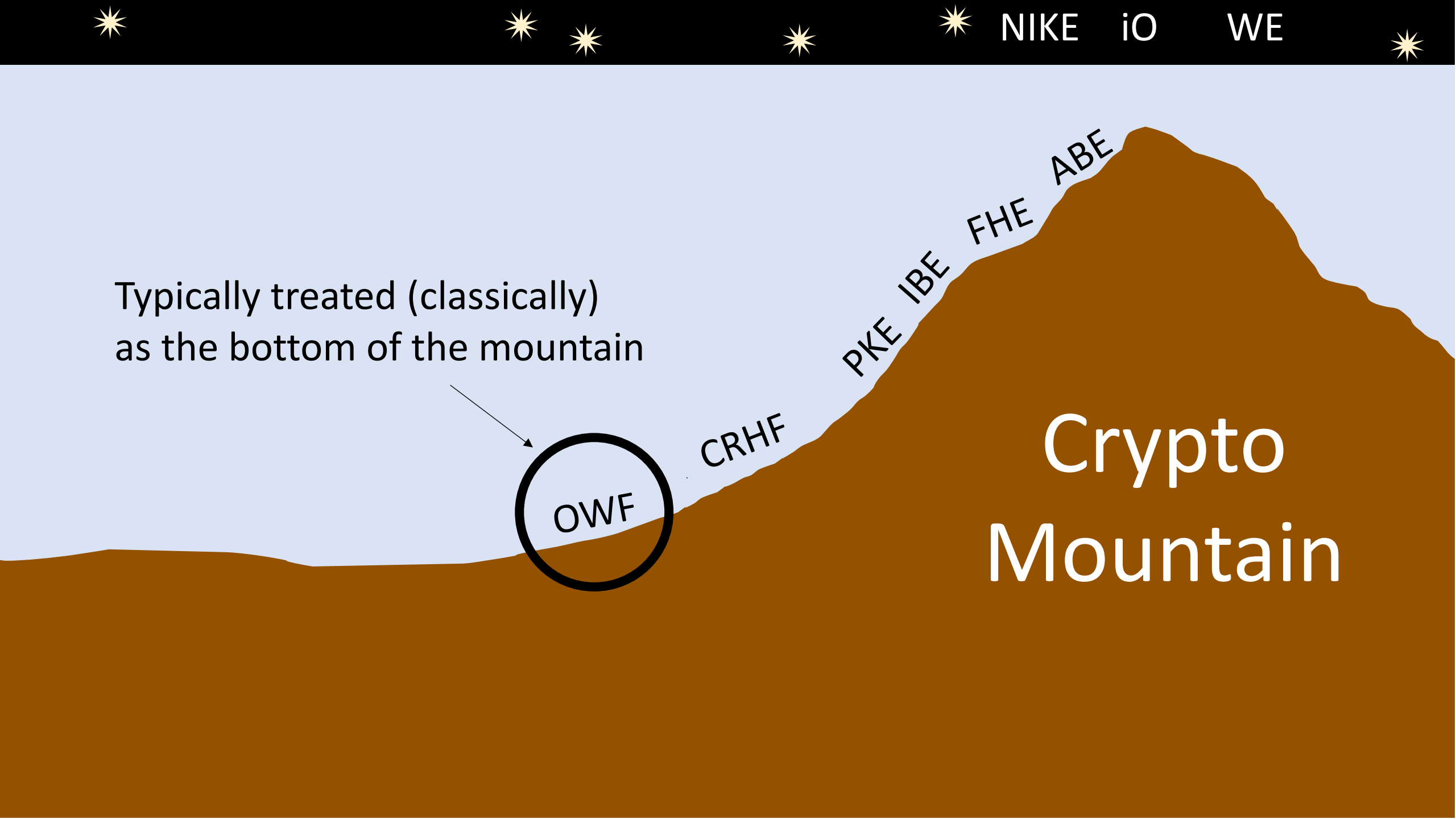
Quantum Minimalism

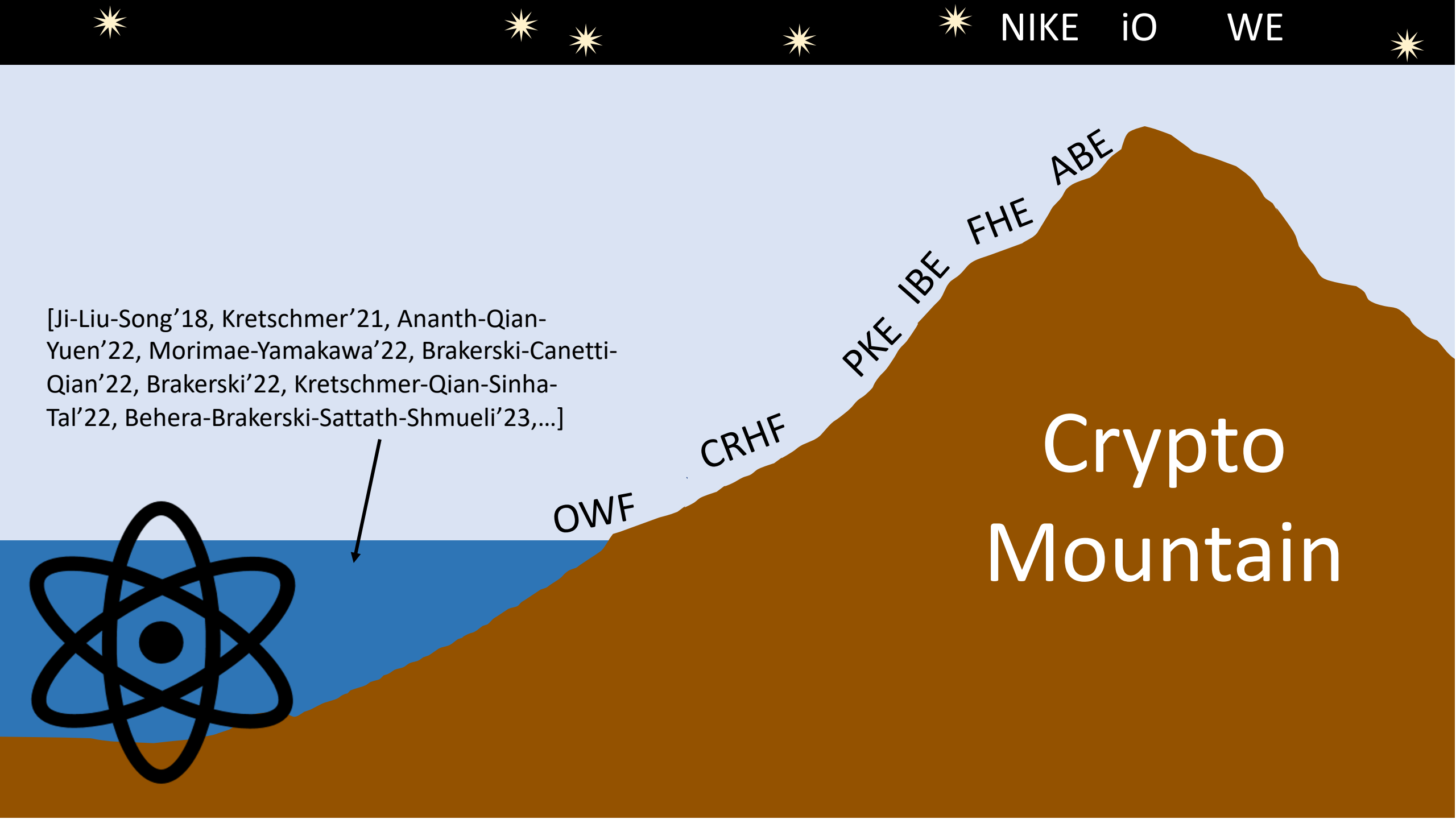
Mark Zhandry
NTT Research

Typical (classical) crypto refrain:

One-way functions = Minimal crypto assumption


NIKE iO WE
Typically treated (classically)
as the bottom of the mountain
OWF
CRHF
PKE
IBE
FHE
ABE
Crypto
Mountain

NIKE iO WE


[Ji-Liu-Song'18, Kretschmer'21, Ananth-Qian-Yuen'22, Morimae-Yamakawa'22, Brakerski-Canetti-Qian'22, Brakerski'22, Kretschmer-Qian-Sinha-Tal'22, Behera-Brakerski-Sattath-Shmueli'23,…]
OWF
CRHF
PKE
IBE
FHE
ABE
Crypto Mountain

Central Q: What should be the new "minimal" quantum crypto assumption

This Talk: Review what makes OWFs minimal,
in order to set the goalposts for this new search

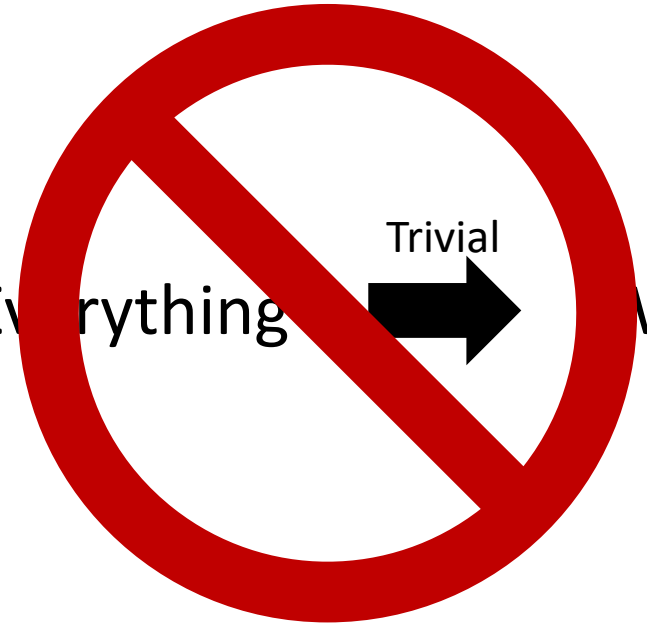
Feature 0: Implied by essentially everything

But “Everything” → OWFs → PRGs, PRFs, PRPs, Signatures, AuthEnc etc

So, e.g., signatures are just as “minimal” as OWFs

Feature 1: *Trivially* implied by most general primitives

Feature 1: *Trivially* implied by most general primitives



Trivial

"Everything" OWF

BUT

Highly non-trivial

OWF → Signatures

Trivial

"Everything" →

[Impagliazzo-Luby'89]

"distributional" OWF → OWF

But maybe close enough?

Feature 2: Trivially and Robustly Implied by Most Concrete Assumptions

Dlog, Factoring, LWE, Isogenies, etc 

OWF

In contrast, Dlog → signatures (in standard model) is very complex

Robustness

Dlog implies $x \rightarrow g^x \ mod \ p$ is one-way, whether:

- x is uniform in Z_{p-1}
- x is uniform in $[0,2^n-1]$, where $p/2 < 2^n \leq p$
- x is uniform in $2Z_{p-1}$

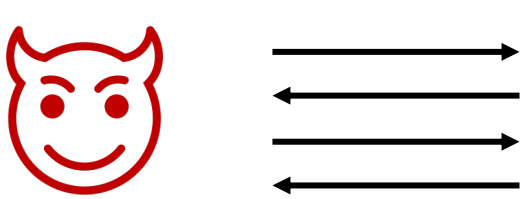
Contrast with DDH

Feature 3: Simple to Define

$$Pr[\ f(\ A(\ f(x)\ )\ ) = f(x)\ ] < negl$$

Feature 4: Falsifiable

[Naor’03,Gentry-Wichs’11]



Challenger

Feature 5: Search Problem

Generally milder assumptions, more robust to how defined

Feature 6: Trivial Combiners and Universal Constructions

$(x_1,x_2) \rightarrow (F_1(x_1),F_1(x_2))$ is one-way, if *either* F_1,F_2 are

[Levin'87] → "Universal" OWF that is secure if *any* OWF exists

→ Immediate combiner/universal construction for anything equivalent to OWFs

Feature 7: Minimal Correctness Requirements

Aside from security, there should be almost no other requirements

Requirements that do exist should be *semantic*

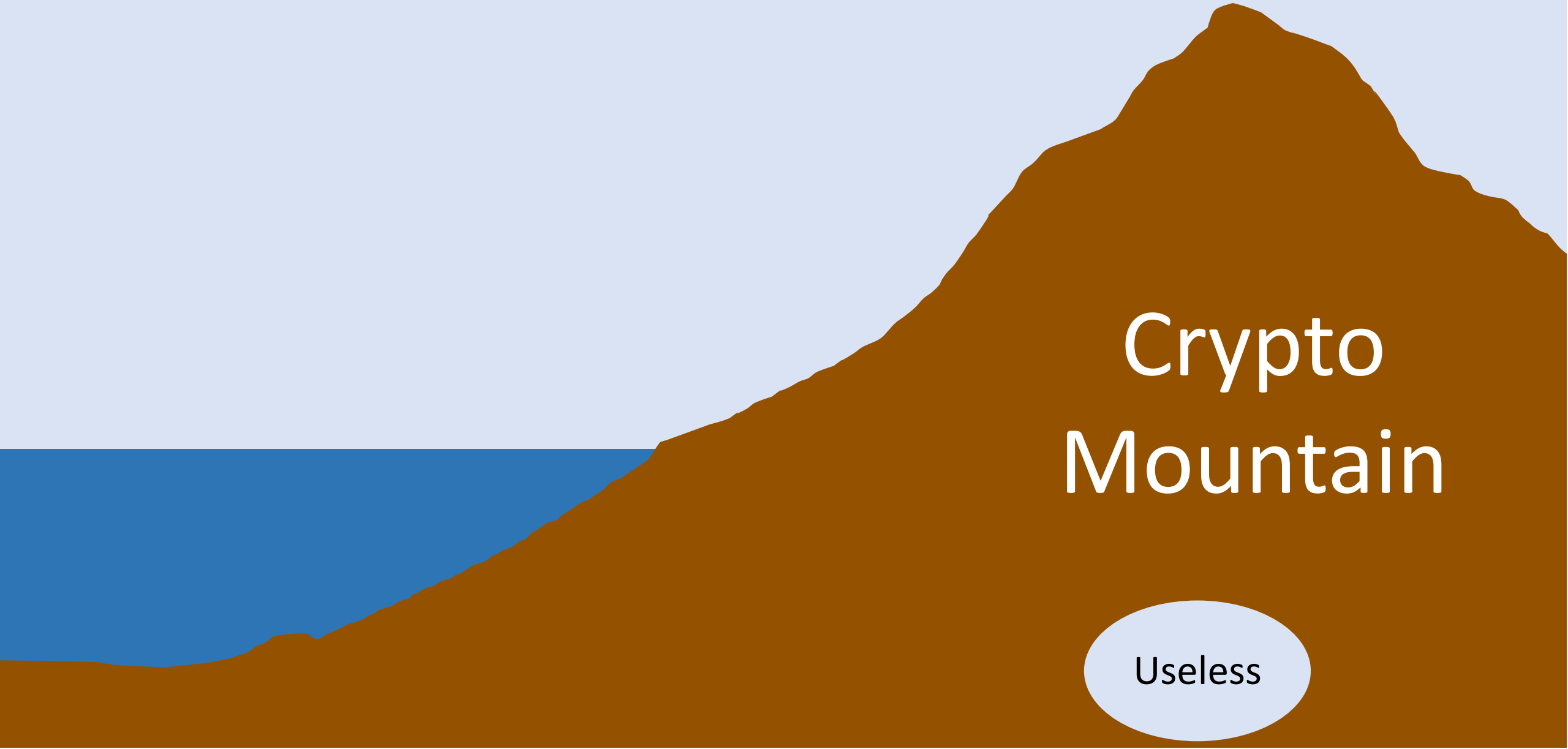
OWFs: classical deterministic f

PRGs: classical deterministic *expanding* G

PRPs: $F^{-1}(k,\ F(k,\ x)\ ) = x$ (not semantic)

Non-semantic → non-trivial to devise *robust* combiners and universal constructions

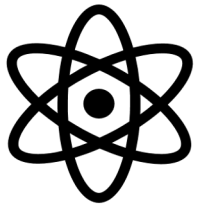
Feature 8: Can Build Crypto



Some Quantum Primitives Below OWFs

Pseudorandom States

[Ji-Liu-Song'18]

$s \in \{0,1\}^\lambda$ ⟶ G ⟶ 

n qubits

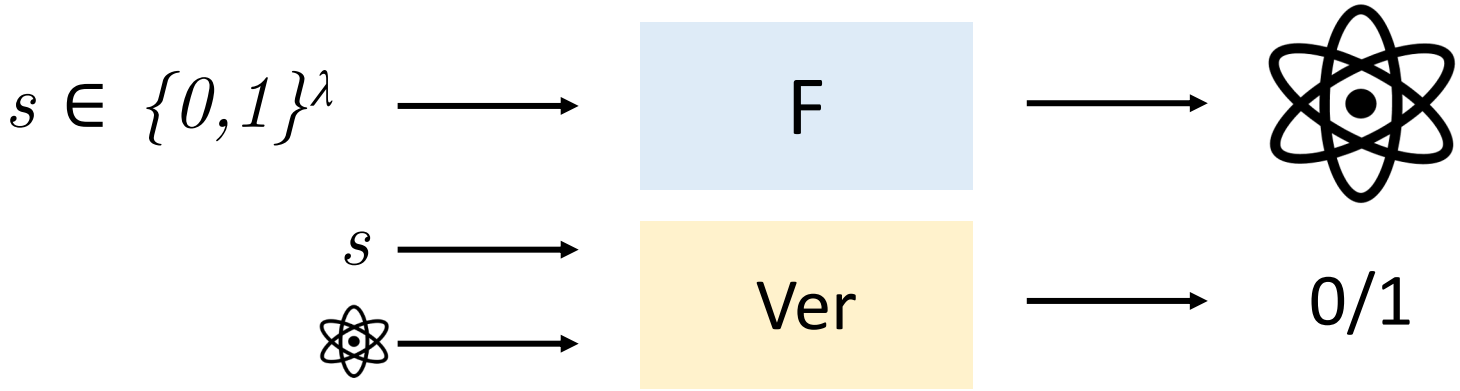
Looks "random", even under poly-many copies

Need crypto if $n > \Theta(log(\lambda))$

1. Trivially implied by general primitives ✗
2. Trivially & robustly implied by concrete assumptions ✗
3. Simple ✓
4. Falsifiable ✓
5. Search Problem ✗
6. Combiners & universal constructions ✗
7. Minimal Correctness ✓
8. Useful ✓

One-way State Generators

[Morimae-Yamakawa'22]



Hard to invert wrt Ver, even given poly-many copies

1. Trivially implied by general primitives ✓
2. Trivially & robustly implied by concrete assumptions ✓
3. Simple ✗
4. Falsifiable ✓
5. Search Problem ✓
6. Combiners & universal constructions ✗
7. Minimal Correctness ✗
8. Useful ✓

Possibility: maybe no good minimal quantum assumption?