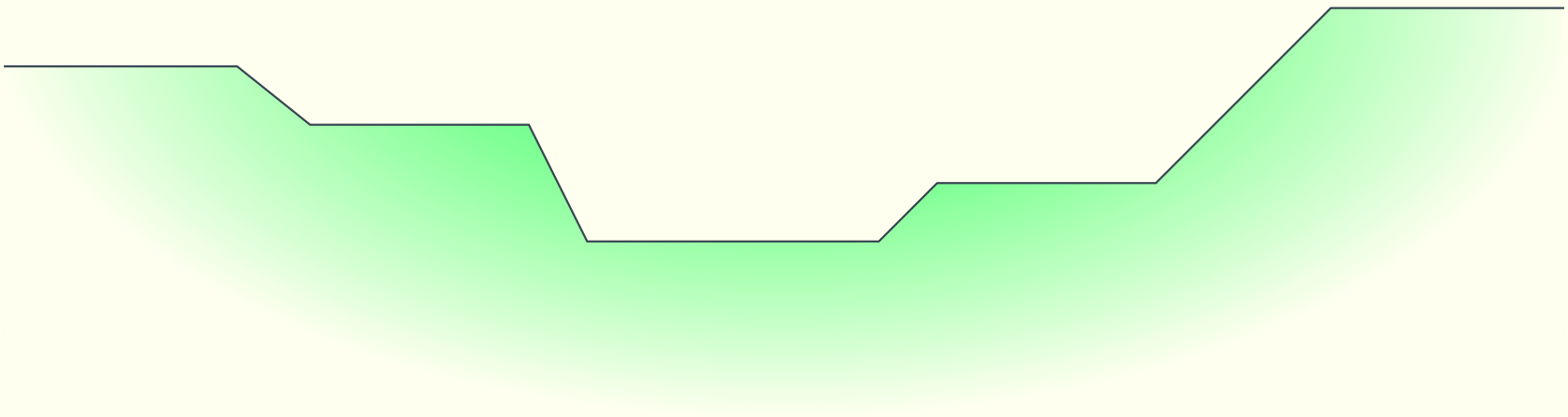




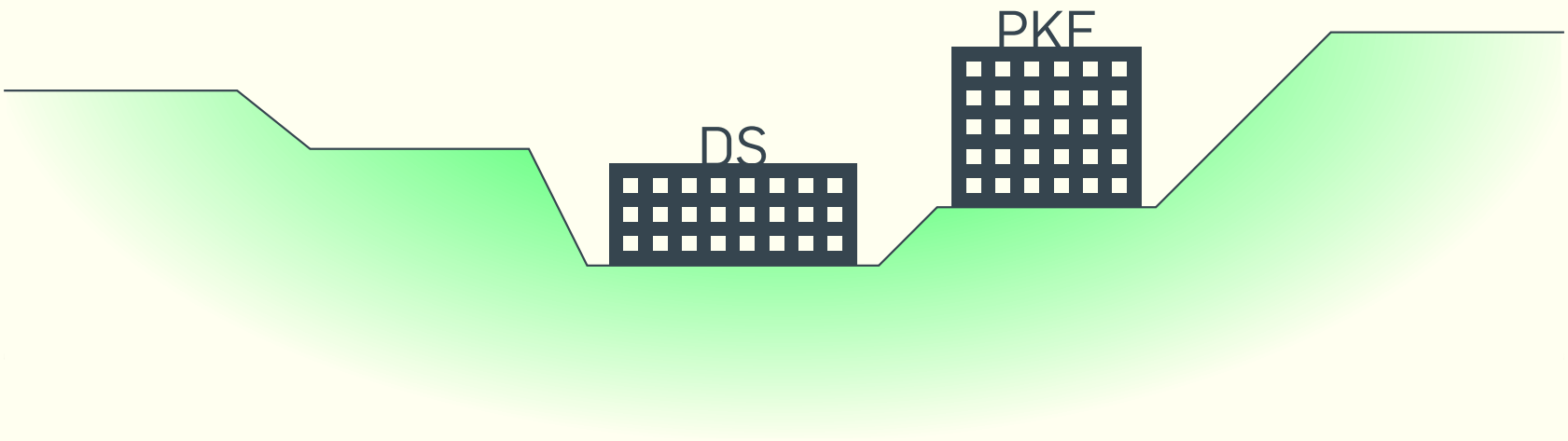
The sad truth is: At the moment we can't! Not really.



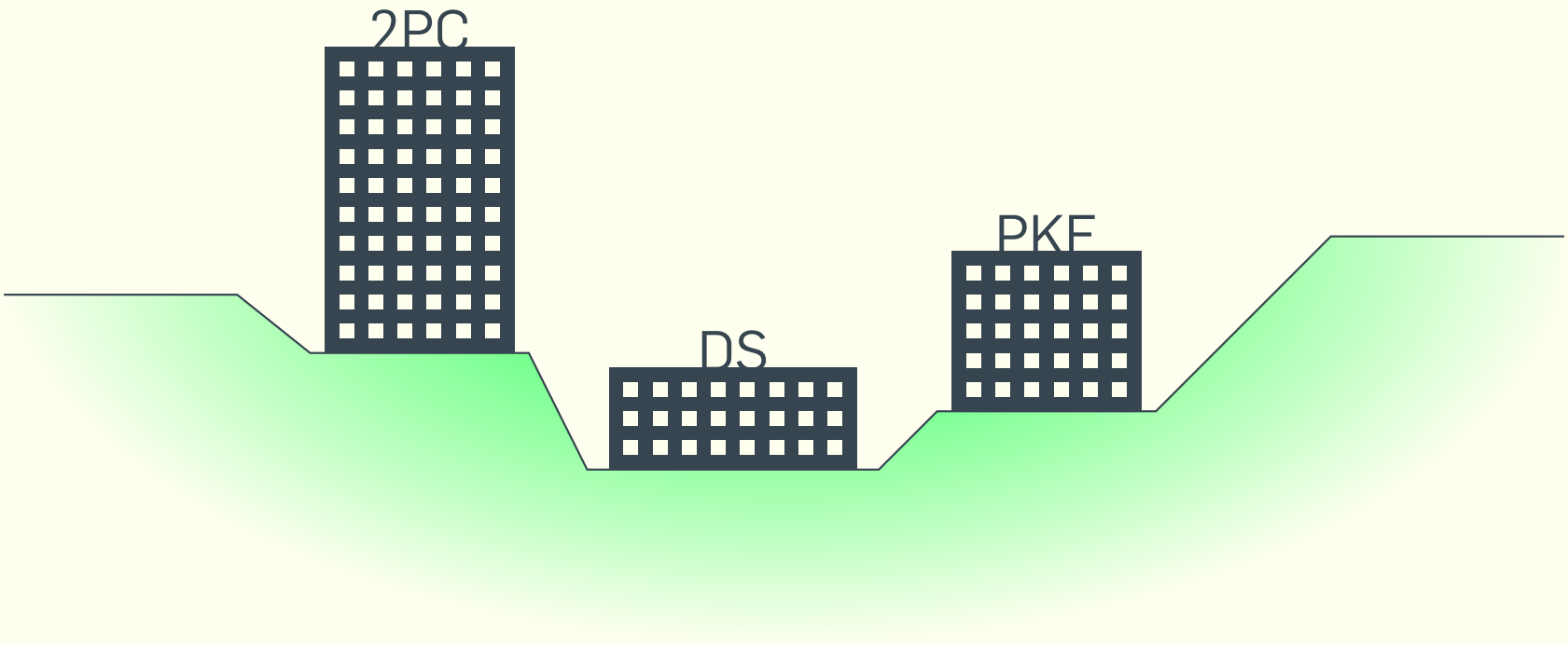
The Cryptographic Landscape



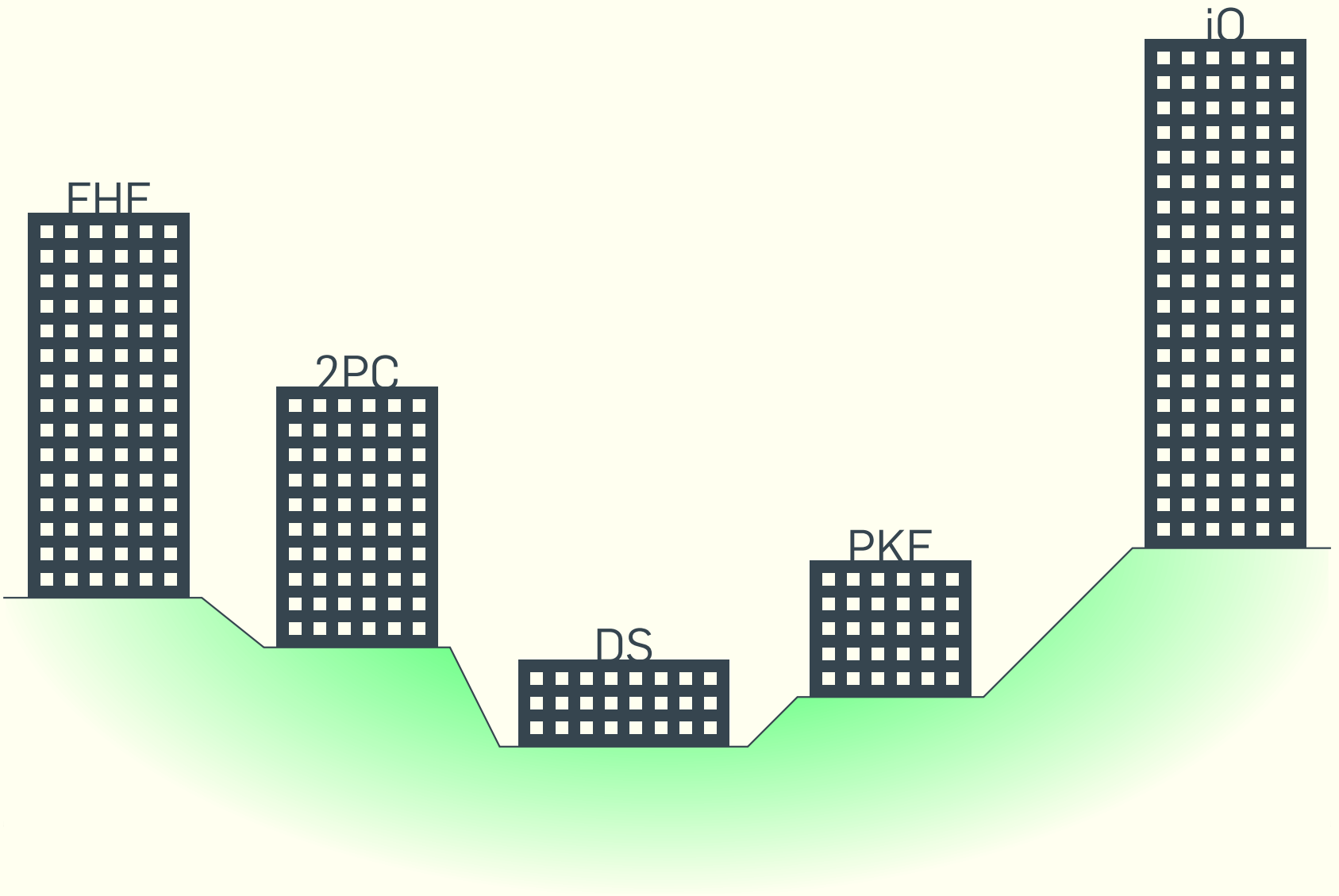
The Cryptographic Landscape



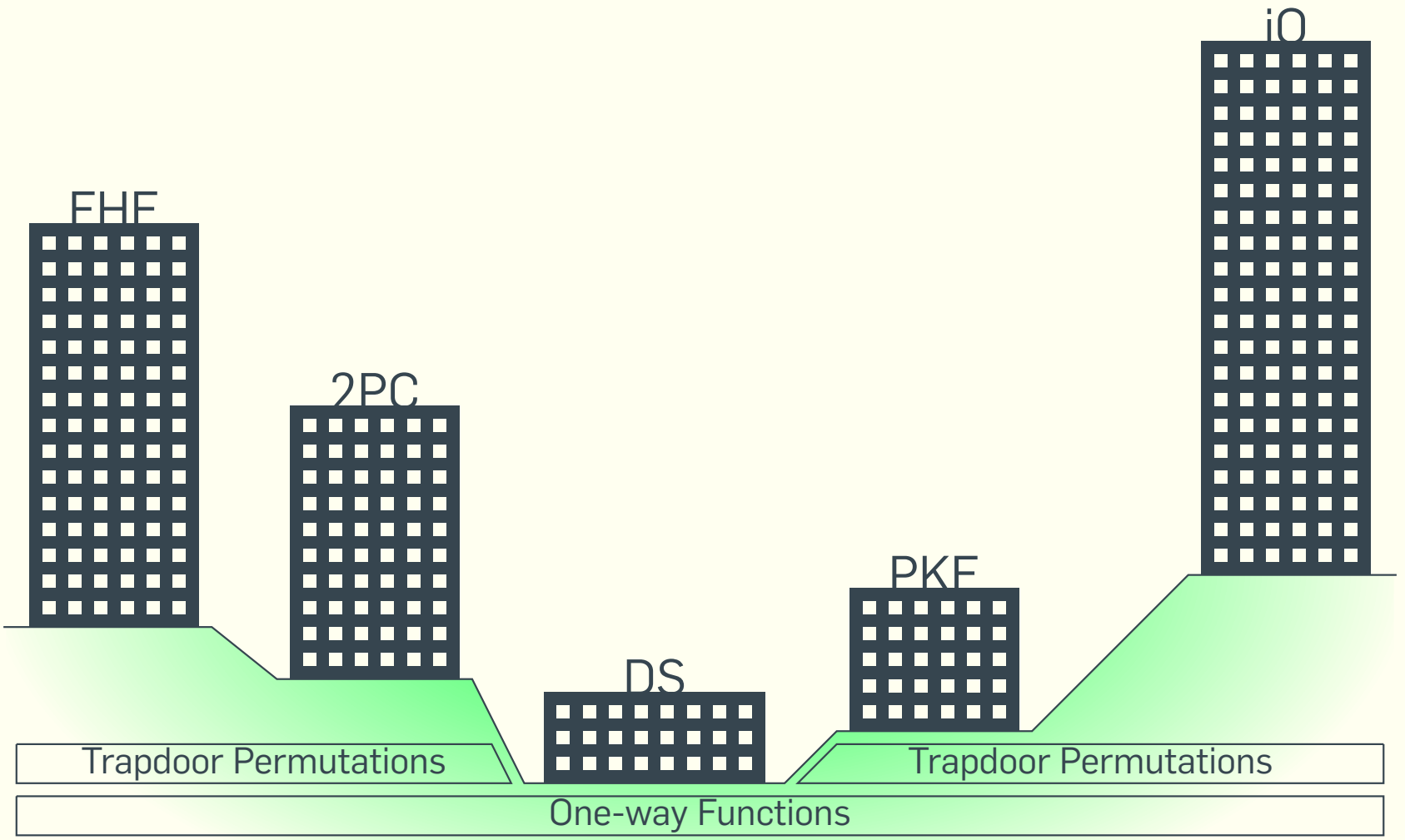
The Cryptographic Landscape



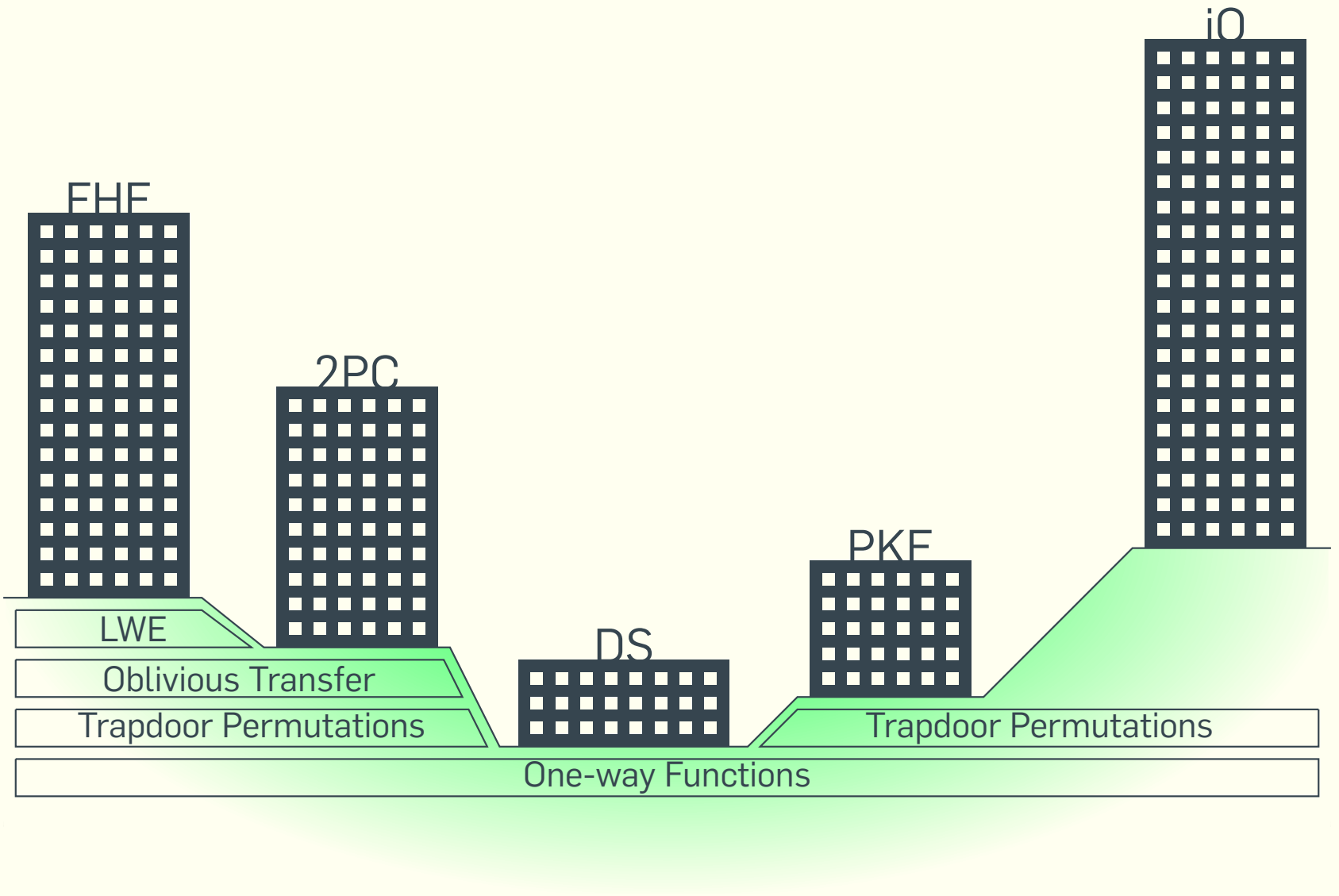
The Cryptographic Landscape



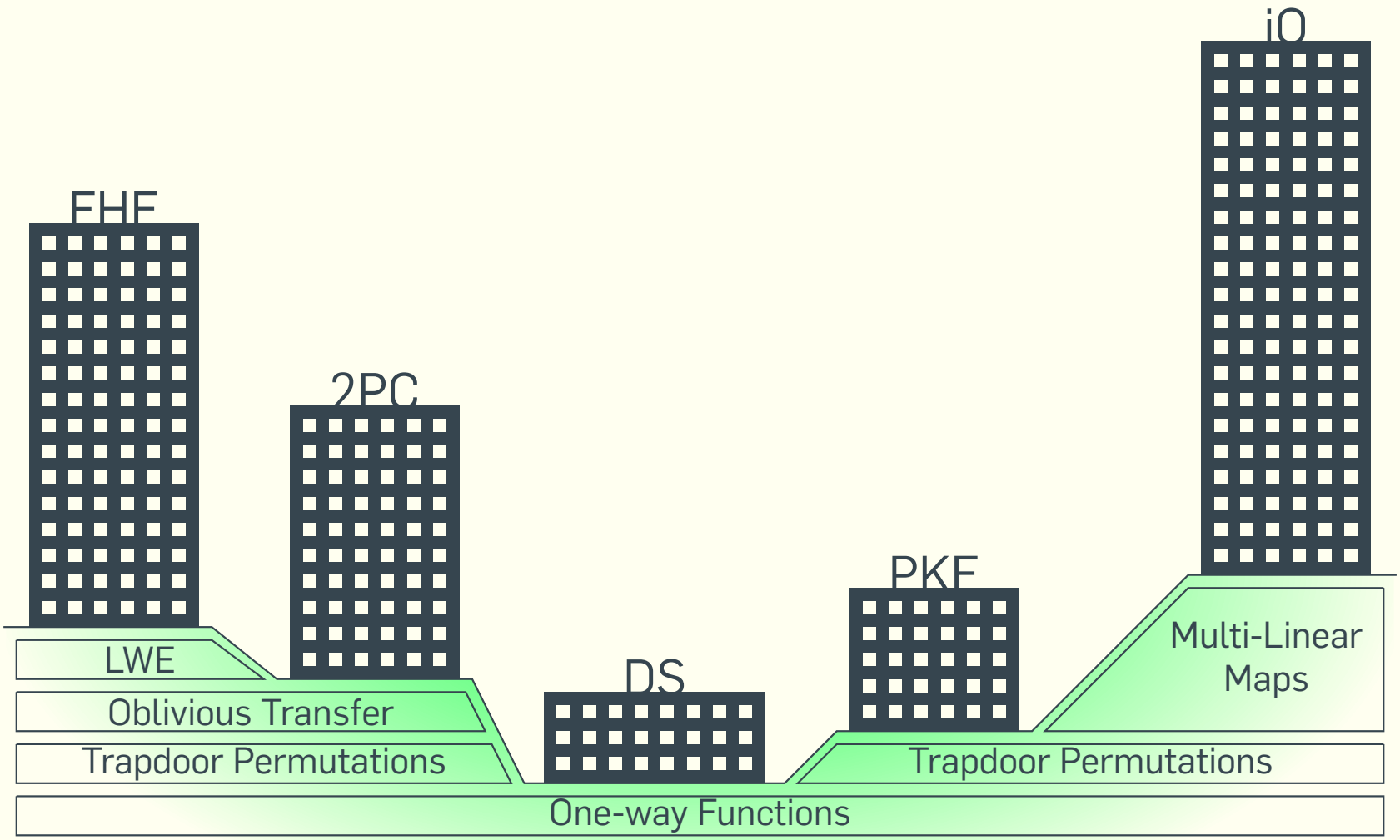
The Cryptographic Landscape



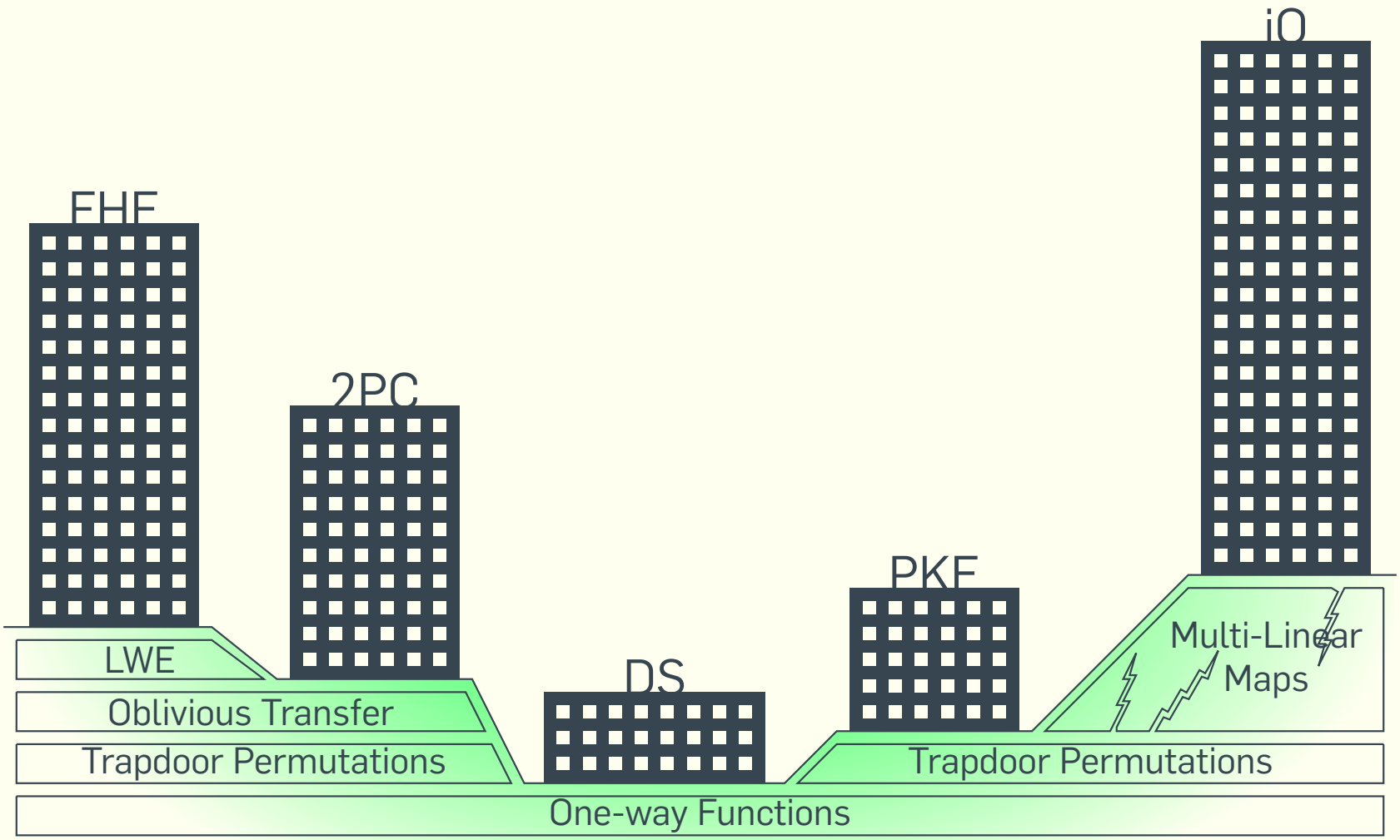
The Cryptographic Landscape



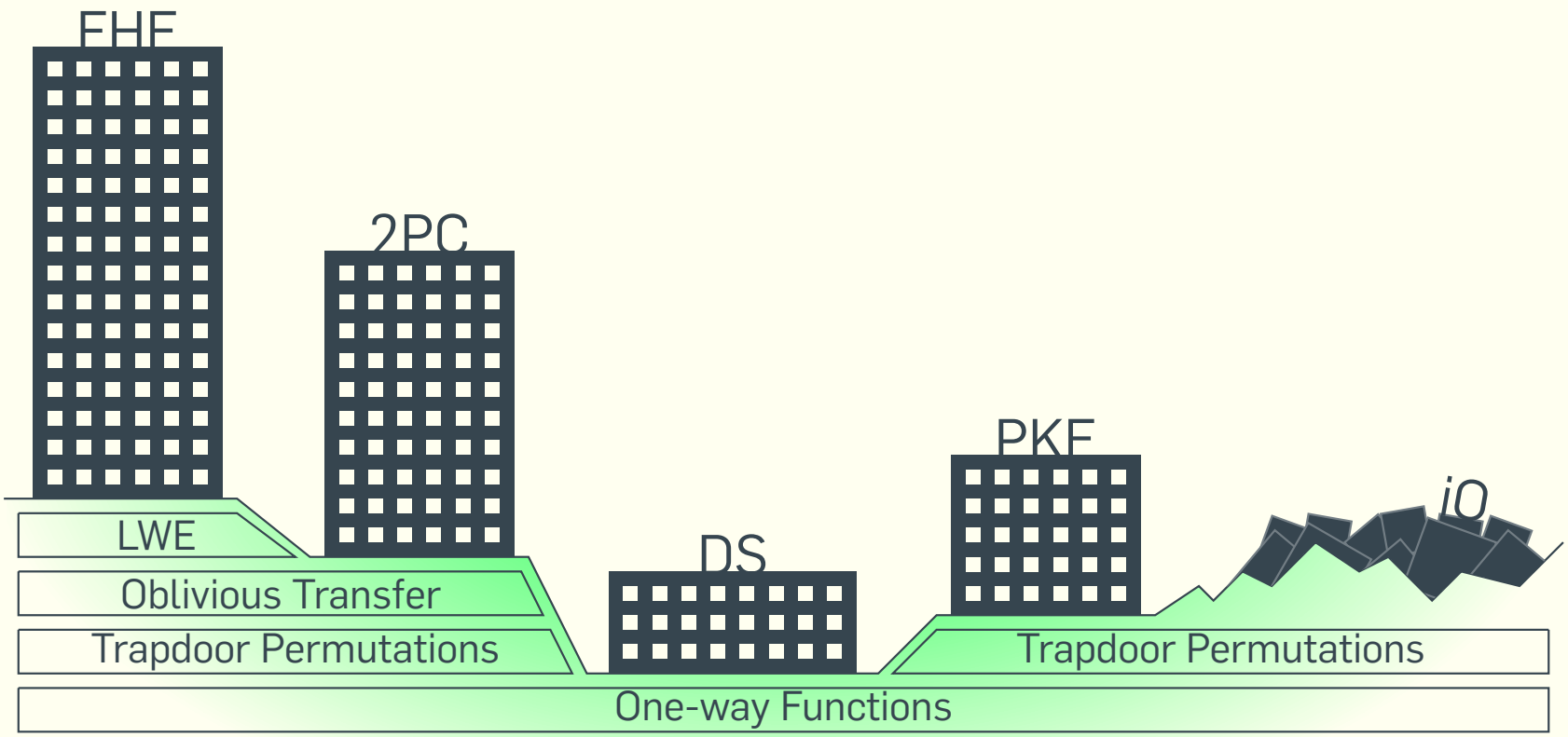
The Cryptographic Landscape



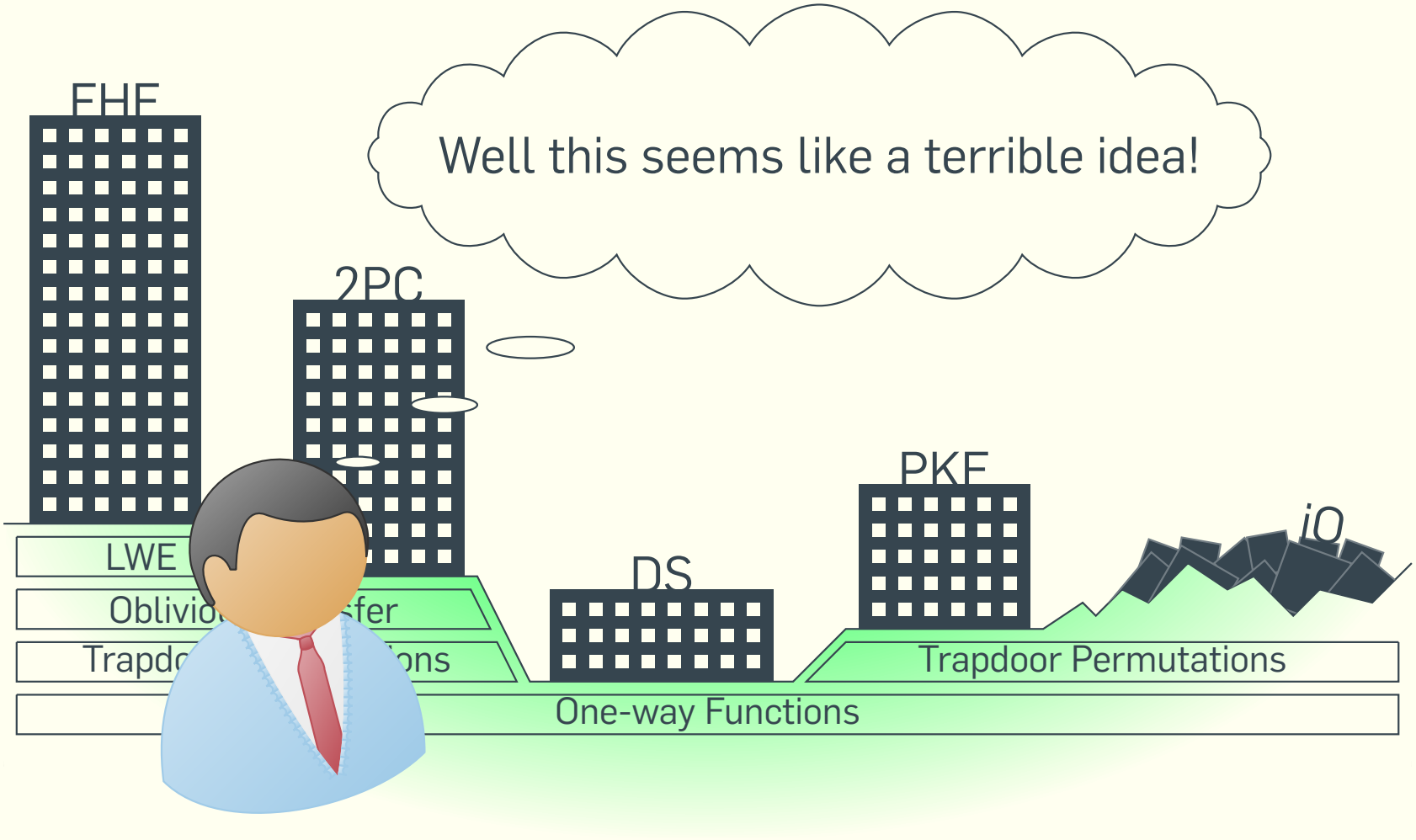
The Cryptographic Landscape



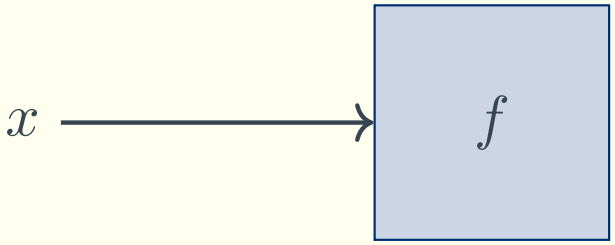
The Cryptographic Landscape



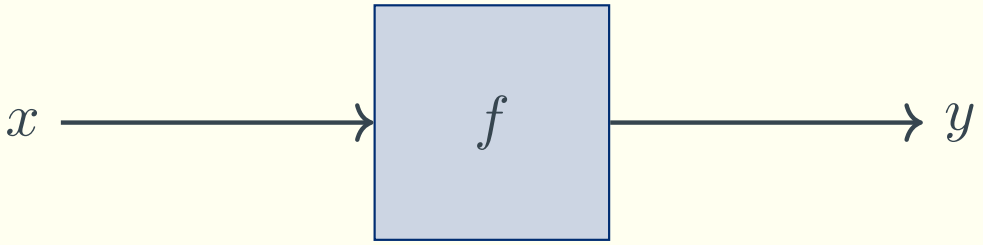
The Cryptographic Landscape



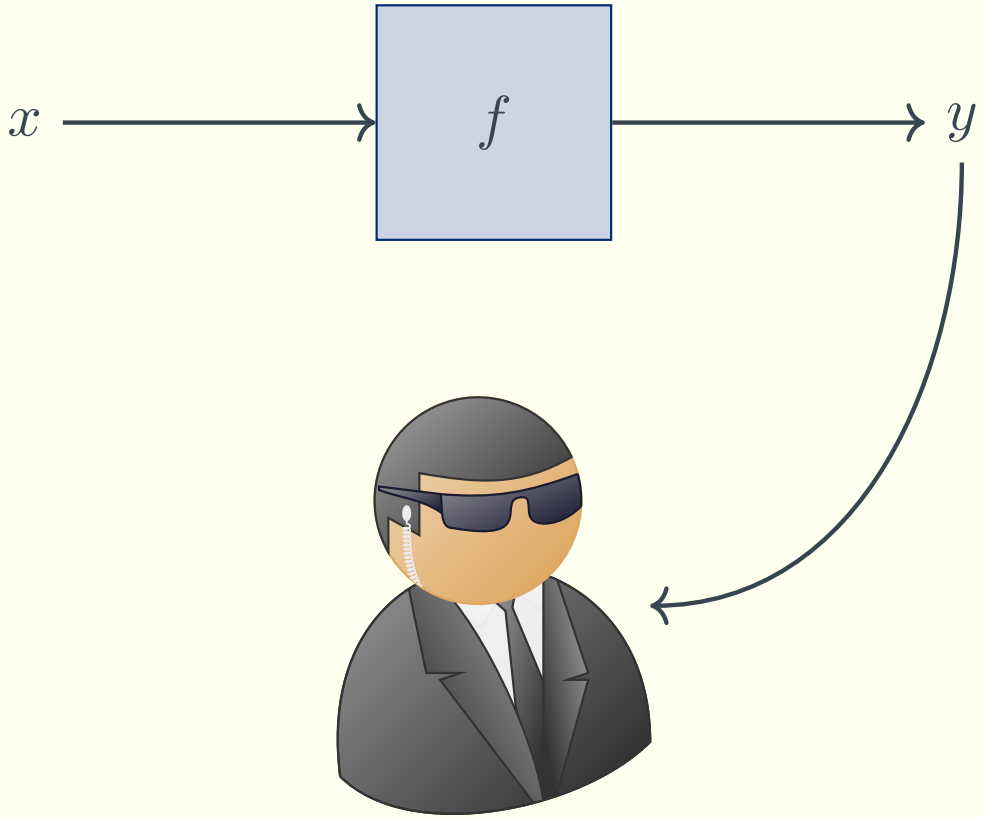
One-Way Functions



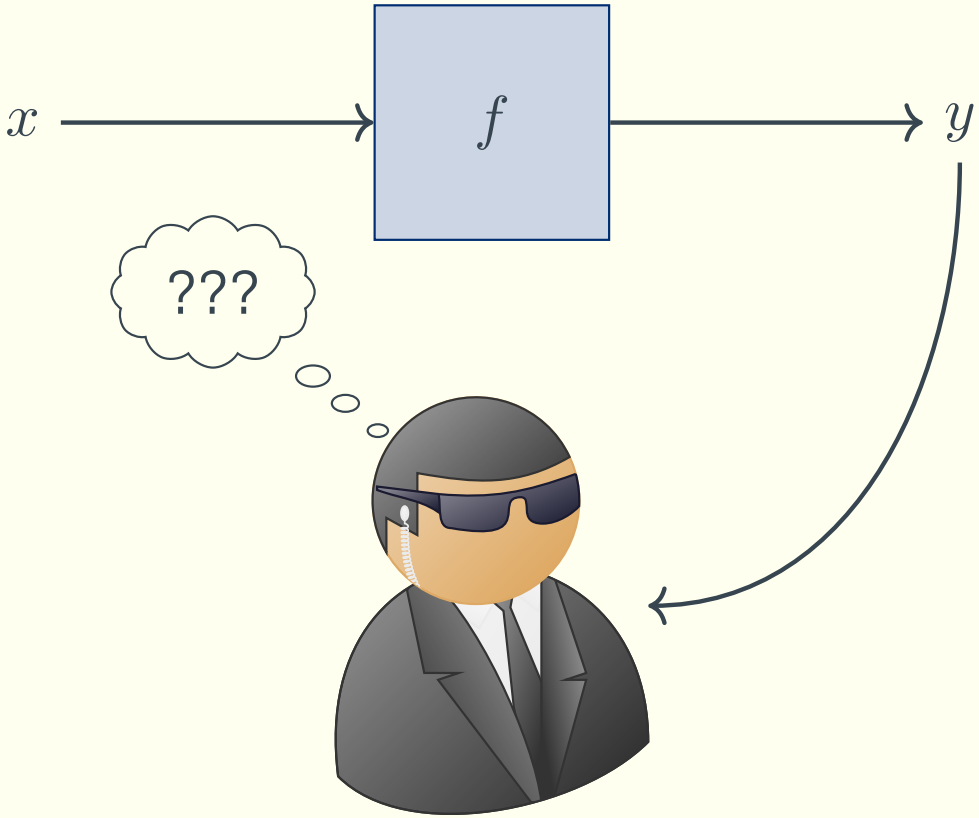
One-Way Functions



One-Way Functions

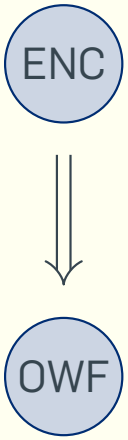


One-Way Functions

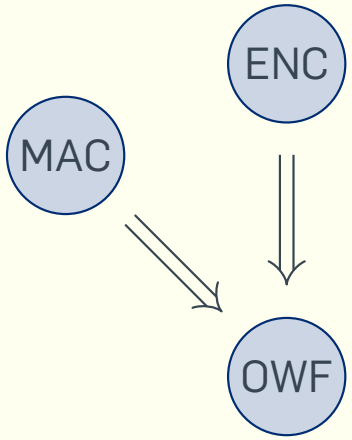


Why We Need to Make Assumptions

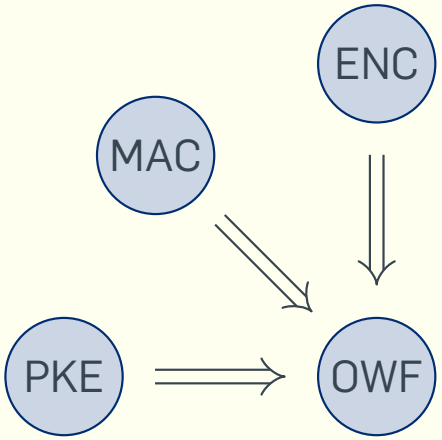
Why We Need to Make Assumptions



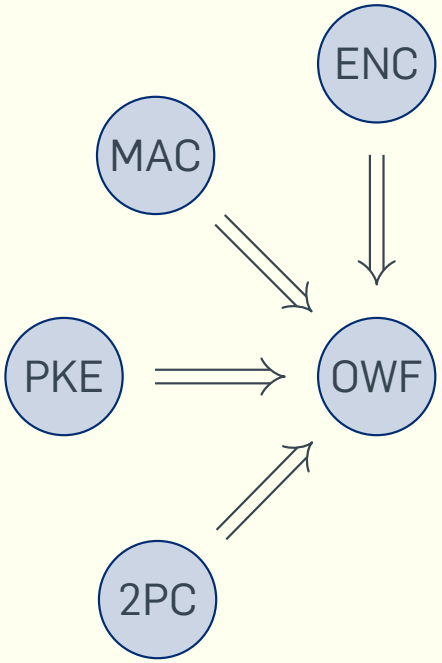
Why We Need to Make Assumptions



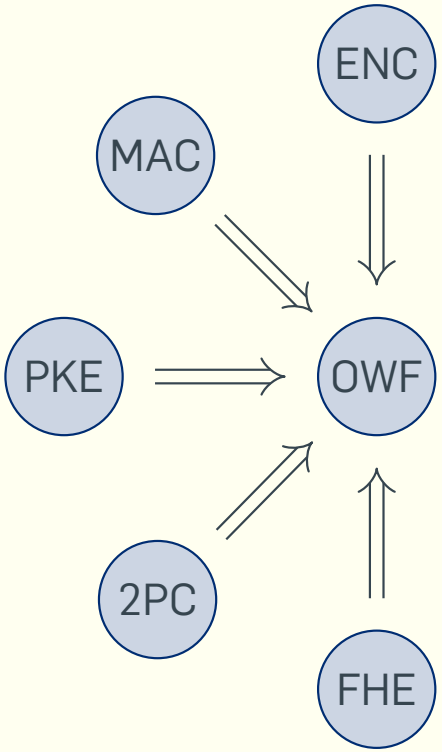
Why We Need to Make Assumptions



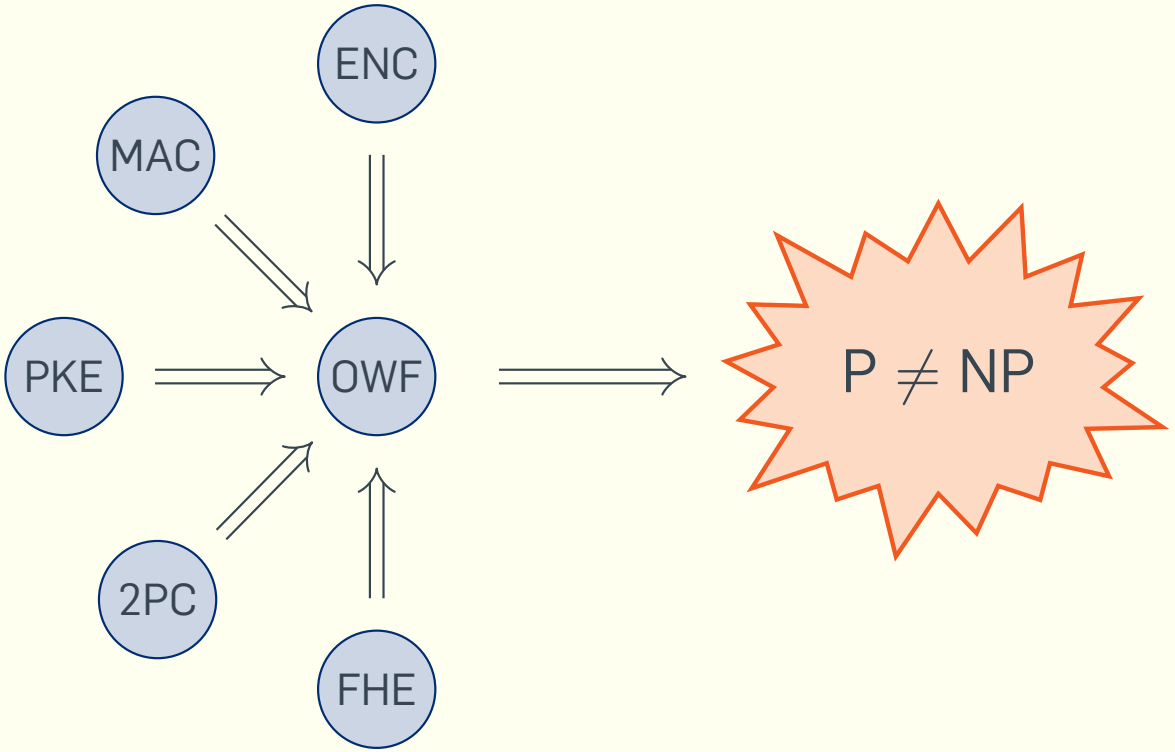
Why We Need to Make Assumptions



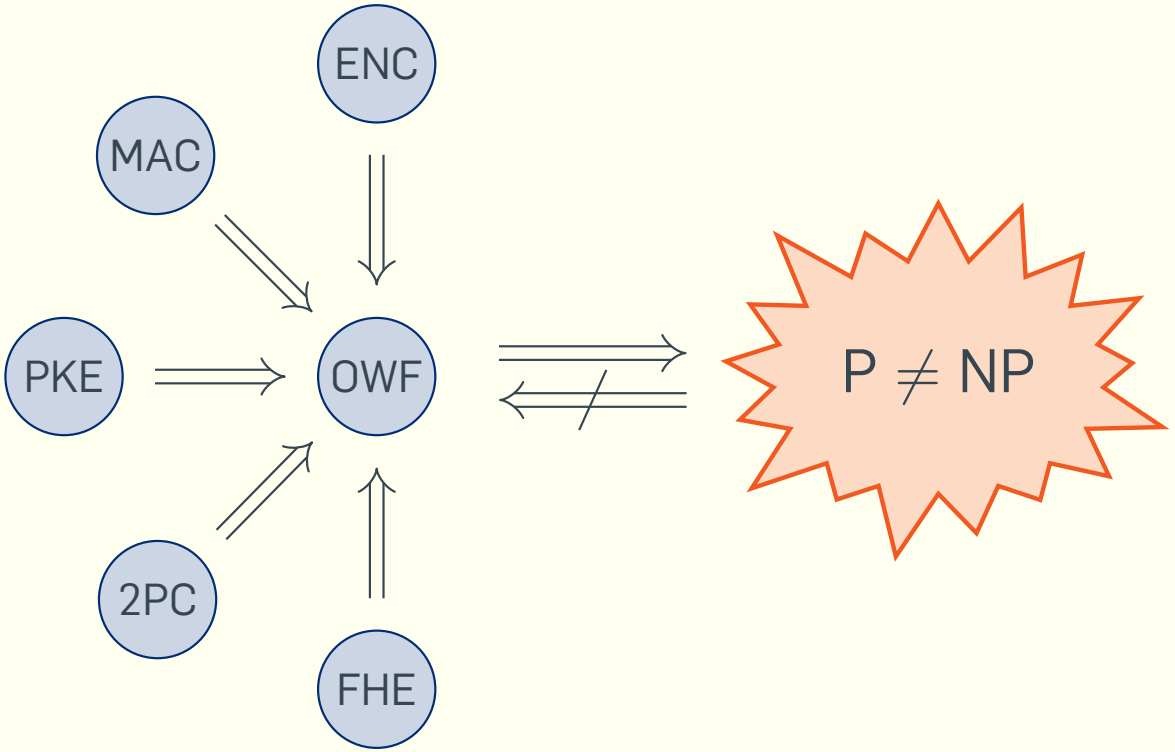
Why We Need to Make Assumptions



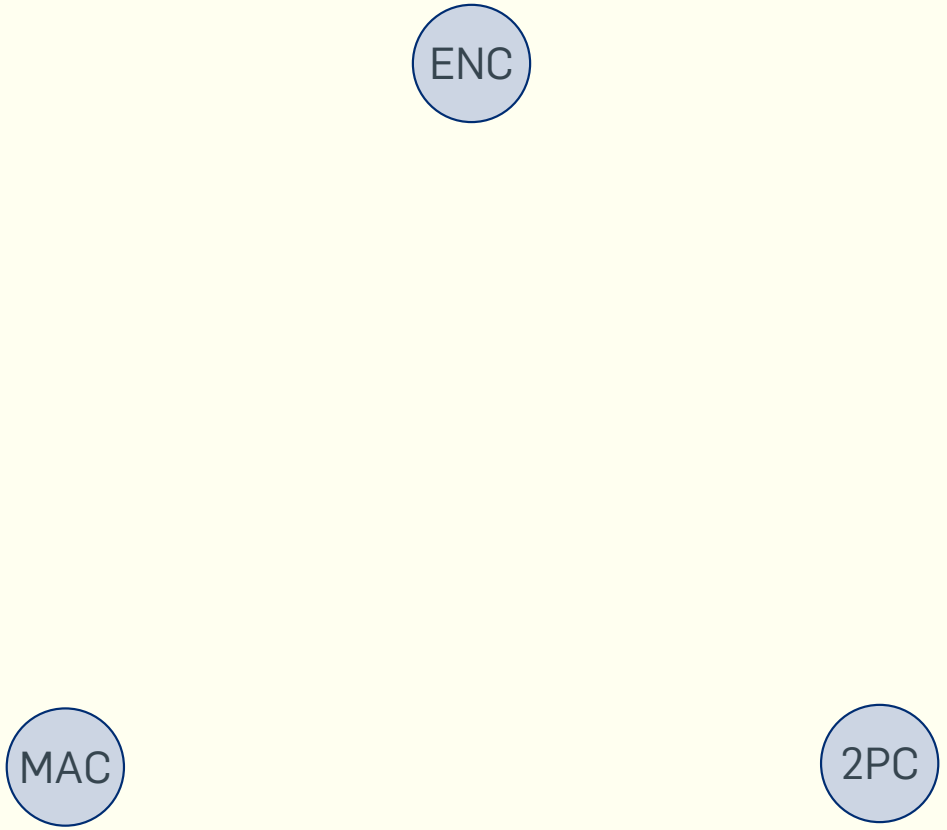
Why We Need to Make Assumptions



Why We Need to Make Assumptions



Idea Behind Provable Security



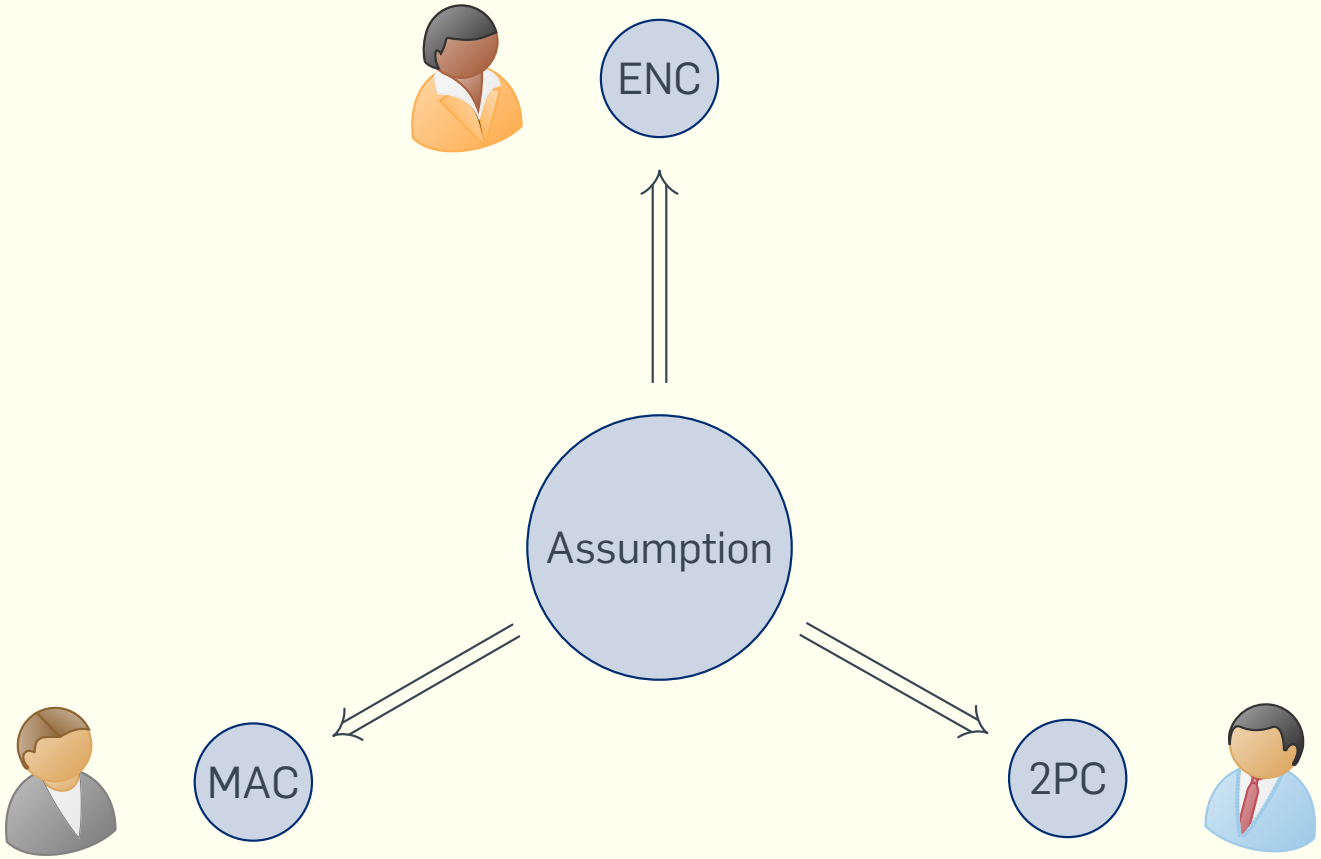
Idea Behind Provable Security

ENC

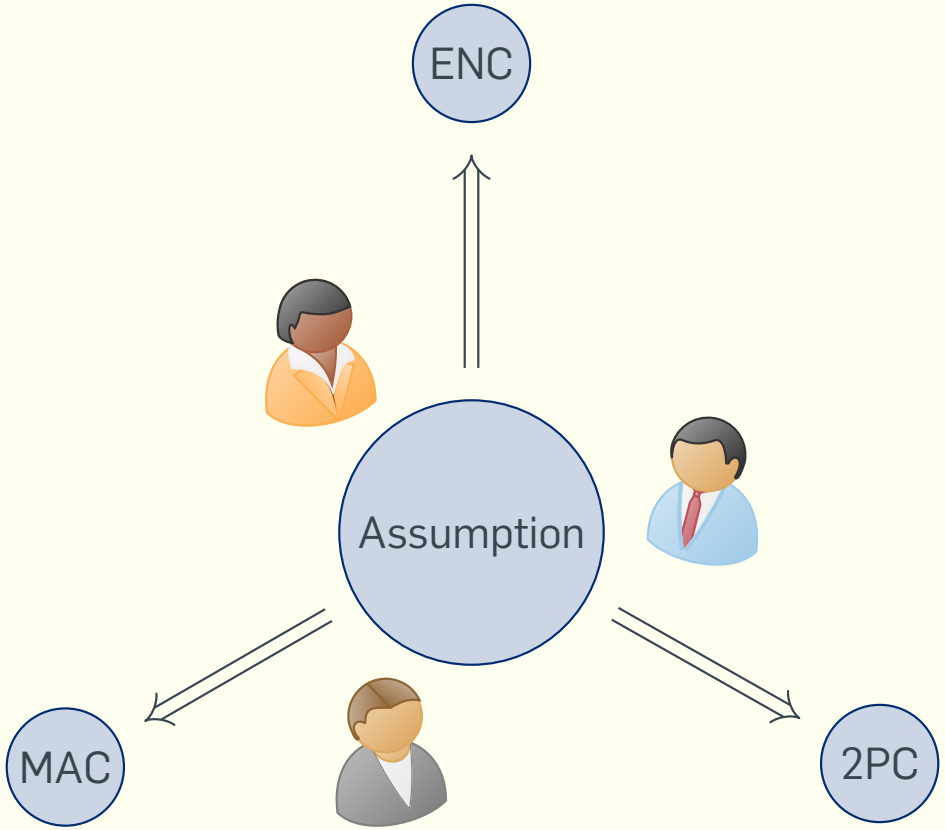
MAC

2PC

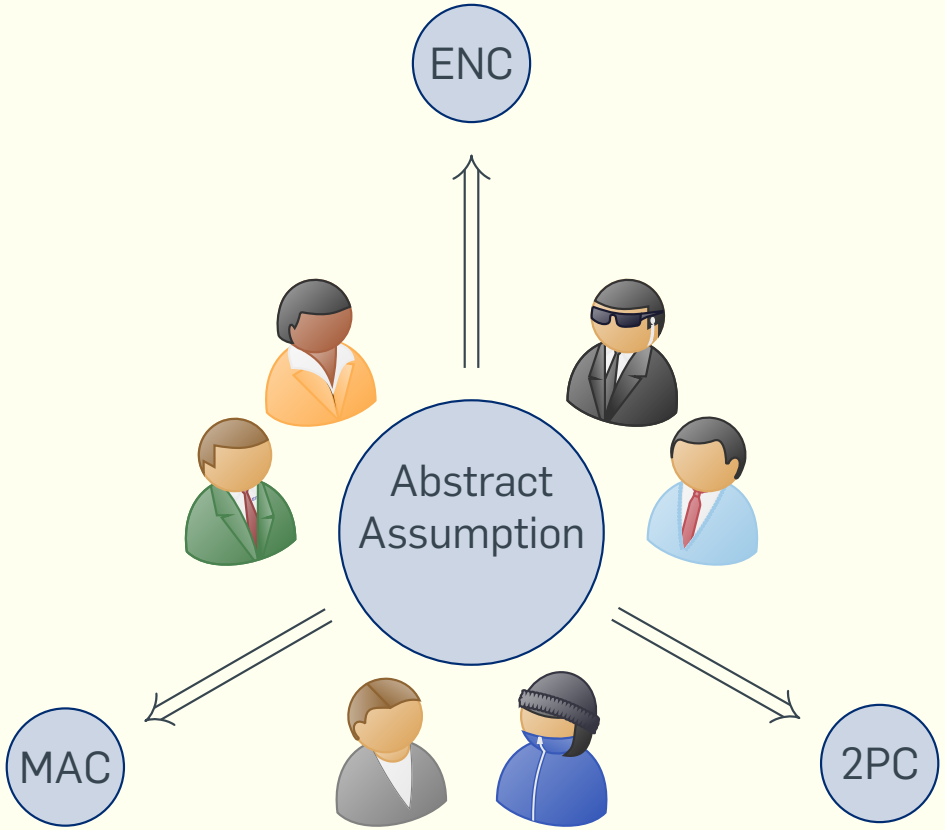
Idea Behind Provable Security



Idea Behind Provable Security



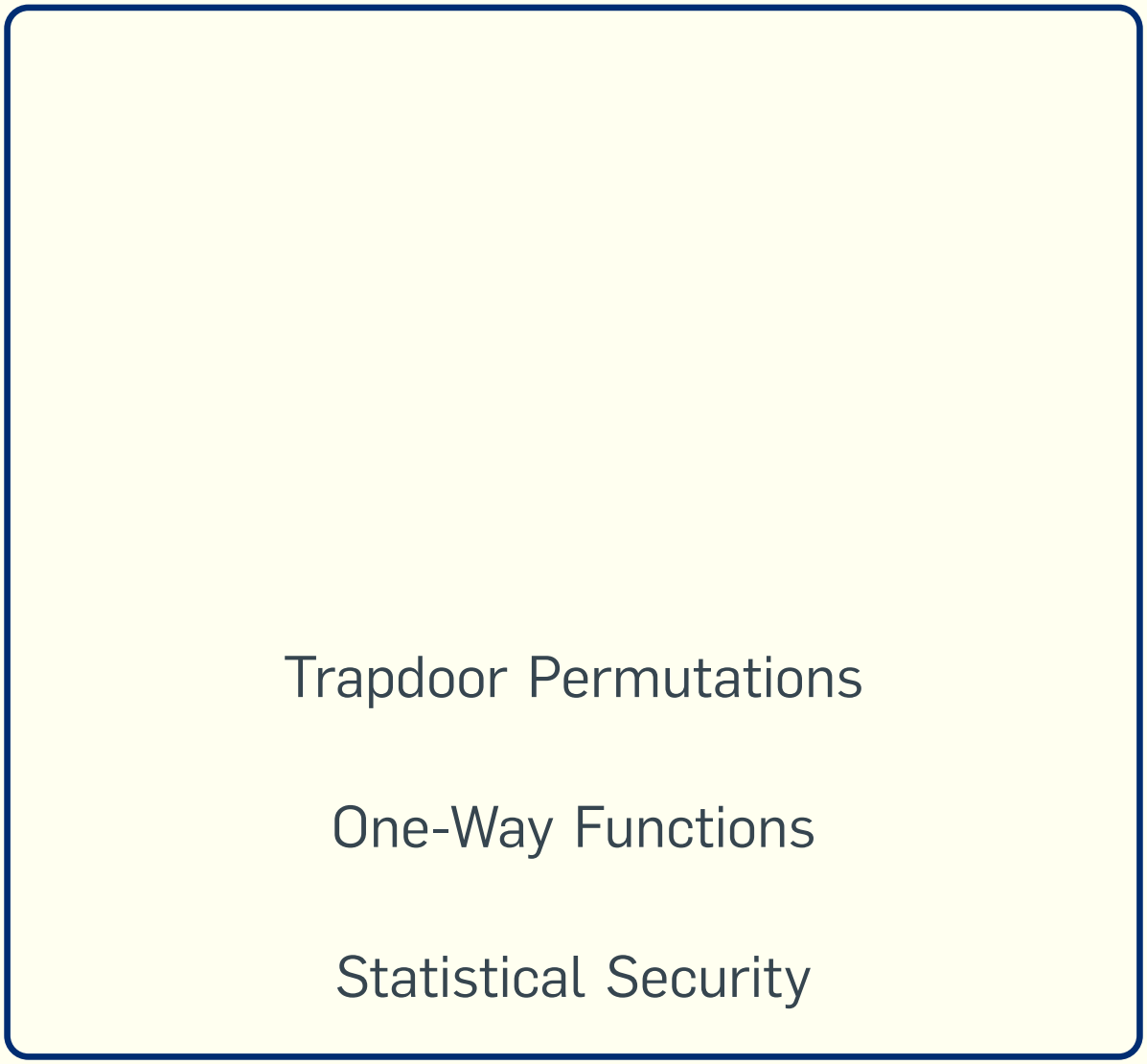
Idea Behind Provable Security



Determining Minimal Assumptions

Determining Minimal Assumptions

Determining Minimal Assumptions



Determining Minimal Assumptions

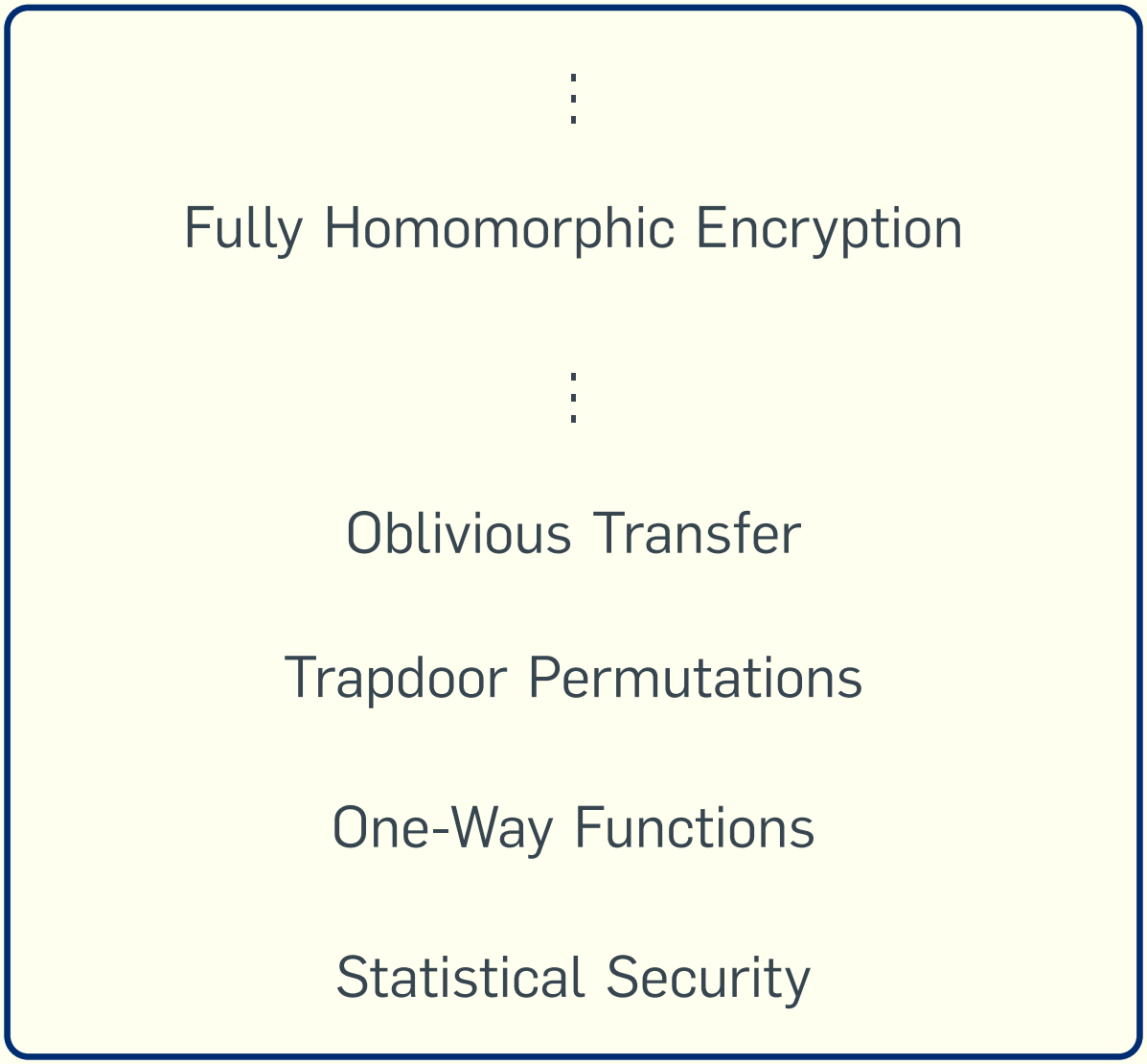
Oblivious Transfer

Trapdoor Permutations

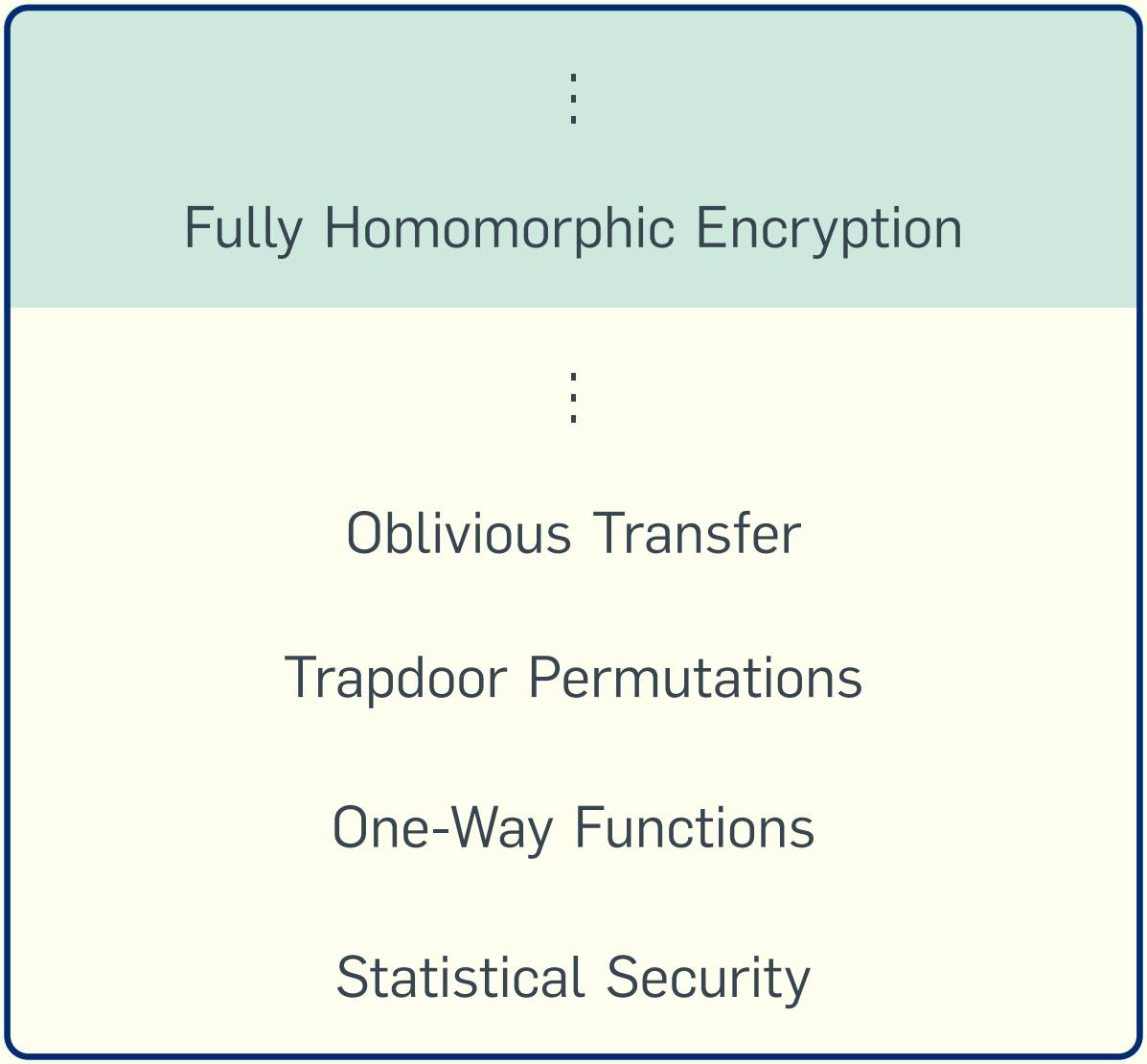
One-Way Functions

Statistical Security

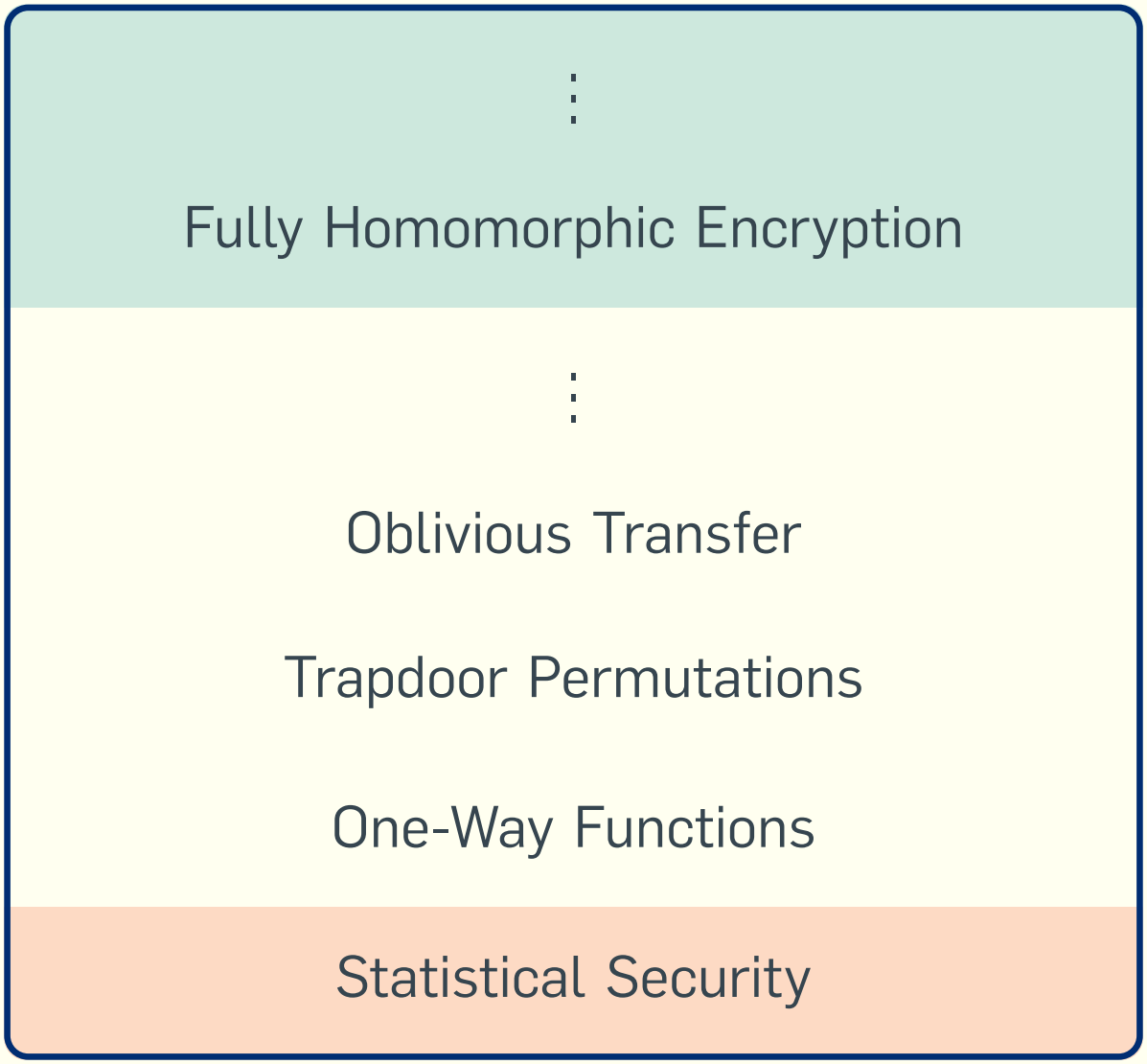
Determining Minimal Assumptions



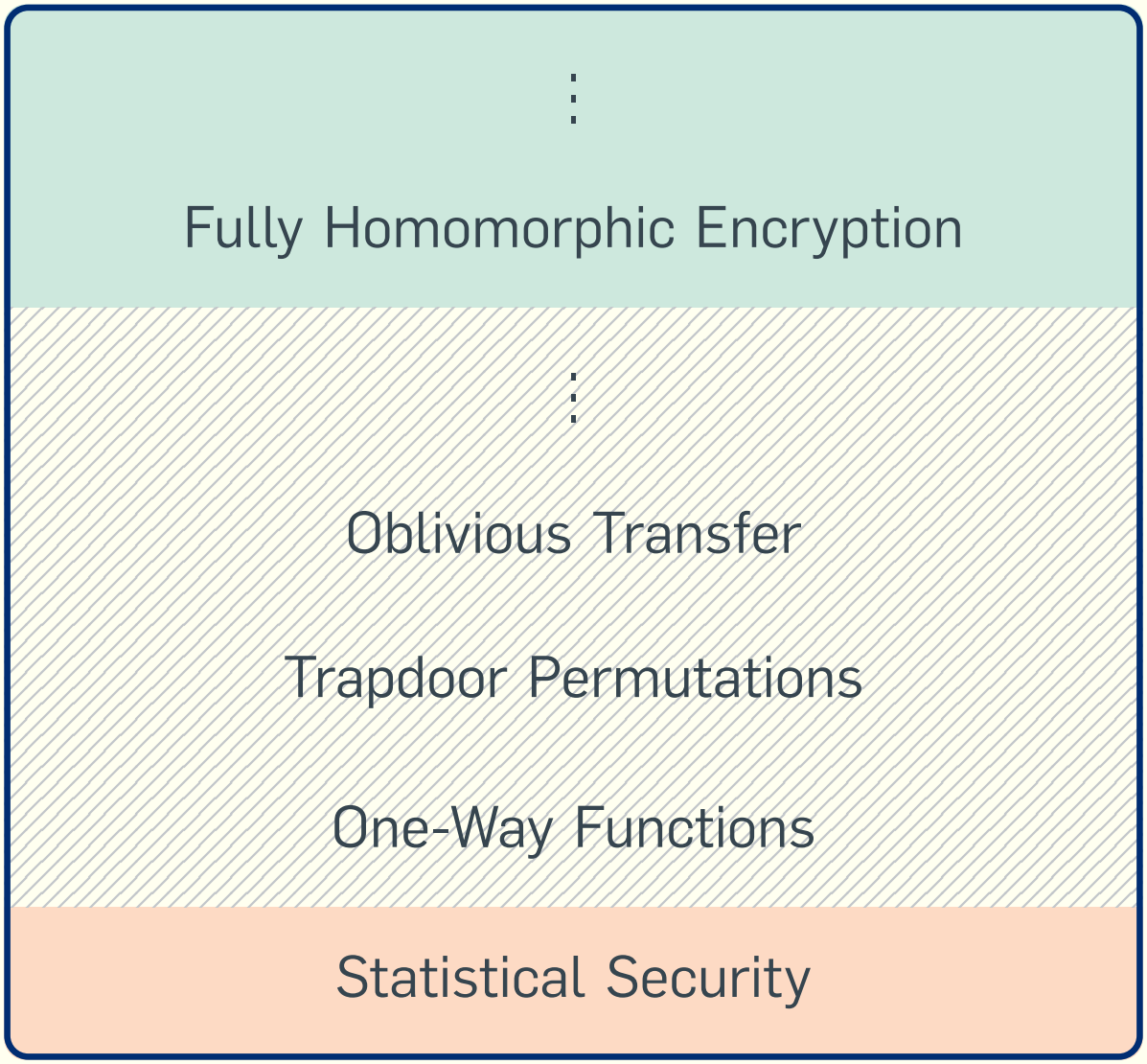
Determining Minimal Assumptions



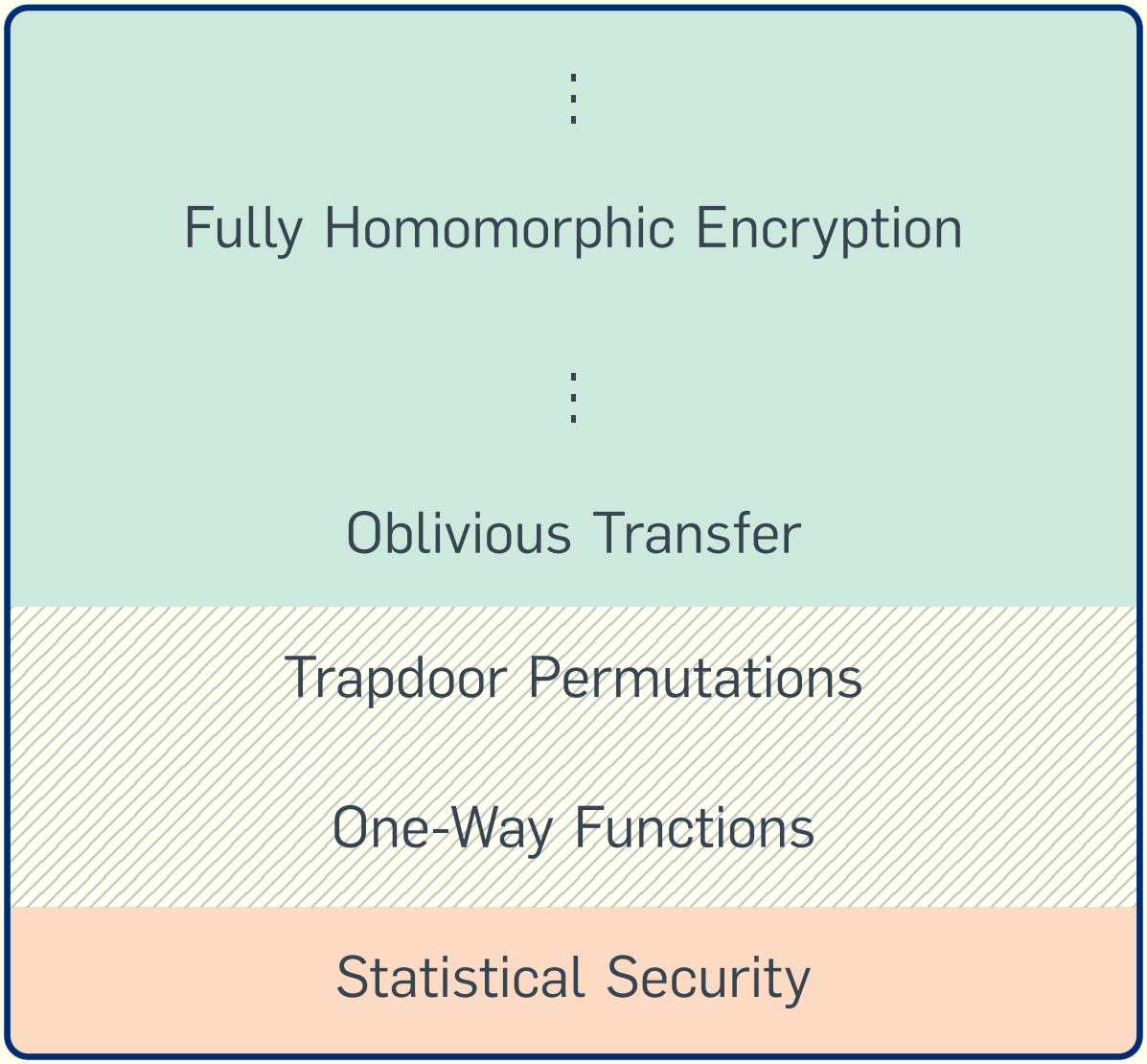
Determining Minimal Assumptions



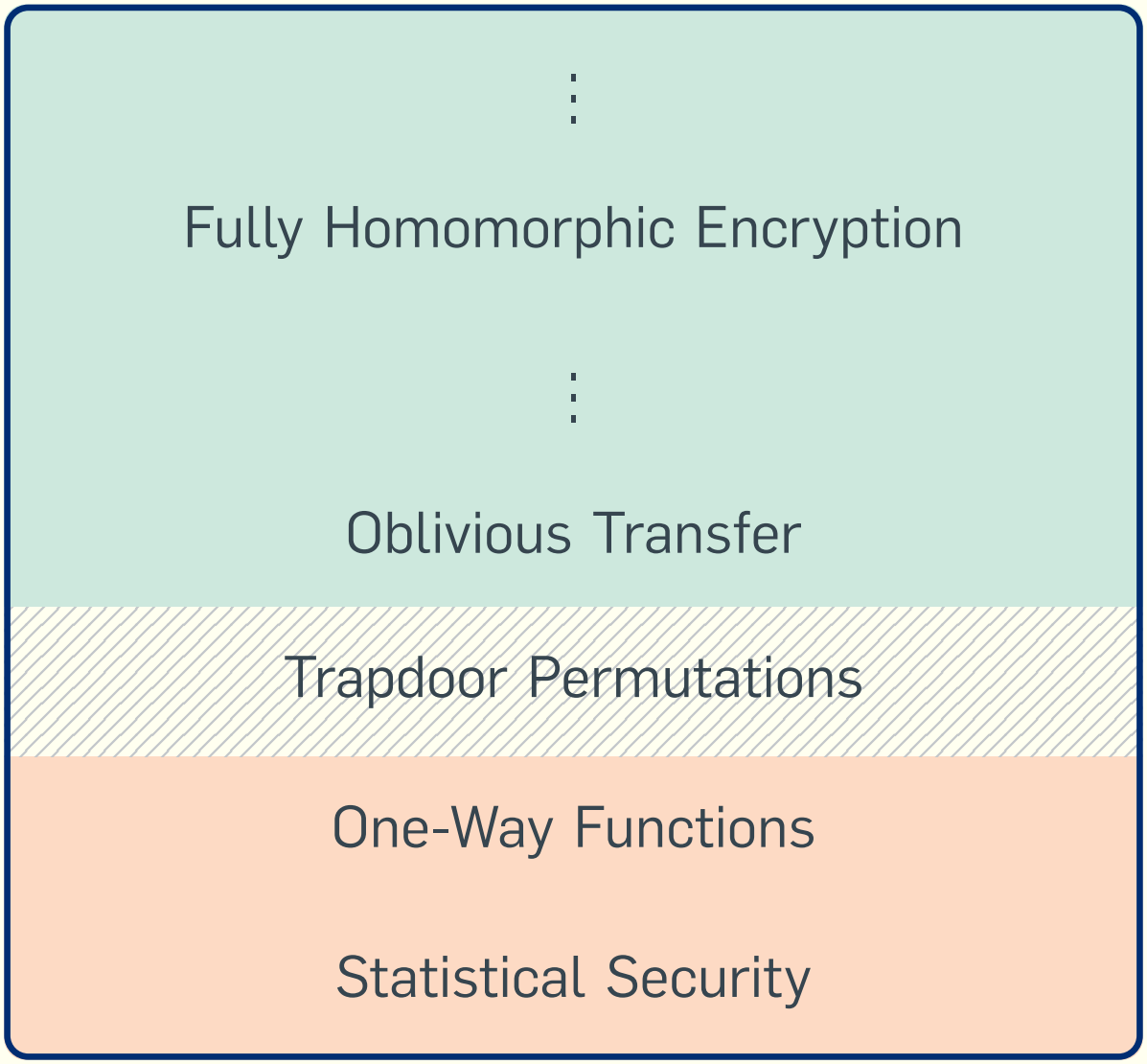
Determining Minimal Assumptions



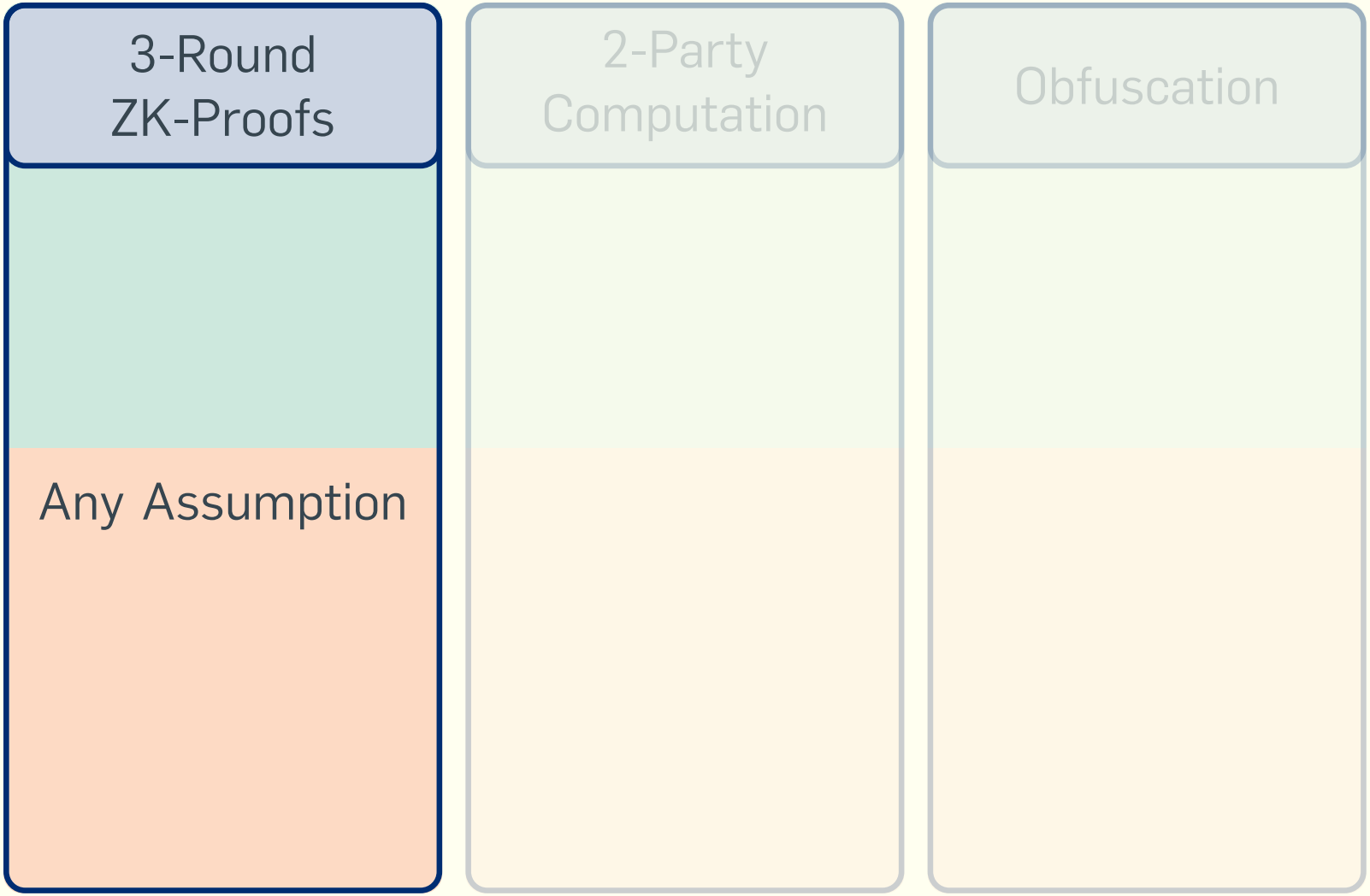
Determining Minimal Assumptions



Determining Minimal Assumptions



3-Round ZK-Proofs	2-Party Computation	Obfuscation


3-Round
ZK-Proofs
2-Party
Computation
Obfuscation
Any Assumption

[FGJ18]

Zero-Knowledge Proof Protocols

- A Zero-Knowledge Proof allows me to to prove that a statement is true without revealing the reason why.

Zero-Knowledge Proof Protocols

- A Zero-Knowledge Proof allows me to to prove that a statement is true without revealing the reason why.
- A ZK-Proof must be
  - Sound

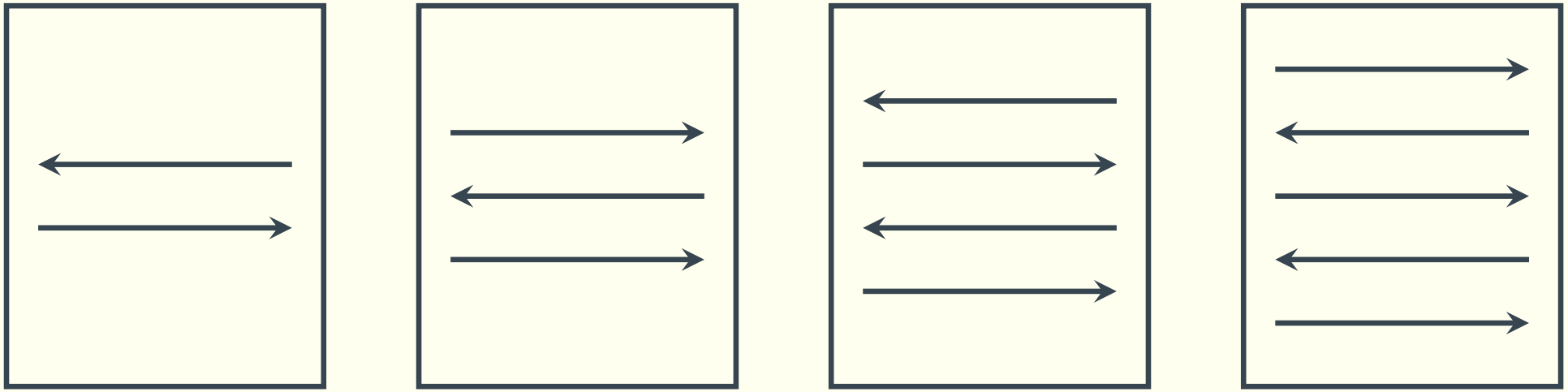
Zero-Knowledge Proof Protocols

- A Zero-Knowledge Proof allows me to to prove that a statement is true without revealing the reason why.
- A ZK-Proof must be
  - Sound
  - Zero-Knowledge

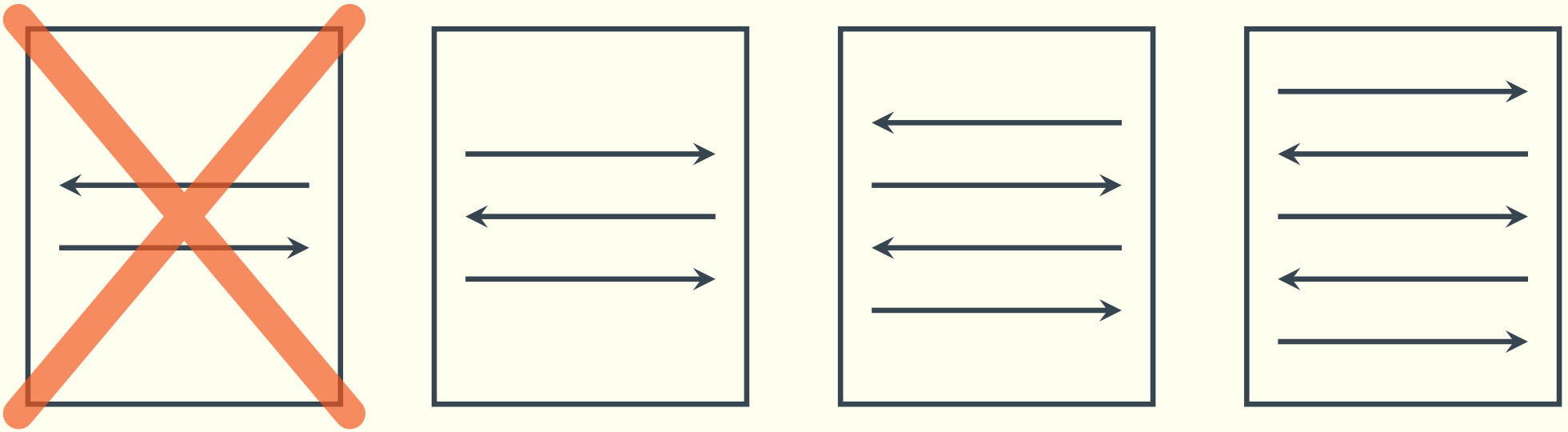
Zero-Knowledge Proof Protocols

- A Zero-Knowledge Proof allows me to to prove that a statement is true without revealing the reason why.
- A ZK-Proof must be
  - Sound
  - Zero-Knowledge
- Incredibly useful tools in Cryptography

Round-Complexity of ZK-Proofs for NP

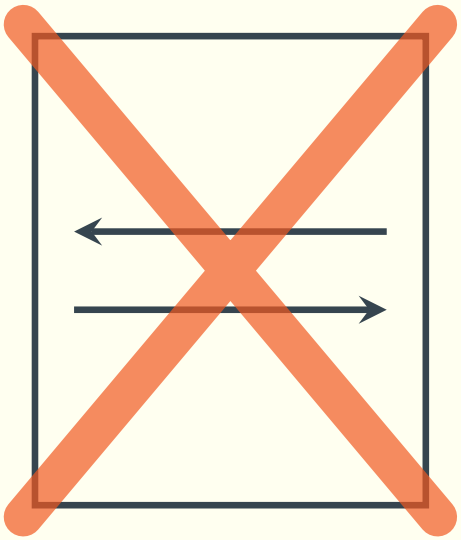


Round-Complexity of ZK-Proofs for NP

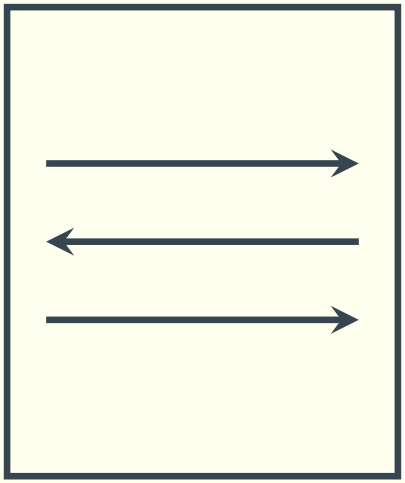


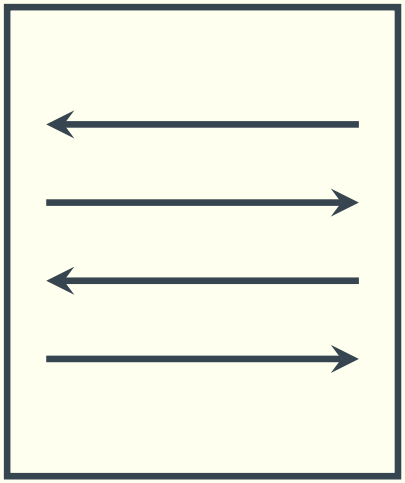
[GO94]

Round-Complexity of ZK-Proofs for NP



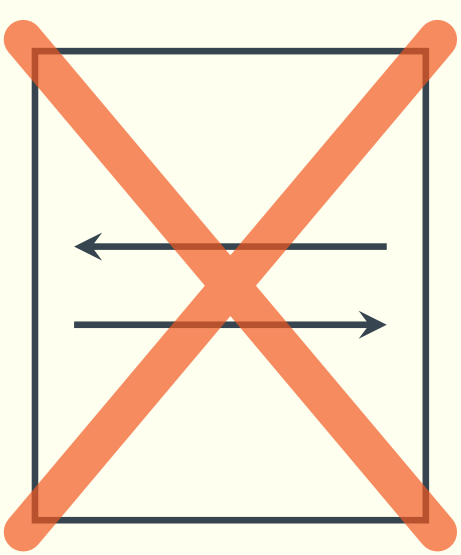
[GO94]



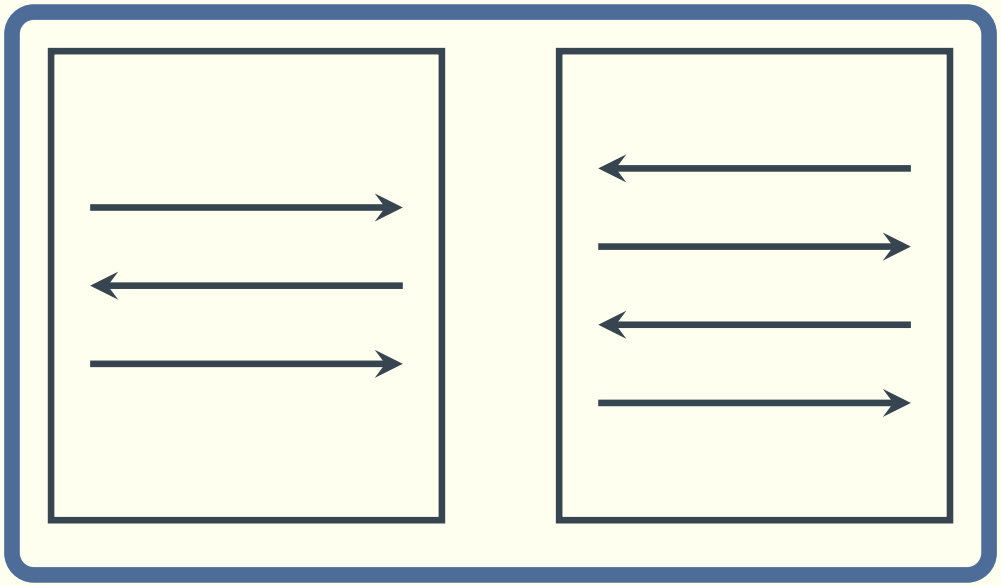


[GK96]

Round-Complexity of ZK-Proofs for NP

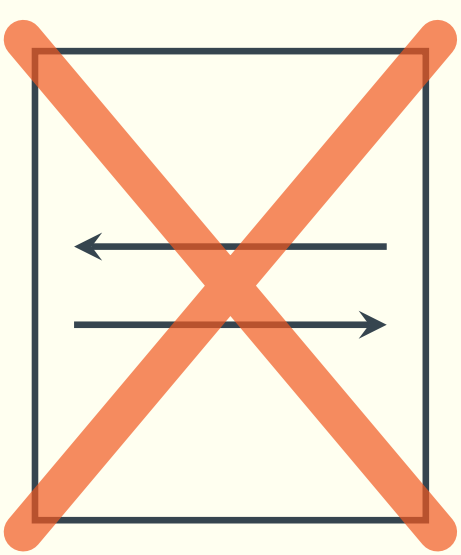


[GO94]

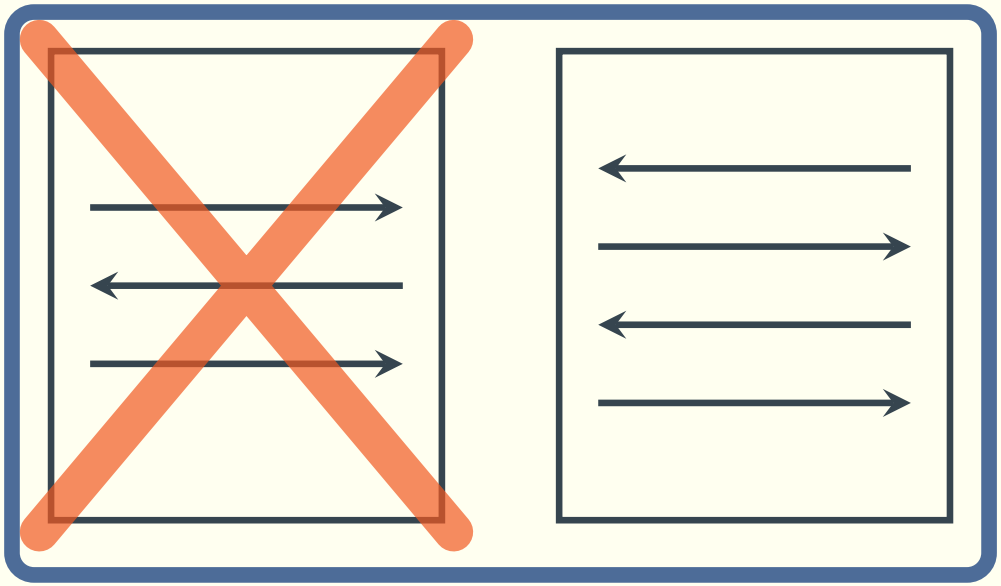


[GK96]

Round-Complexity of ZK-Proofs for NP

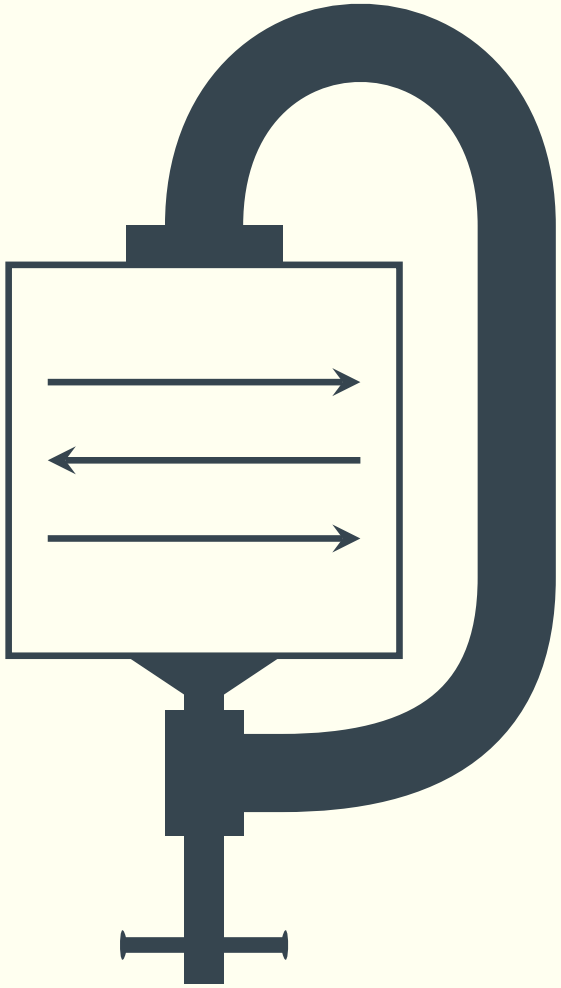


[GO94]

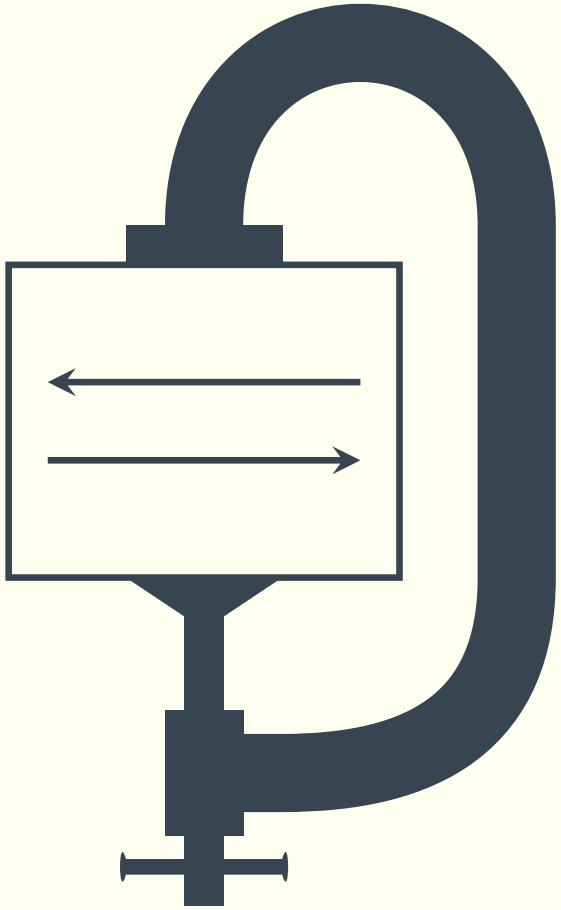


[GK96]

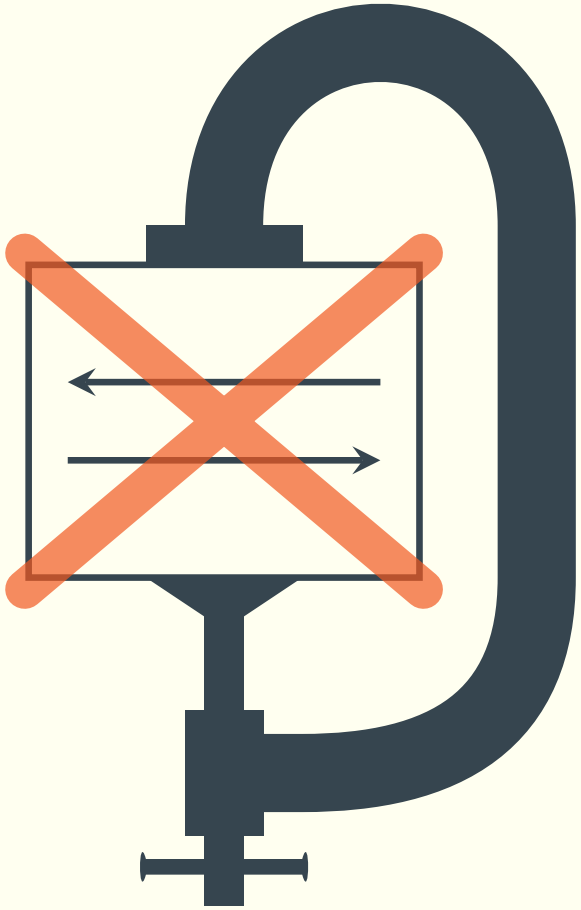
Compressing Proofs

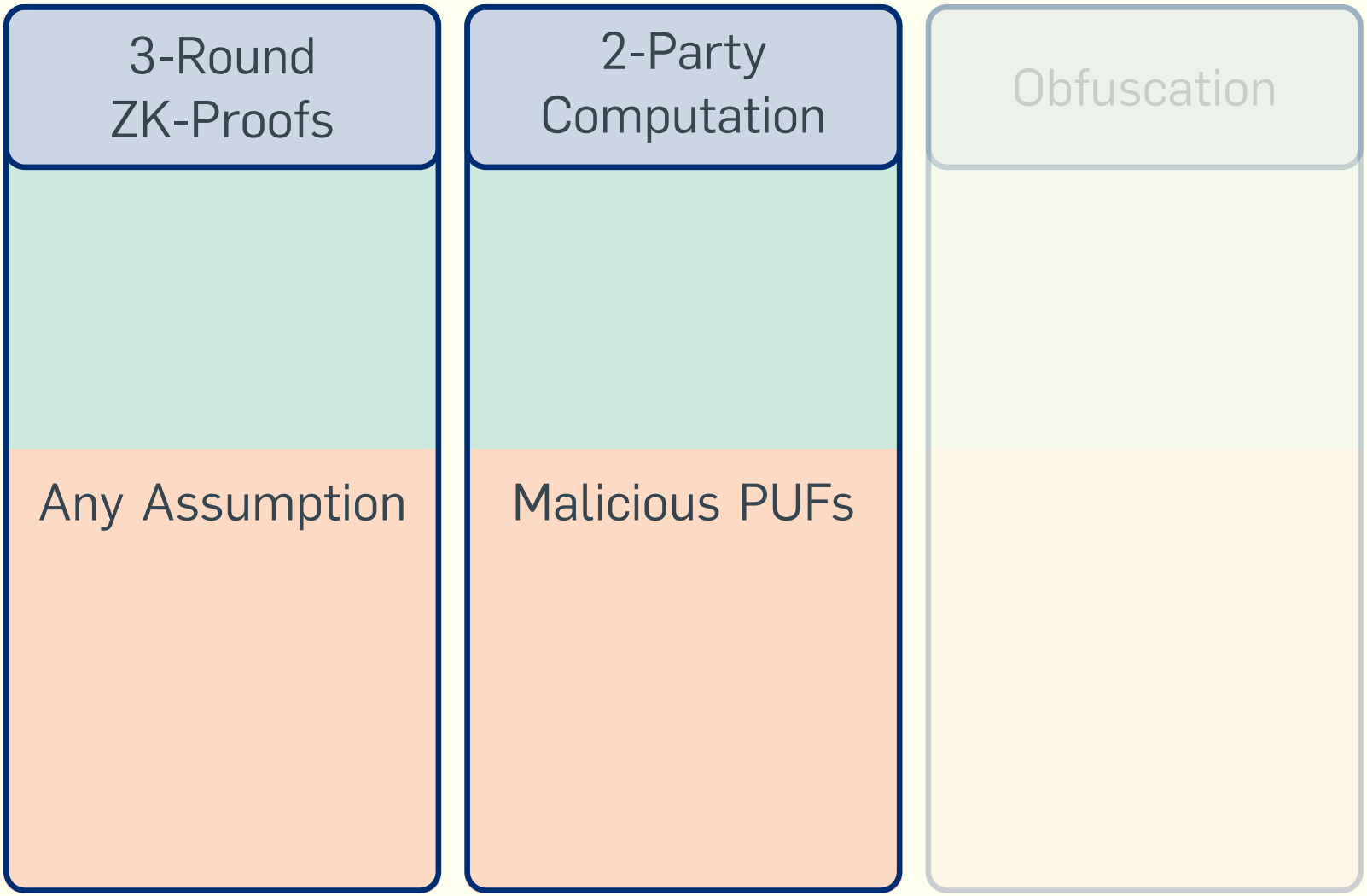


Compressing Proofs



Compressing Proofs




3-Round
ZK-Proofs
2-Party
Computation
Obfuscation
Any Assumption
Malicious PUFs
[FGJ18]
[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

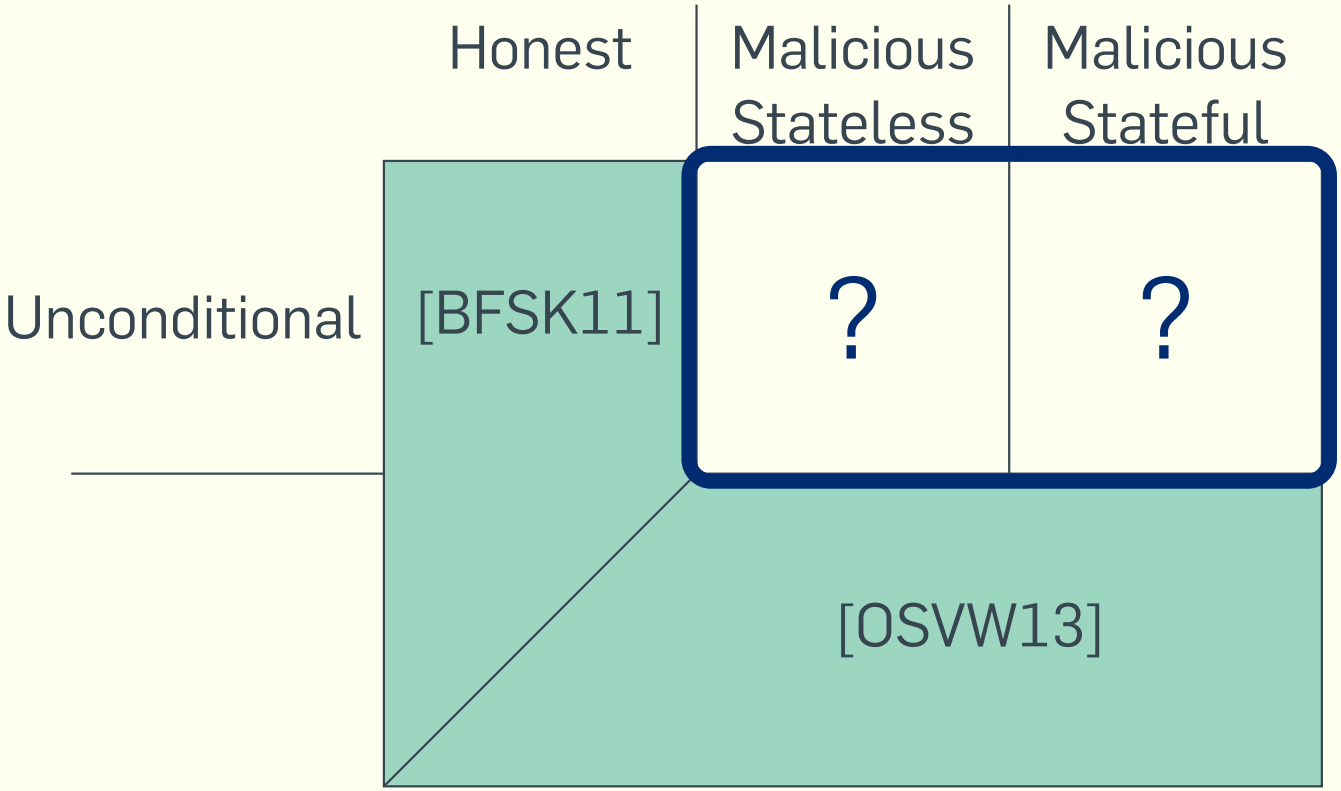
Secure Two-Party Computation from PUFs

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

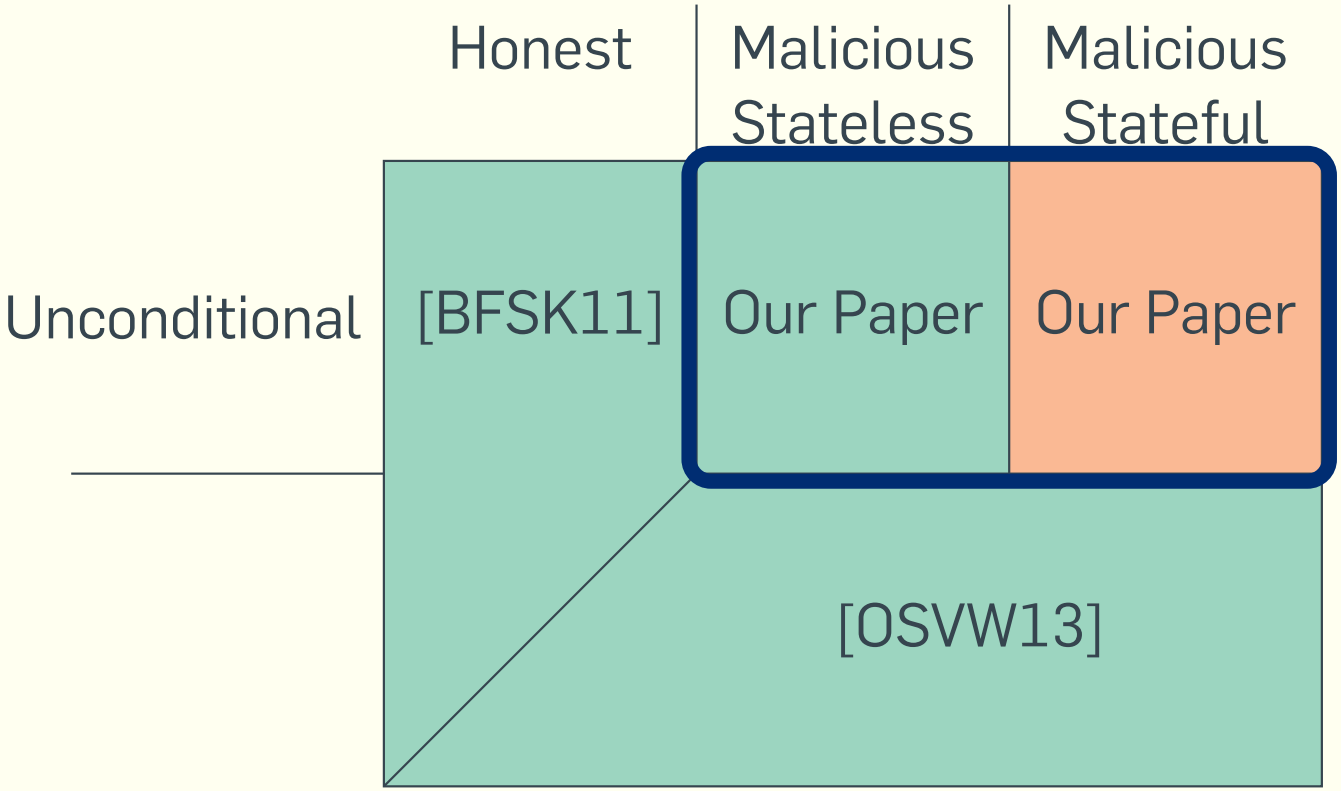
Secure Two-Party Computation from PUFs

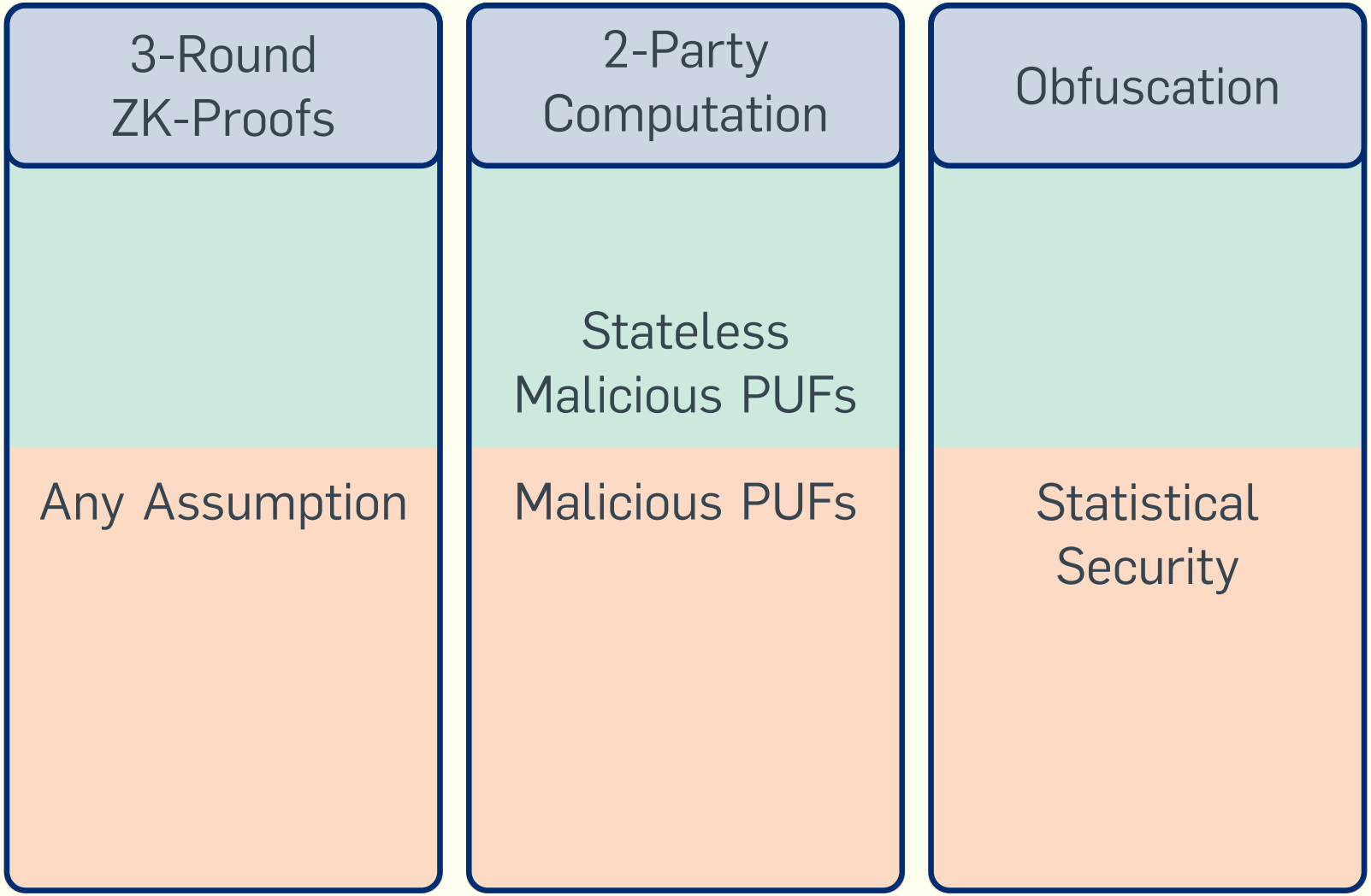
- The idea: Use secure hardware to overcome impossibility of information theoretically secure 2-PC.
- Use Physically Uncloneable Functions
  - Behave like random functions.
  - Cannot be copied.

Secure Computation from PUFs

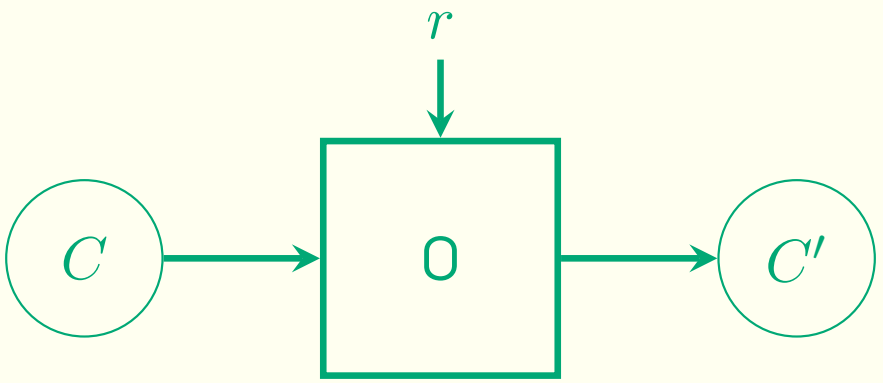


Secure Computation from PUFs

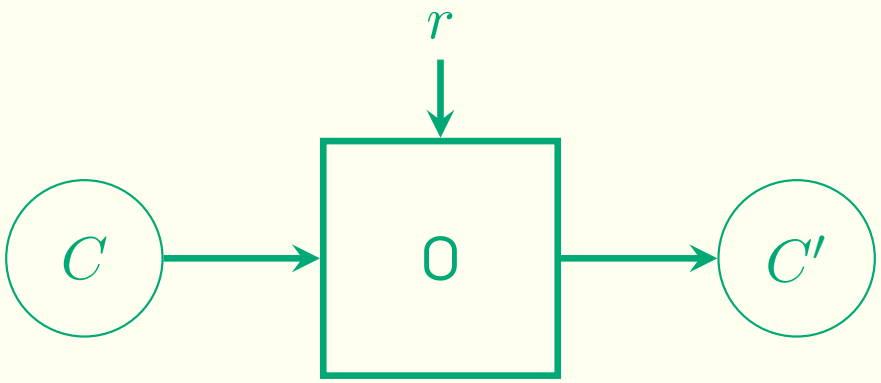



3-Round ZK-Proofs
2-Party Computation
Obfuscation
Stateless Malicious PUFs
Any Assumption
Malicious PUFs
Statistical Security
[FGJ18]
[DFKLS14]
[BBF16]

Statistically Secure Obfuscation



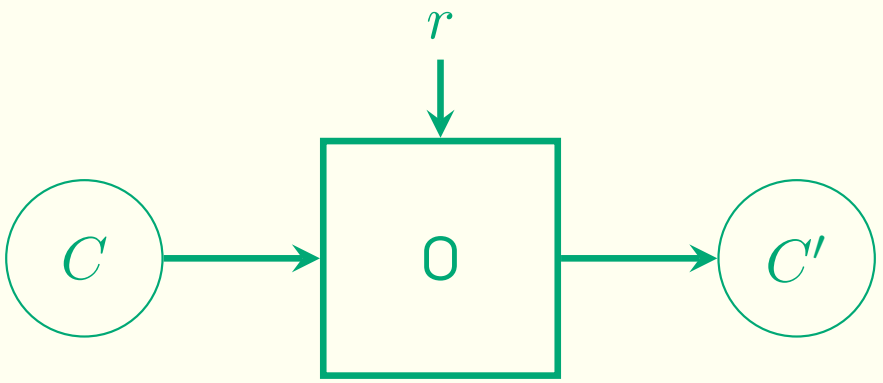
Statistically Secure Obfuscation



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

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

Statistically Secure Obfuscation



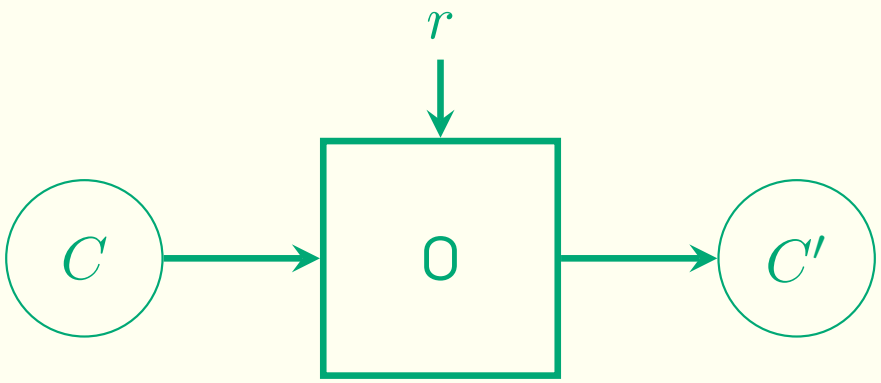
- ~~**Perfect Correctness:** For any circuit C~~

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

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

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

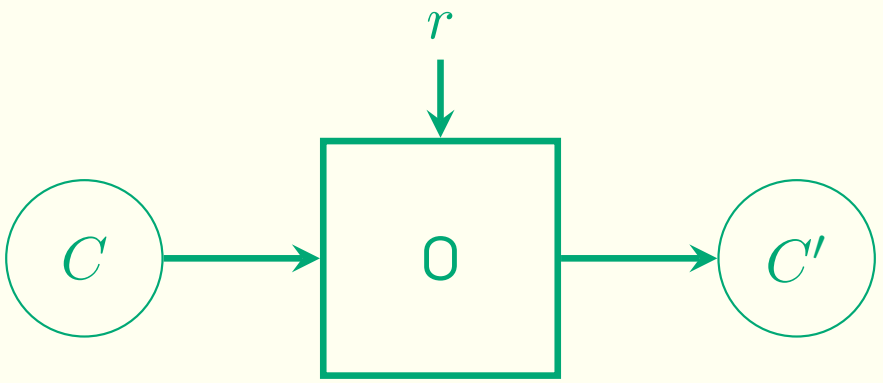
Statistically Secure Obfuscation



- **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 $|C_1| = |C_2|$

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

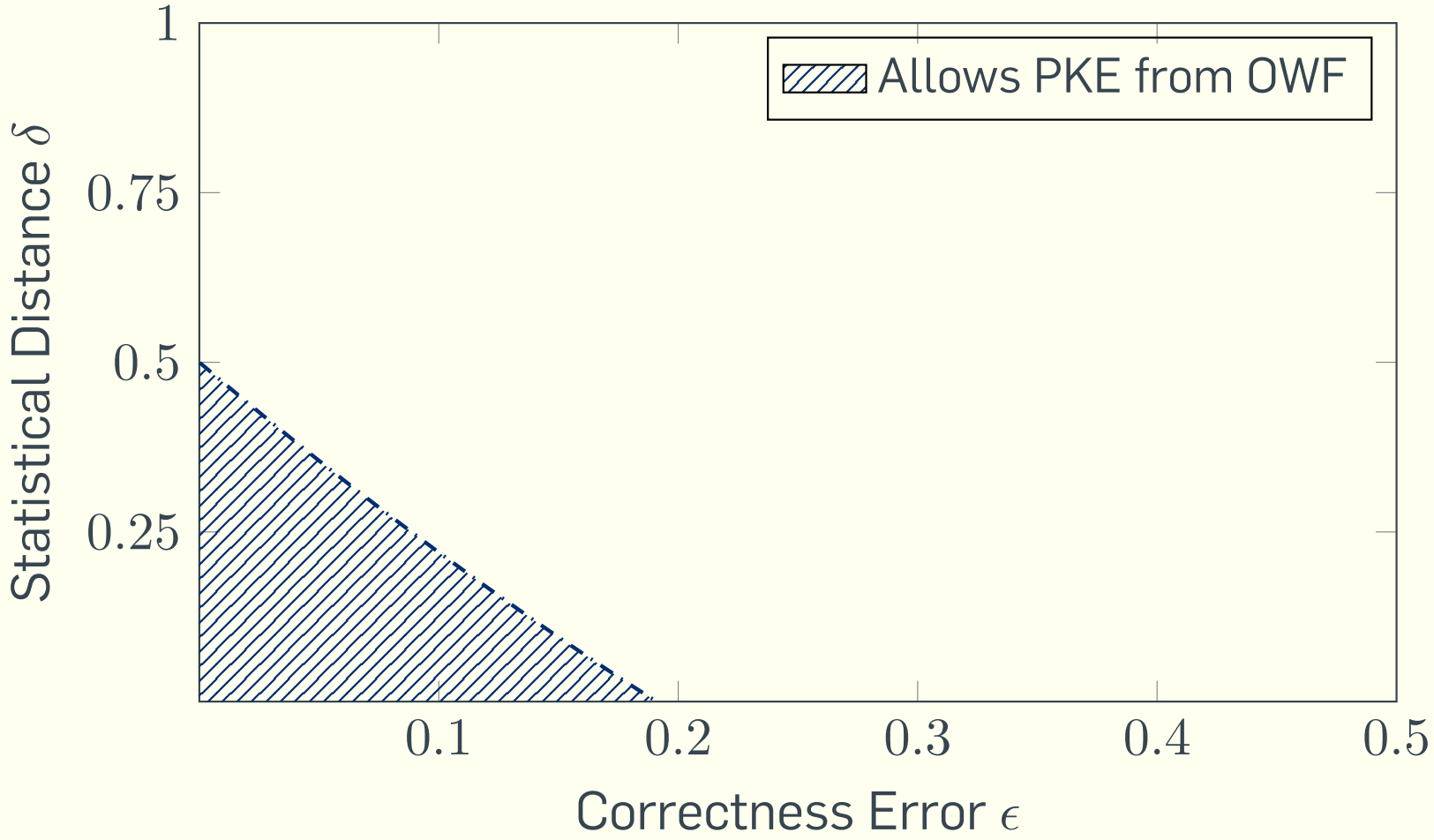
- $(1-\delta)$**-Correlation Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

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

Why Do We Even Care About Approximate Correctness?

Because approximate obfuscation is useful!

[MMNPs16,SW14,Hol06]



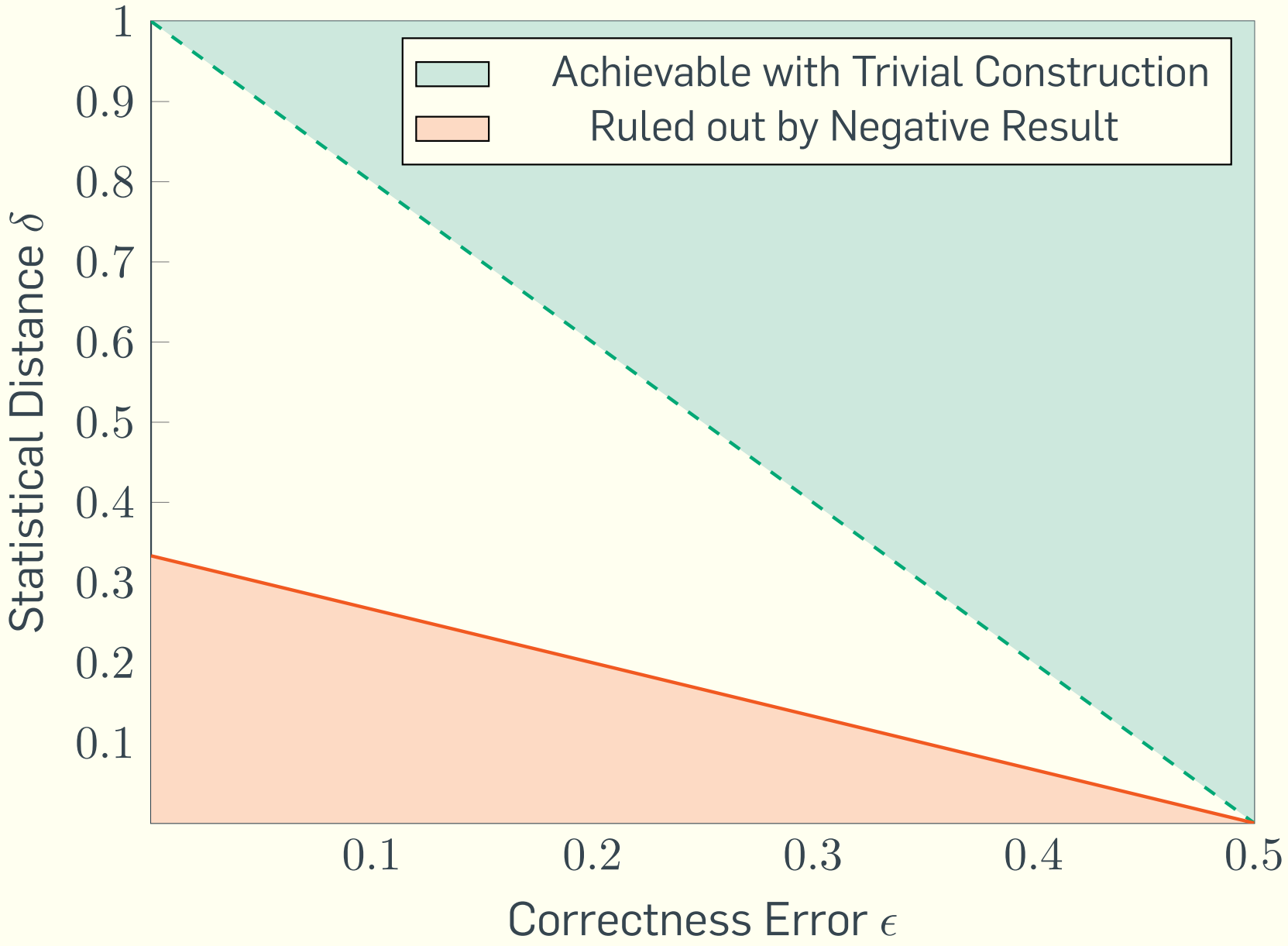
Main Result

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