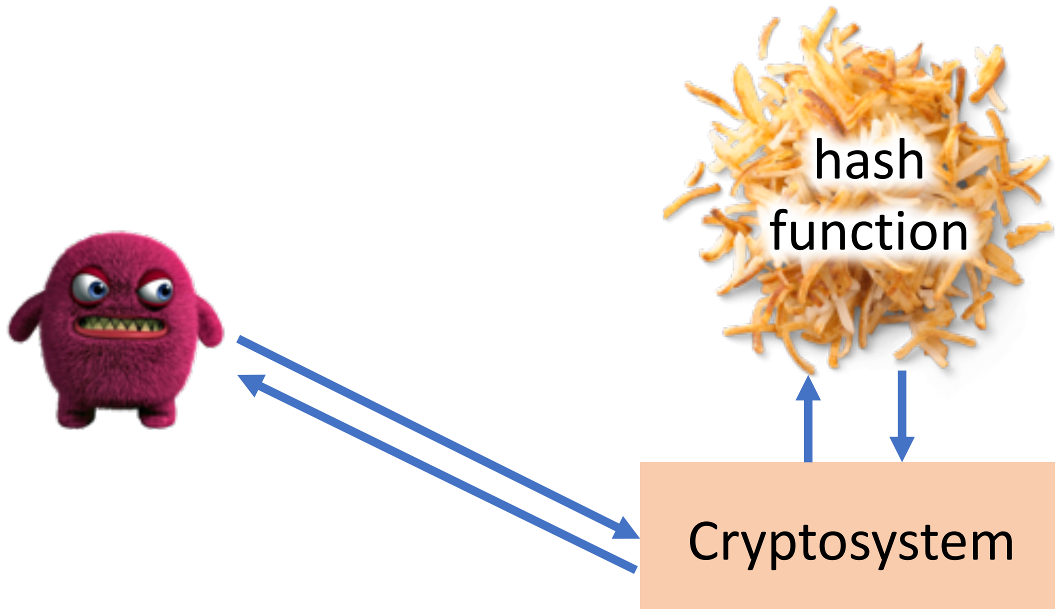
Quantum Random Oracle Model, Part 2

Mark Zhandry (Princeton & NTT Research)

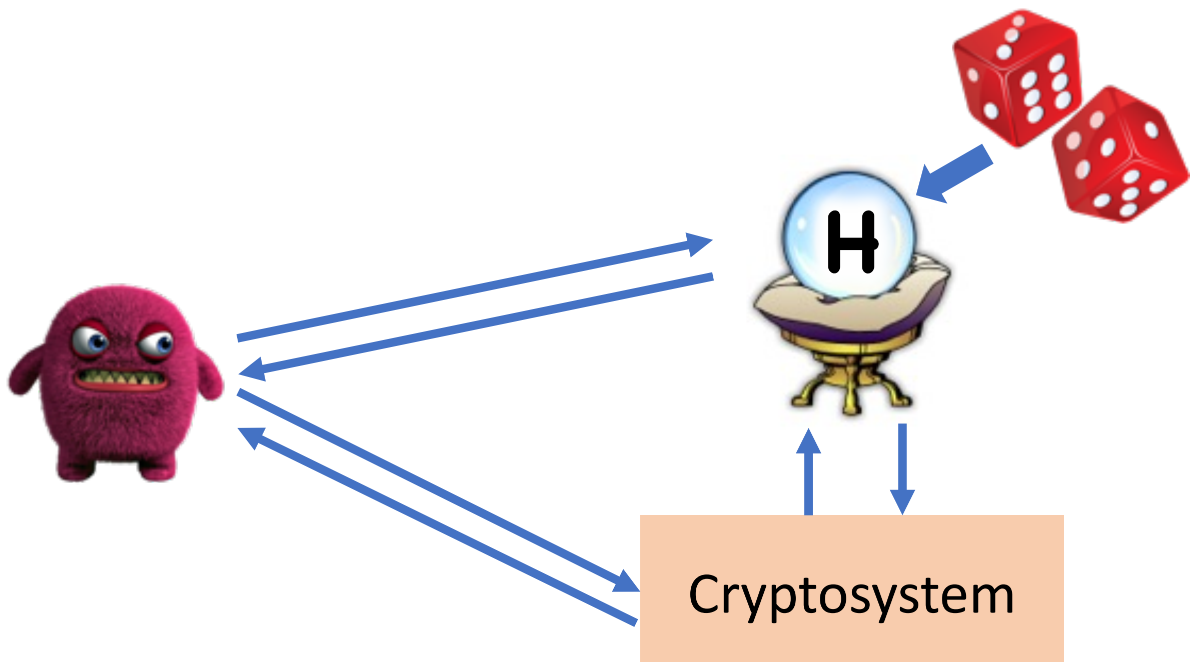
Recap: Classical ROM

[Bellare-Rogaway’93]



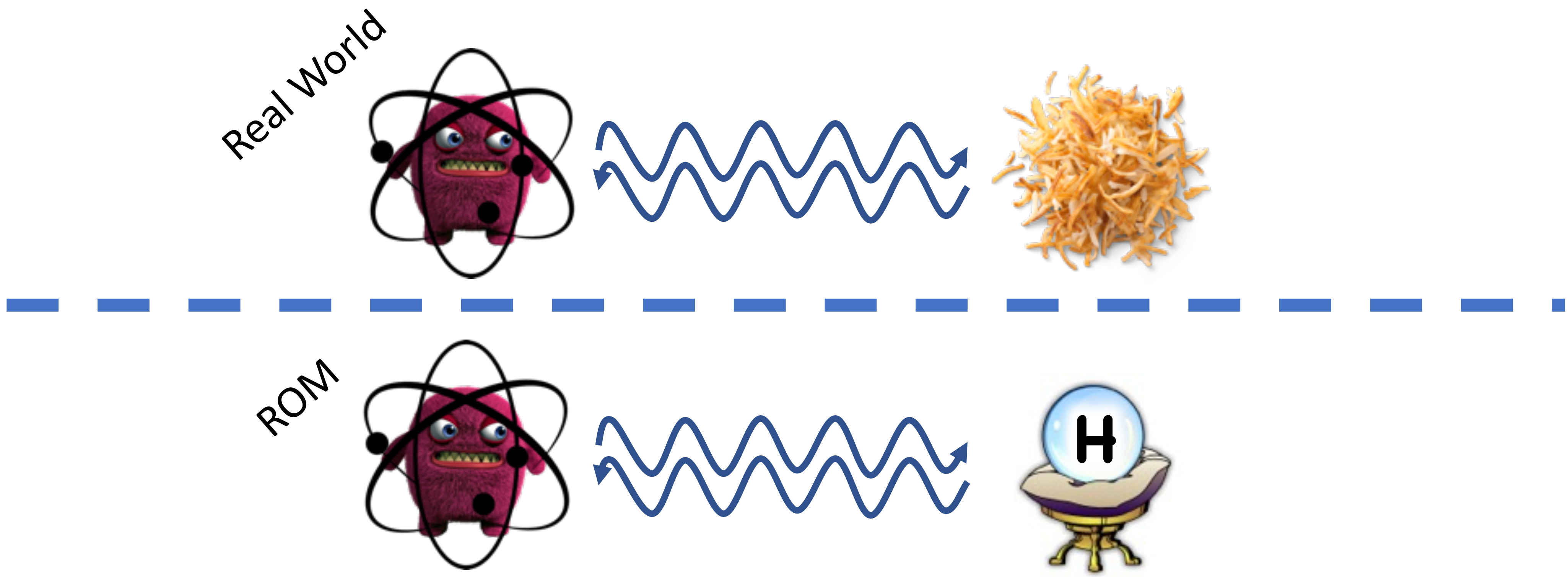
Examples: OAEP, Fujisaki-Okamoto, Full-Domain Hash, …

Recap: Classical ROM
[Bellare-Rogaway'93]



The Quantum Random Oracle Model (QROM)

[Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11]



Now standard in post-quantum crypto

Security Proof Challenges

Typical QROM reductions commit to entire function H at beginning, remain consistent throughout

[Zhang-Yu-Feng-Fan-Zhang'19]: "Committed programming reductions"

Limits of Committed Programming Reductions

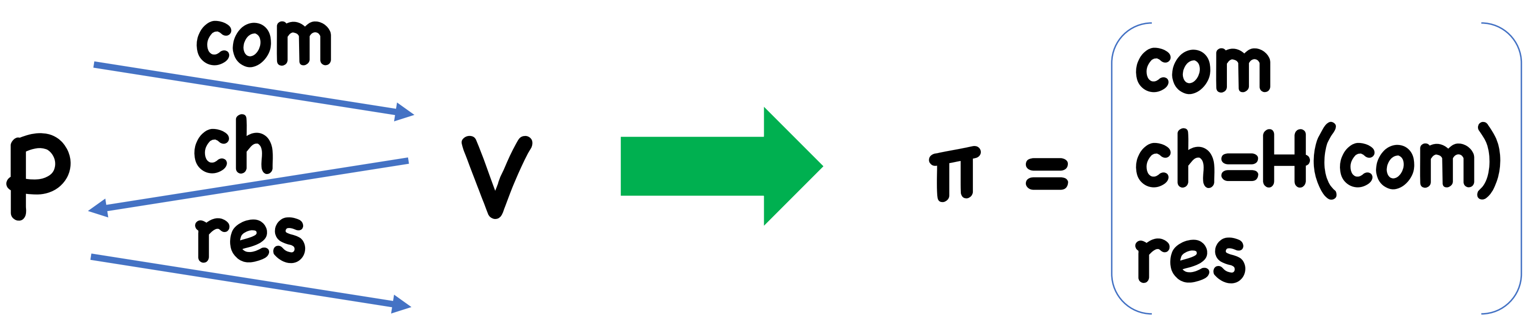
What classical ROM proofs admit CPReds, and which don't?

What to do if no CPRed?

Example: The Fiat-Shamir Transform
[Fiat-Shamir'87]

(public coin, HV)
3-Round Proof (of Knowledge)

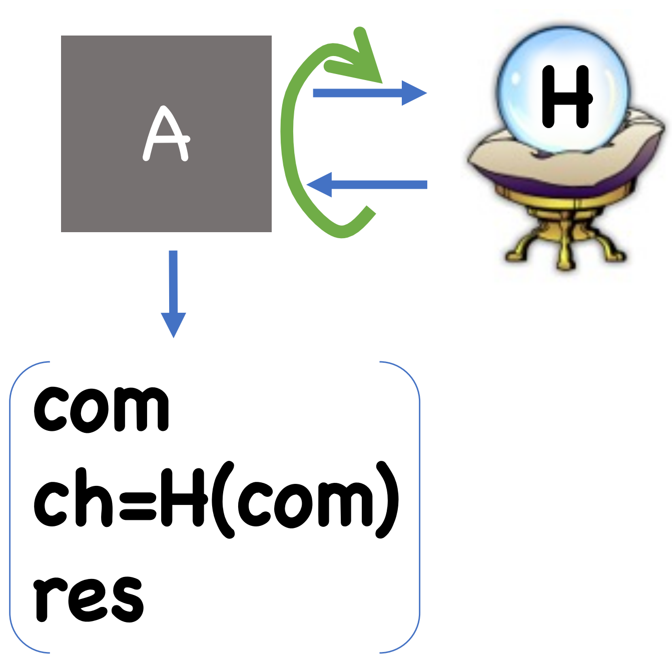
NI Proof (of Knowledge)



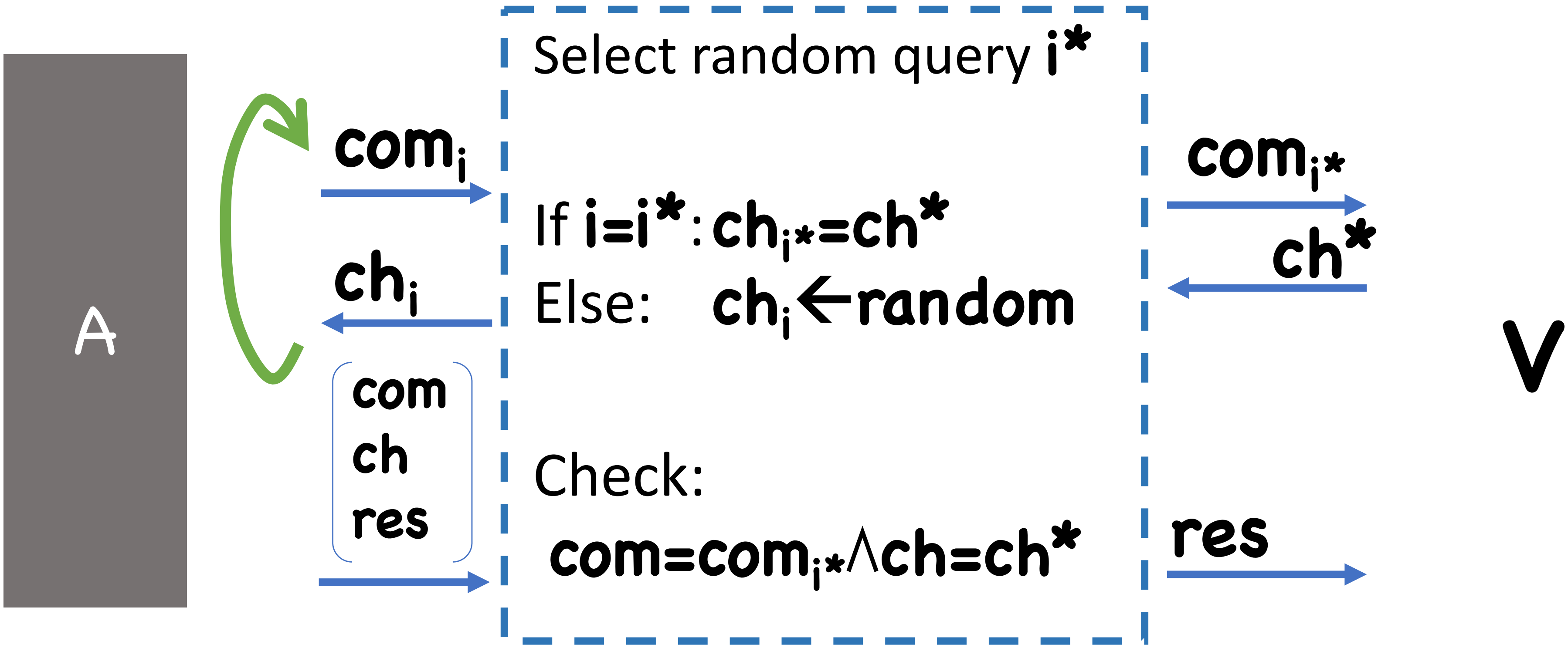
Also: Identification protocols → signatures

Classical Fiat-Shamir Proof

Assume:



Classical Fiat-Shamir Proof



Problems with Fiat-Shamir in QROM

Quantum analog of selecting random query?

Use small range distributions!?

Query extraction:
$\mathcal{A}$'s state disturbed by extracting $\mathbf{com}_{i^*}$

Adaptive Programming:
Can only set $\mathbf{H}(\mathbf{com}_{i^*})$ *after* queries already made

Problems with Fiat-Shamir in QROM

Thm [Dagdelen-Fischlin-Gagliardoni'13]:
There is no CPRed for Fiat-Shamir

Intuition: two cases:

(1) H committed before sending com to V

→ V's ch independent of A's ch

(2) H committed after sending com to V

→ A's com independent of reduction's com

Solutions?

[Unruh'15]: Use different conversion
Idea: A commits to all possible responses → can open using knowledge of RO
Problem: Less efficient

[Dagdelen-Fischlin-Gagliardoni'13,Unruh'17, Kiltz-Lyubashevsky-Schaffner'18]: Assume extra properties (e.g. statistical soundness) of proof system
Problem: Less efficient, maybe only proof (not PoK)

A Different Conversion

[Unruh'15]

Rough idea: $\pi = \begin{pmatrix} \text{com} \\ \{ H(\text{res}(\text{ch})) \}_{\text{ch}} \end{pmatrix}$

Proof sketch:

- Simulate RO s.t. reduction can efficiently invert
- Invert π on verifier's ch
- Lots of details to make sure A doesn't cheat

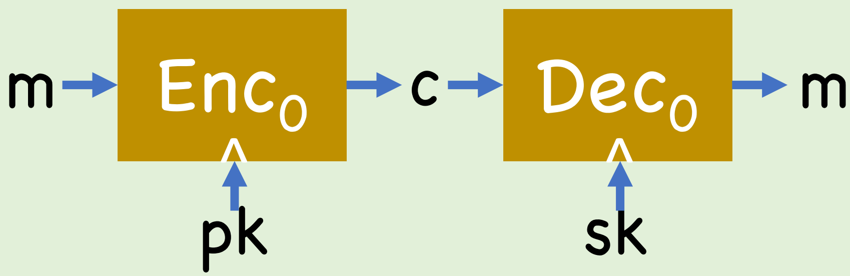
Simulating Invertible Random Oracles

How to simulate H so that reduction can invert?

Recall: already simulating as 2q-wise independent function
→ Can use degree $2q$ polynomial over finite field
→ Invertible by solving polynomial equations

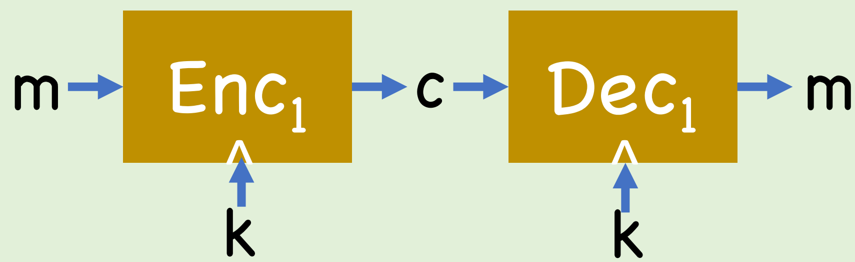
Example: Fujisaki-Okamoto

Building Block: One-*way* PKE



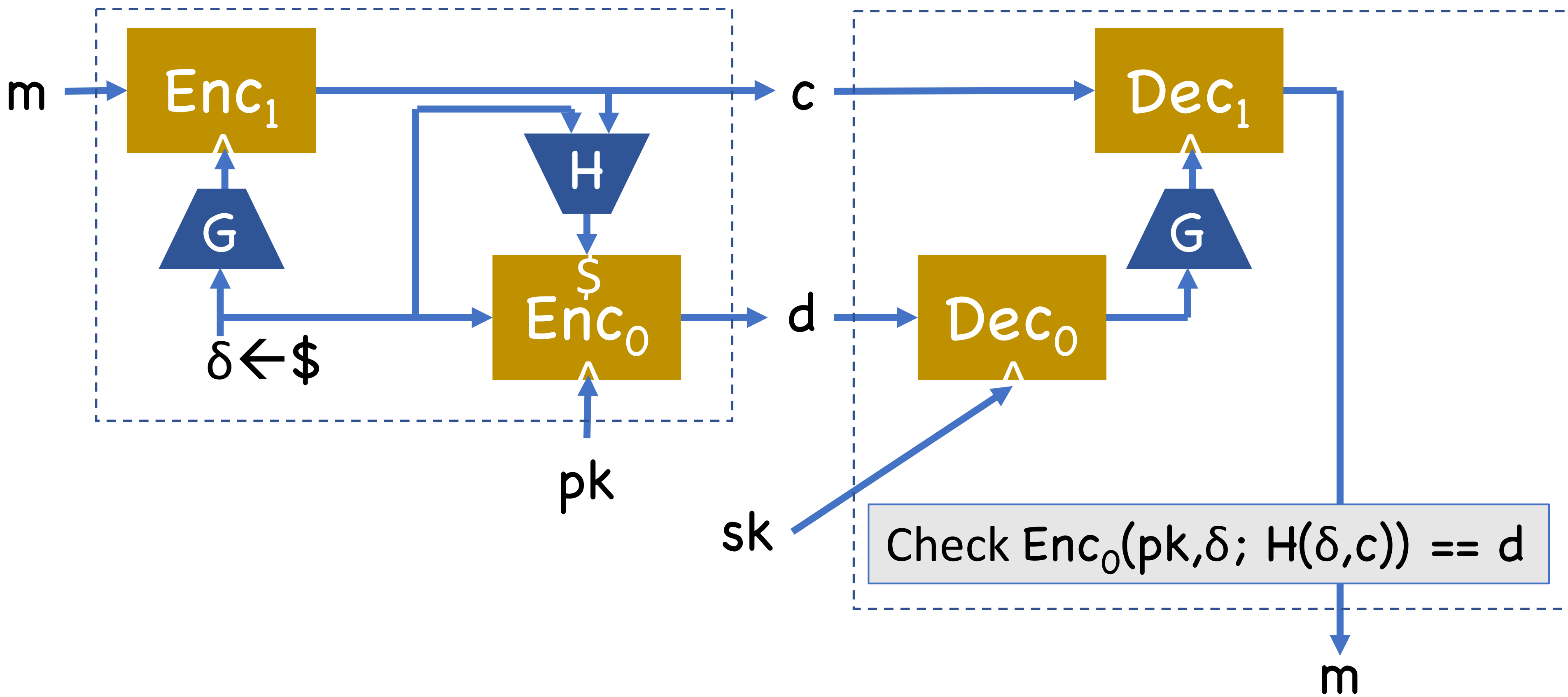
Security: $Enc_0(pk,m)$ one-way

Building Block: One-*time* SKE

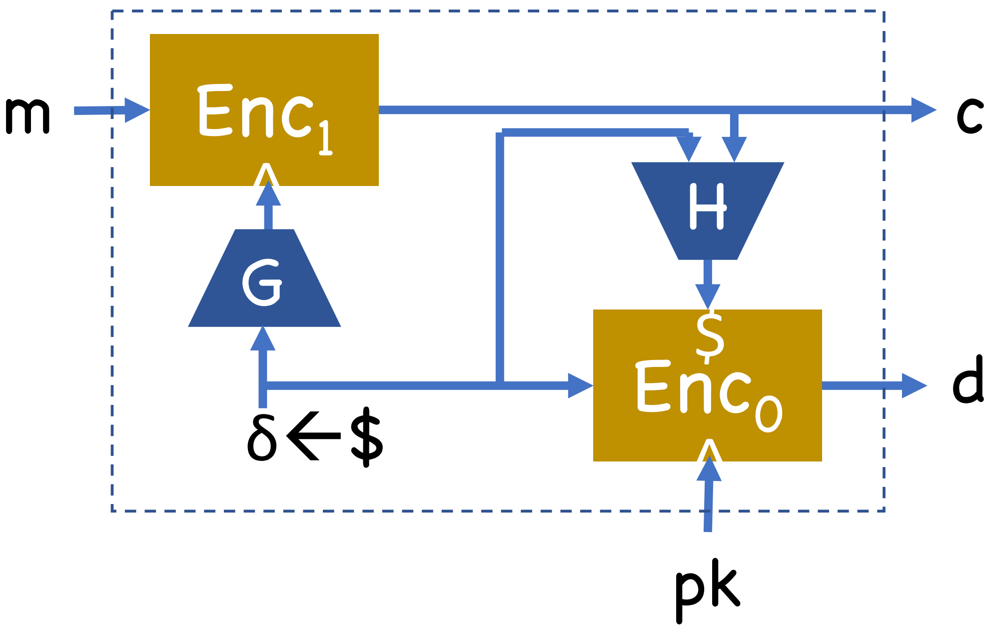


Security: $Enc_1(k,m_0) \approx Enc_1(k,m_1)$,
$H_\infty(Enc(k,m))$ large

Example: Fujisaki-Okamoto



Example: Fujisaki-Okamoto



CCA security intuition:
Only way to obtain valid (c,d) is to have queried H on some (δ,c)

→Look at prior queries to H to answer CCA queries

QROM problem: CPReds can't look at prior RO queries!

Example: Fujisaki-Okamoto

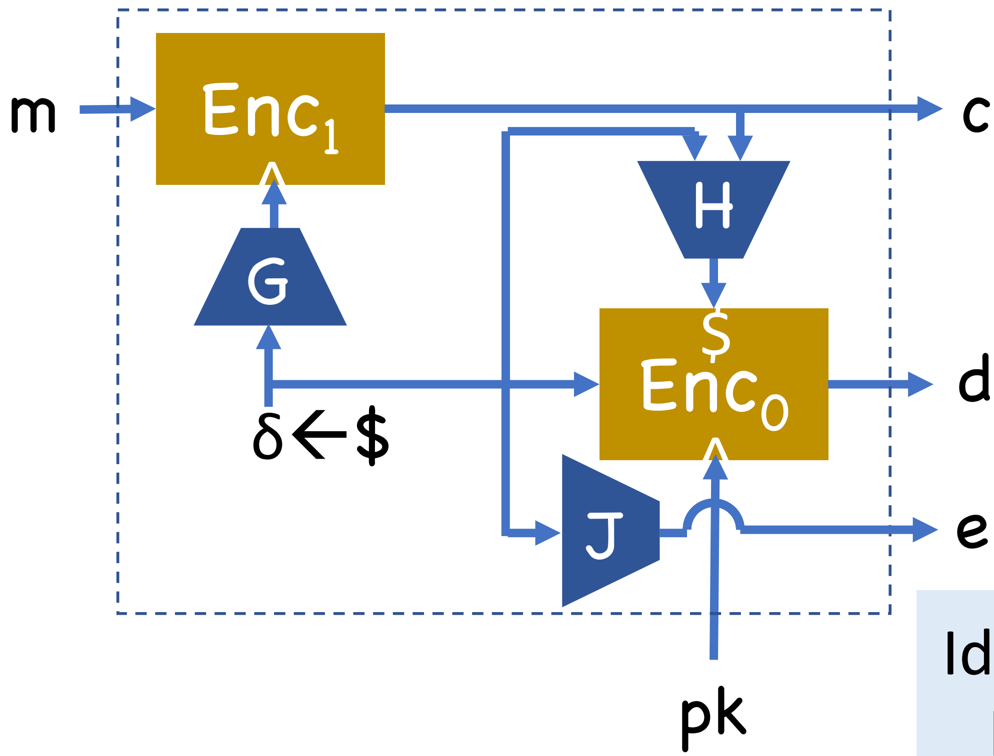
CPRed Impossibility? Open for FO, but I expect one exists

Given (c,d), no way to even tell which RO inputs or outputs used
→ RO seems useless

Impos. of CPReds for OAEP [Zhang-Yu-Feng-Fan-Zhang'19]

A Tweaked Conversion

[Targhi-Unruh'15]

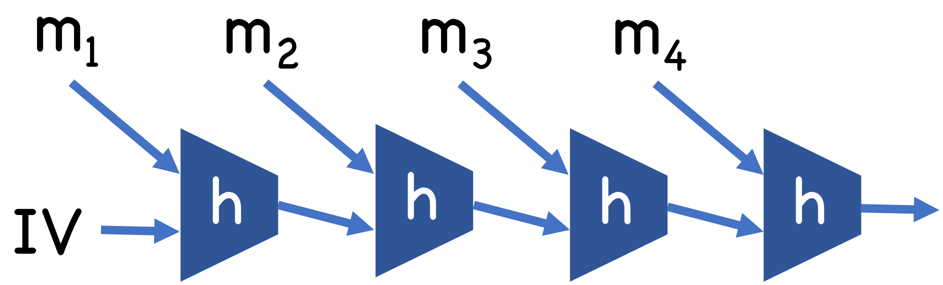


Idea: answer CCA queries by computing $\delta = J^{-1}(e)$

Example: Domain Extension for RO

Most hash functions built from lower-level objects

E.g. Merkle-Damgård (SHA1,SHA2)



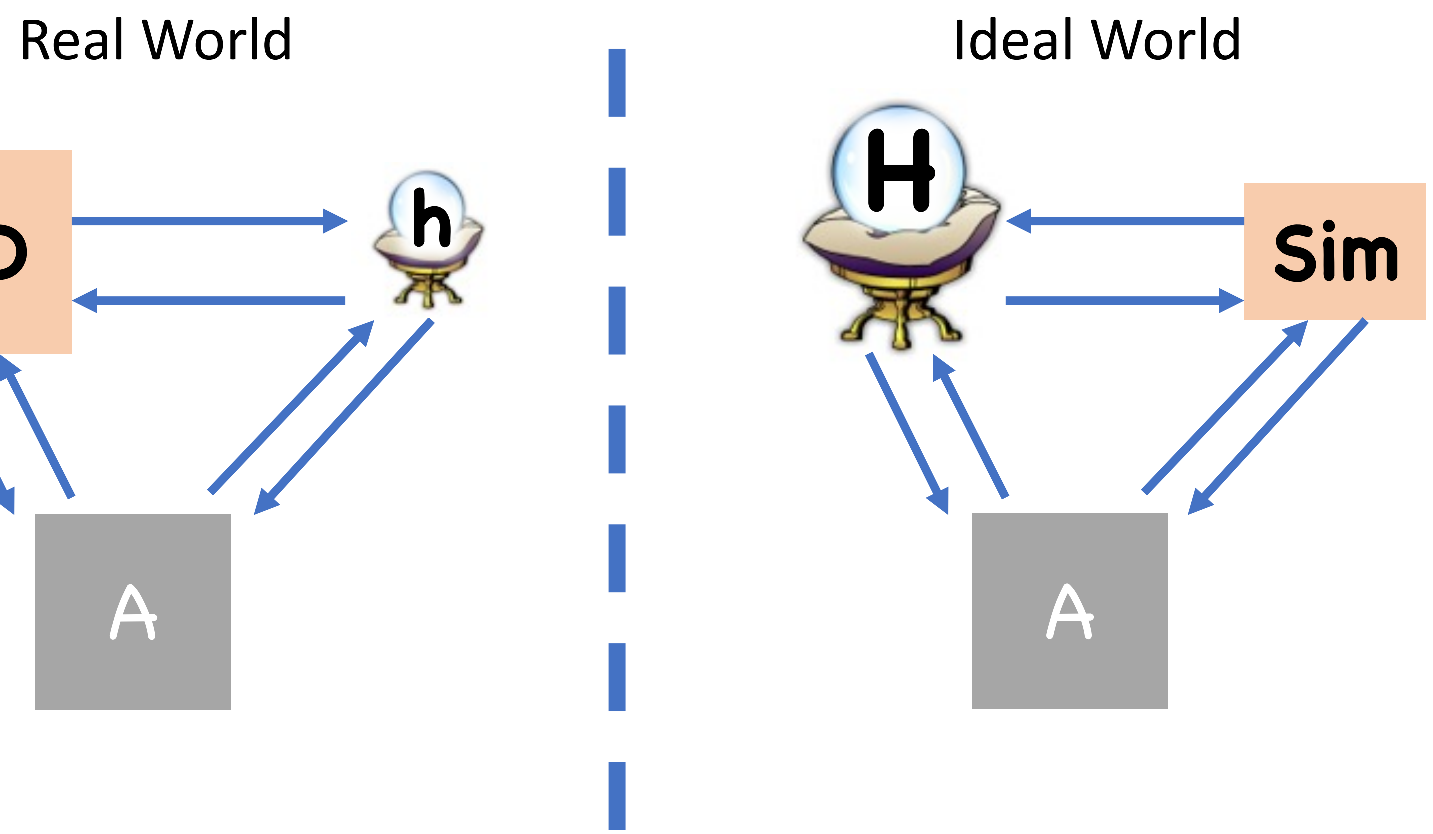
Problem: sometimes structure can be exploited for attack, even if **h** is assumed ideal

Example: Domain Extension for RO

Can we nevertheless justify the "RO Assumption", despite structure?

Yes(ish): indifferentiability [Maurer-Renner-Holenstein'04]

Indifferentiability



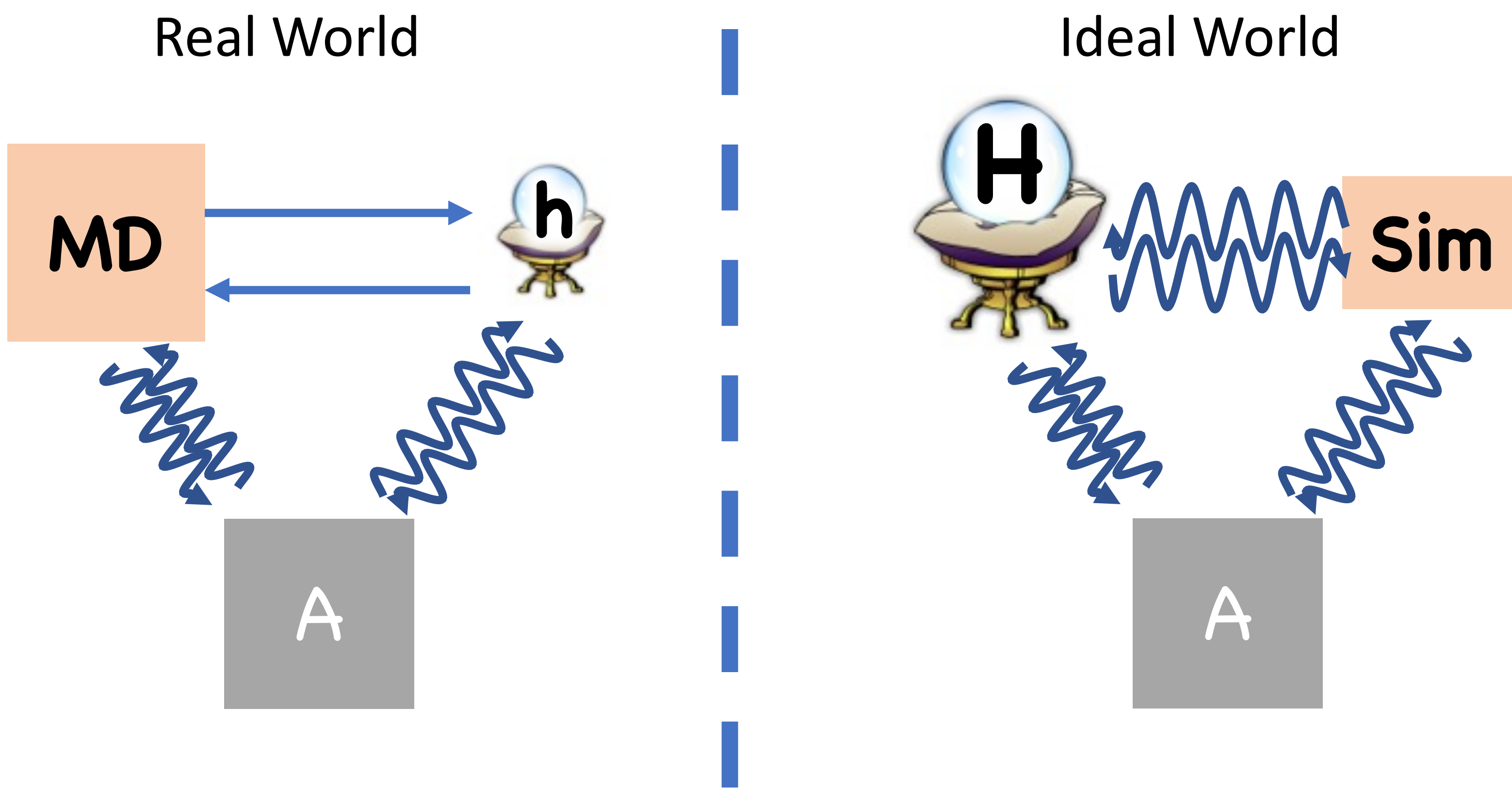
Indifferentiability

Thm [Ristenpart-Shacham-Shrimpton'11]:
Indifferentiability $\Rightarrow$ as good as RO for "single stage games"

Thm [Coron-Dodis-Malinaud-Puniya'05]
MD is classically indifferentiable under appropriate padding

Proof idea: Simulator can figure out when A is trying to evaluate MD by looking at past oracle queries

Quantum Indifferentiability



Quantum Indifferentiability

Fact: No CPRed (stateless simulator) for indifferentiable domain extension, *regardless of construction*

Proof idea:

- Size(truth table of Sim^H) << Size(truth table of H)
- And yet, Sim^H allows for computing H

→ Compression for random strings

What’s next?

Certain protocols, and even certain tasks, are unprovable under CPReds

Final hour: non-committed programming reductions