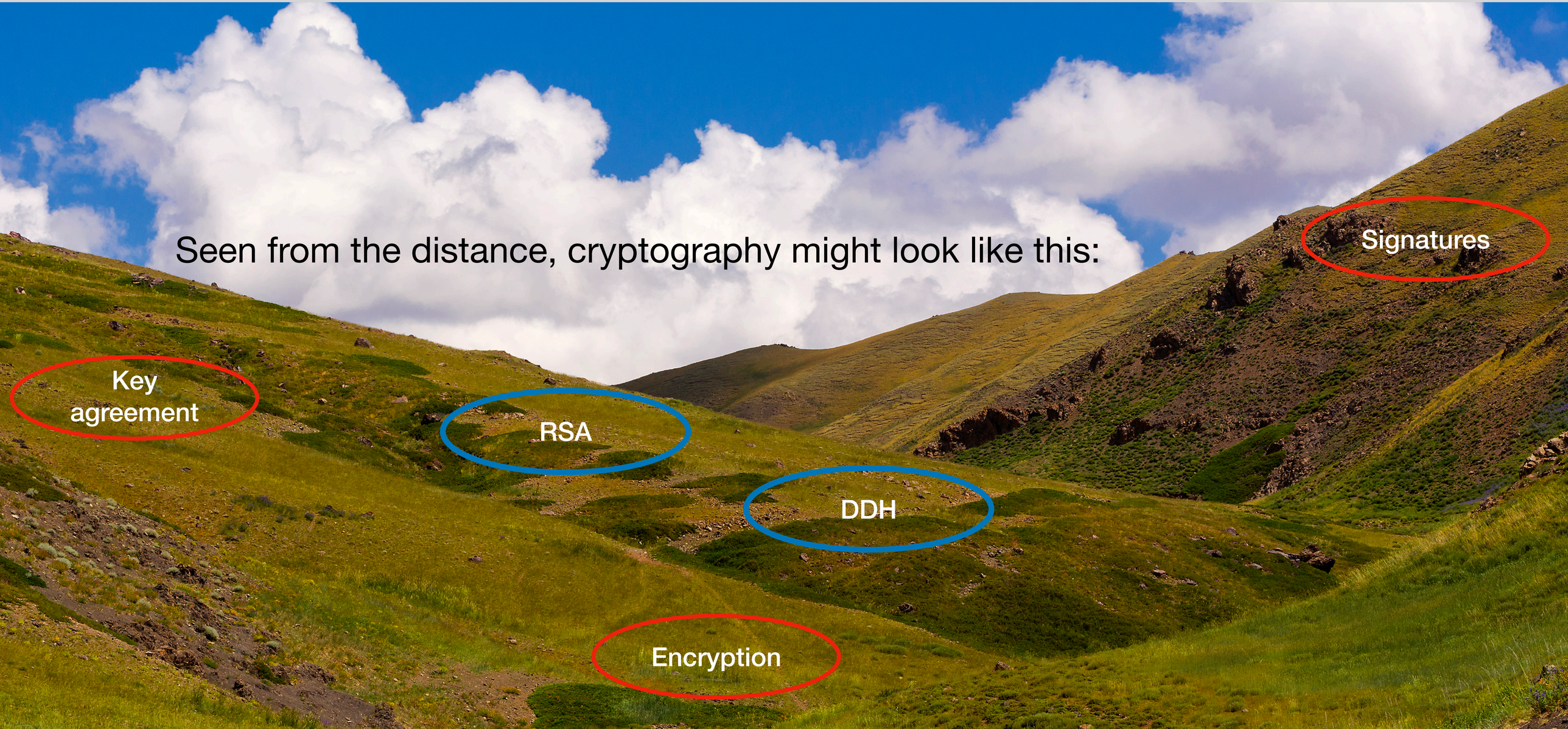
Black-Box Uselessness:

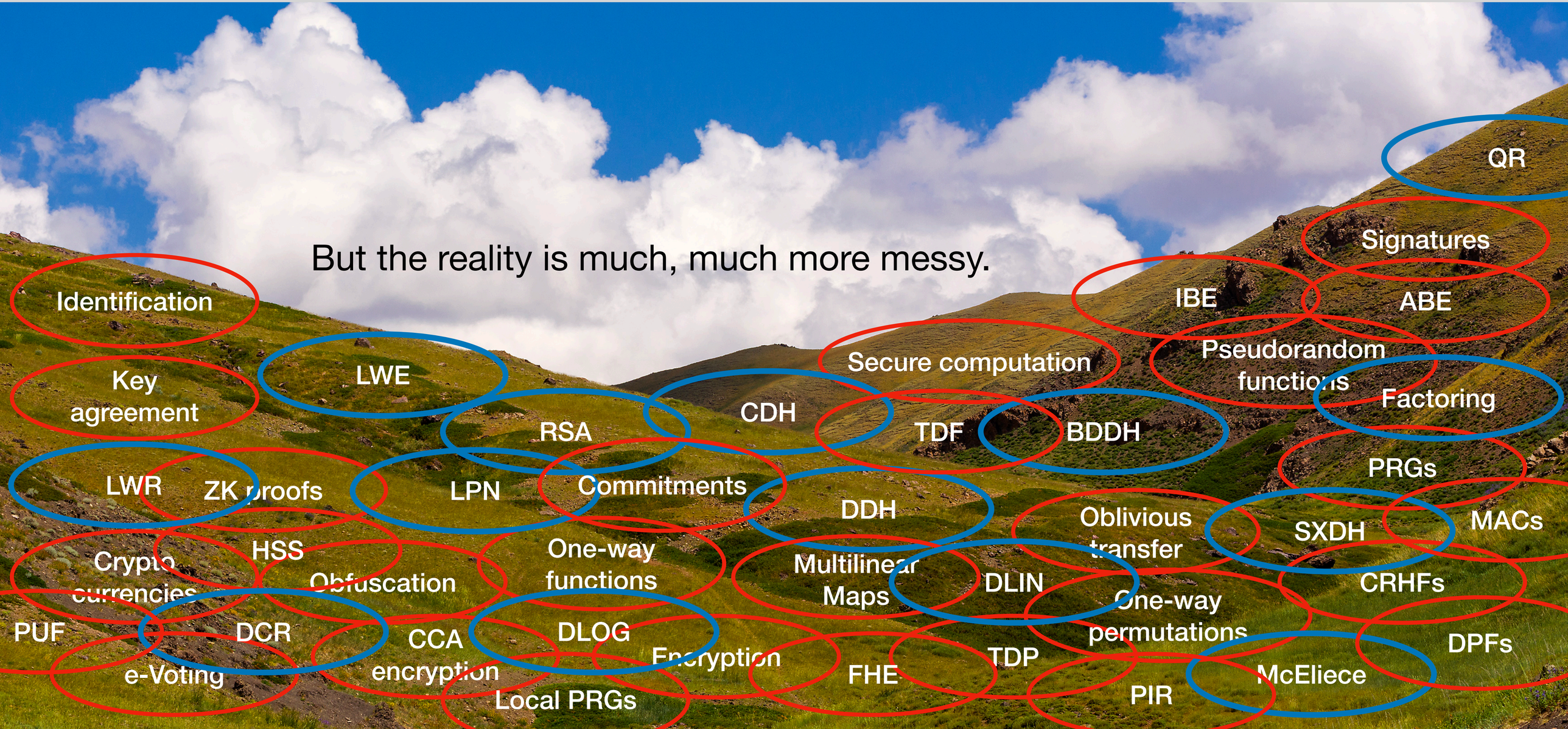
Composing Separations in Cryptography

Geoffroy Couteau, Pooya Farshim, and Mohammad Mahmoody

The Landscape of Cryptography



The Landscape of Cryptography



Reduction-Based Cryptography

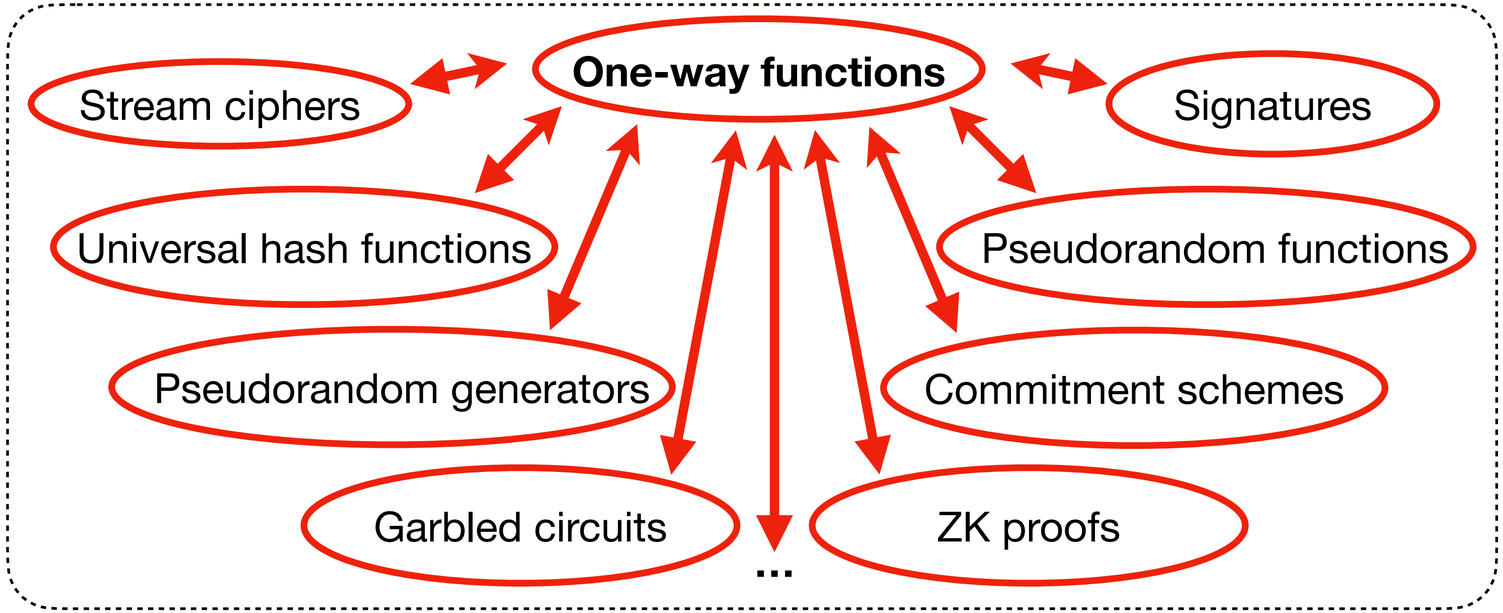
Problem: cryptographic primitives rely on unproven assumption (e.g. P vs NP).

Cryptographic reductions aim to cope with this unsatisfying state of affairs. Advantages:

- Conceptually simplifies the landscape into islands of equivalent primitives
- Provides new connections between problems with seemingly different structures
- Provides new constructions of various primitives under well-studied assumptions

Reduction-Based Cryptography

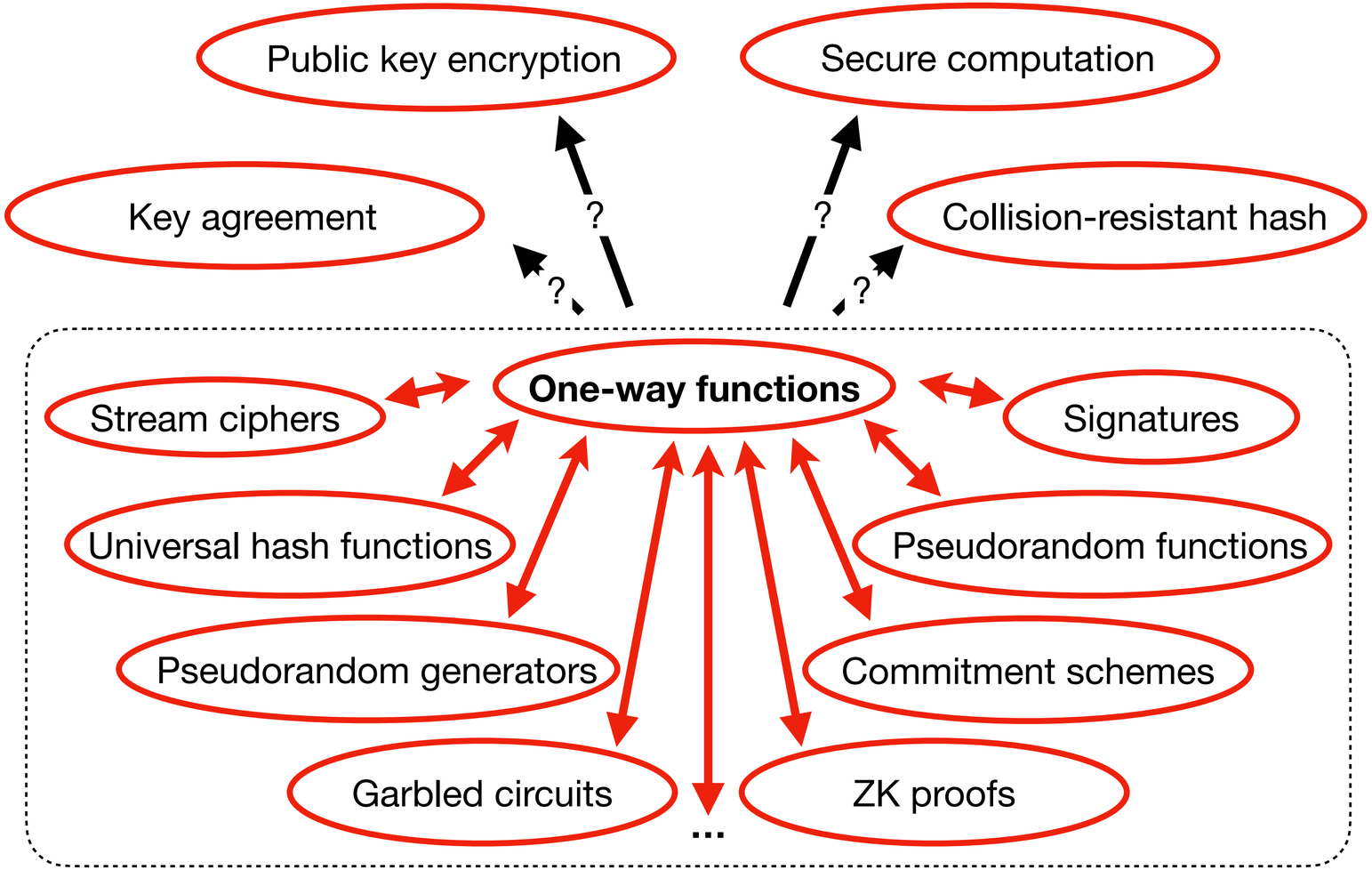
Reduction-based crypto enjoyed many celebrated successes. E.g. in *private-key* crypto:



Reduction-Based Cryptography

Reduction-based crypto enjoyed many celebrated successes. E.g. in *private-key* crypto:

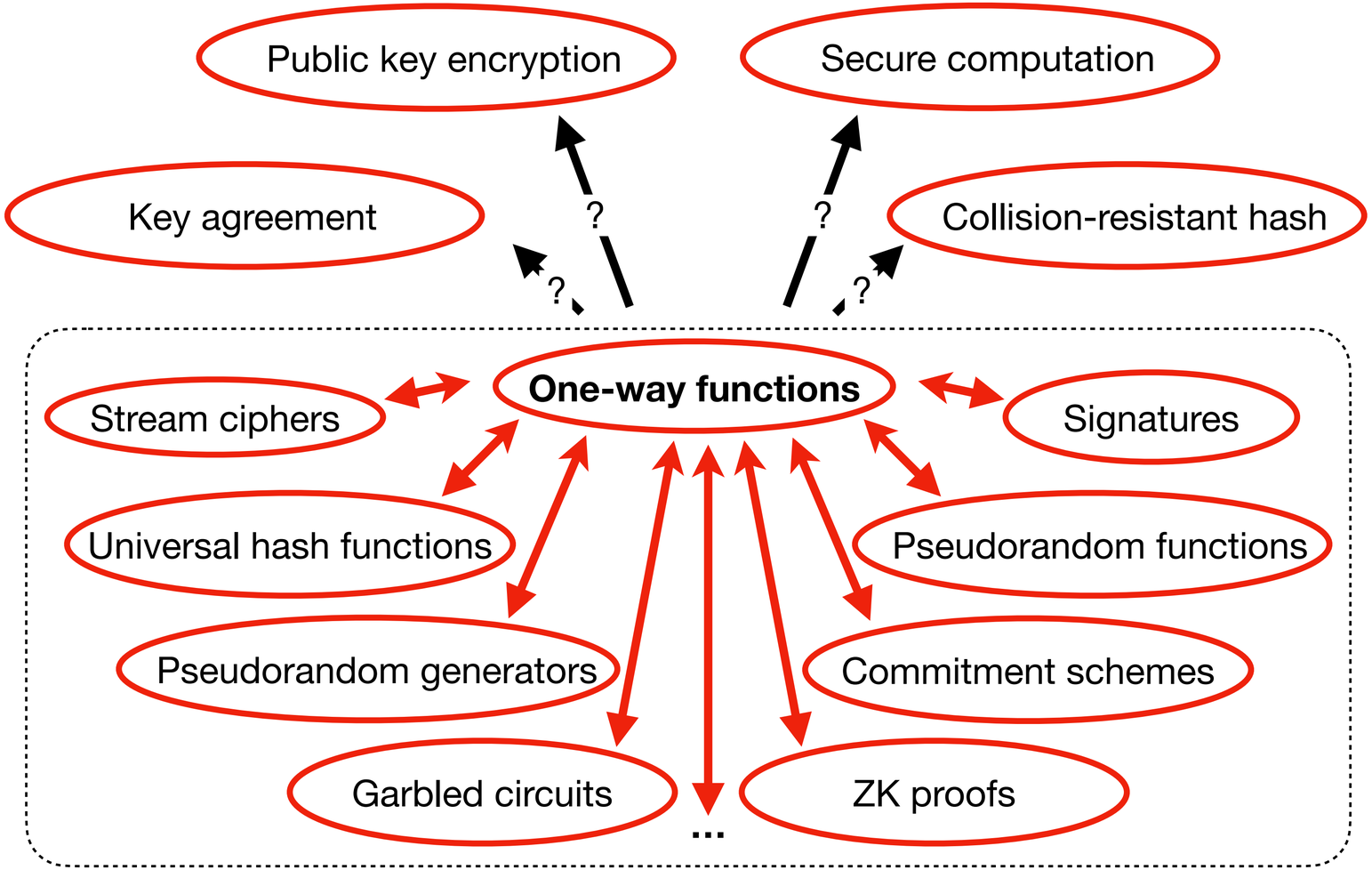
However, there are countless cases where no reductions are known.



Reduction-Based Cryptography

Reduction-based crypto enjoyed many celebrated successes. E.g. in *private-key* crypto:

However, there are countless cases where no reductions are known.



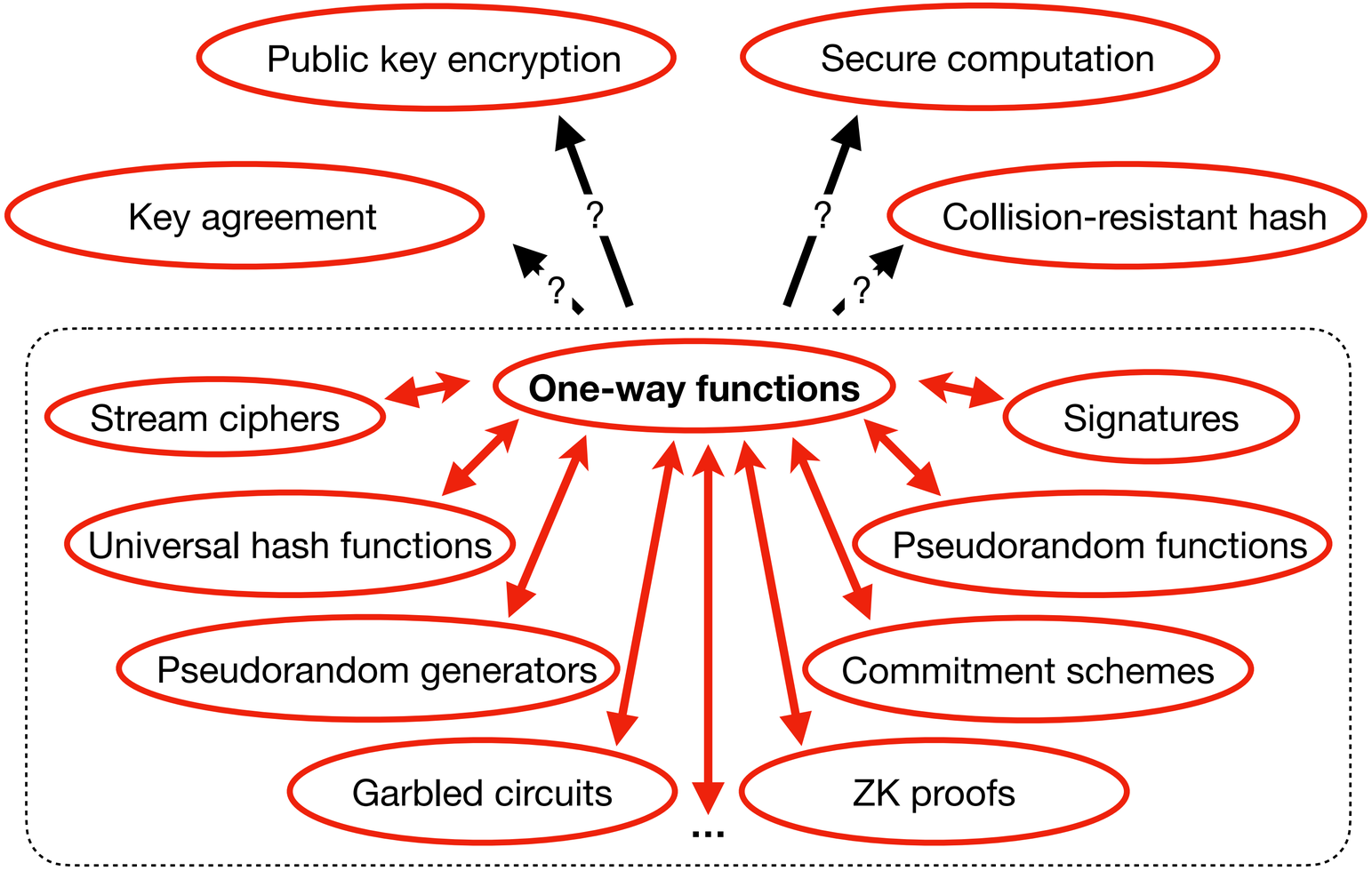
Yet, if we believe (A,B) *exist*, there must be reductions between A & B: consider the reduction that ignores A and builds B from scratch!

-> Lack of a reduction = limitation of *techniques*. Can we identify which one?

Reduction-Based Cryptography

Reduction-based crypto enjoyed many celebrated successes. E.g. in *private-key* crypto:

However, there are countless cases where no reductions are known.



Yet, if we believe (A,B) *exist*, there must be reductions between A & B: consider the reduction that ignores A and builds B from scratch!

-> Lack of a reduction = limitation of *techniques*. Can we identify which one?

Core insight: (Impagliazzo-Rudich 1989) most crypto reductions are *black-box* : they are oblivious to the specific implementation of the source primitive and of the adversary against it.

Black-Box Reductions

There is a black-box reduction from a primitive B to a primitive A if there exists an efficient implementation of B that only uses the input-output behavior of A (and is oblivious to its concrete implementation).

A bit more formally [RTV04]: there is a black-box reduction from a primitive B to a primitive A if there exists a construction (P,S) of B from *any implementation* a of A such that:

- Whenever the construction is instantiated with an *efficient* implementation a of A, P^a is an efficient implementation of B.
- For any adversary Adv that breaks P^a, S^{a,Adv} breaks a.

Black-Box Reductions

There is a black-box reduction from a primitive B to a primitive A if there exists an efficient implementation of B that only uses the input-output behavior of A (and is oblivious to its concrete implementation).

A bit more formally [RTV04]: there is a black-box reduction from a primitive B to a primitive A if there exists a construction (P,S) of B from *any implementation* a of A such that:

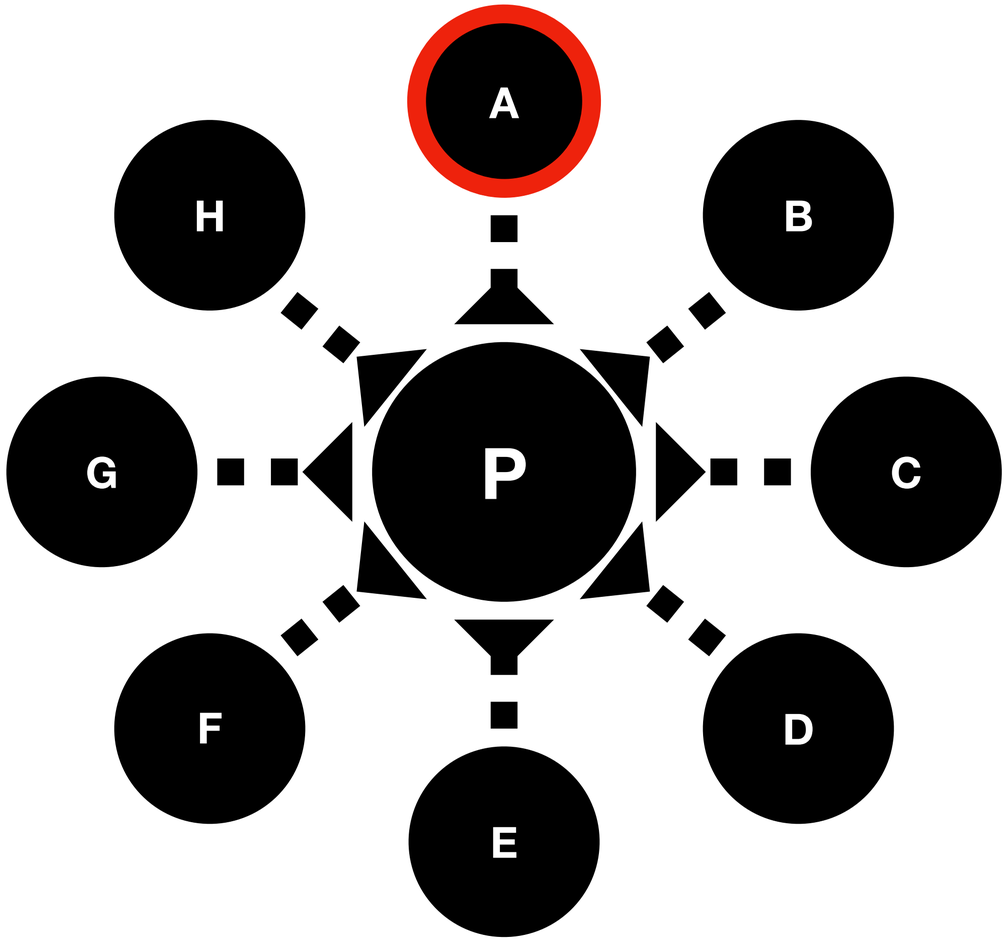
- Whenever the construction is instantiated with an *efficient* implementation a of A, P^a is an efficient implementation of B.
- For any adversary Adv that breaks P^a, S^{a,Adv} breaks a.

[**Impagliazzo-Rudich, 1989] (seminal result):** there is no BB reduction from key agreement to OWF.

There has been a tremendous number of black-box separations between primitives. They explain precisely the limits of our techniques, and guide future constructions by ruling out a large class of methods.

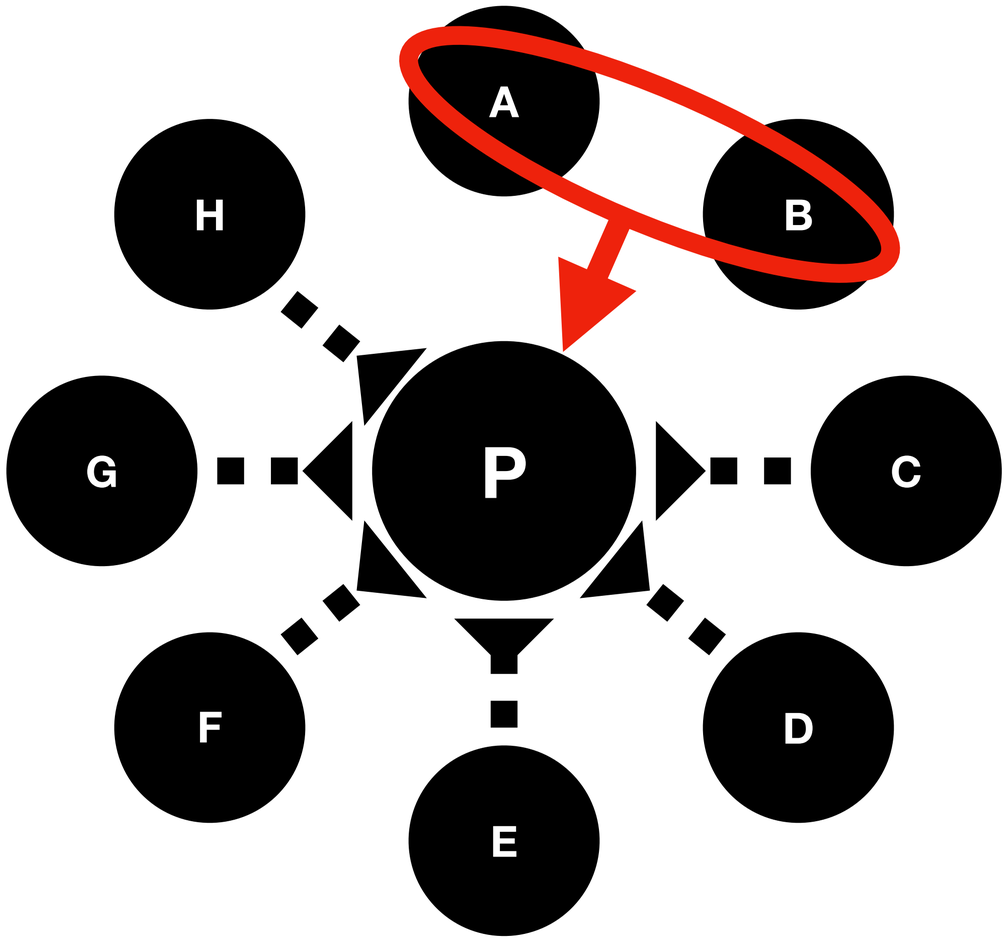
Non-Composability of Black-Box Separations

- A large number of BB separations have been proven over the past decades
- However, a BB separation between A and P only rules out BB constructions of P *from A alone*



Non-Composability of Black-Box Separations

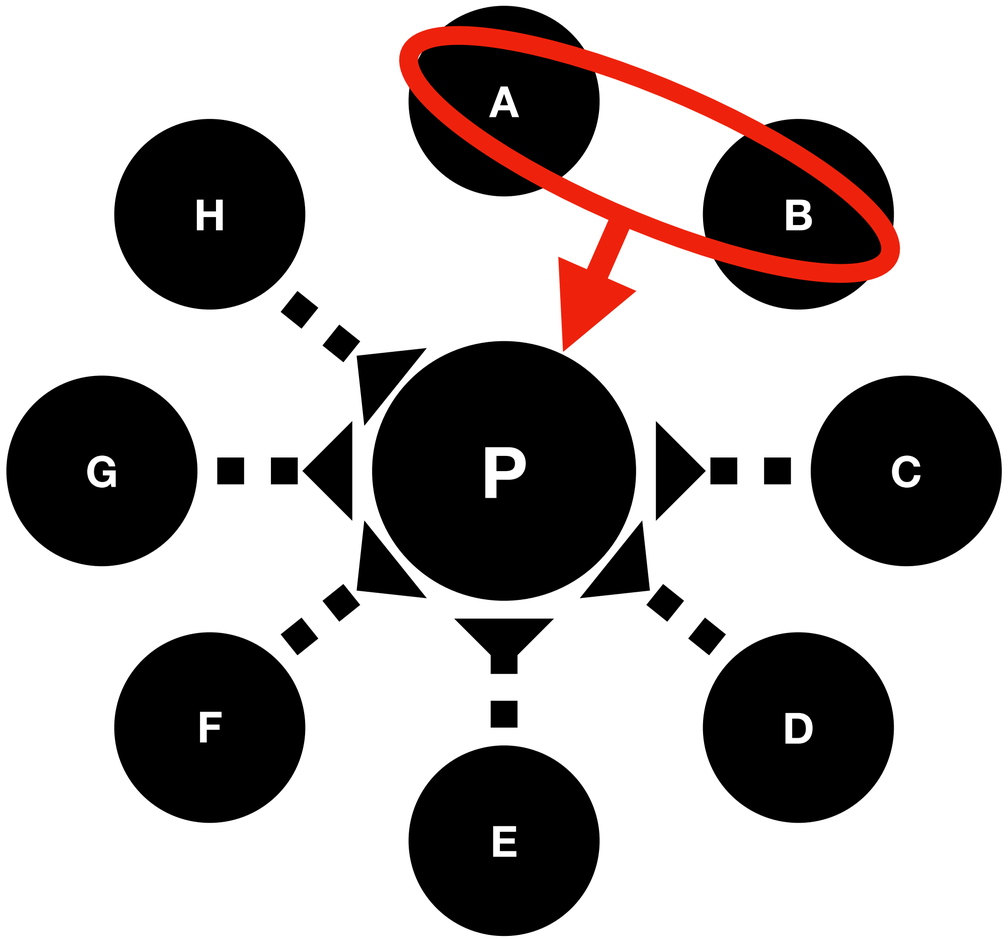
- A large number of BB separations have been proven over the past decades
- However, a BB separation between A and P only rules out BB constructions of P *from A alone*
- Not ruled out: maybe P can be BB constructed from A and B, even if each of A and B cannot imply P alone.
- **This creates an undesirable situation:** if we want to rule out the possibility of *combining* primitives to BB-construct P, we must prove a separation for *each possible subset of primitives.*



Non-Composability of Black-Box Separations

- A large number of BB separations have been proven over the past decades
- However, a BB separation between A and P only rules out BB constructions of P *from A alone*
- Not ruled out: maybe P can be BB constructed from A and B, even if each of A and B cannot imply P alone.
- **This creates an undesirable situation:** if we want to rule out the possibility of *combining* primitives to BB-construct P, we must prove a separation for *each possible subset of primitives.*

Can we find a *composable* notion?



A Stronger, Composable Notion: Black-Box Uselessness

We want a way of saying that a primitive *cannot possibly be useful* in a black-box construction of P.

Informal definition (black-box uselessness). A primitive A is *black-box useless* for P if for *any auxiliary primitive Z*, if there exists a black-box construction of P from (A, Z), then there must already exist a construction of P from Z alone.

Composability theorem (easy). If A is BBU for P and B is BBU for P, then (A,B) is BBU for P.

Proof: let Z be such that there is a BB construction of P from (A, B, Z).

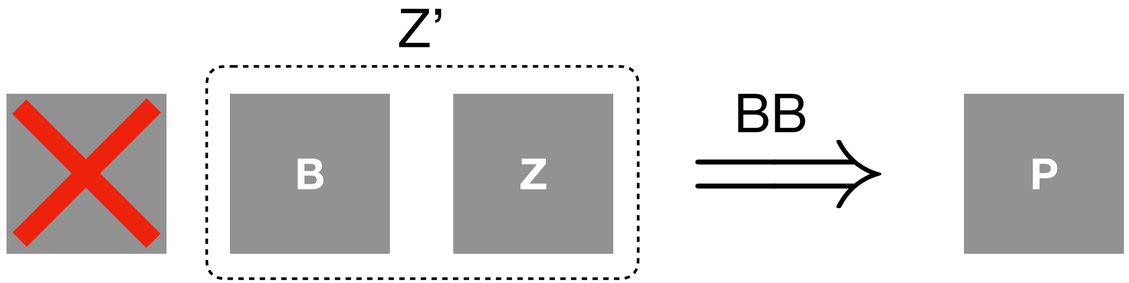
A Stronger, Composable Notion: Black-Box Uselessness

We want a way of saying that a primitive *cannot possibly be useful* in a black-box construction of P.

Informal definition (black-box uselessness). A primitive A is *black-box useless* for P if for *any auxiliary primitive Z*, if there exists a black-box construction of P from (A, Z), then there must already exist a construction of P from Z alone.

Composability theorem (easy). If A is BBU for P and B is BBU for P, then (A,B) is BBU for P.

Proof: Since A is BBU for P, there is a BB construction of P from Z' = (B,Z).



A Stronger, Composable Notion: Black-Box Uselessness

We want a way of saying that a primitive *cannot possibly be useful* in a black-box construction of P.

Informal definition (black-box uselessness). A primitive A is *black-box useless* for P if for *any auxiliary primitive Z*, if there exists a black-box construction of P from (A, Z), then there must already exist a construction of P from Z alone.

Composability theorem (easy). If A is BBU for P and B is BBU for P, then (A,B) is BBU for P.

Proof: Since B is BBU for P, there is a BB construction of P from Z.

Our Results

Definitions, composition

Are OWFs BBU for key agreement?

Probably yes

Extending existing separations to the BBU regime

Are OWFs BB *helpful* for CRHFs?

Probably yes

Our Results

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

Extending existing separations to the BBU regime

Are OWFs BB *helpful* for CRHFs?

Probably yes

Our Results

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

Extending existing separations to the BBU regime

- Large class of methods for BB separations: the *compiling-out* paradigm
- We show that BB separations in this paradigm *relativize* and therefore imply BBU
- As a result, extend many existing results to BBU

Are OWFs BB *helpful* for CRHFs?

Probably yes

Our Results

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

- Perhaps **the most fundamental question** is whether OWFs are BBU for KA.
- Preliminary results in this direction: OWFs are BBU in any *unbalanced* KA (where one party makes a constant #of queries to the OWF)

Extending existing separations to the BBU regime

- Large class of methods for BB separations: the *compiling-out* paradigm
- We show that BB separations in this paradigm *relativize* and therefore imply BBU
- As a result, extend many existing results to BBU

Are OWFs BB *helpful* for CRHFs?

Probably yes

Our Results

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

- Perhaps **the most fundamental question** is whether OWFs are BBU for KA.
- Preliminary results in this direction: OWFs are BBU in any *unbalanced* KA (where one party makes a constant #of queries to the OWF)

Extending existing separations to the BBU regime

- Large class of methods for BB separations: the *compiling-out* paradigm
- We show that BB separations in this paradigm *relativize* and therefore imply BBU
- As a result, extend many existing results to BBU

Are OWFs BB *helpful* for CRHFs?

Probably yes

- Are there primitives which are black-box *helpful* for other primitives (even when they are BB separated)?
- Conjecture: OWFs are BB helpful for collision resistant hashing; related to natural conjectures about ROs.

Our Results

Already covered (informally)

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

- Perhaps **the most fundamental question** is whether OWFs are BBU for KA.
- Preliminary results in this direction: OWFs are BBU in any *unbalanced* KA (where one party makes a constant #of queries to the OWF)

Extending existing separations to the BBU regime

- Large class of methods for BB separations: the *compiling-out* paradigm
- We show that BB separations in this paradigm *relativize* and therefore imply BBU
- As a result, extend many existing results to BBU

Are OWFs BB *helpful* for CRHFs?

Probably yes

- Are there primitives which are black-box *helpful* for other primitives (even when they are BB separated)?
- Conjecture: OWFs are BB helpful for collision resistant hashing; related to natural conjectures about ROs.

Our Results

Already covered (informally)

Main focus of the talk

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

- Perhaps **the most fundamental question** is whether OWFs are BBU for KA.
- Preliminary results in this direction: OWFs are BBU in any *unbalanced* KA (where one party makes a constant #of queries to the OWF)

Extending existing separations to the BBU regime

- Large class of methods for BB separations: the *compiling-out* paradigm
- We show that BB separations in this paradigm *relativize* and therefore imply BBU
- As a result, extend many existing results to BBU

Are OWFs BB *helpful* for CRHFs?

Probably yes

- Are there primitives which are black-box *helpful* for other primitives (even when they are BB separated)?
- Conjecture: OWFs are BB helpful for collision resistant hashing; related to natural conjectures about ROs.

Our Results

Already covered (informally)

Main focus of the talk

Definitions, composition

- Identify flavors of BBU, in the RTV framework
- Generalize to other setting (BBU w.r.t. subsets of primitives, BBU for *efficiency* separations, etc)
- Formally prove:
  [A BBU for C]+[B BBU for C] => [A+B BBU for C]

Are OWFs BBU for key agreement?

Probably yes

- Perhaps **the most fundamental question** is whether OWFs are BBU for KA.
- Preliminary results in this direction: OWFs are BBU in any *unbalanced* KA (where one party makes a constant #of queries to the OWF)

Extending existing separations to the BBU regime

- Large class of methods for BB separations: the *compiling-out* paradigm
- We show that BB separations in this paradigm *relativize* and therefore imply BBU
- As a result, extend many existing results to BBU

Next slide

Are OWFs BB *helpful* for CRHFs?

Probably yes

- Are there primitives which are black-box *helpful* for other primitives (even when they are BB separated)?
- Conjecture: OWFs are BB helpful for collision resistant hashing; related to natural conjectures about ROs.

Black-Box Uselessness from Compiling Out - Teaser

Black-Box Uselessness from Compiling Out - Teaser

Black-box separations via the **compiling-out paradigm** relativize: the compilation can be carried in the presence of another auxiliary oracle Z.

Black-Box Uselessness from Compiling Out - Teaser

Black-box separations via the **compiling-out paradigm** relativize: the compilation can be carried in the presence of another auxiliary oracle Z.

We list a few consequences of this observation to illustrate its power:

- **Using [GGKT05]**
  - OWP are BBU for constructing *efficient* PRG : $\{0,1\}^k \mapsto \{0,1\}^{k+n}$ (making less than O(n / log k) calls to the OWP)
  - OWP are BBU for constructing *efficient* universal one-way hash functions, digital signatures, or private-key encryption
  - OWF are BBU for constructing PKE if #calls to OWF << message length
- **Using [CKP15, GMM17a, GMM17b]**
  - OWF are BBU for constructing approximate indistinguishability obfuscation
  - Witness-encryption, predicate encryption, fully homomorphic encryption, Boolean functional encryption, are all BBU for constructing approximate iO

Are OWFs BBU for Key Agreement?

Are OWFs BBU for Key Agreement?

Roadmap

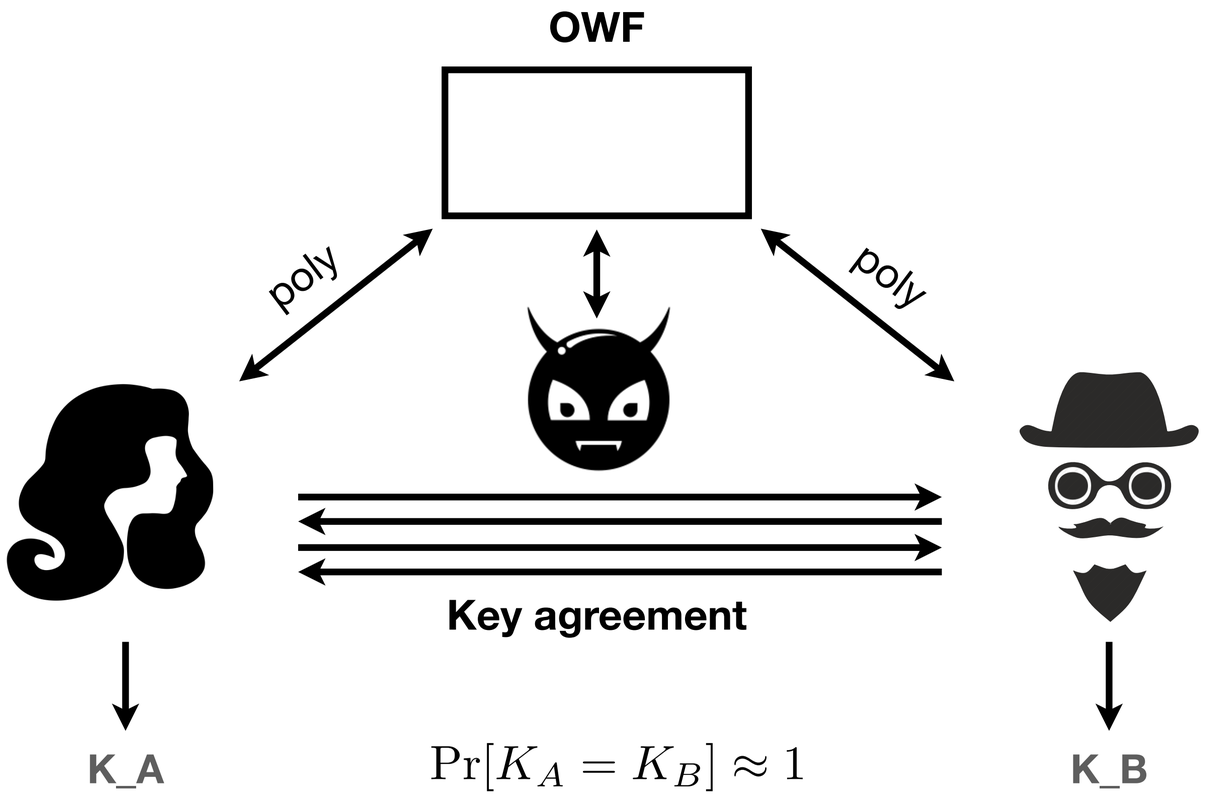
- The (Impagliazzo-Rudich 1989) black-box separation between one-way functions and key agreement
- Ruling out a natural candidate auxiliary primitive
- Our result and its caveats
- Overview of the proof

The Impagliazzo-Rudich Black-Box Separation

KA making black-box use of an arbitrary OWF:

- **Correctness:** $\Pr[K_A = K_B] \approx 1$
- Eve (😈) sees the transcript and queries the OWF
- **Efficiency:** A and B make poly many calls to the OWF

Construction is BB: works even with an *inefficient* implementation of the OWF.



The Impagliazzo-Rudich Black-Box Separation

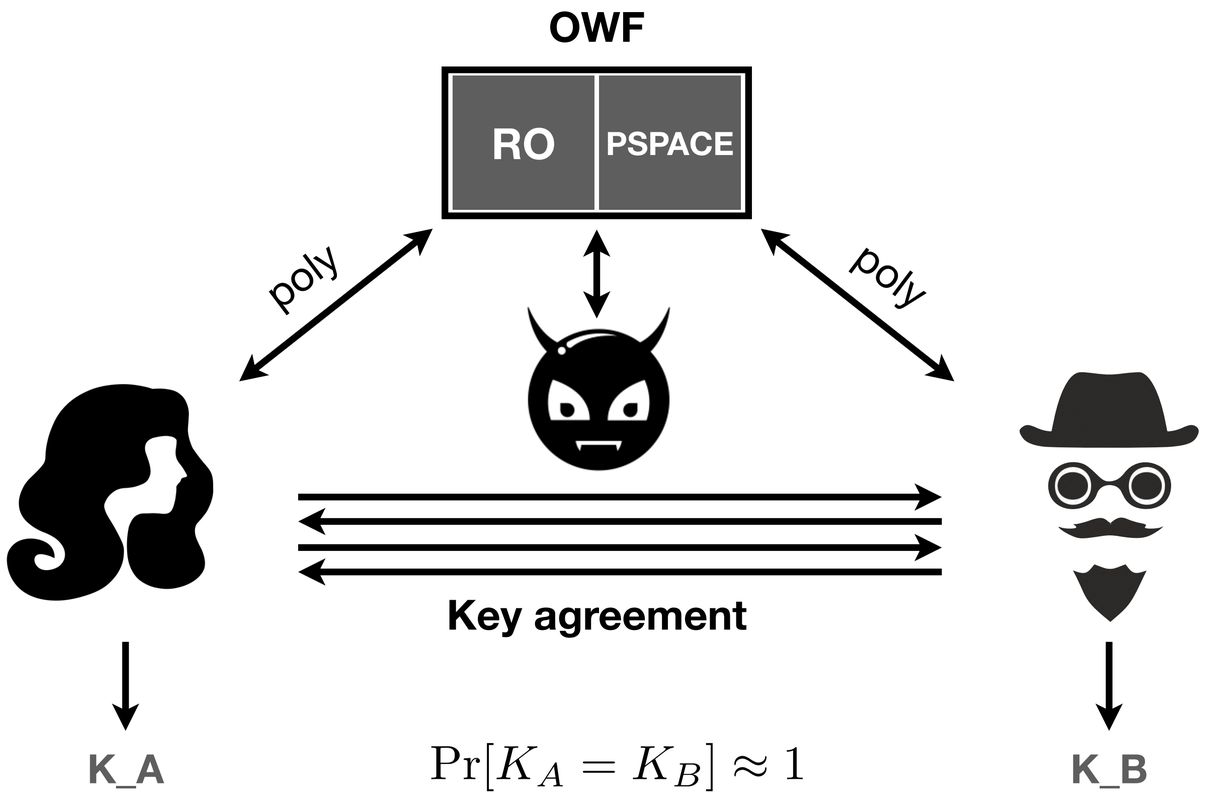
KA making black-box use of an arbitrary OWF:

- **Correctness:** $\Pr[K_A = K_B] \approx 1$
- Eve (😈) sees the transcript and queries the OWF
- **Efficiency:** A and B make poly many calls to the OWF

Construction is BB: works even with an *inefficient* implementation of the OWF.

Core idea: implement the OWF with a pair (random oracle, PSPACE oracle)

- [IR89]: a random oracle is one-way (works even in the presence of a PSPACE oracle)
- [IR89]: there is a **poly-query** attack against any such key agreement

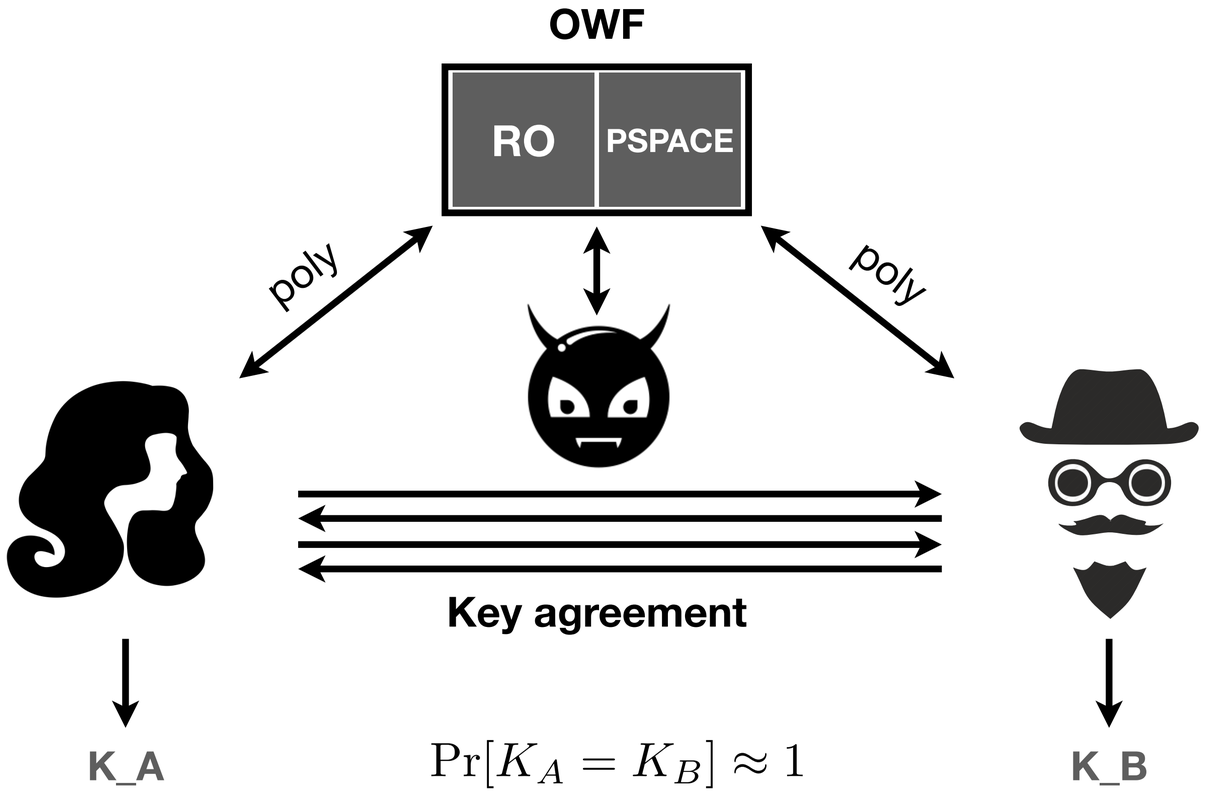


The Impagliazzo-Rudich Black-Box Separation

The [IR89] attack - [BKSY11] simplified version

- **Intuition:** queries that matter = those A & B are likely to both make in the same execution -> *intersection queries*
- **Step 1:** Eve samples views of Alice in many executions, using a *simulated* RO (consistent with previous queries from Eve to the true RO).
- **Step 2:** Eve makes all queries of A to the RO.
- **Step 3:** after 2*query_B+1 repetitions of Steps 1&2, output the majority key.

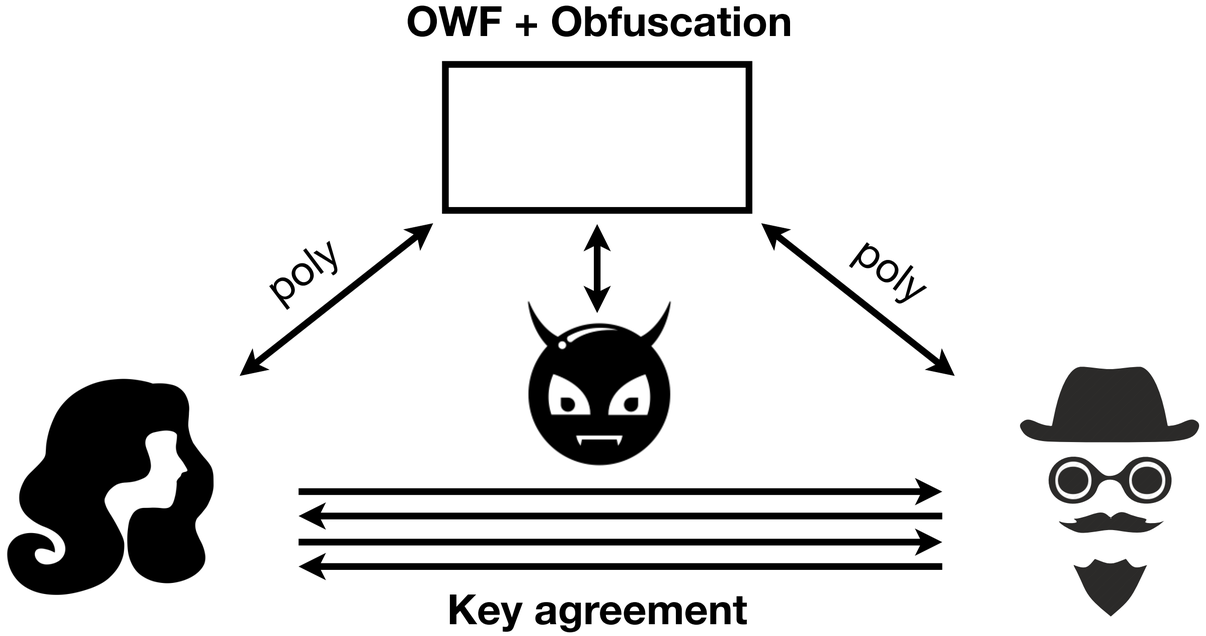
Eve makes O(query_A*query_B) queries. W.h.p she finds all intersection queries & computes the right bit in a majority of runs.



Are OWFs BBU for Key Agreement?

- If you are familiar with obfuscation, you might recall that obfuscation + OWF implies key agreement, but obfuscation alone does not.
- However, this construction is *non black-box.*
- Interesting observation: [IR89] already implies that this is inherent!

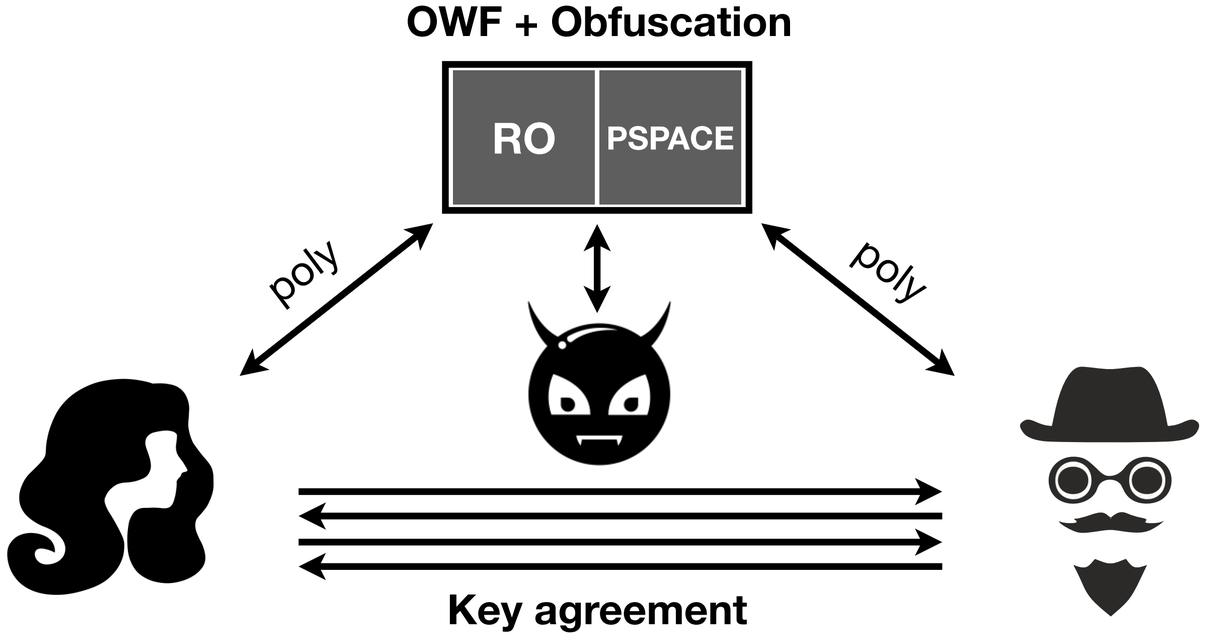
Observation: a PSPACE oracle implies an obfuscation oracle! (Use the PSPACE oracle to find the lexicographically first equivalent circuit) -> The [IR89] attacks already proves that OWF+iO does not BB imply key agreement.



Are OWFs BBU for Key Agreement?

- If you are familiar with obfuscation, you might recall that obfuscation + OWF implies key agreement, but obfuscation alone does not.
- However, this construction is *non black-box.*
- Interesting observation: [IR89] already implies that this is inherent!

Observation: a PSPACE oracle implies an obfuscation oracle! (Use the PSPACE oracle to find the lexicographically first equivalent circuit) -> The [IR89] attacks already proves that OWF+iO does not BB imply key agreement.



Are OWFs BBU for Key Agreement?

The ‘dream result’

For any primitive Z, if there exists a black-box construction of key agreement from an OWF and another primitive Z then there exists a black-box construction of key agreement from Z alone.

Are OWFs BBU for Key Agreement?

The ‘dream result’

For any primitive Z, if there exists a black-box construction of key agreement from an OWF and another primitive Z then there exists a black-box construction of key agreement from Z alone.

The caveats

- (in blue) as an artifact of our proof techniques, it only applies to *infinitely-often* OWFs (which are only guaranteed to be secure on infinitely-many security parameters)
- (In red) it only rules out a restricted family of constructions, where one party makes a constant number of queries to the random oracle (but any number of queries to Z)

Are OWFs BBU for Key Agreement?

The ‘dream result’

For any primitive Z, if there exists a black-box construction of (possibly i.o.-) key agreement from an infinitely-often OWF and another primitive Z

then there exists a black-box construction of (possibly i.o.-) key agreement from Z alone.

The caveats

- (in blue) as an artifact of our proof techniques, it only applies to *infinitely-often* OWFs (which are only guaranteed to be secure on infinitely-many security parameters)
- (In red) it only rules out a restricted family of constructions, where one party makes a constant number of queries to the random oracle (but any number of queries to Z)

Are OWFs BBU for Key Agreement?

The ‘dream result’

For any primitive Z, if there exists a black-box construction of (possibly i.o.-) key agreement from an infinitely-often OWF and another primitive Z where one of the parties makes a constant number of queries to the OWF, then there exists a black-box construction of (possibly i.o.-) key agreement from Z alone.

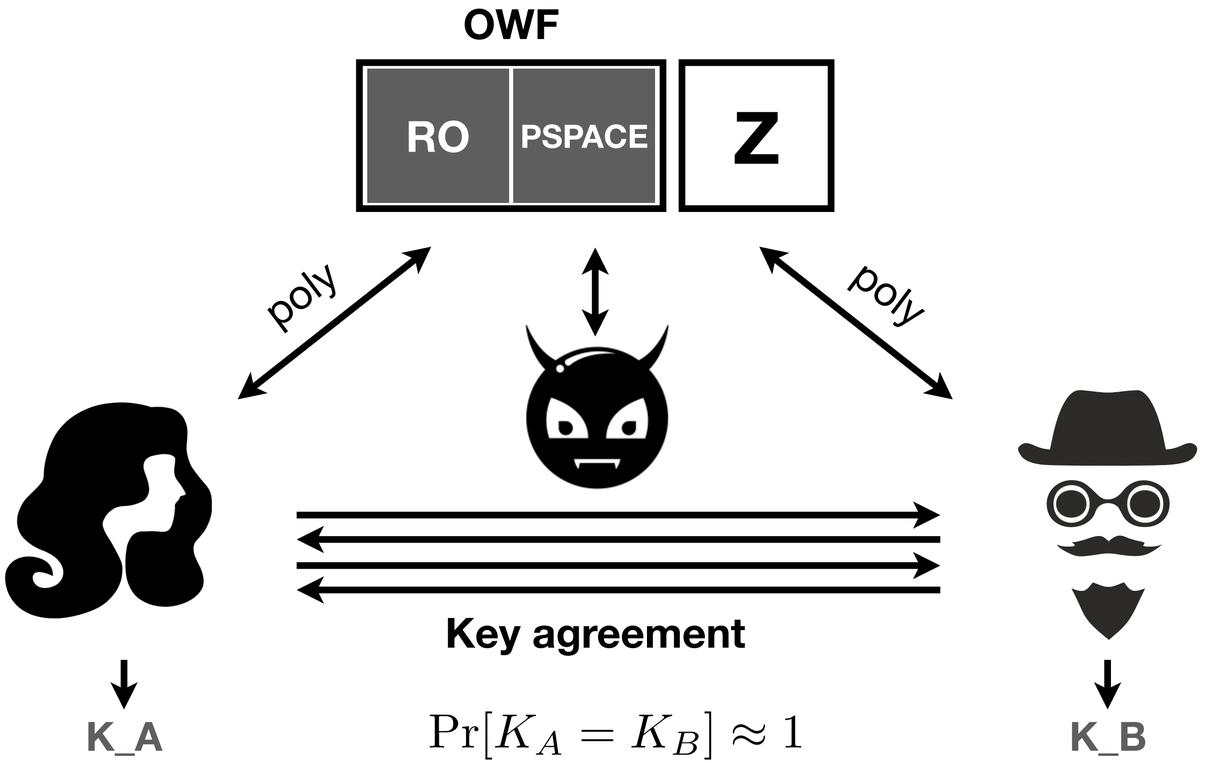
The caveats

- (in blue) as an artifact of our proof techniques, it only applies to *infinitely-often* OWFs (which are only guaranteed to be secure on infinitely-many security parameters)
- (In red) it only rules out a restricted family of constructions, where one party makes a constant number of queries to the random oracle (but any number of queries to Z)

Are OWFs BBU for Key Agreement?

A and B have access to a OWF and an auxiliary oracle Z. Start from [IR89]:

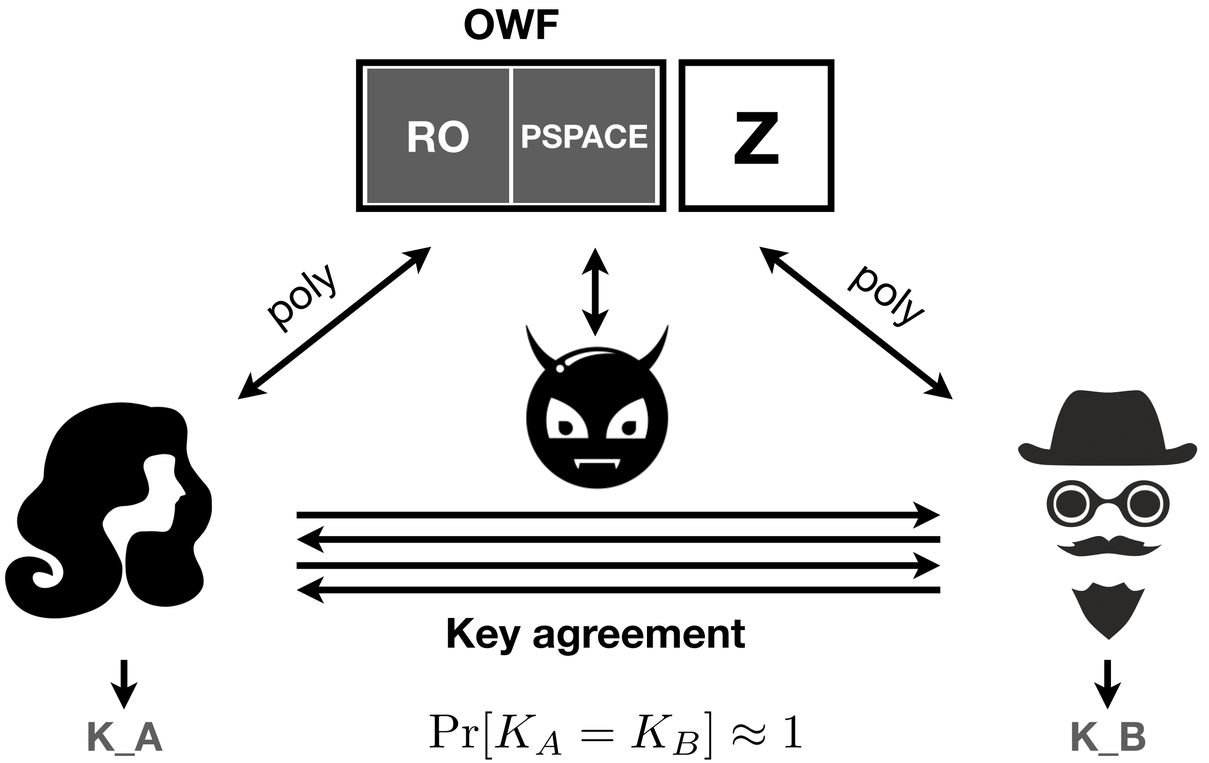
- Implement the OWF with RO+PSPACE
- Eve creates many views of A in her head w.r.t. a simulated RO *and the true oracle Z.*
- **Issue:** this could require exponentially many calls to Z (which is *not* simulated)!
- **Core observation:** sampling a view consistent with a transcript amounts to *sampling a preimage of an efficient function of Z.*



Are OWFs BBU for Key Agreement?

A and B have access to a OWF and an auxiliary oracle Z. Start from [IR89]:

- Implement the OWF with RO+PSPACE
- Eve creates many views of A in her head w.r.t. a simulated RO *and the true oracle Z.*
- **Issue:** this could require exponentially many calls to Z (which is *not* simulated)!
- **Core observation:** sampling a view consistent with a transcript amounts to *sampling a preimage of an efficient function of Z.*



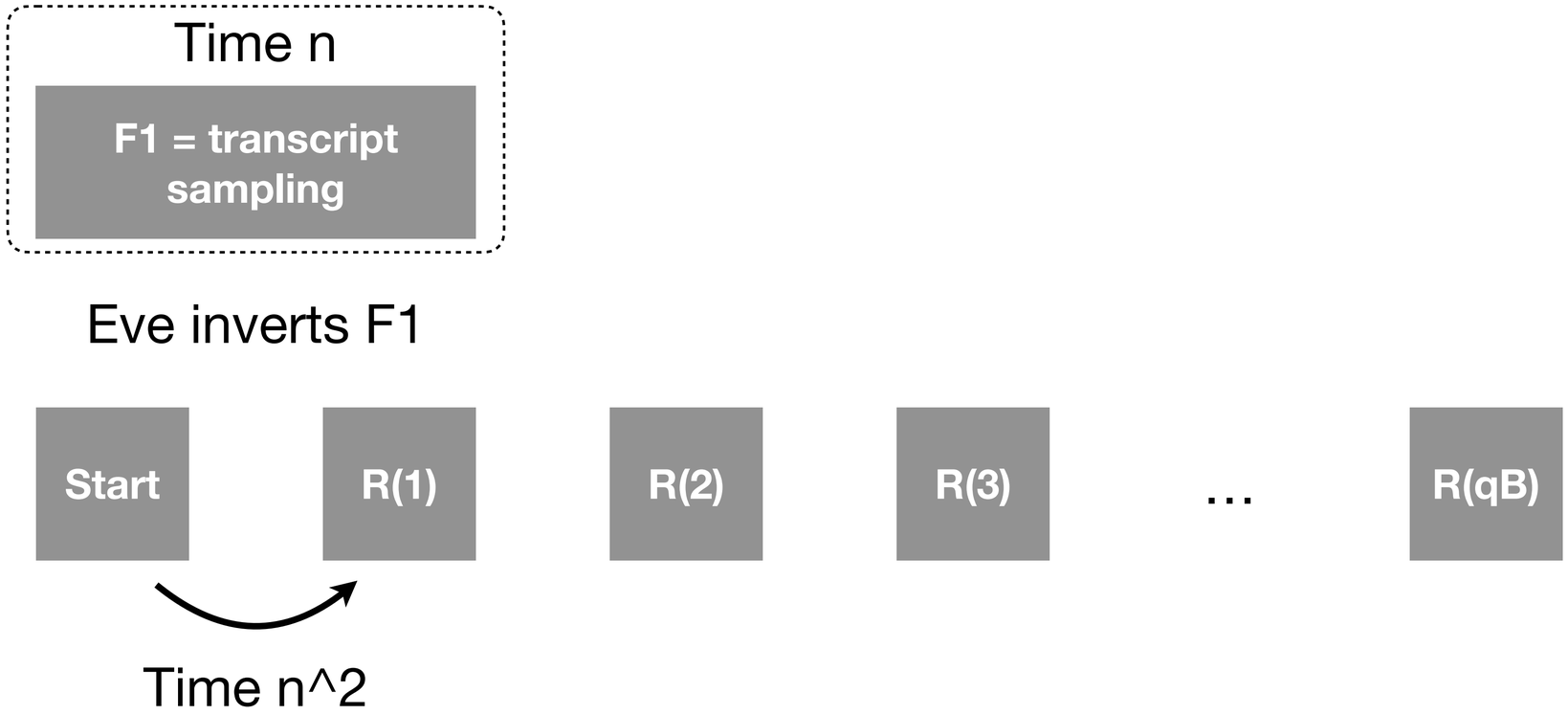
Core idea. We make a case disjunction:

- Either there exists no OWF relative to Z; in which case, the preimage sampling can be implemented efficiently;
- Or there exists a OWF relative to Z, in which case we get a key agreement from Z alone by implementing the OWF from Z!

Are OWFs BBU for Key Agreement?

Caveat 1: Bob must make a constant number of queries.

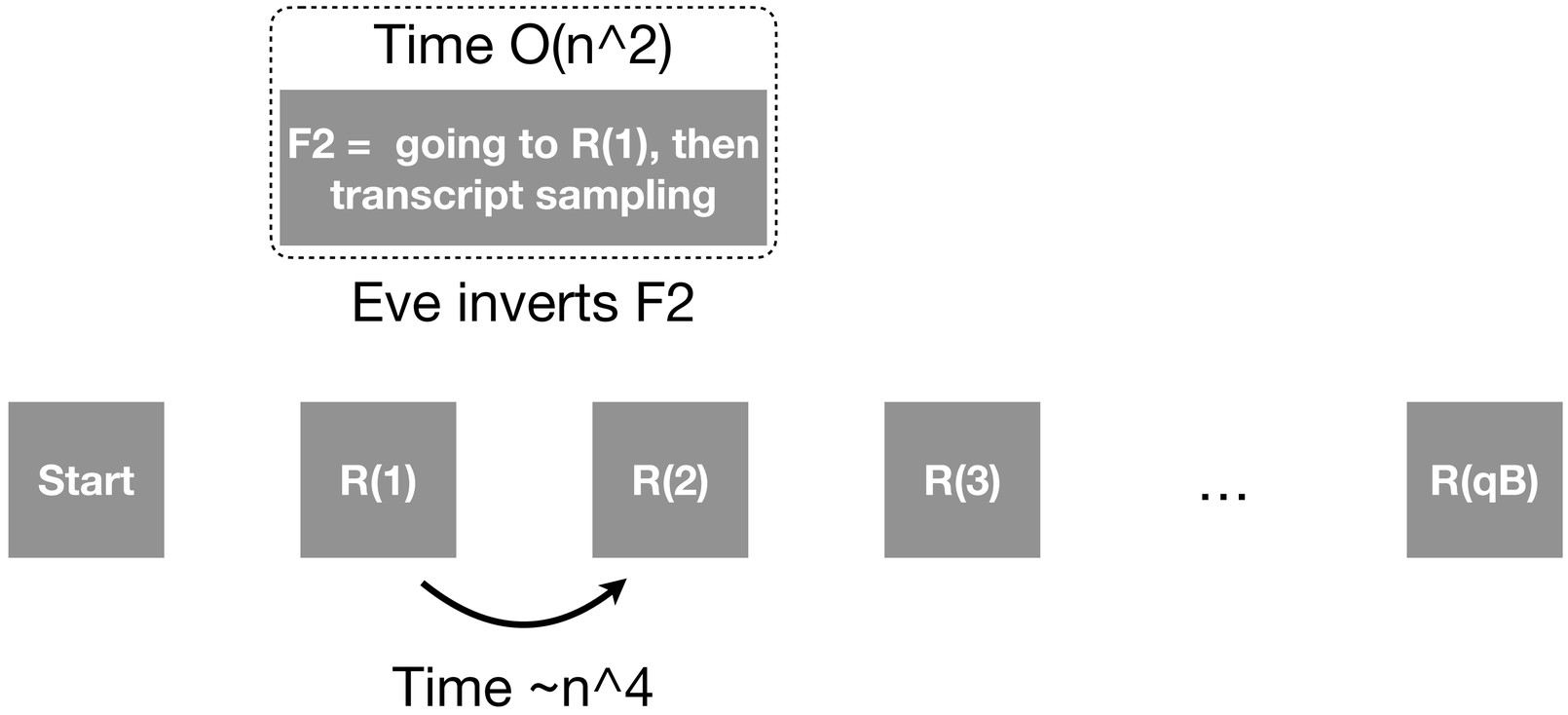
Suppose for simplicity that any N-query OWF can be inverted in N^2 queries to Z:



Are OWFs BBU for Key Agreement?

Caveat 1: Bob must make a constant number of queries.

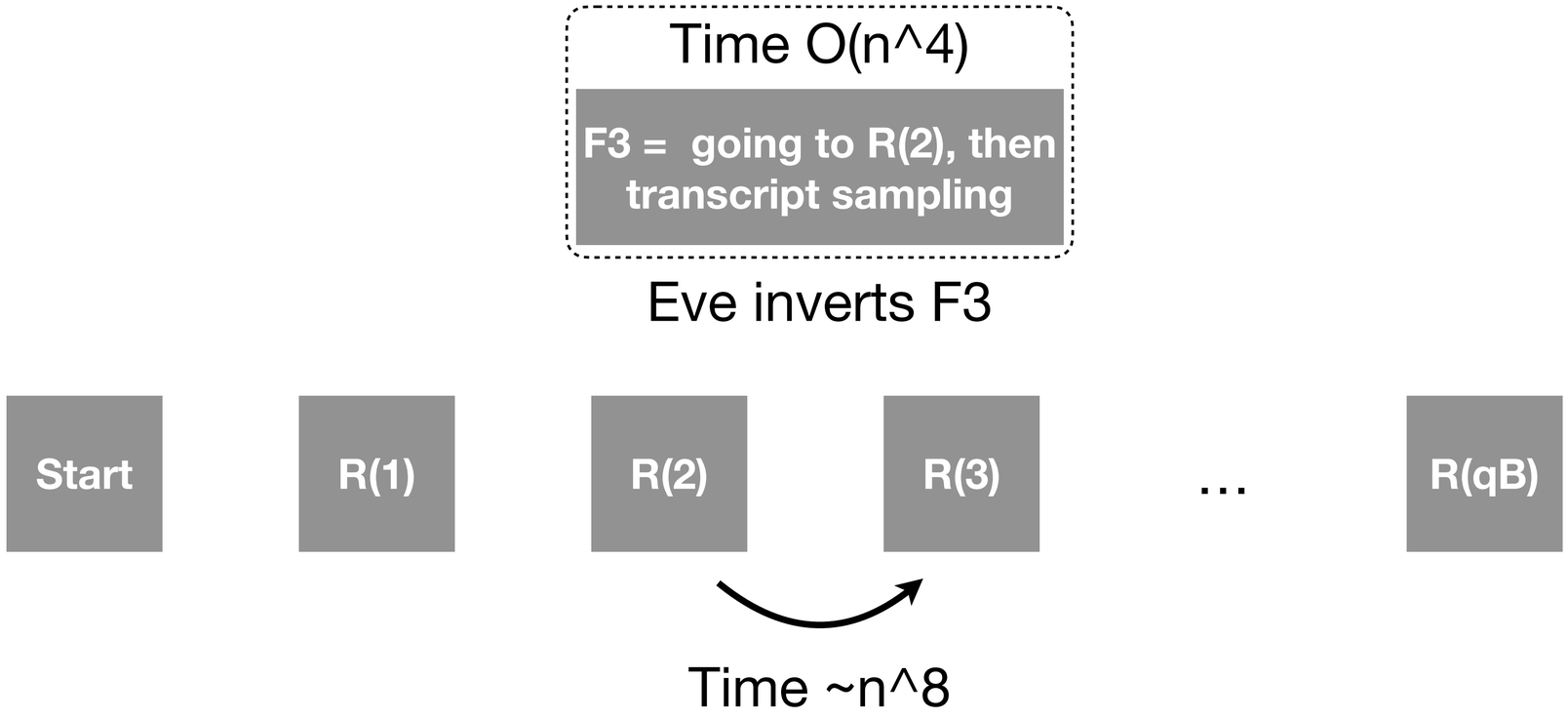
Suppose for simplicity that any N-query OWF can be inverted in N^2 queries to Z:



Are OWFs BBU for Key Agreement?

Caveat 1: Bob must make a constant number of queries.

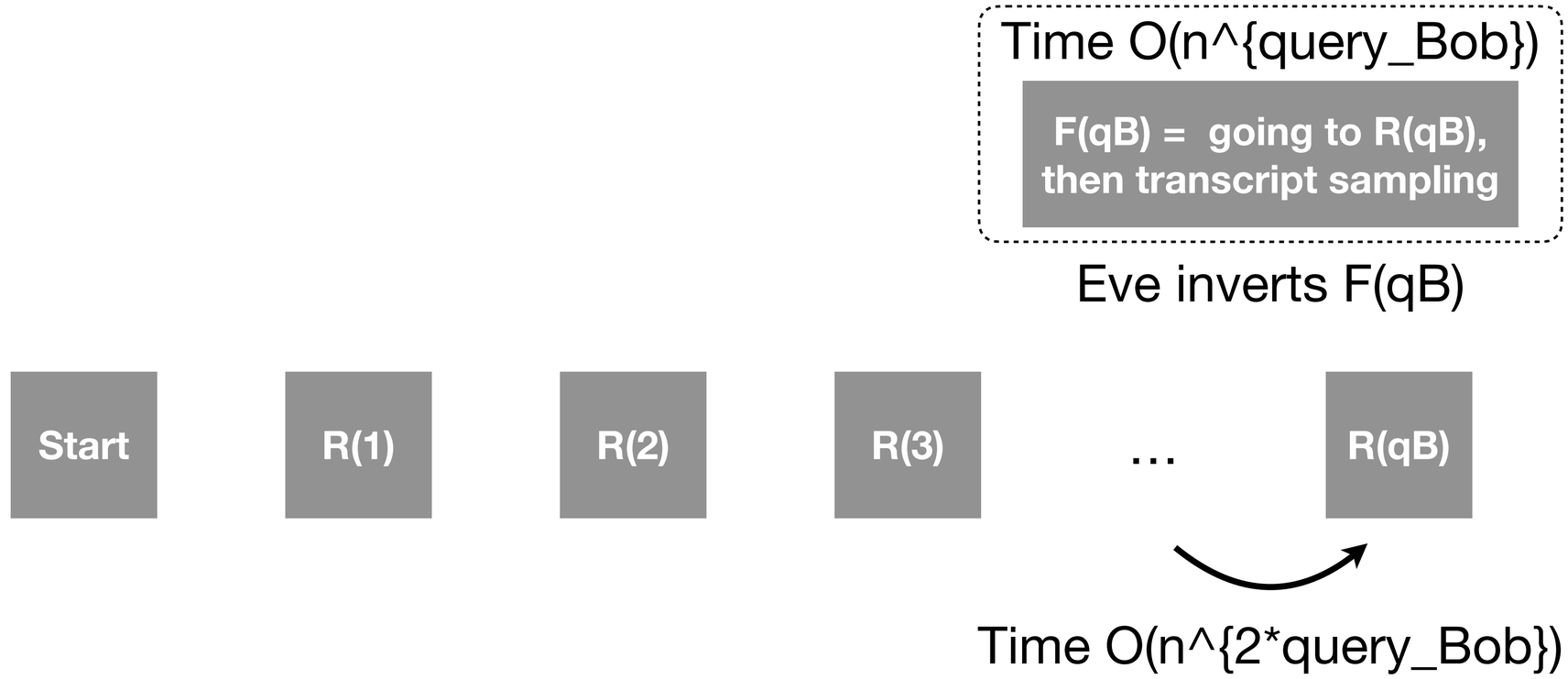
Suppose for simplicity that any N-query OWF can be inverted in N^2 queries to Z:



Are OWFs BBU for Key Agreement?

Caveat 1: Bob must make a constant number of queries.

Suppose for simplicity that any N-query OWF can be inverted in N^2 queries to Z:



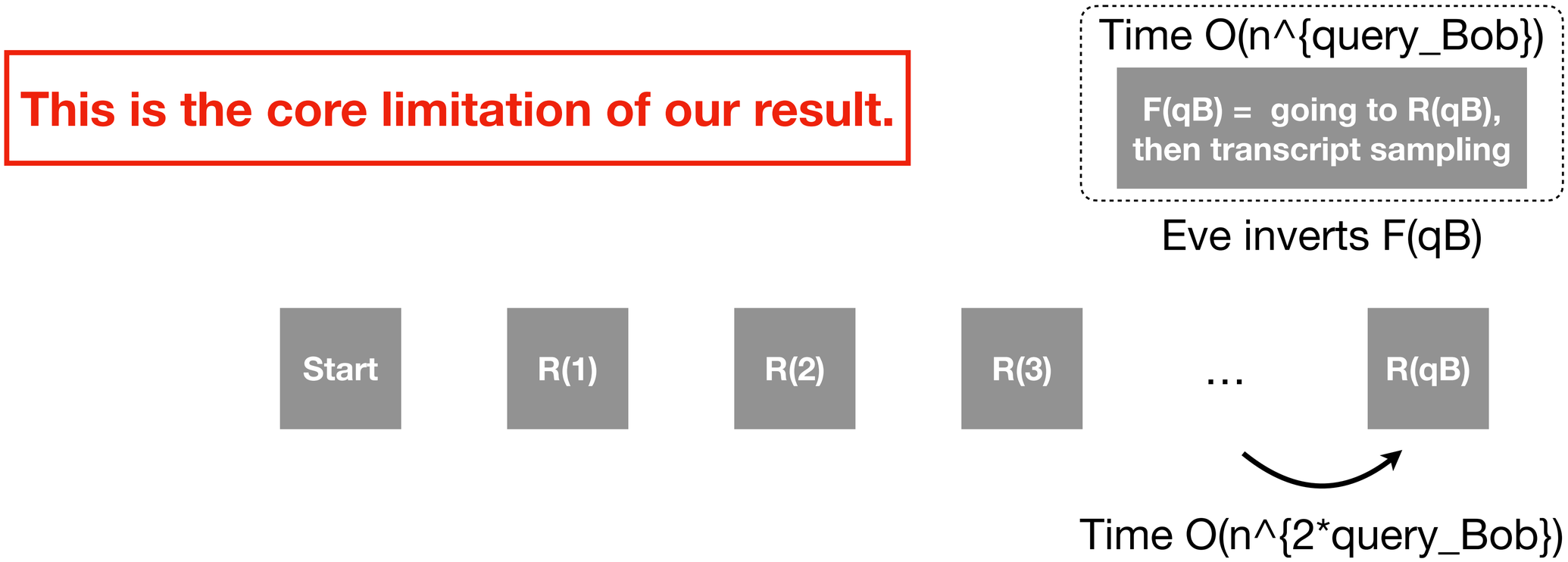
The time (= queries to Z) grows exponentially with query_Bob!

Are OWFs BBU for Key Agreement?

Caveat 1: Bob must make a constant number of queries.

Suppose for simplicity that any N-query OWF can be inverted in N^2 queries to Z:

This is the core limitation of our result.



The time (= queries to Z) grows exponentially with query_Bob!

Are OWFs BBU for Key Agreement?

Caveat 2: restricted to *infinitely-often* one-way functions

Recall that Eve must invert O(query_Bob) OWFs relative to Z.

- *Inexistence of OWFs relative to Z* only implies an *infinitely-often* OWF inverter.
- No guarantee that there is a security parameter s.t. we can invert all OWFs simultaneously!
- **Way around:** case distinction based on the existence of i.o.-OWFs relative to Z (their inexistence gives an *almost-everywhere* inverter for any OWF)

Note that there is no known example of black-box reductions that does not translate directly to the infinitely-often regime, hence the result remains meaningful.

Open Questions

Open Questions

- Can we extend our result to all key agreement protocols?

  We conjecture that the answer is yes
- Which other separation techniques can be extended to the BBU setting?
- Can we prove that OWFs are black-box *helpful* for collision-resistant hash functions?

Thanks for your attention!

summary of our results:

Definitions, composition

- We define *black-box uselessness*, which strengthens black-box separations and makes them composable.

Are OWFs BBU for key agreement?

- We provide preliminary results indicating that OWFs are perhaps BBU for key agreement.

Extending existing separations to the BBU regime

- We show that a large class of existing methods for black-box separations can be generalized to the BBU setting.

Are OWFs BB *helpful* for CRHFs?

- We identify collision-resistant hashing as a primitive for which OWFs are plausibly *not* BBU, even though they are black-box separated.