Non-Observable Quantum Random Oracle Model

Varun Maram
Applied Cryptography Group
ETH Zurich

APPLIED CRYPTO GROUP

Joint work with Navid Alamati and Daniel Masny

[Full version of paper: https://eprint.iacr.org/2023/1126.pdf]

NO QROM(!)

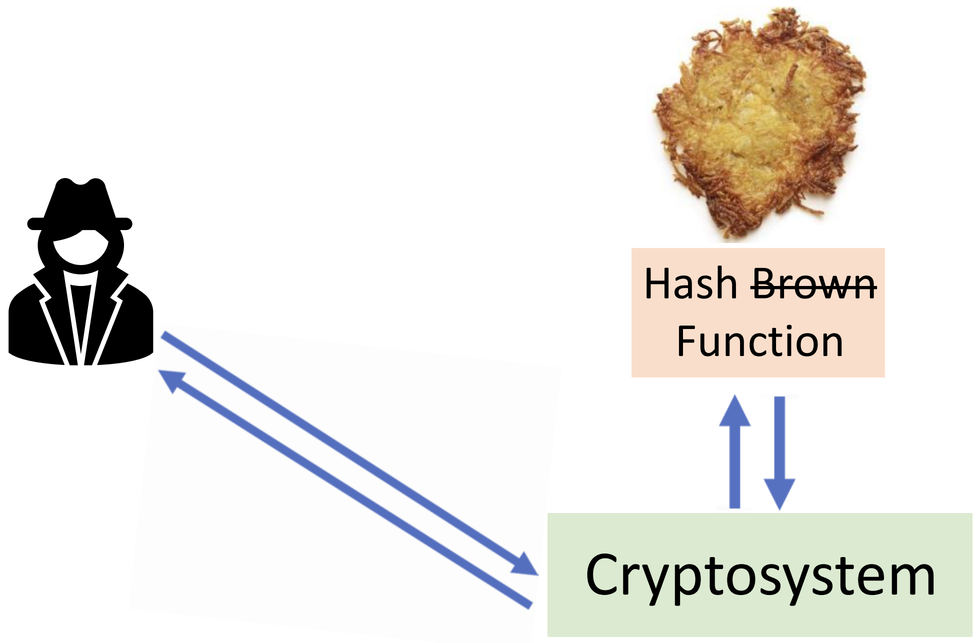
Varun Maram
Applied Cryptography Group
ETH Zurich

APPLIED CRYPTO GROUP

Joint work with Navid Alamati and Daniel Masny

[Full version of paper: https://eprint.iacr.org/2023/1126.pdf]

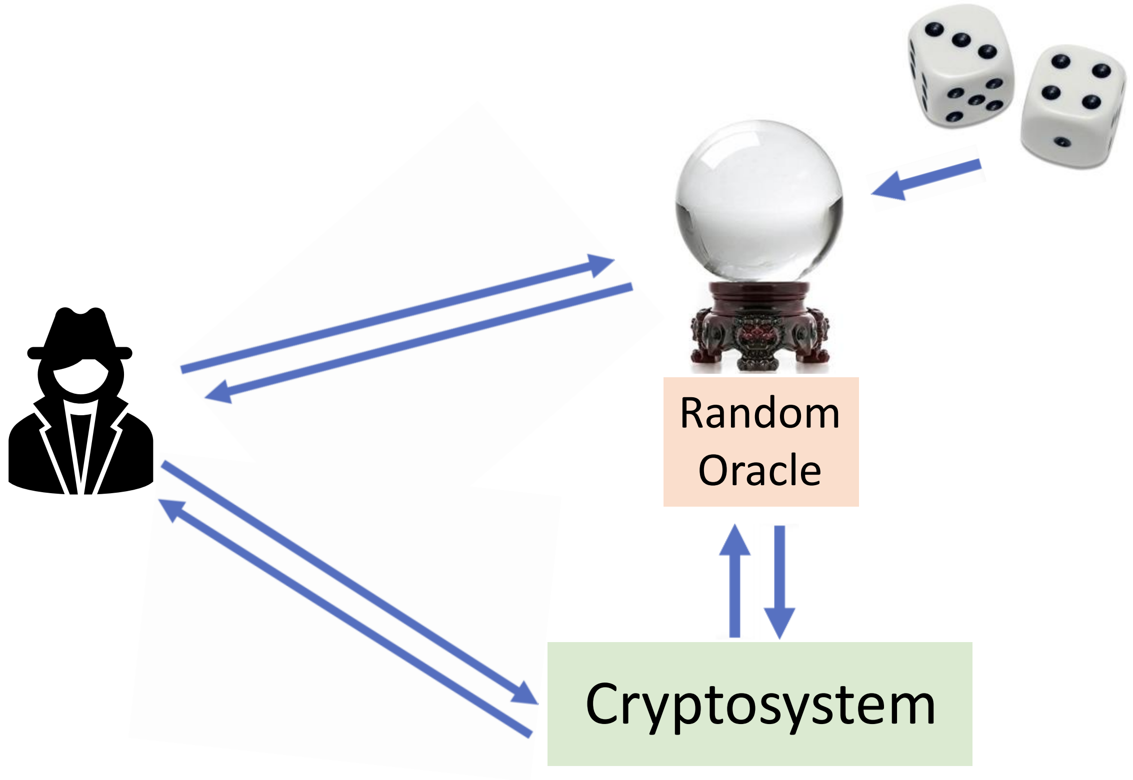
Random Oracle Model (ROM)



- Formalized by [Bellare-Rogaway'93].

(Inspired by Mark Zhandry's slides on the QROM at the 11th BIU Winter School on Cryptography.)

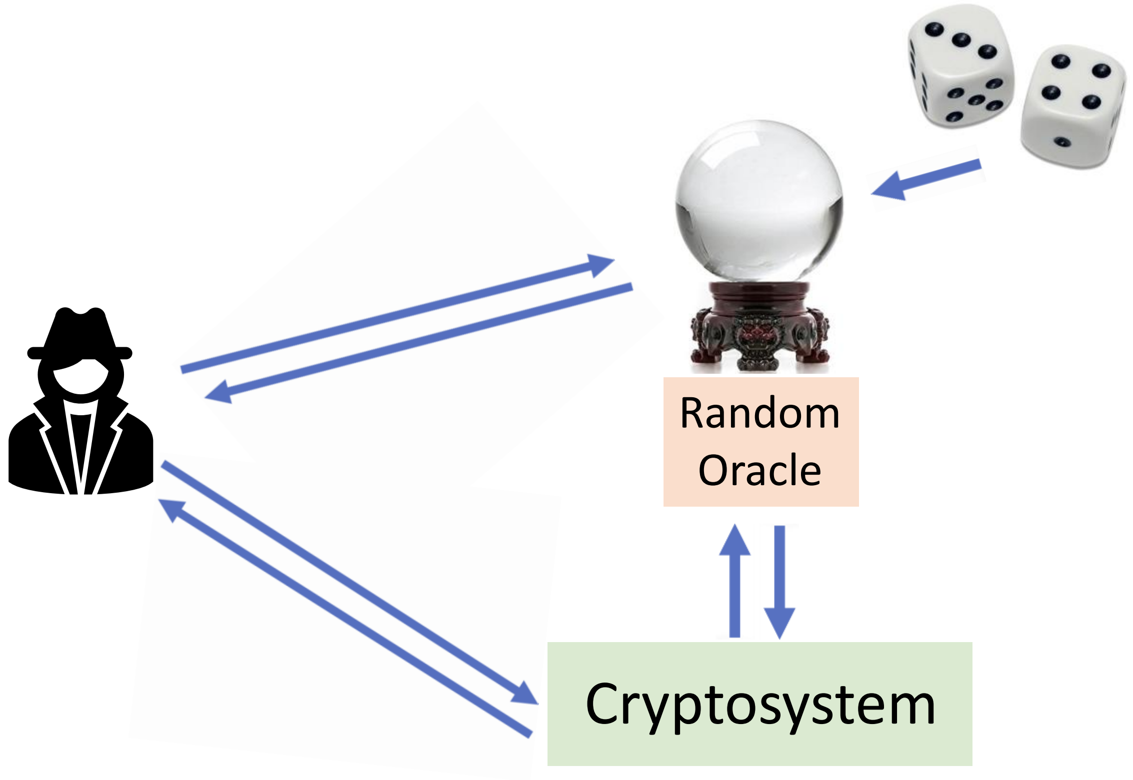
Random Oracle Model (ROM)



- Formalized by [Bellare-Rogaway'93].

(Inspired by Mark Zhandry's slides on the QROM at the 11th BIU Winter School on Cryptography.)

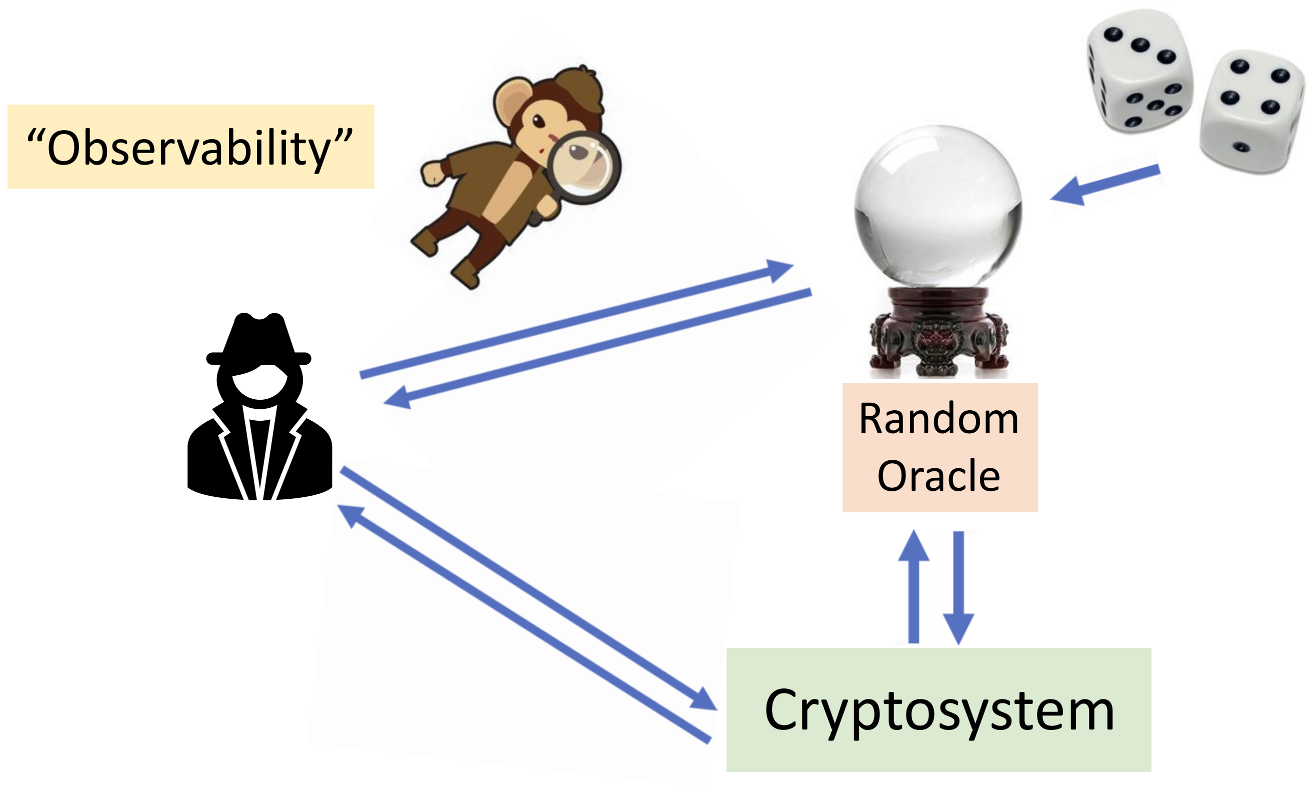
Random Oracle Model (ROM)



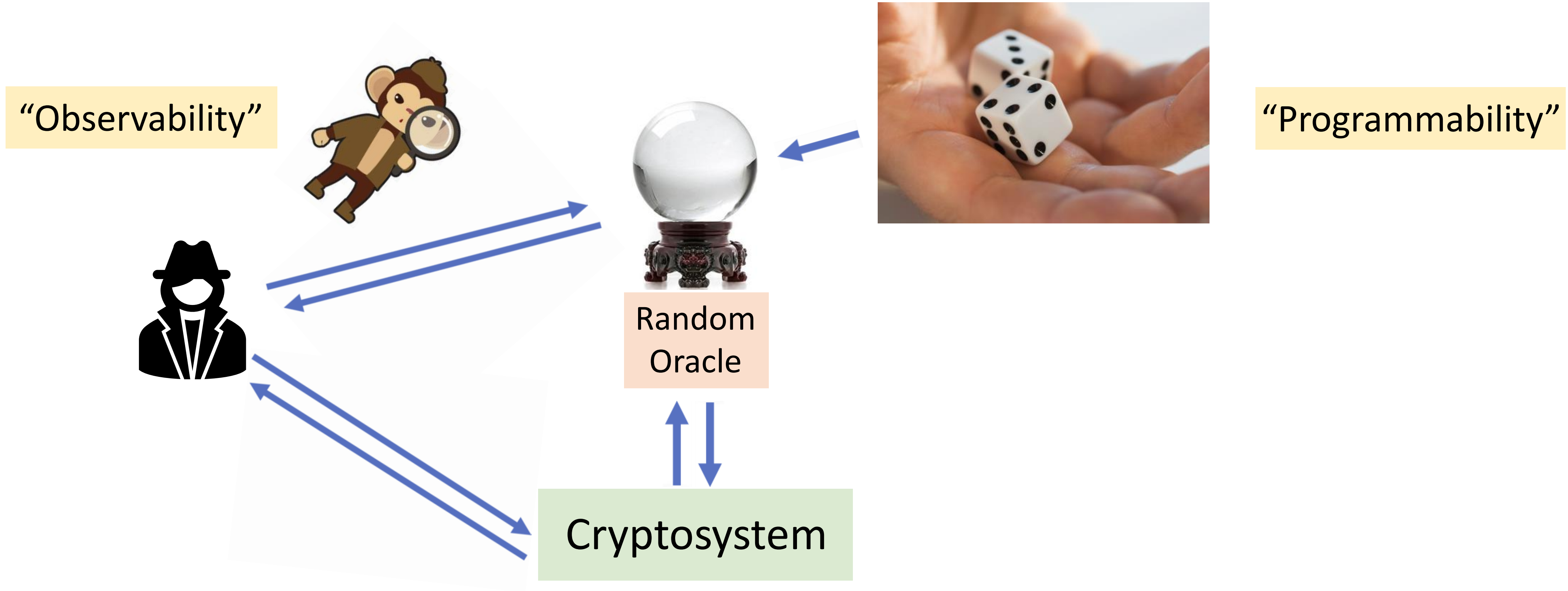
- Formalized by [Bellare-Rogaway'93].
- Highly influential model to argue <u>heuristic</u> security of efficient and practical cryptosystems.

(Inspired by Mark Zhandry's slides on the QROM at the 11th BIU Winter School on Cryptography.)

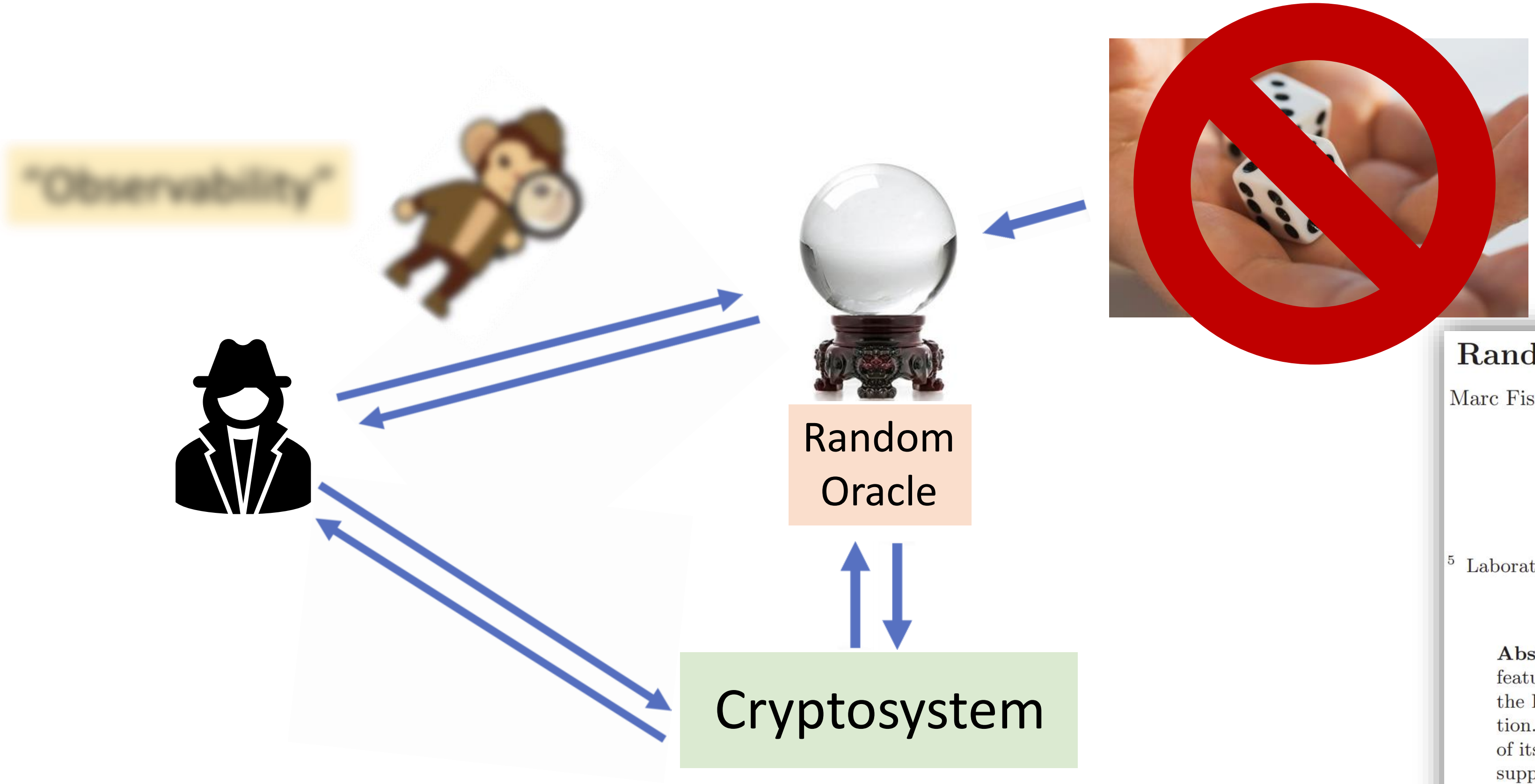
Random Oracle Model (ROM)



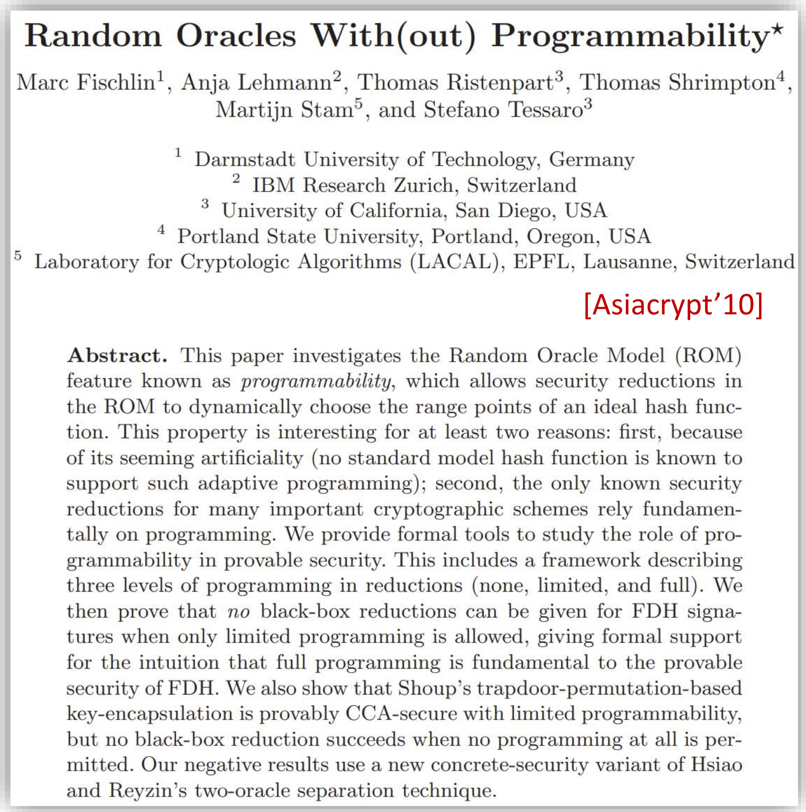
Random Oracle Model (ROM)



Random Oracle Model (ROM)



"Non-Programmability"



Random Oracles With(out) Programmability*

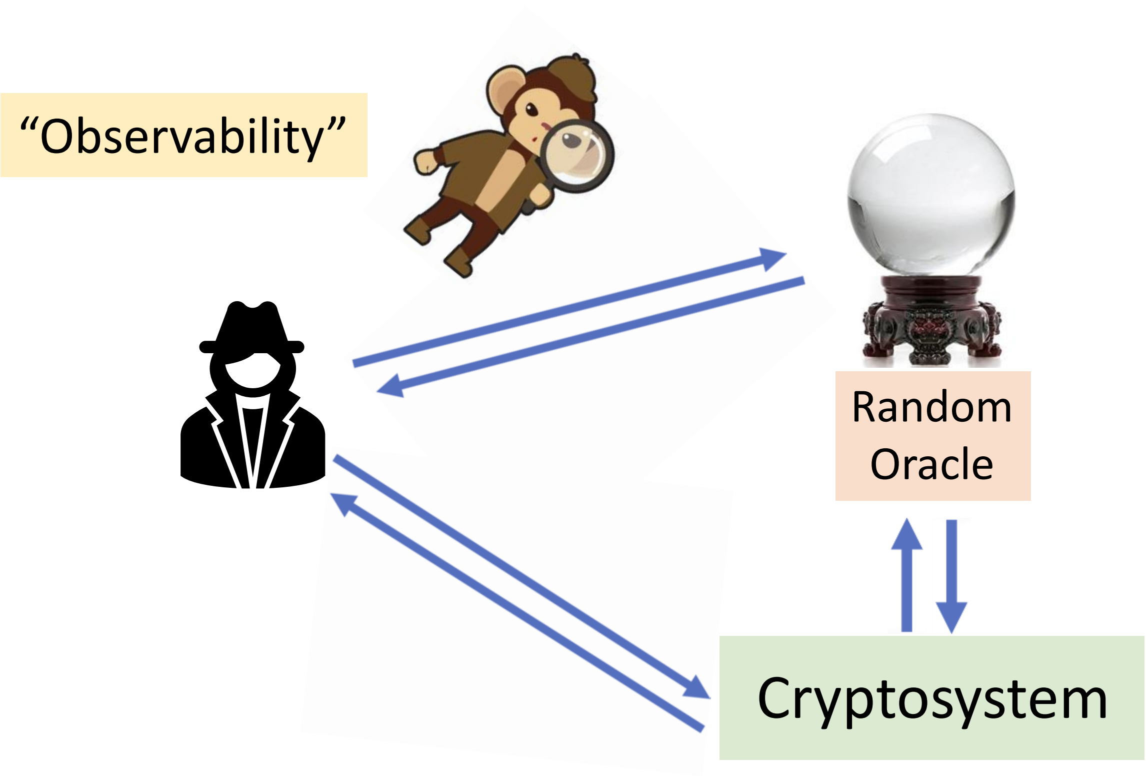
Marc Fischlin[1], Anja Lehmann[2], Thomas Ristenpart[3], Thomas Shrimpton[4], Martijn Stam[5], and Stefano Tessaro[3]

[1] Darmstadt University of Technology, Germany
[2] IBM Research Zurich, Switzerland
[3] University of California, San Diego, USA
[4] Portland State University, Portland, Oregon, USA
[5] Laboratory for Cryptologic Algorithms (LACAL), EPFL, Lausanne, Switzerland

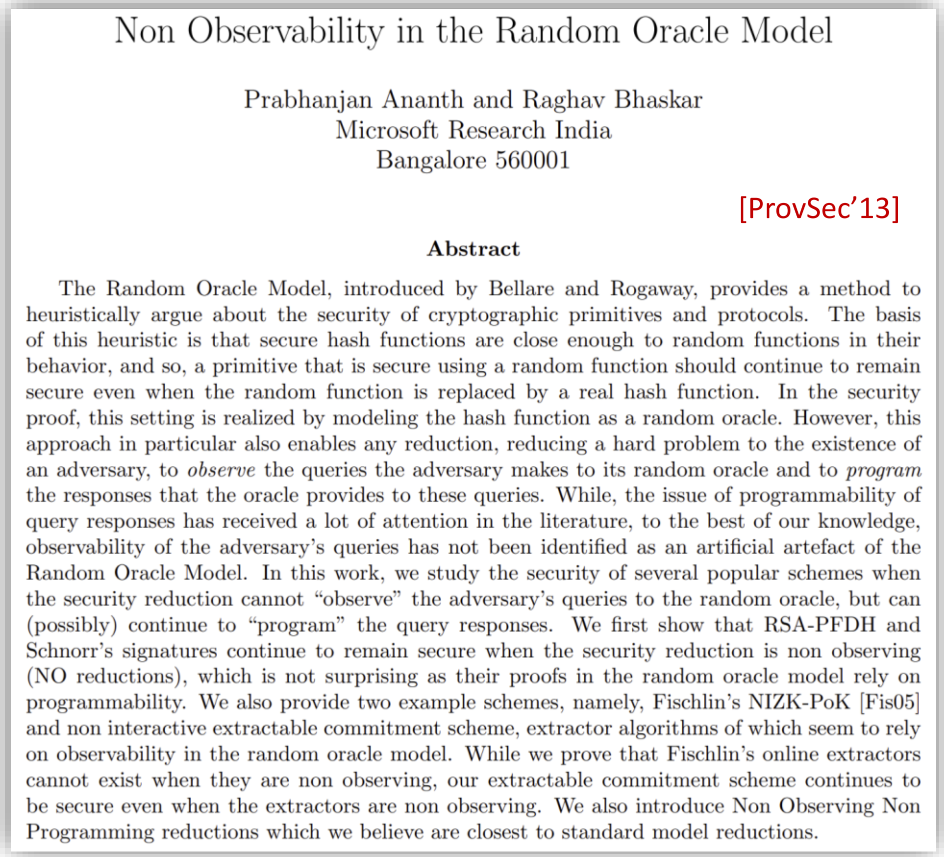
[Asiacrypt'10]

Abstract. This paper investigates the Random Oracle Model (ROM) feature known as *programmability*, which allows security reductions in the ROM to dynamically choose the range points of an ideal hash function. This property is interesting for at least two reasons: first, because of its seeming artificiality (no standard model hash function is known to support such adaptive programming); second, the only known security reductions for many important cryptographic schemes rely fundamentally on programming. We provide formal tools to study the role of programmability in provable security. This includes a framework describing three levels of programming in reductions (none, limited, and full). We then prove that *no* black-box reductions can be given for FDH signatures when only limited programming is allowed, giving formal support for the intuition that full programming is fundamental to the provable security of FDH. We also show that Shoup's trapdoor-permutation-based key-encapsulation is provably CCA-secure with limited programmability, but no black-box reduction succeeds when no programming at all is permitted. Our negative results use a new concrete-security variant of Hsiao and Reyzin's two-oracle separation technique.

Random Oracle Model (ROM)



Non-Observable ROM (NO ROM)



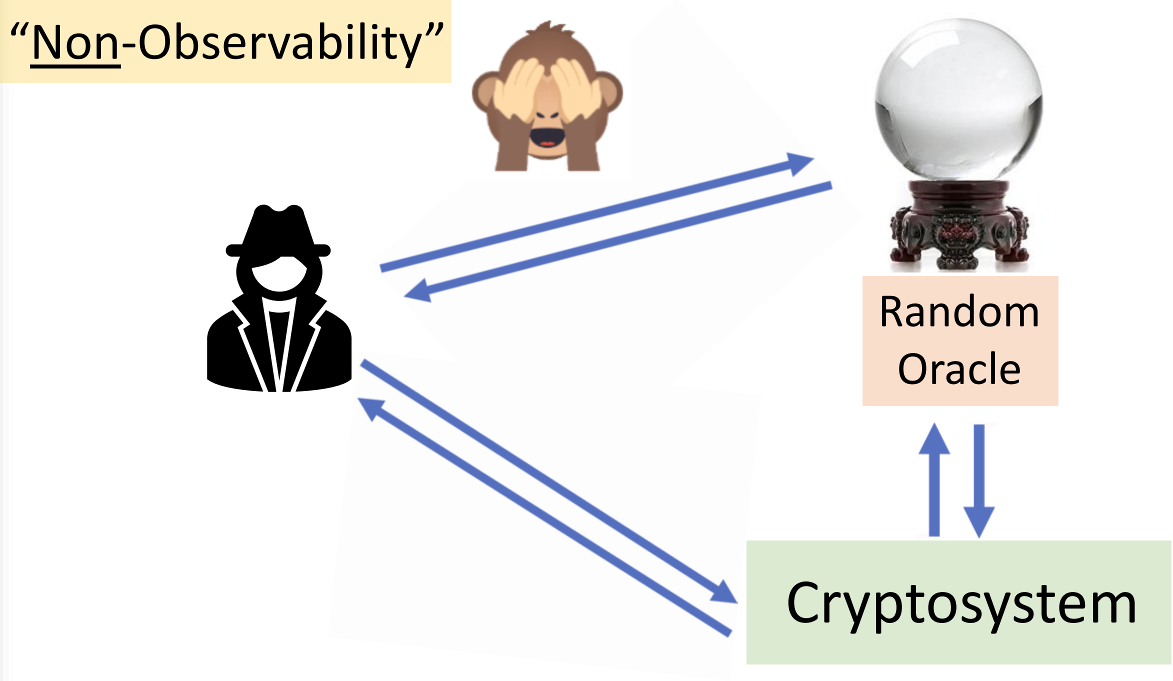
Non Observability in the Random Oracle Model

Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

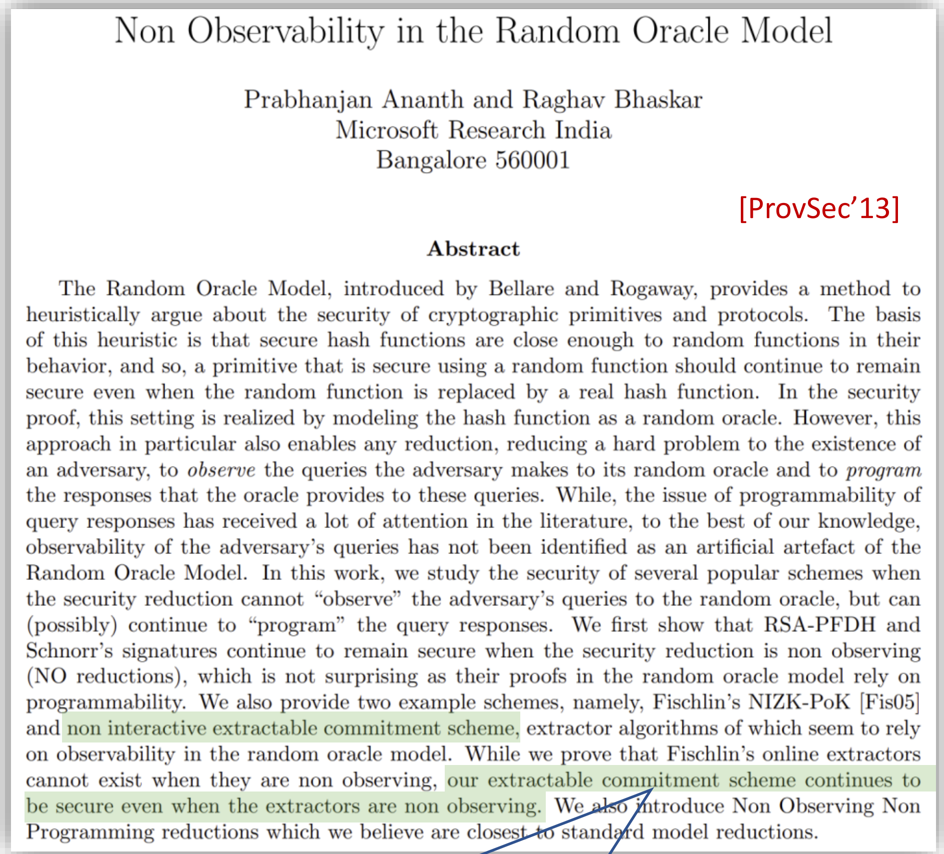
[ProvSec'13]

Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.



Non-Observable ROM (NO ROM)



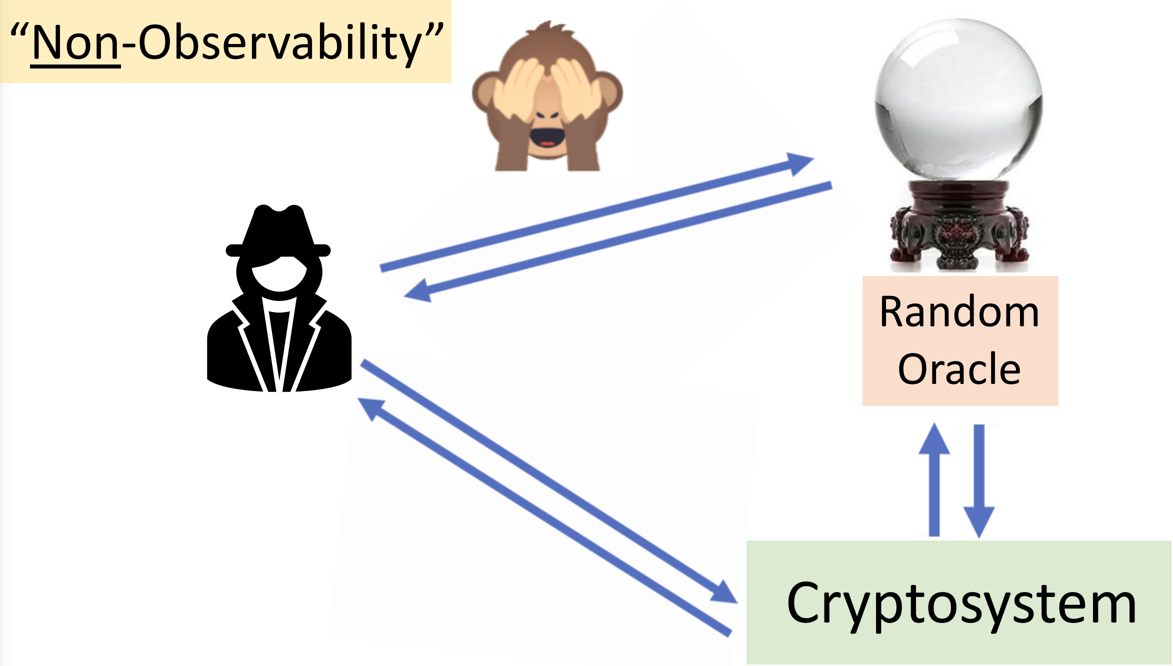
Non Observability in the Random Oracle Model

Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

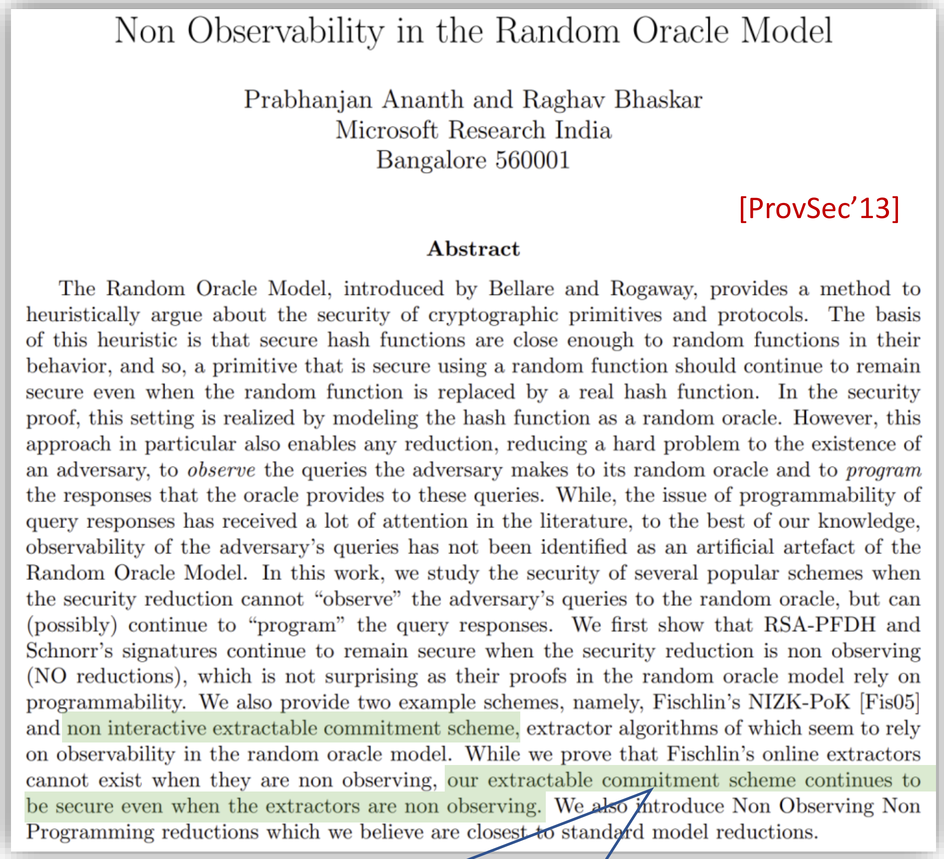
Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.



Construct a hash-based extractable commitment in the NO ROM.

Non-Observable ROM (NO ROM)



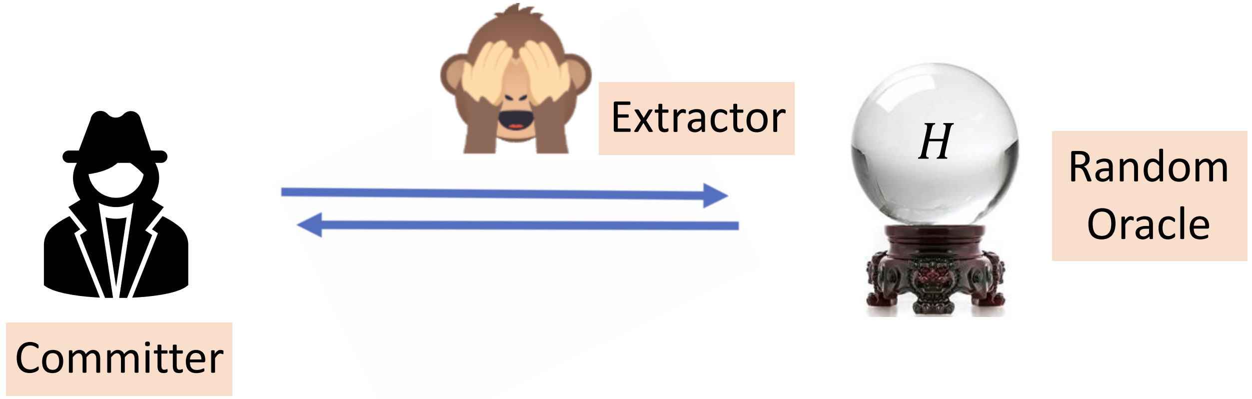
Non Observability in the Random Oracle Model

Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

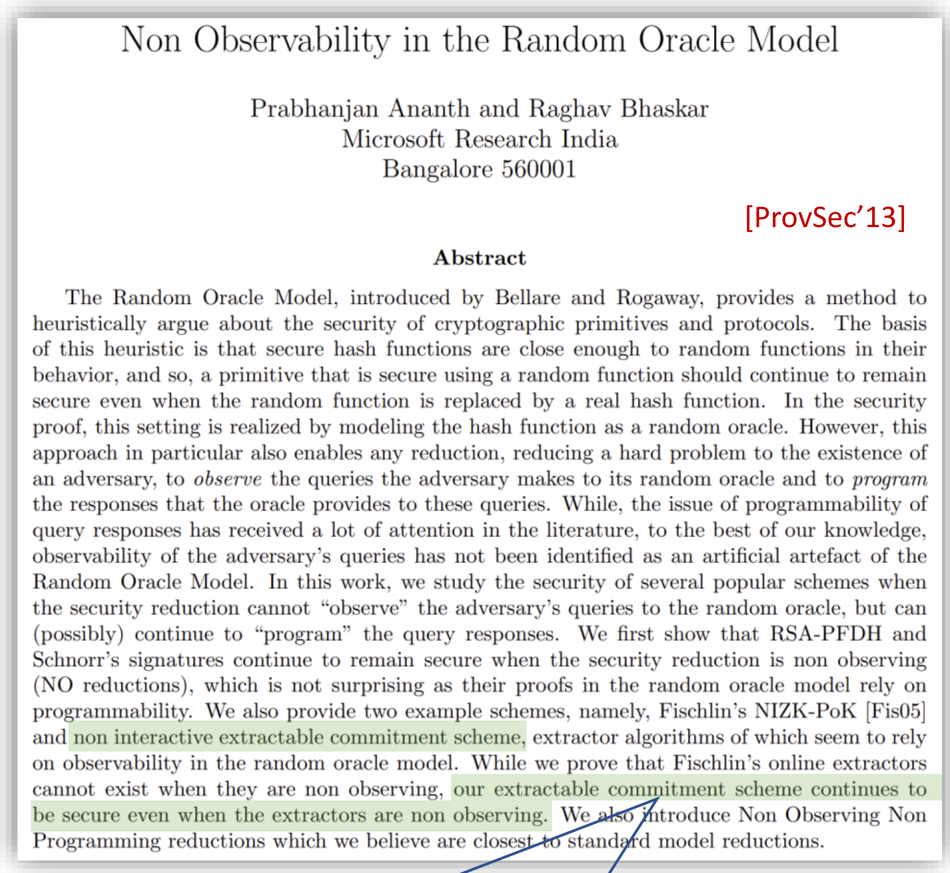
Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.



Construct a hash-based extractable commitment in the NO ROM.

Non-Observable ROM (NO ROM)



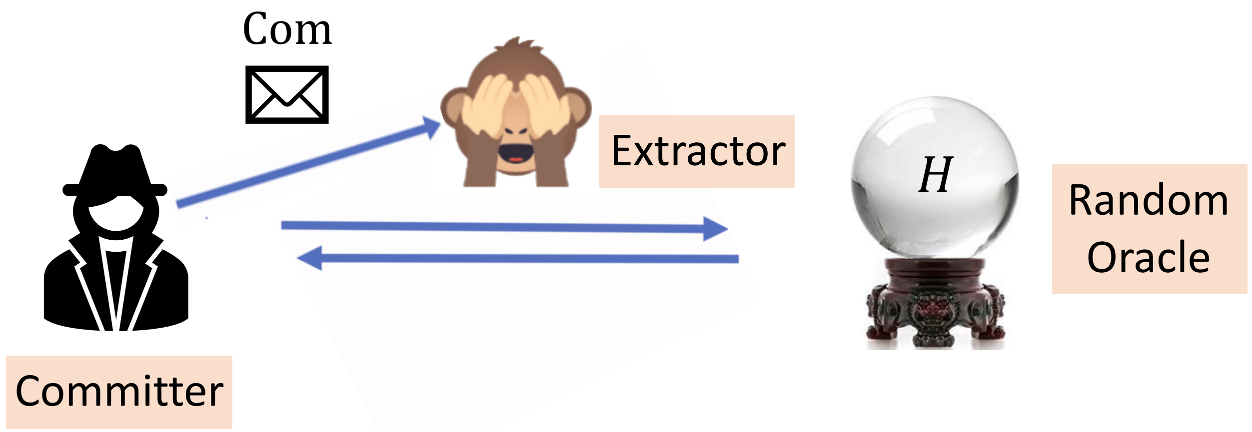
Non Observability in the Random Oracle Model

Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

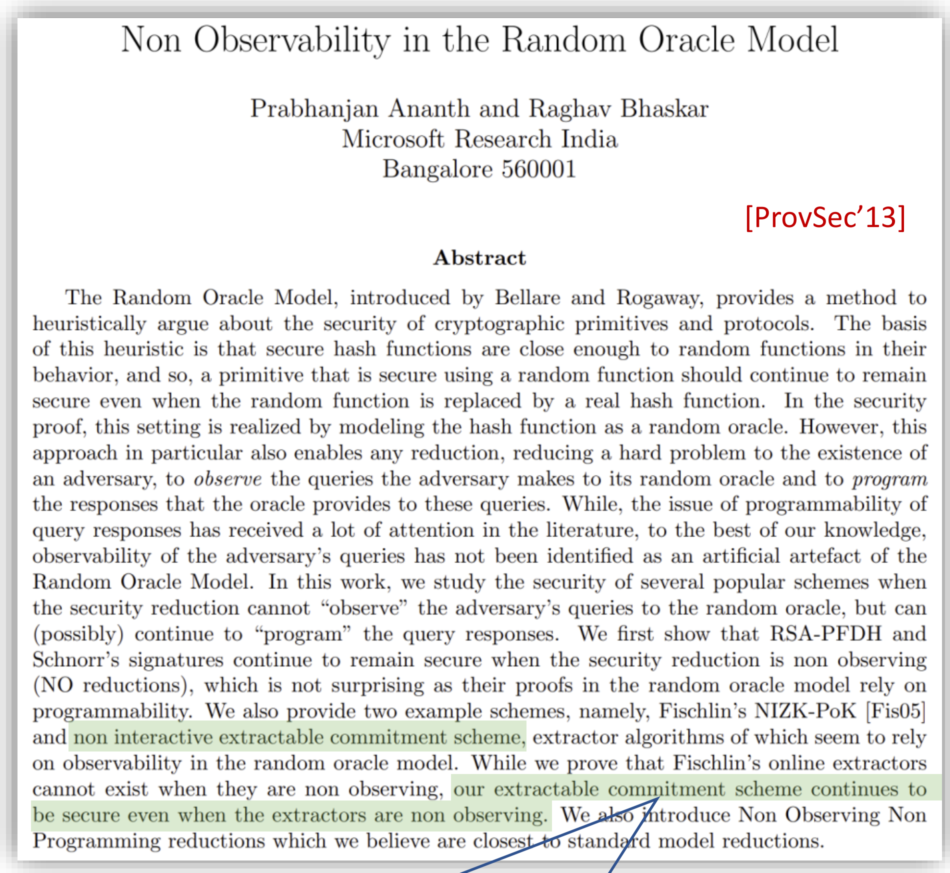
Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.



Construct a hash-based extractable commitment in the NO ROM.

Non-Observable ROM (NO ROM)


Non Observability in the Random Oracle Model

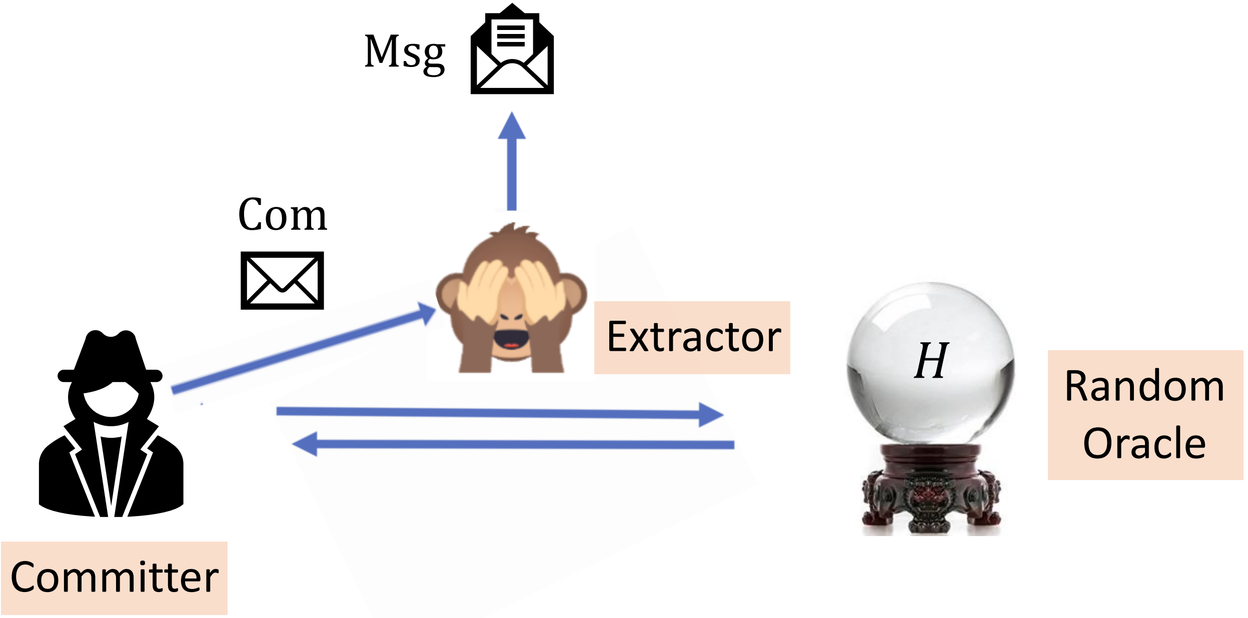
Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

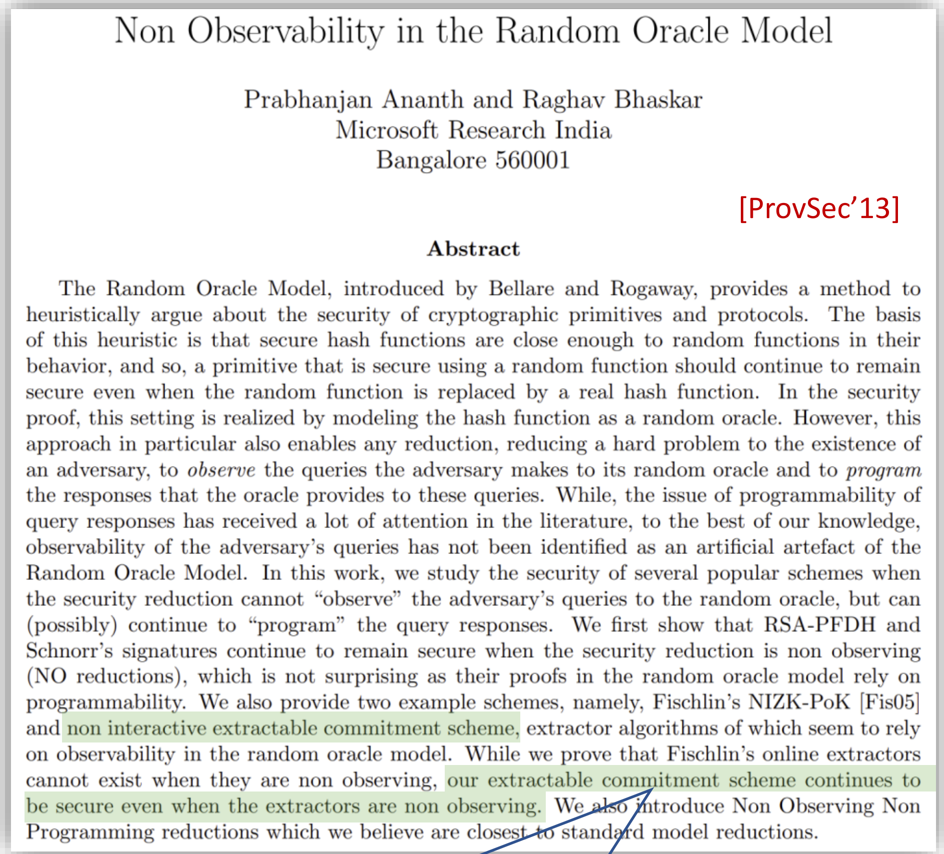
Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.

Construct a hash-based extractable commitment in the NO ROM.



Non-Observable ROM (NO ROM)



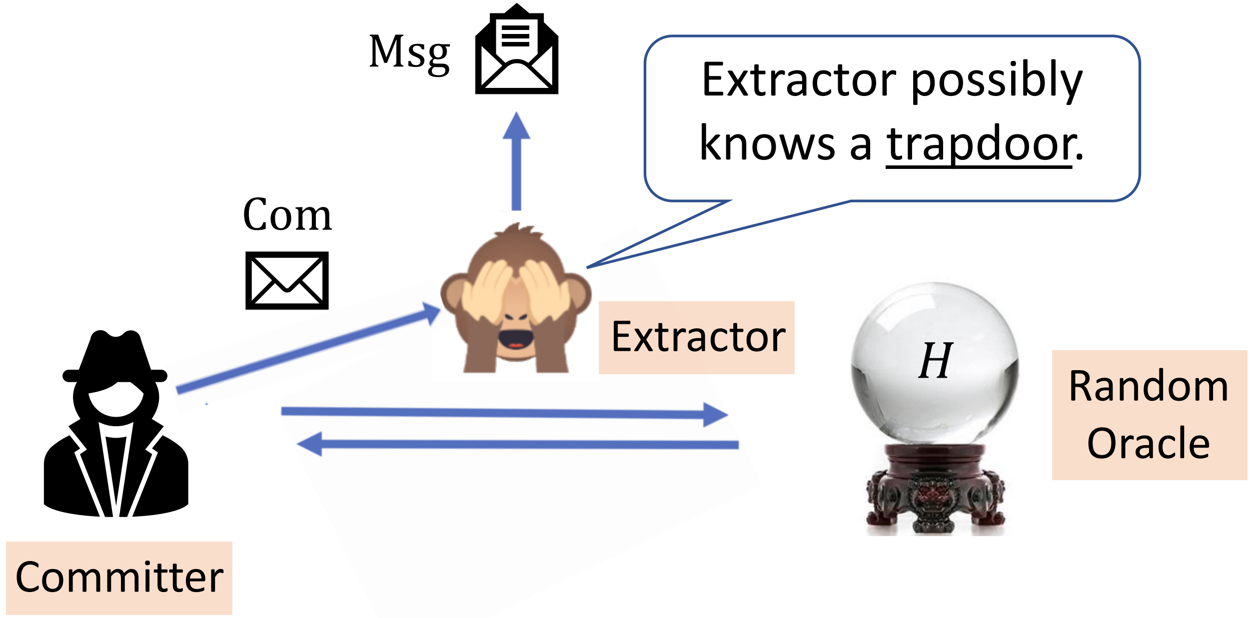
Non Observability in the Random Oracle Model

Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

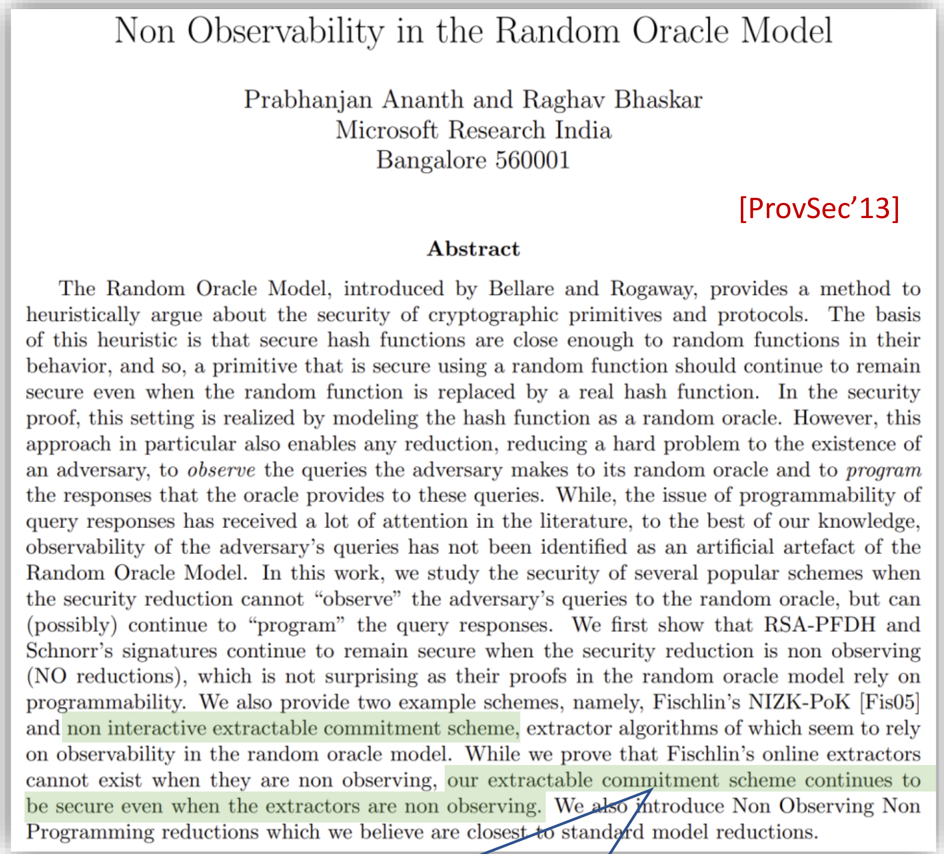
Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.



Construct a hash-based <u>extractable commitment</u> in the NO ROM.

Non-Observable ROM (NO ROM)



Non Observability in the Random Oracle Model

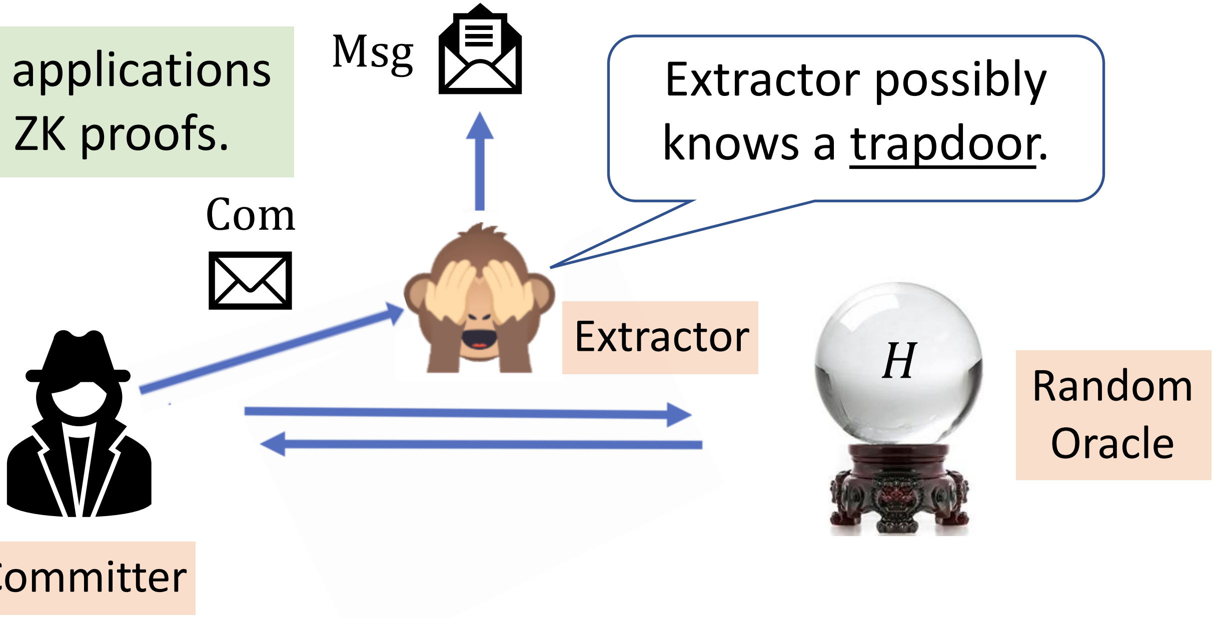
Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

Abstract

The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.

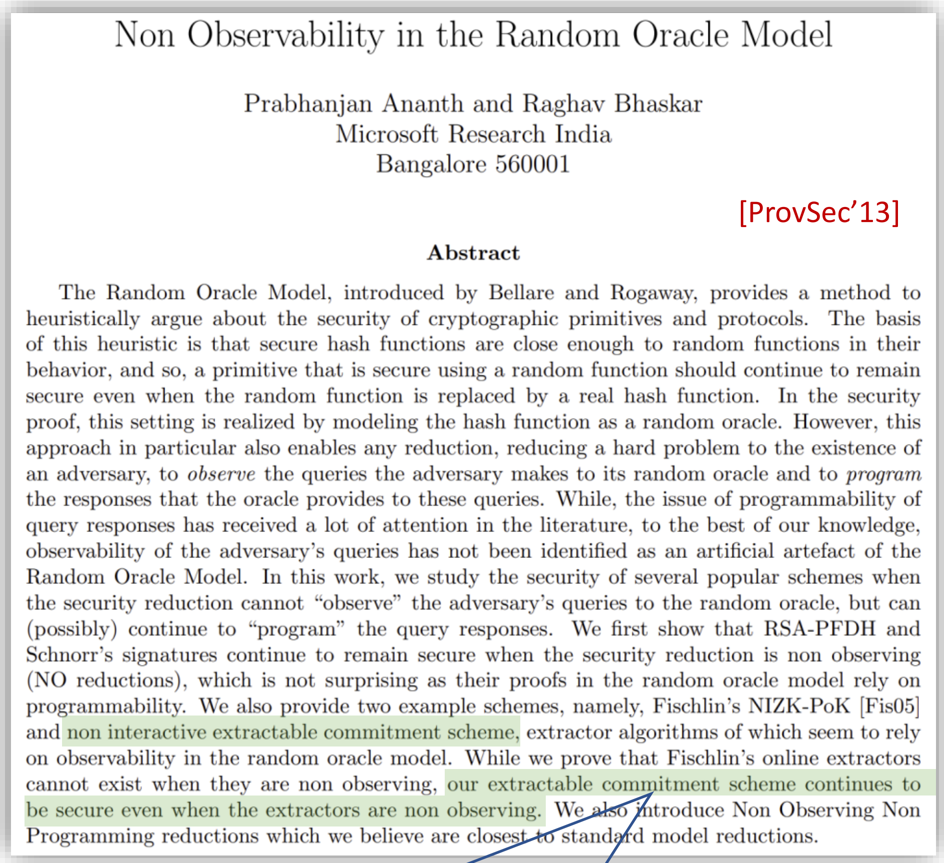
Has applications in ZK proofs.



Extractor possibly knows a trapdoor.

Construct a hash-based extractable commitment in the NO ROM.

Non-Observable ROM (NO ROM)



Non Observability in the Random Oracle Model

Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

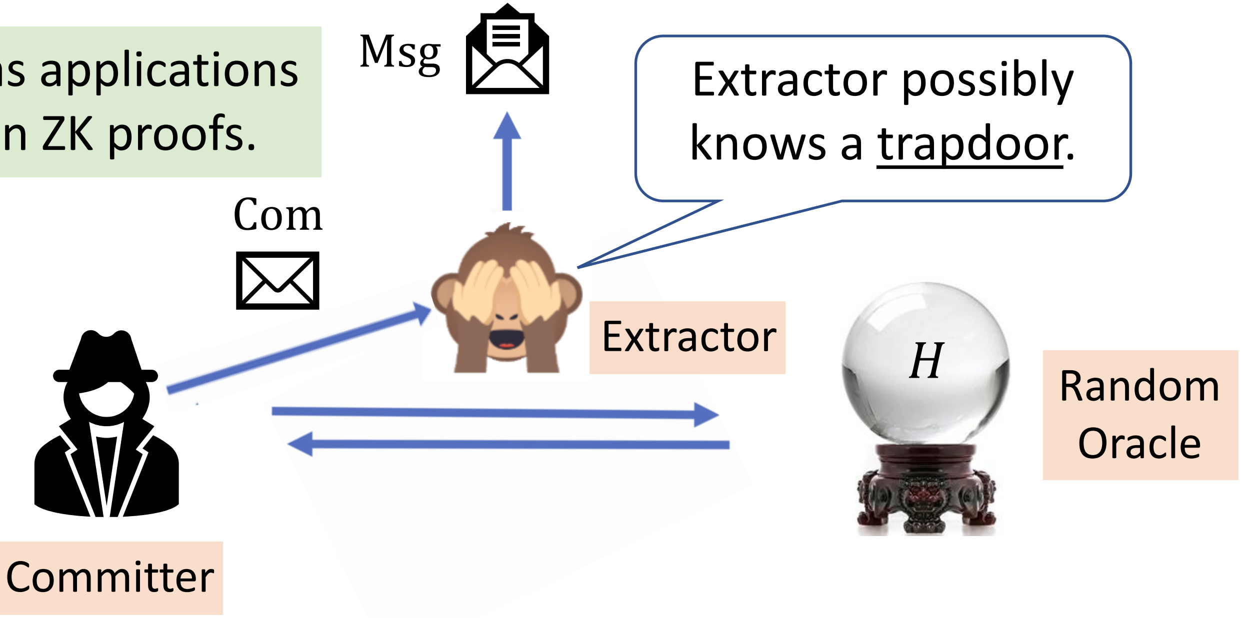
Abstract

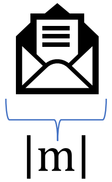
The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.

Construct a hash-based extractable commitment in the NO ROM.

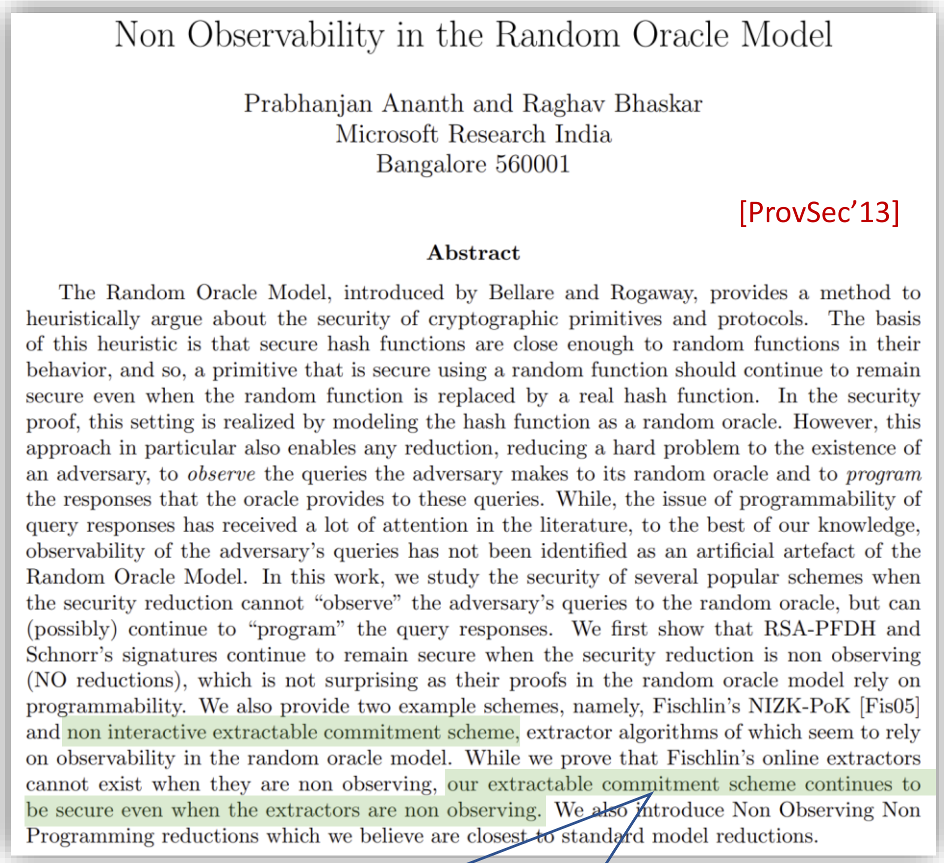
Has applications in ZK proofs.

Extractor possibly knows a trapdoor.





Non-Observable ROM (NO ROM)



Non Observability in the Random Oracle Model

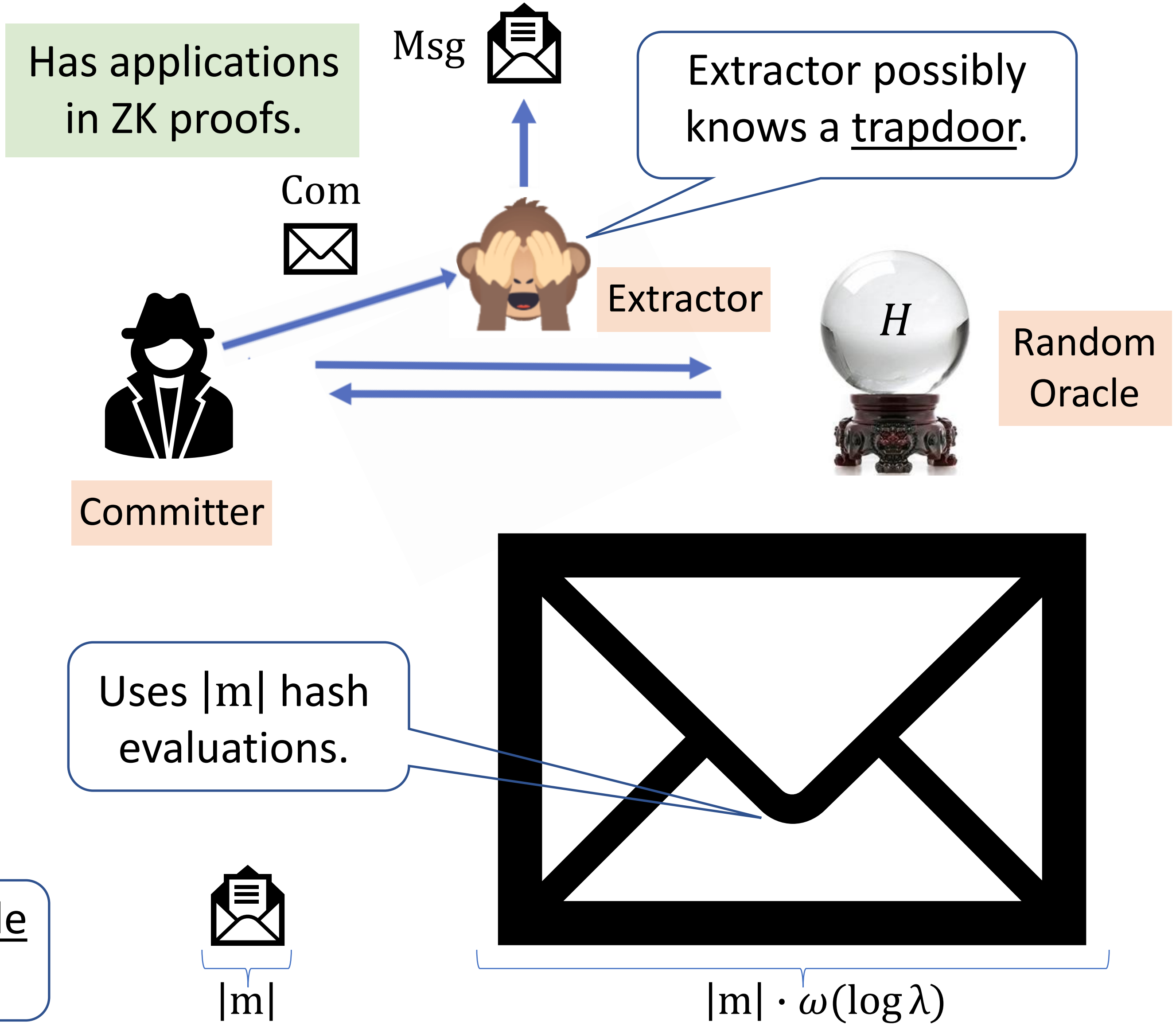
Prabhanjan Ananth and Raghav Bhaskar
Microsoft Research India
Bangalore 560001

[ProvSec'13]

Abstract

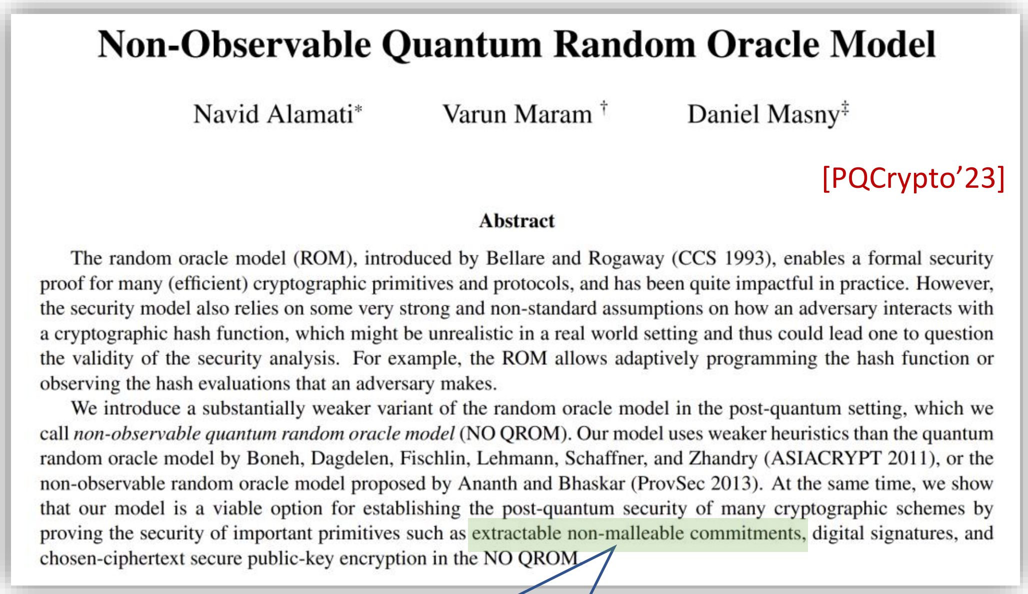
The Random Oracle Model, introduced by Bellare and Rogaway, provides a method to heuristically argue about the security of cryptographic primitives and protocols. The basis of this heuristic is that secure hash functions are close enough to random functions in their behavior, and so, a primitive that is secure using a random function should continue to remain secure even when the random function is replaced by a real hash function. In the security proof, this setting is realized by modeling the hash function as a random oracle. However, this approach in particular also enables any reduction, reducing a hard problem to the existence of an adversary, to *observe* the queries the adversary makes to its random oracle and to *program* the responses that the oracle provides to these queries. While, the issue of programmability of query responses has received a lot of attention in the literature, to the best of our knowledge, observability of the adversary's queries has not been identified as an artificial artefact of the Random Oracle Model. In this work, we study the security of several popular schemes when the security reduction cannot "observe" the adversary's queries to the random oracle, but can (possibly) continue to "program" the query responses. We first show that RSA-PFDH and Schnorr's signatures continue to remain secure when the security reduction is non observing (NO reductions), which is not surprising as their proofs in the random oracle model rely on programmability. We also provide two example schemes, namely, Fischlin's NIZK-PoK [Fis05] and non interactive extractable commitment scheme, extractor algorithms of which seem to rely on observability in the random oracle model. While we prove that Fischlin's online extractors cannot exist when they are non observing, our extractable commitment scheme continues to be secure even when the extractors are non observing. We also introduce Non Observing Non Programming reductions which we believe are closest to standard model reductions.

Construct a hash-based extractable commitment in the NO ROM.



Non-Observable ROM (NO ROM)

Has applications in ZK proofs.



Non-Observable Quantum Random Oracle Model

Navid Alamati* Varun Maram † Daniel Masny‡

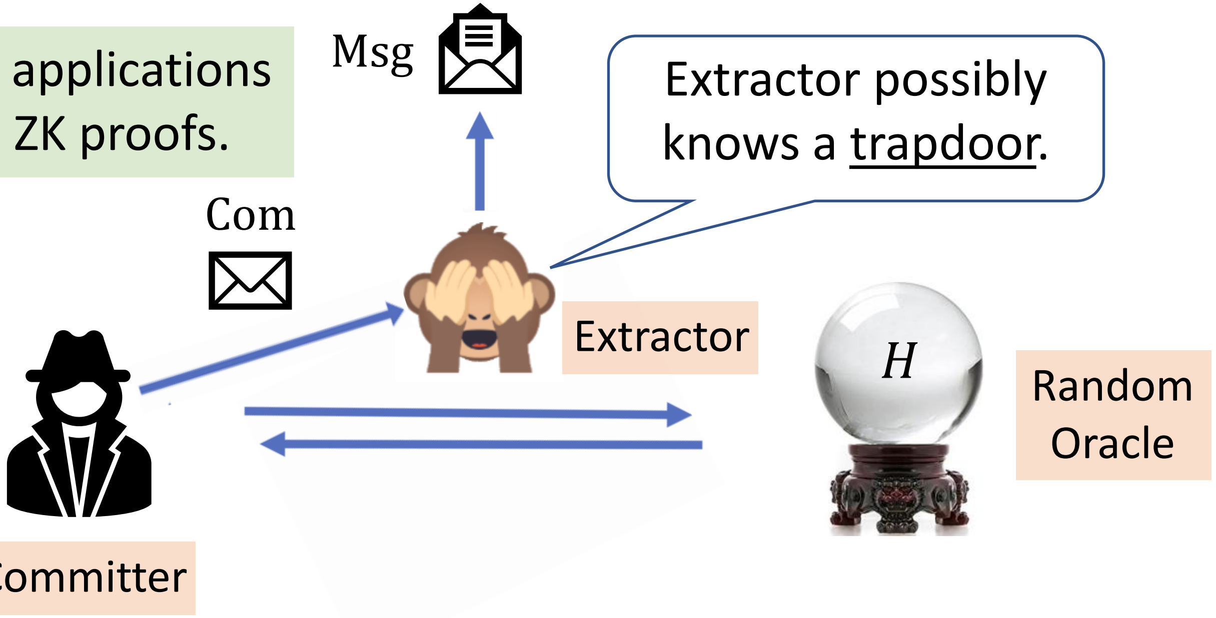
[PQCrypto'23]

Abstract

The random oracle model (ROM), introduced by Bellare and Rogaway (CCS 1993), enables a formal security proof for many (efficient) cryptographic primitives and protocols, and has been quite impactful in practice. However, the security model also relies on some very strong and non-standard assumptions on how an adversary interacts with a cryptographic hash function, which might be unrealistic in a real world setting and thus could lead one to question the validity of the security analysis. For example, the ROM allows adaptively programming the hash function or observing the hash evaluations that an adversary makes.

We introduce a substantially weaker variant of the random oracle model in the post-quantum setting, which we call *non-observable quantum random oracle model* (NO QROM). Our model uses weaker heuristics than the quantum random oracle model by Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry (ASIACRYPT 2011), or the non-observable random oracle model proposed by Ananth and Bhaskar (ProvSec 2013). At the same time, we show that our model is a viable option for establishing the post-quantum security of many cryptographic schemes by proving the security of important primitives such as extractable non-malleable commitments, digital signatures, and chosen-ciphertext secure public-key encryption in the NO QROM.

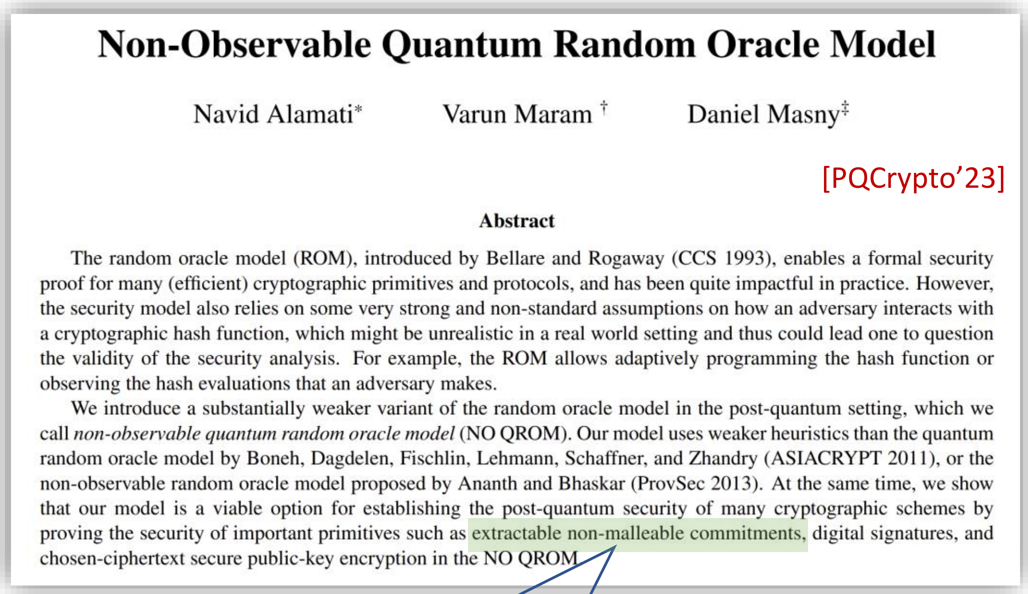
Construct a hash-based <u>extractable commitment</u> in the NO ROM.



Extractor possibly knows a <u>trapdoor</u>.

Uses $O(1)$ hash evaluations.

Non-Observable ROM (NO ROM)



Non-Observable Quantum Random Oracle Model

Navid Alamati* Varun Maram † Daniel Masny‡

[PQCrypto'23]

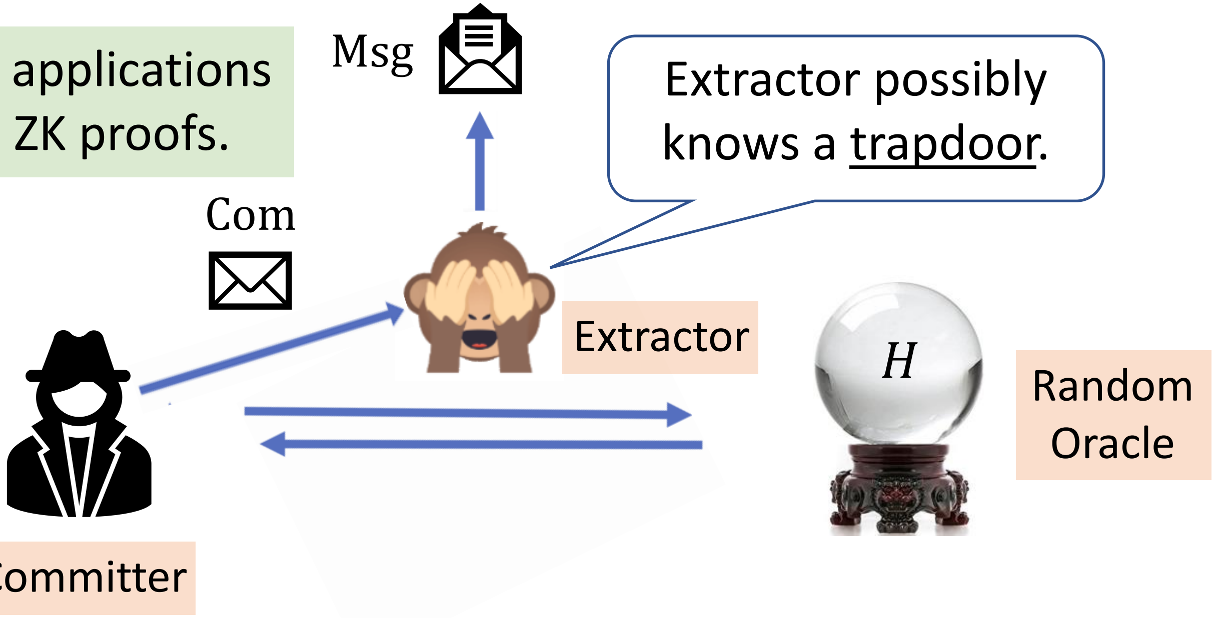
Abstract

The random oracle model (ROM), introduced by Bellare and Rogaway (CCS 1993), enables a formal security proof for many (efficient) cryptographic primitives and protocols, and has been quite impactful in practice. However, the security model also relies on some very strong and non-standard assumptions on how an adversary interacts with a cryptographic hash function, which might be unrealistic in a real world setting and thus could lead one to question the validity of the security analysis. For example, the ROM allows adaptively programming the hash function or observing the hash evaluations that an adversary makes.

We introduce a substantially weaker variant of the random oracle model in the post-quantum setting, which we call *non-observable quantum random oracle model* (NO QROM). Our model uses weaker heuristics than the quantum random oracle model by Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry (ASIACRYPT 2011), or the non-observable random oracle model proposed by Ananth and Bhaskar (ProvSec 2013). At the same time, we show that our model is a viable option for establishing the post-quantum security of many cryptographic schemes by proving the security of important primitives such as extractable non-malleable commitments, digital signatures, and chosen-ciphertext secure public-key encryption in the NO QROM.

Construct a hash-based <u>extractable commitment</u> in the NO ROM.

Has applications in ZK proofs.

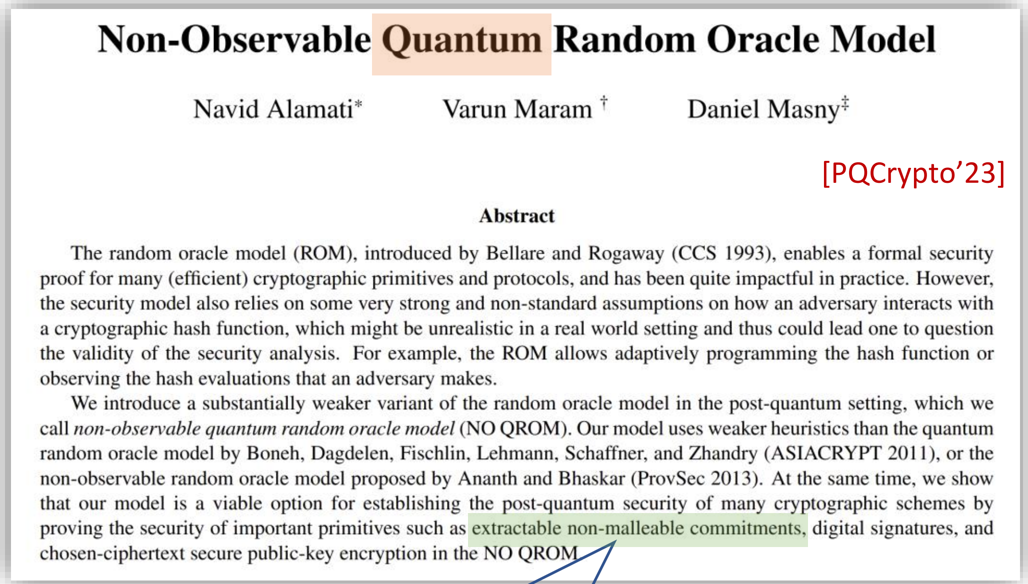


Extractor possibly knows a <u>trapdoor</u>.

"Textbook" hash-based commitment: $\mathrm{Com} = H(\mathrm{Msg}, r)$

Uses $O(1)$ hash evaluations.

Non-Observable QROM (NO QROM)



Non-Observable Quantum Random Oracle Model

Navid Alamati* Varun Maram † Daniel Masny‡

[PQCrypto'23]

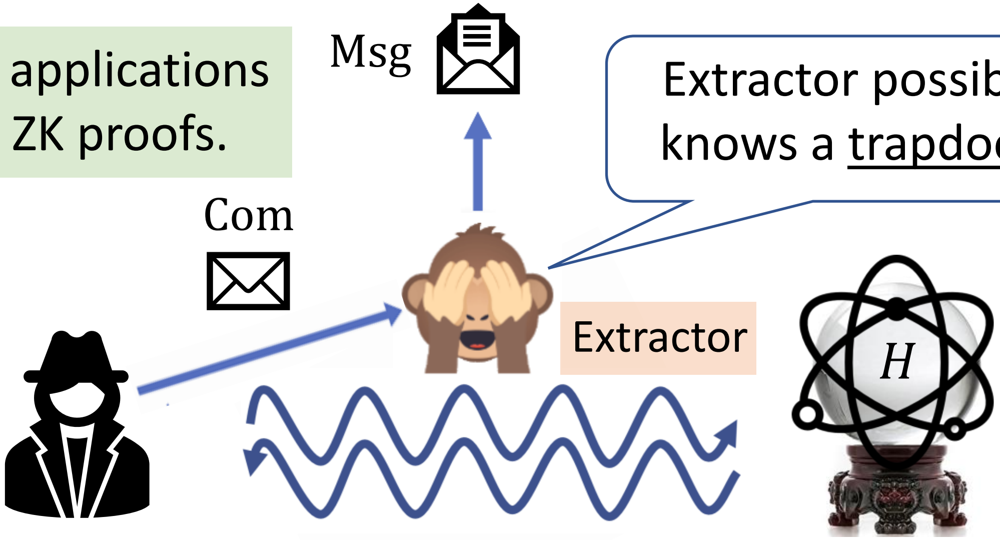
Abstract

The random oracle model (ROM), introduced by Bellare and Rogaway (CCS 1993), enables a formal security proof for many (efficient) cryptographic primitives and protocols, and has been quite impactful in practice. However, the security model also relies on some very strong and non-standard assumptions on how an adversary interacts with a cryptographic hash function, which might be unrealistic in a real world setting and thus could lead one to question the validity of the security analysis. For example, the ROM allows adaptively programming the hash function or observing the hash evaluations that an adversary makes.

We introduce a substantially weaker variant of the random oracle model in the post-quantum setting, which we call *non-observable quantum random oracle model* (NO QROM). Our model uses weaker heuristics than the quantum random oracle model by Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry (ASIACRYPT 2011), or the non-observable random oracle model proposed by Ananth and Bhaskar (ProvSec 2013). At the same time, we show that our model is a viable option for establishing the post-quantum security of many cryptographic schemes by proving the security of important primitives such as extractable non-malleable commitments, digital signatures, and chosen-ciphertext secure public-key encryption in the NO QROM.

Construct a hash-based extractable commitment in the NO QROM.

Has applications in ZK proofs.

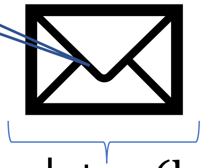


Extractor possibly knows a trapdoor.

Uses $O(1)$ hash evaluations.

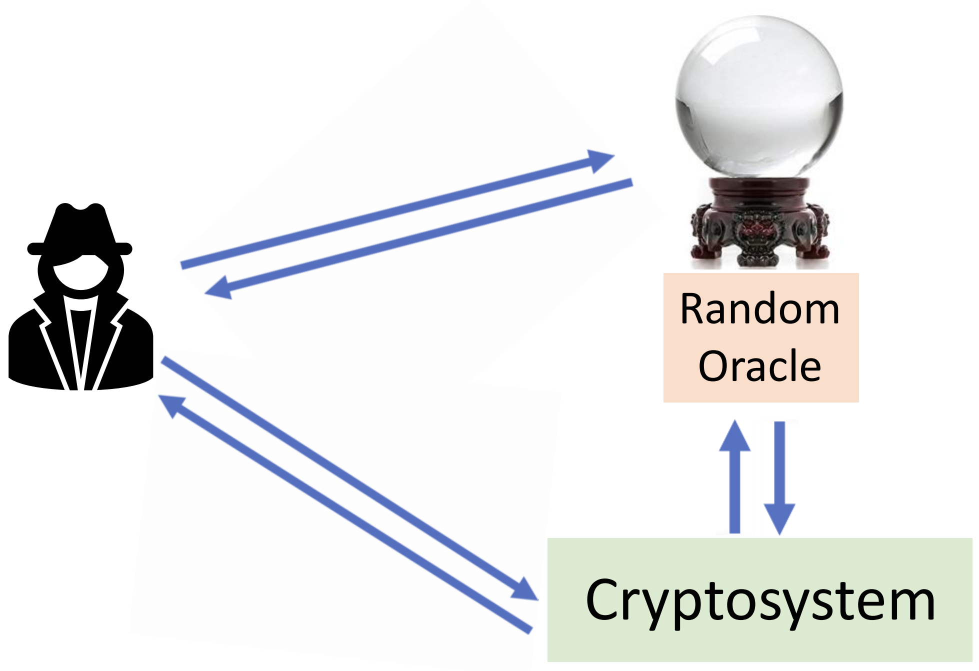
"Textbook" hash-based commitment: $\mathrm{Com} = H(\mathrm{Msg}, r)$

$|\mathrm{m}|$



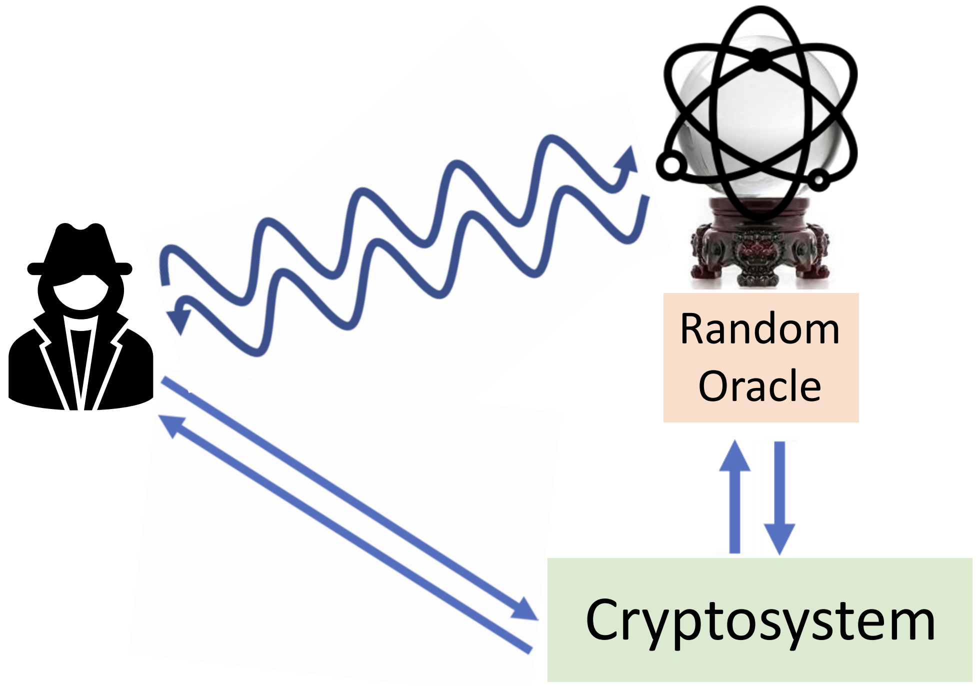
$|\mathrm{m}| + \omega(\log \lambda)$

(Classical) Random Oracle Model (ROM)



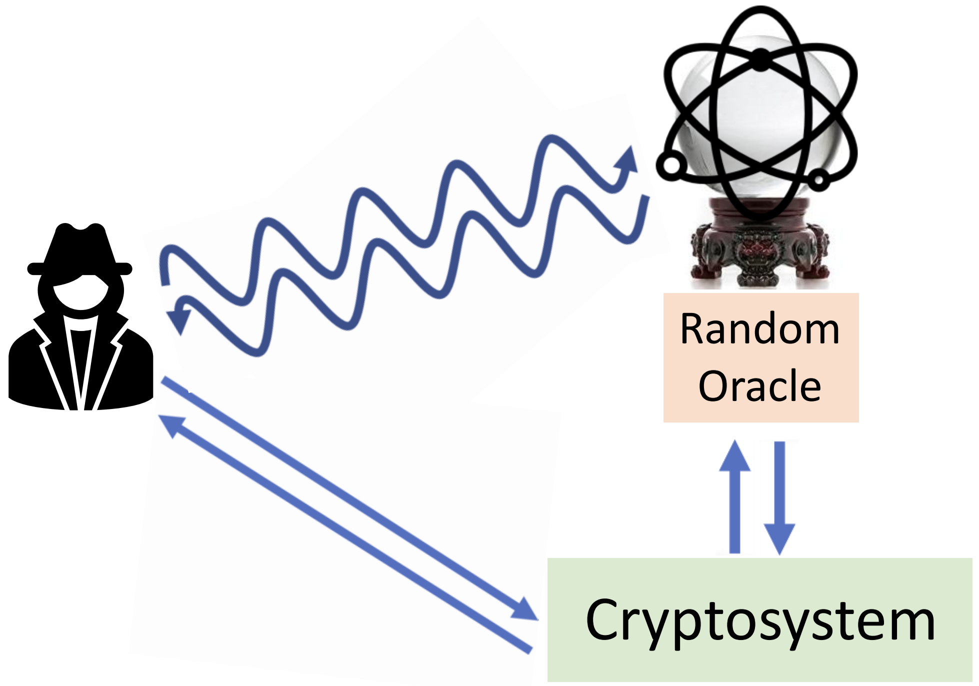
Formalized by [Bellare-Rogaway’93].

Quantum Random Oracle Model (QROM)



Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

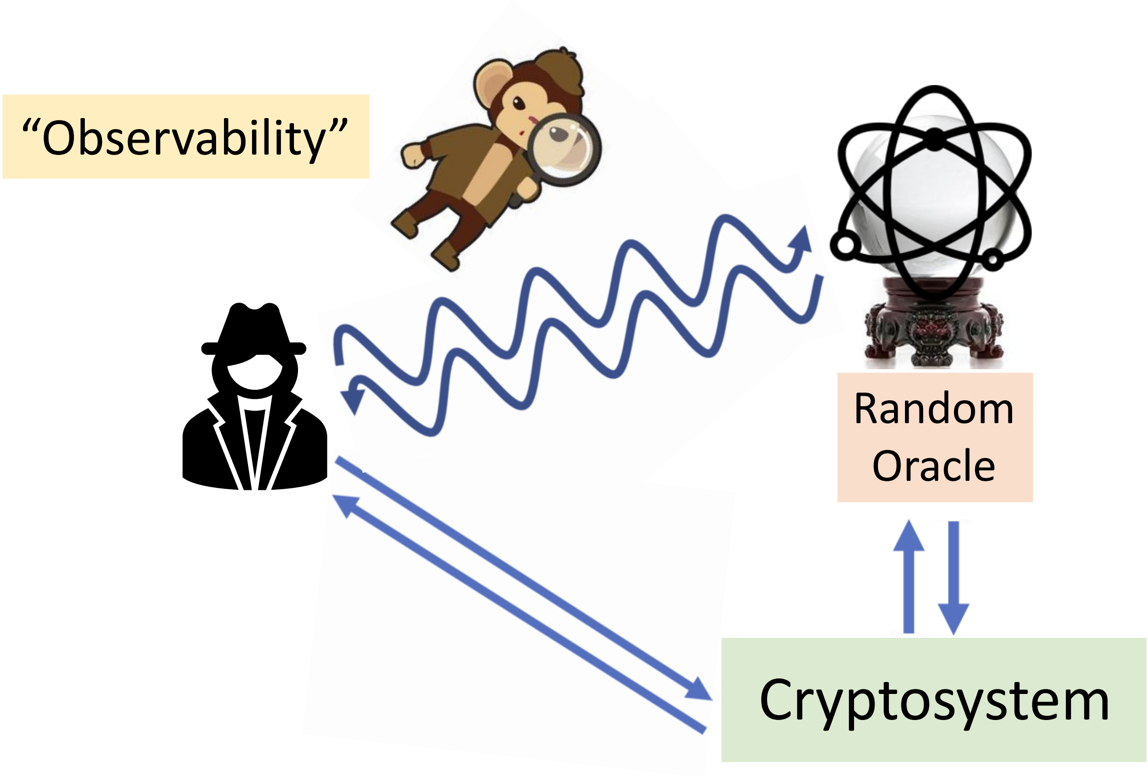
Quantum Random Oracle Model (QROM)



Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

- Captures ability of an adversary to evaluate a public hash function in superposition in a PQ setting.
- Tremendous progress has been made to adapt ROM security proofs to the QROM setting.

Quantum Random Oracle Model (QROM)

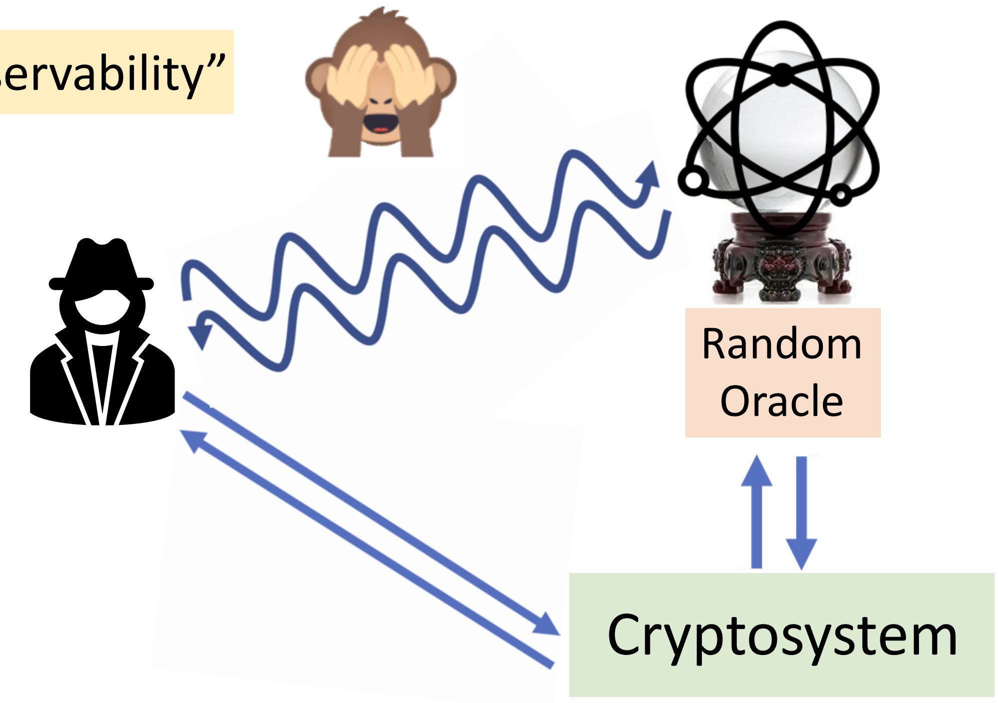


Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

- Captures ability of an adversary to evaluate a <u>public</u> hash function in superposition in a PQ setting.
- Tremendous progress has been made to adapt ROM security proofs to the QROM setting.
- However, most proofs rely on <u>observing/measuring</u> an adversary's quantum queries to random oracle.

Non-Observable QROM (NO QROM)

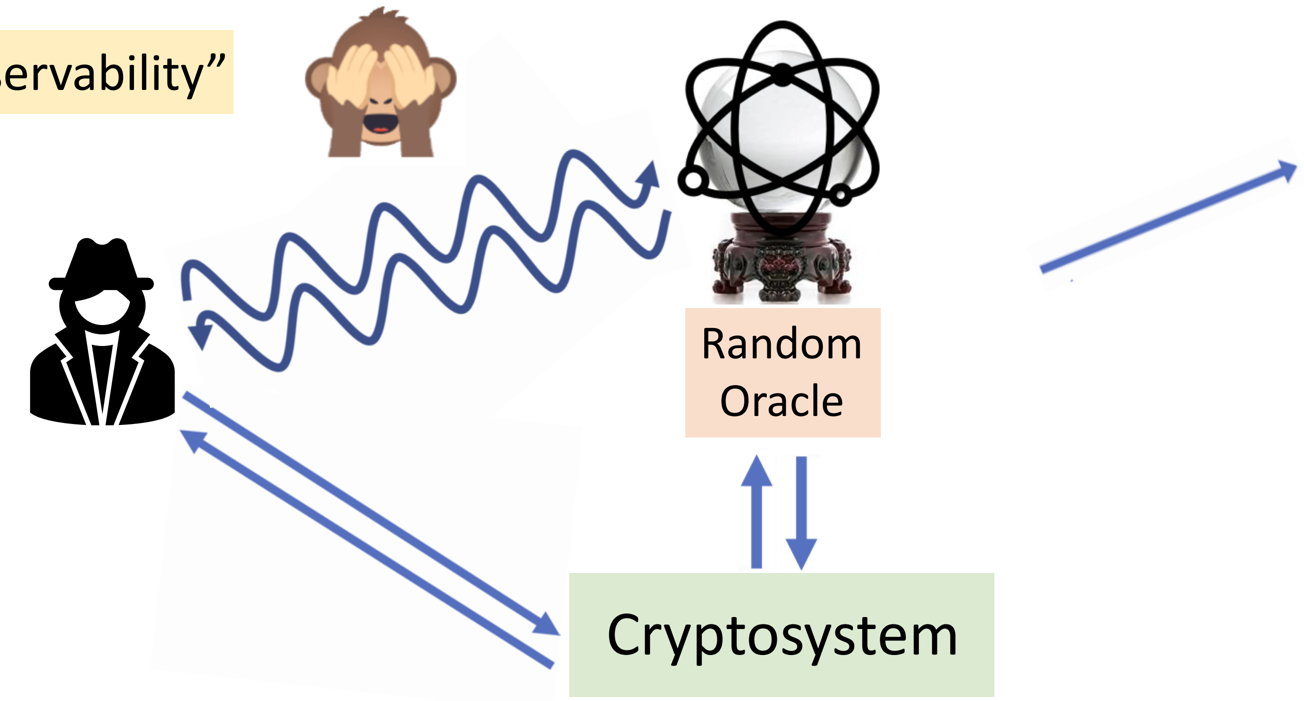
“Non-Observability”



Formalized by [Alamati-Maram-Masny’23].

Non-Observable QROM (NO QROM)

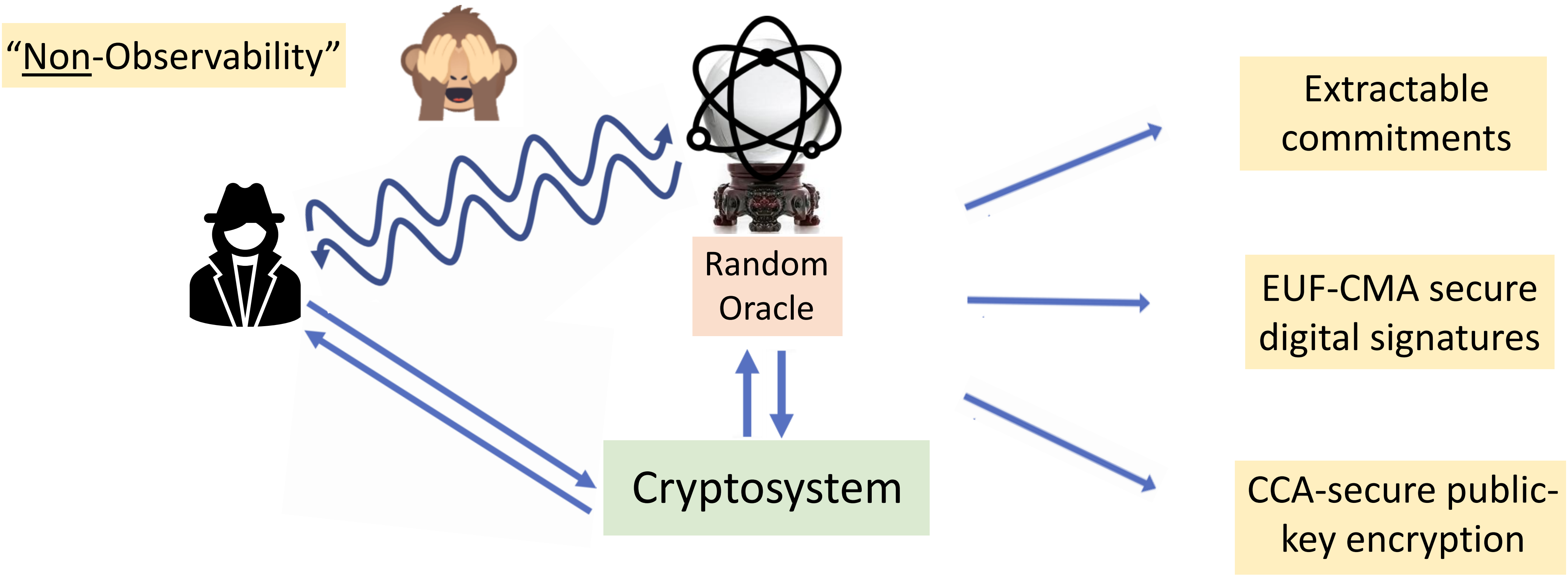
"Non-Observability"



Extractable commitments

Formalized by [Alamati-Maram-Masny'23].

Non-Observable QROM (NO QROM)



Formalized by [Alamati-Maram-Masny’23].

Non-Observable QROM (NO QROM)

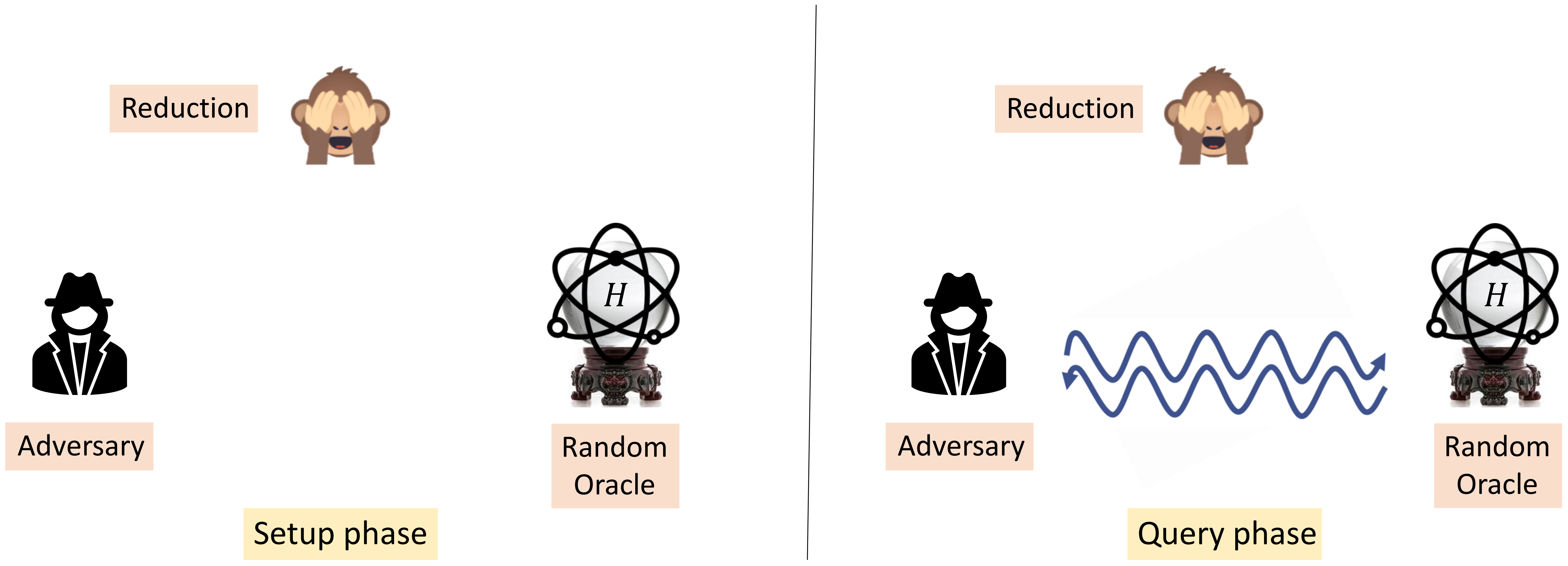
Reduction

Adversary

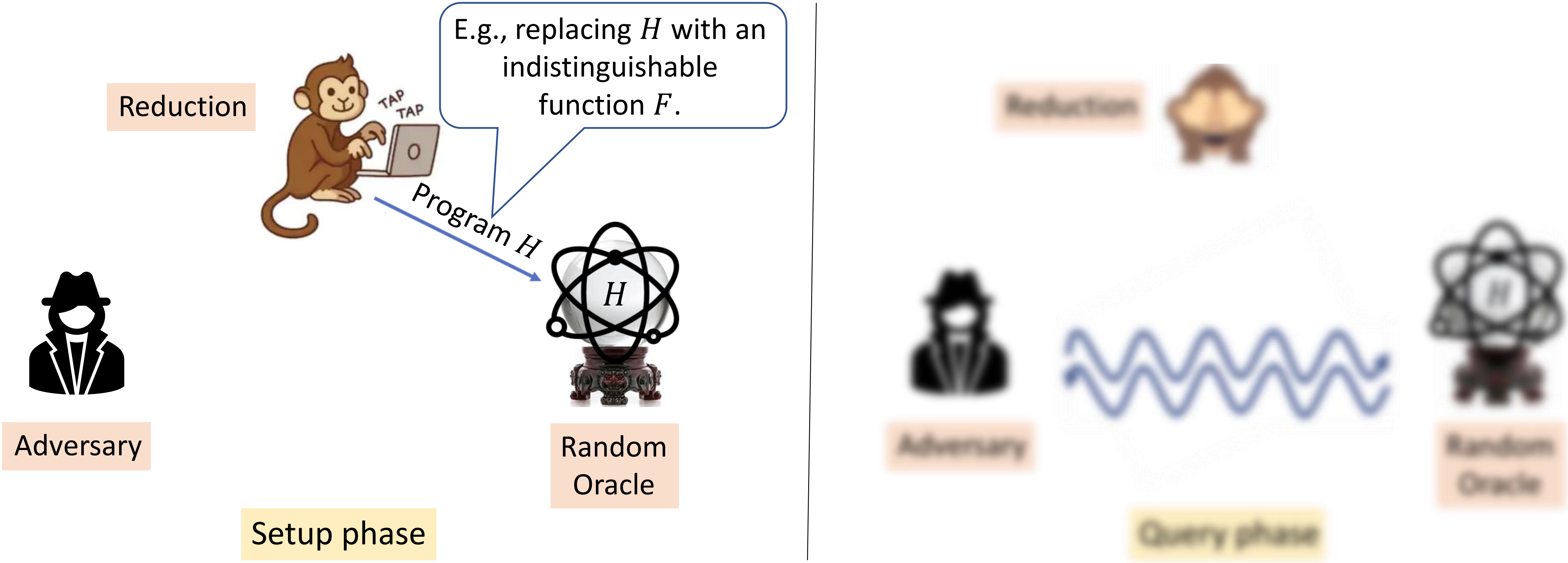
Random Oracle

Setup phase

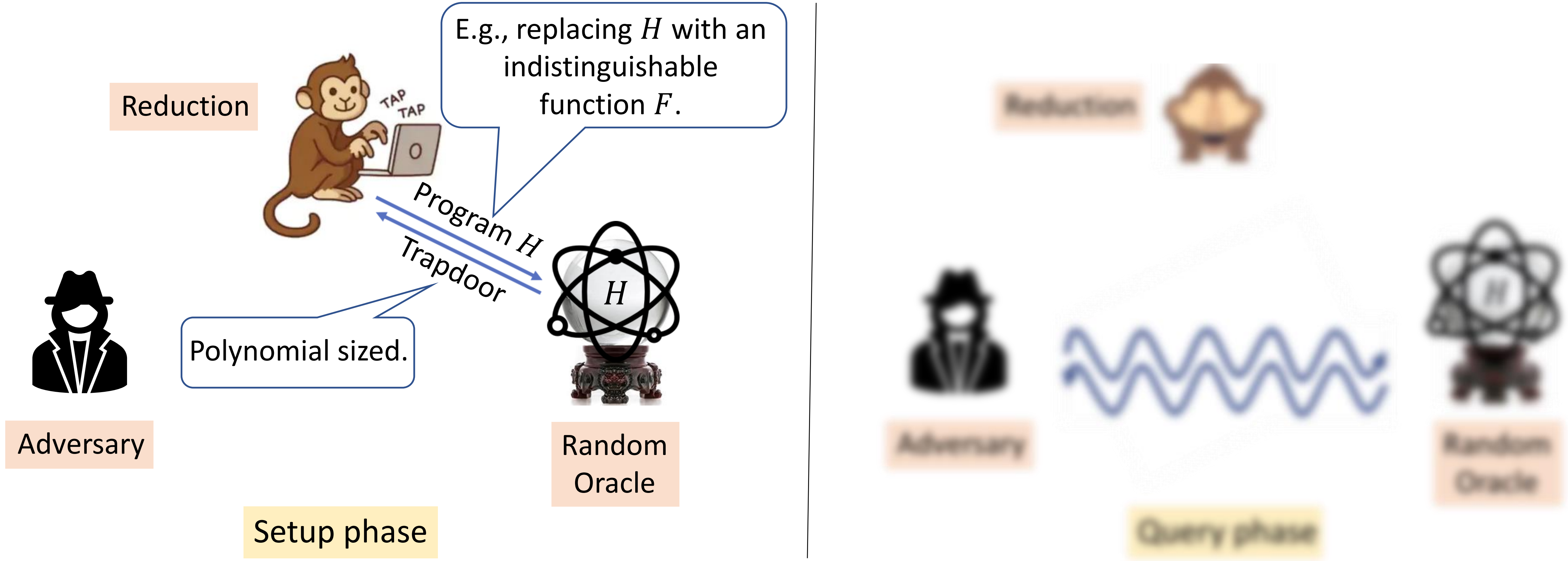
Non-Observable QROM (NO QROM)



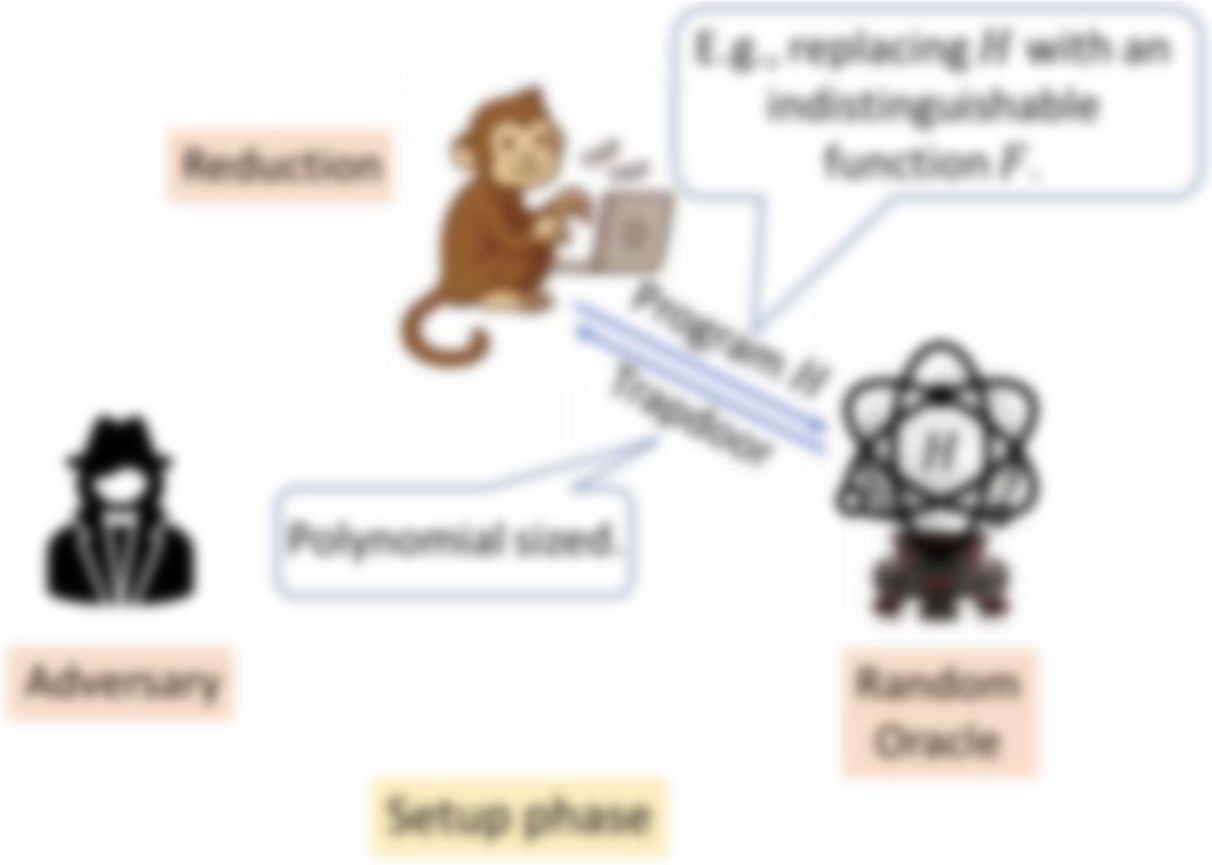
Non-Observable QROM (NO QROM)

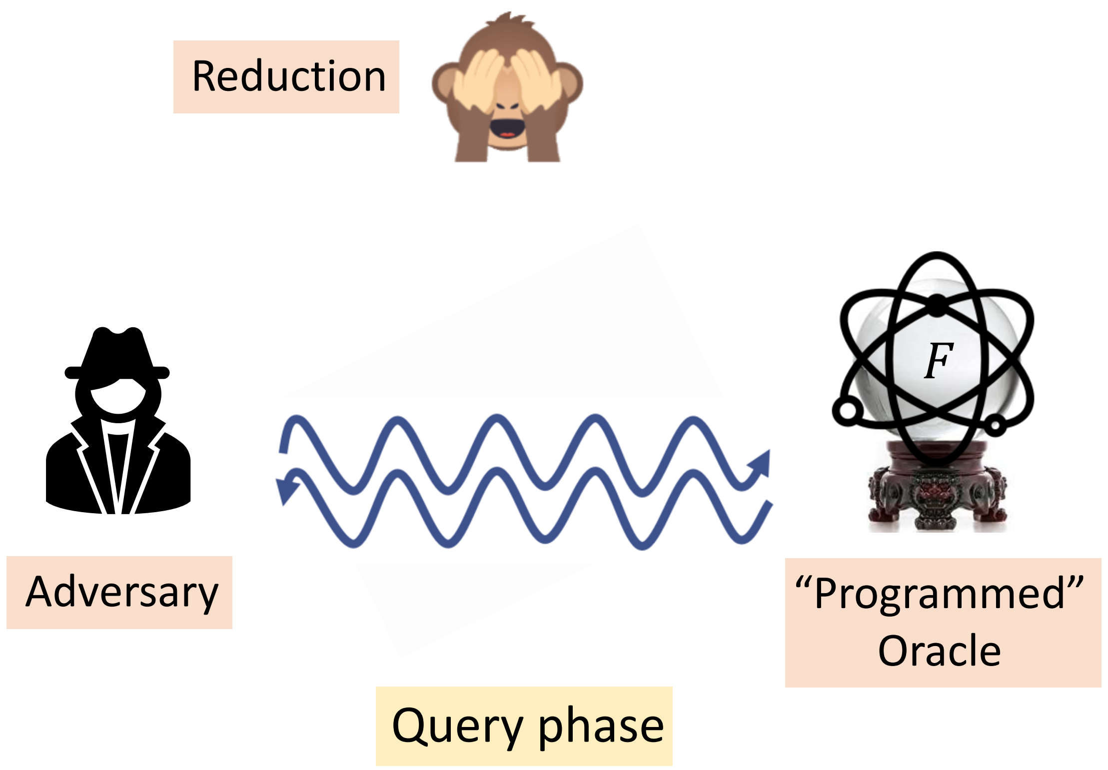


Non-Observable QROM (NO QROM)

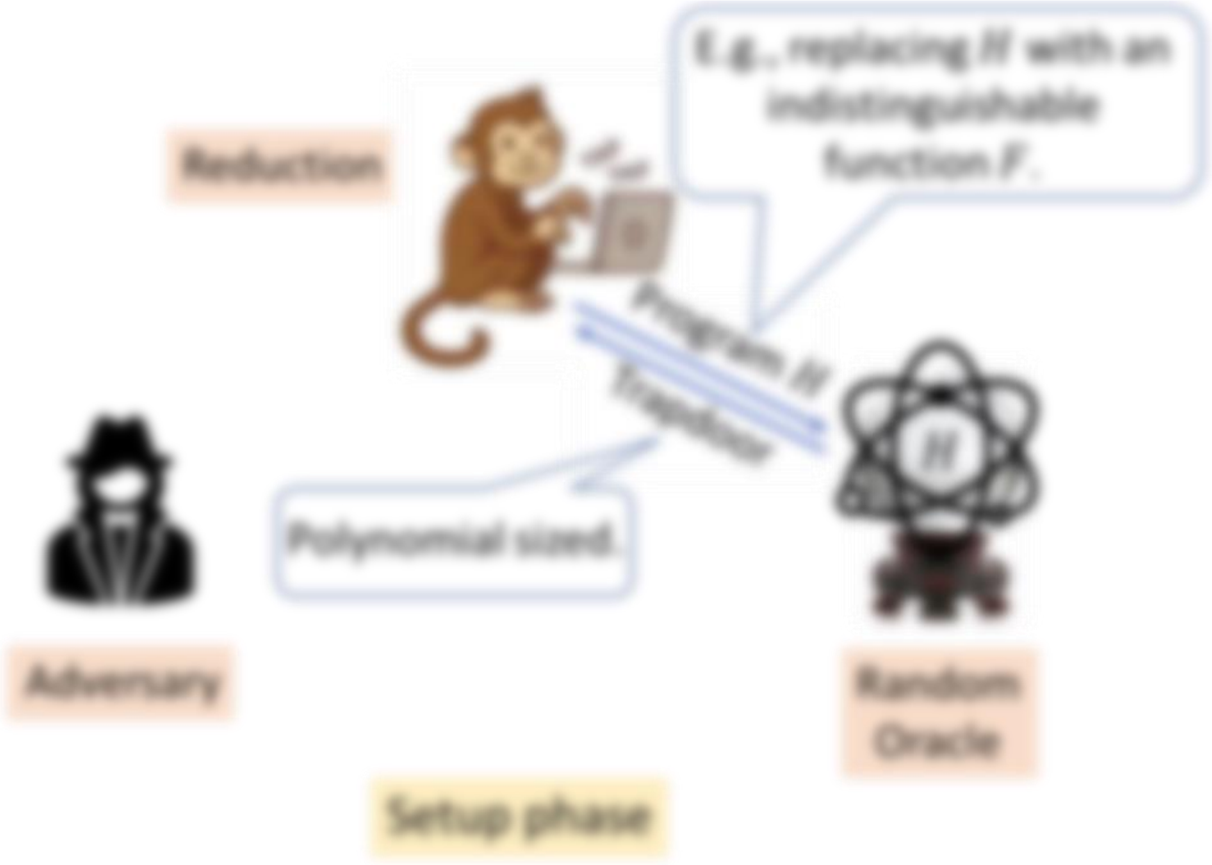


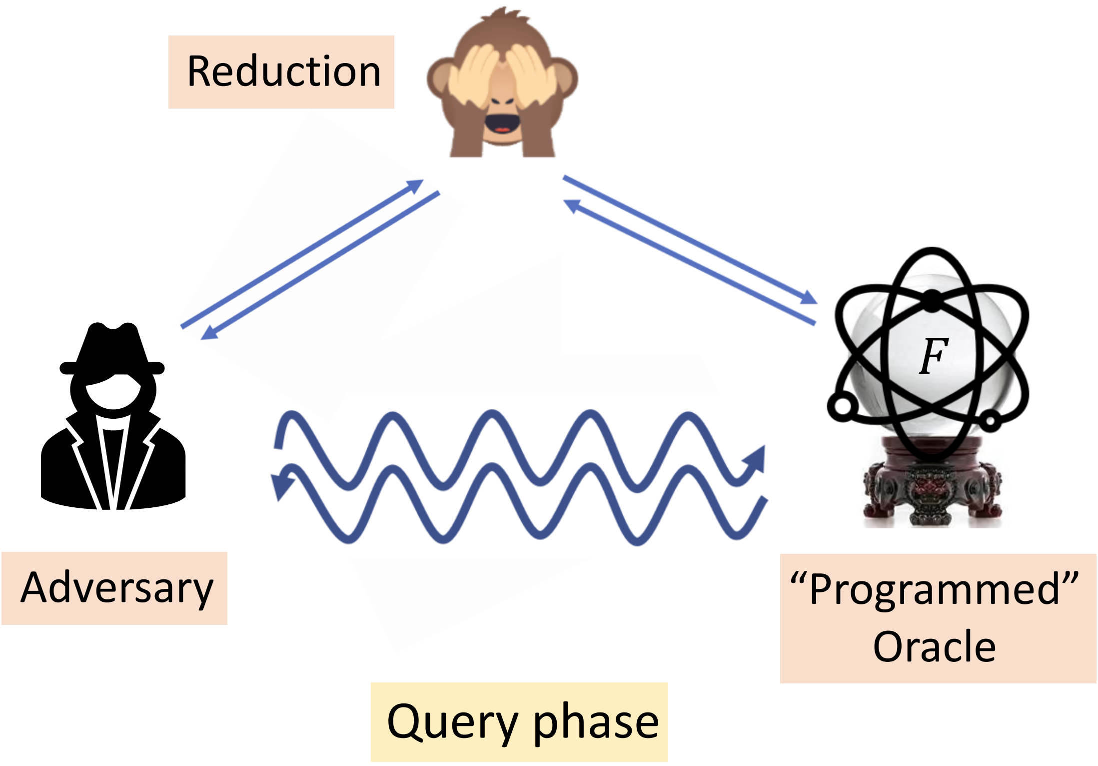
Non-Observable QROM (NO QROM)



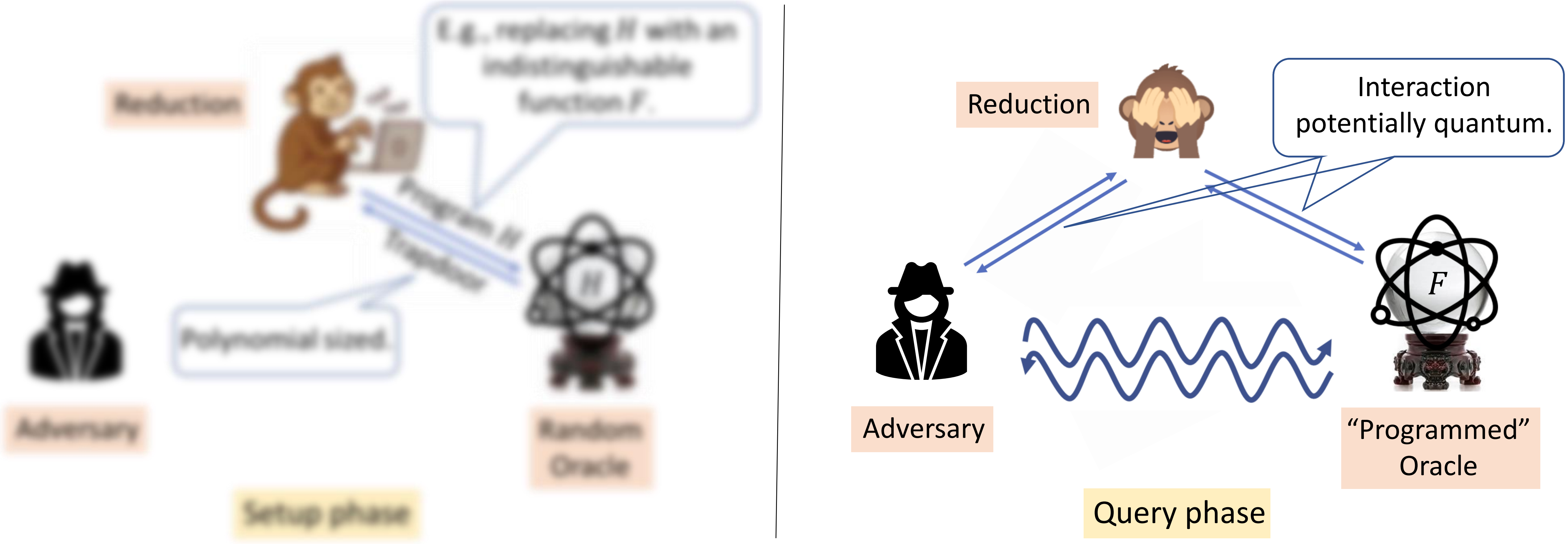


Non-Observable QROM (NO QROM)

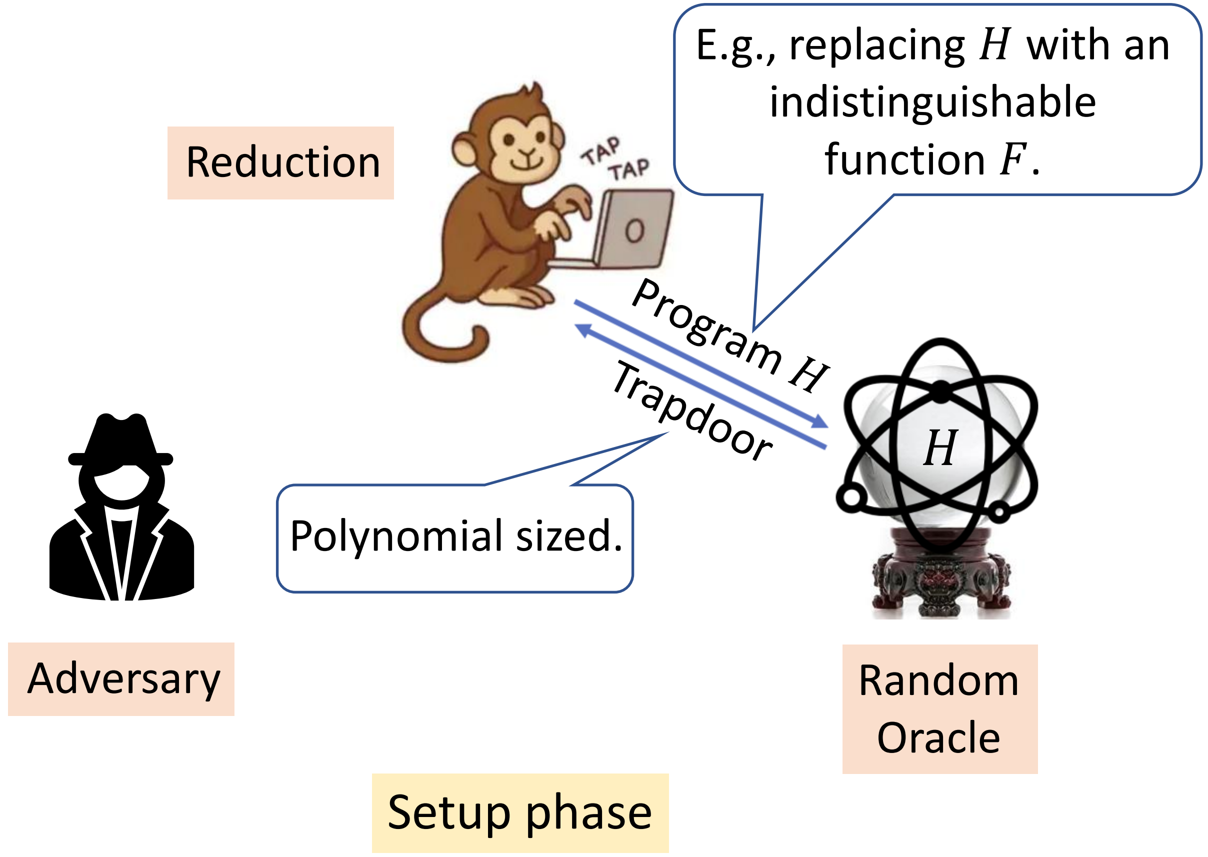


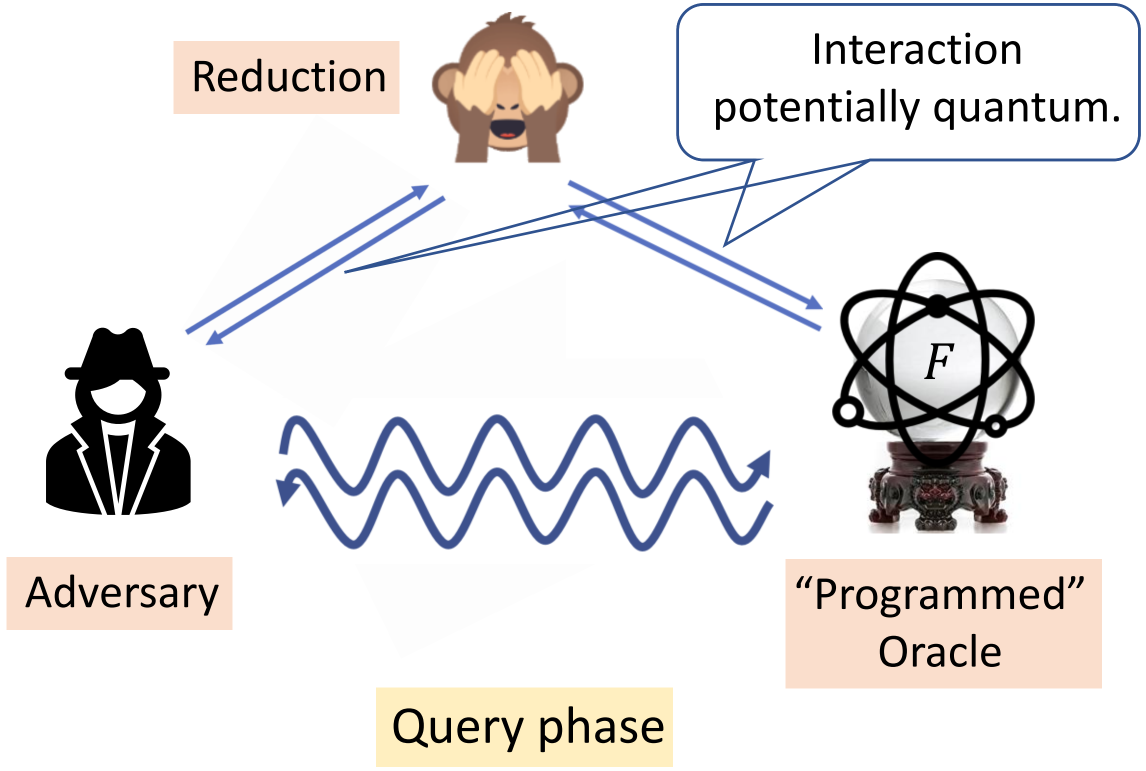


Non-Observable QROM (NO QROM)



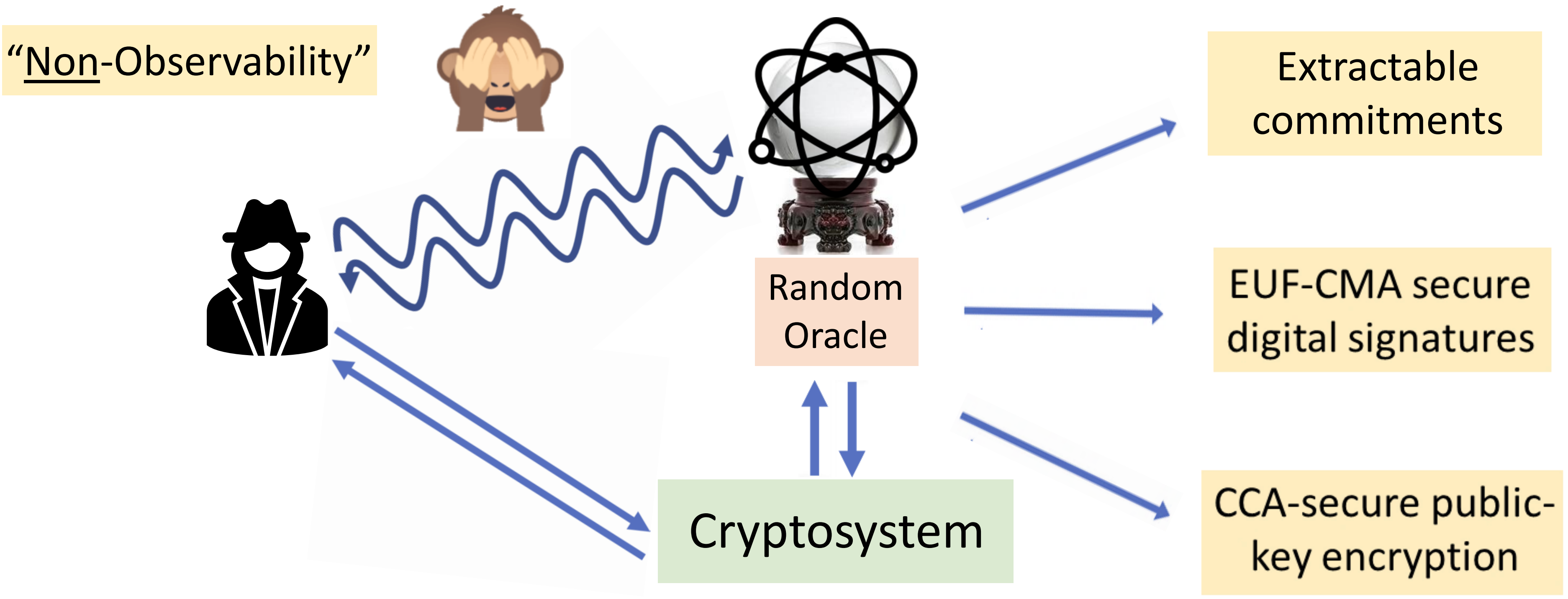
Non-Observable QROM (NO QROM)





- Our above model also allows non-adaptive (but not adaptive) programmability.
- Classical NO ROM of [Ananth-Bhaskar'13] uses a stateful Turing machine to model random oracle.
  - Maintaining a state incompatible w.r.t. random oracle queries in quantum superposition.

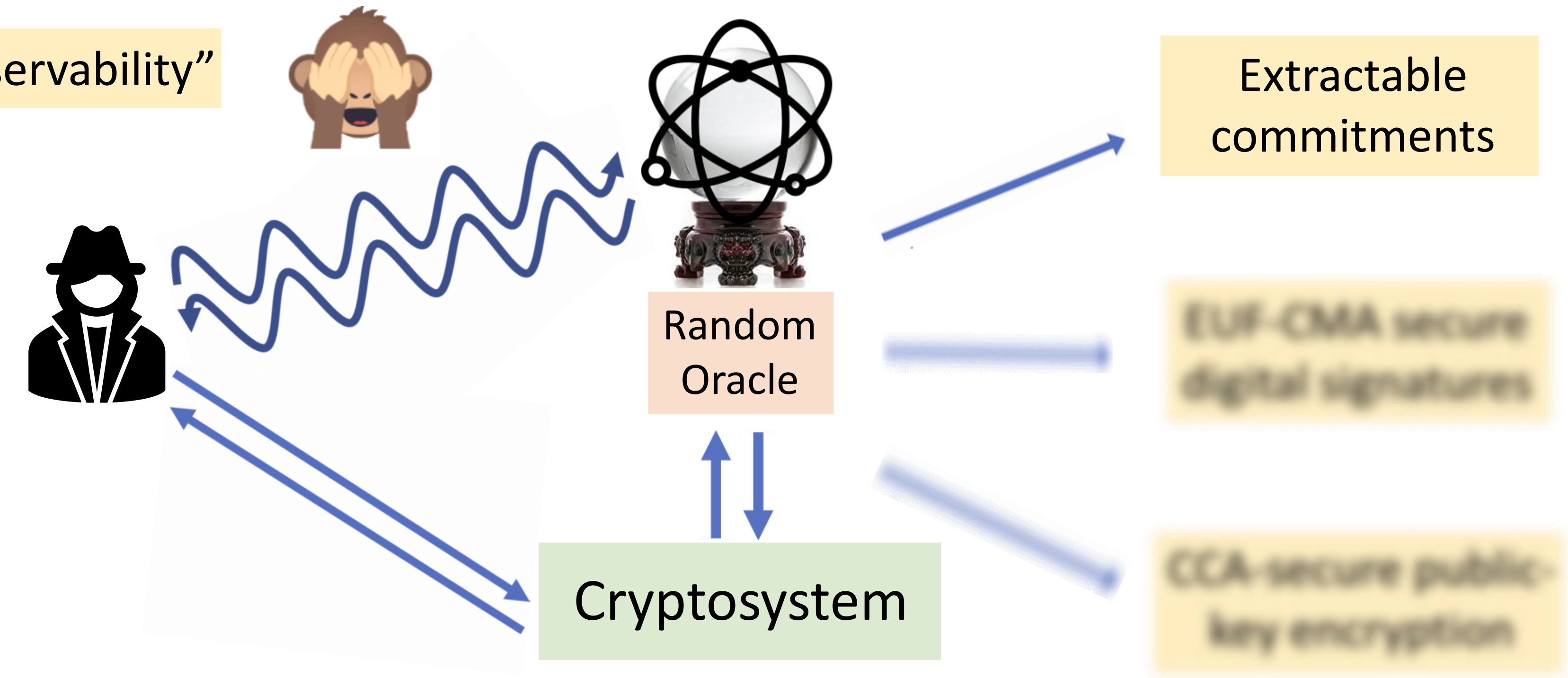
Non-Observable QROM (NO QROM)



Formalized by [Alamati-Maram-Masny’23].

Non-Observable QROM (NO QROM)

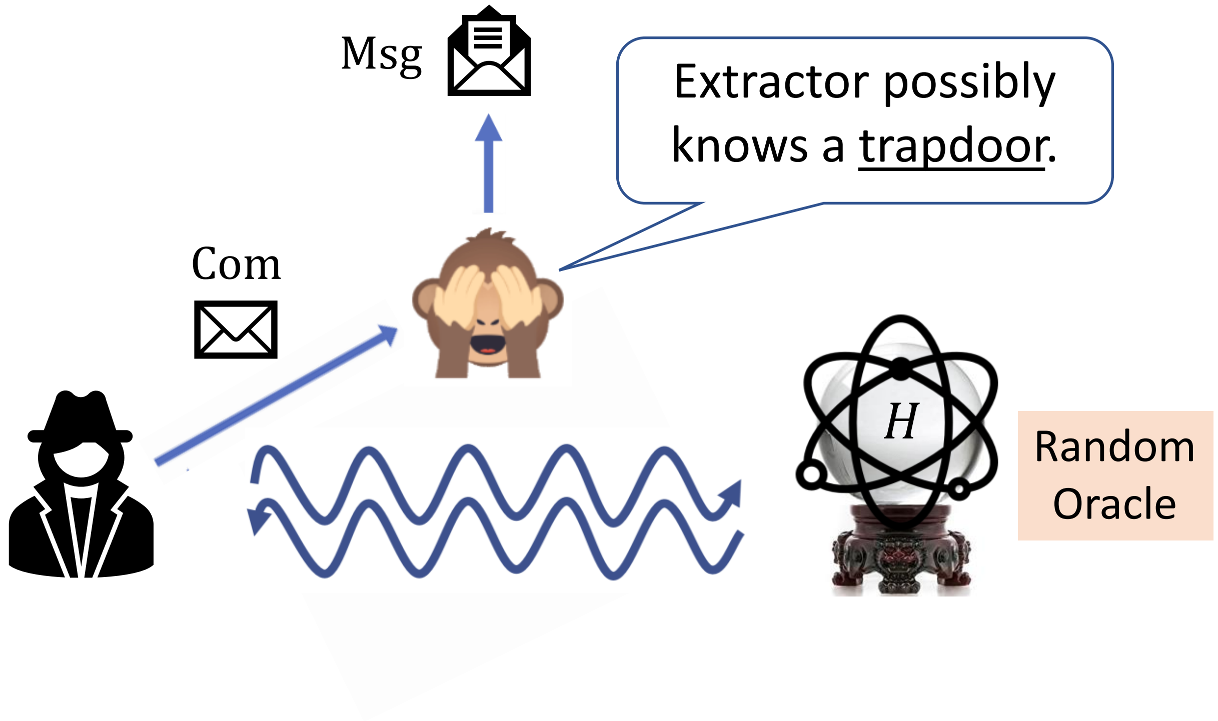
"Non-Observability"



Formalized by [Alamati-Maram-Masny'23].

Extractable Commitments in NO QROM

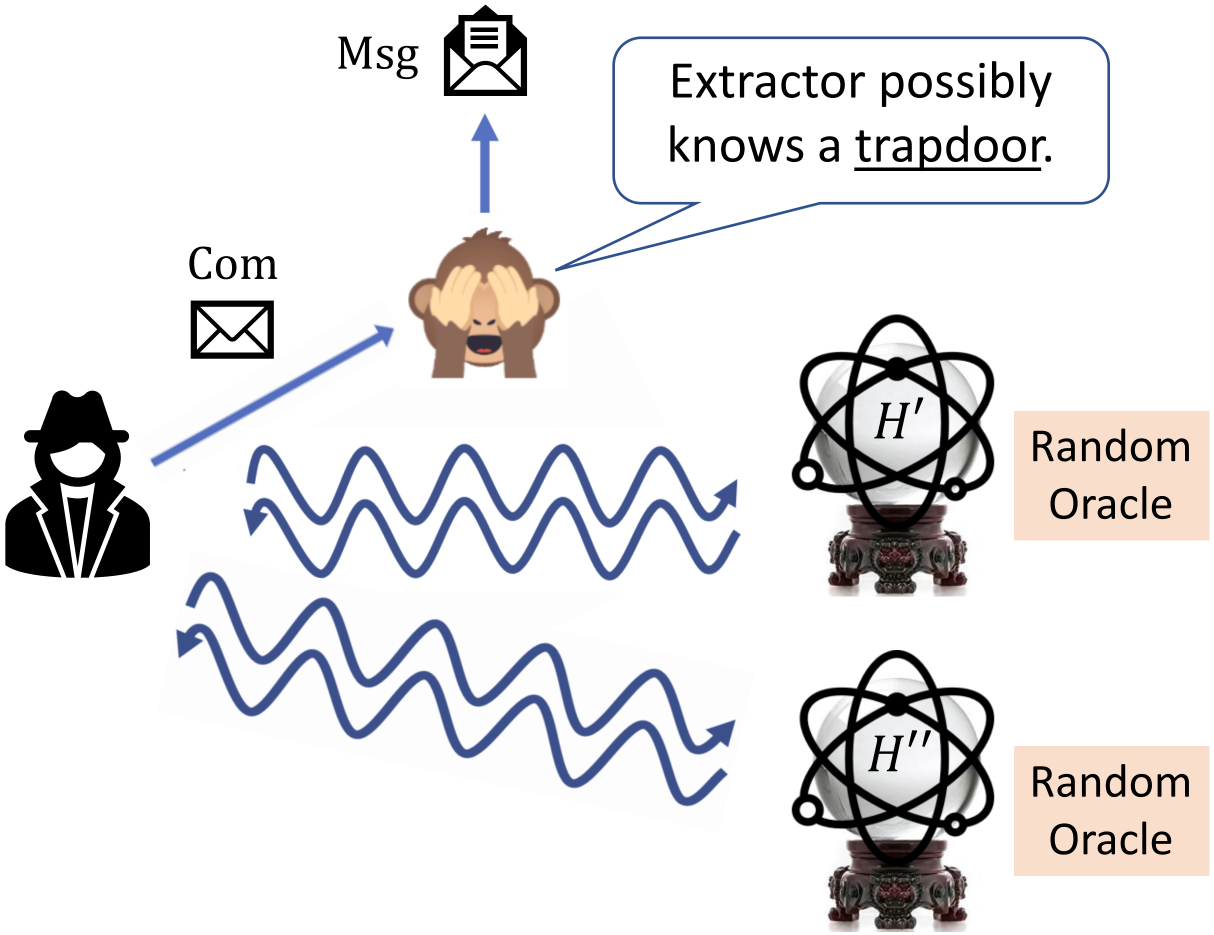
“Textbook” hash-based commitment:
$\text{Com} = H(\text{Msg}, r)$



Extractable Commitments in NO QROM

"Textbook" hash-based commitment:

$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)\end{aligned}$$



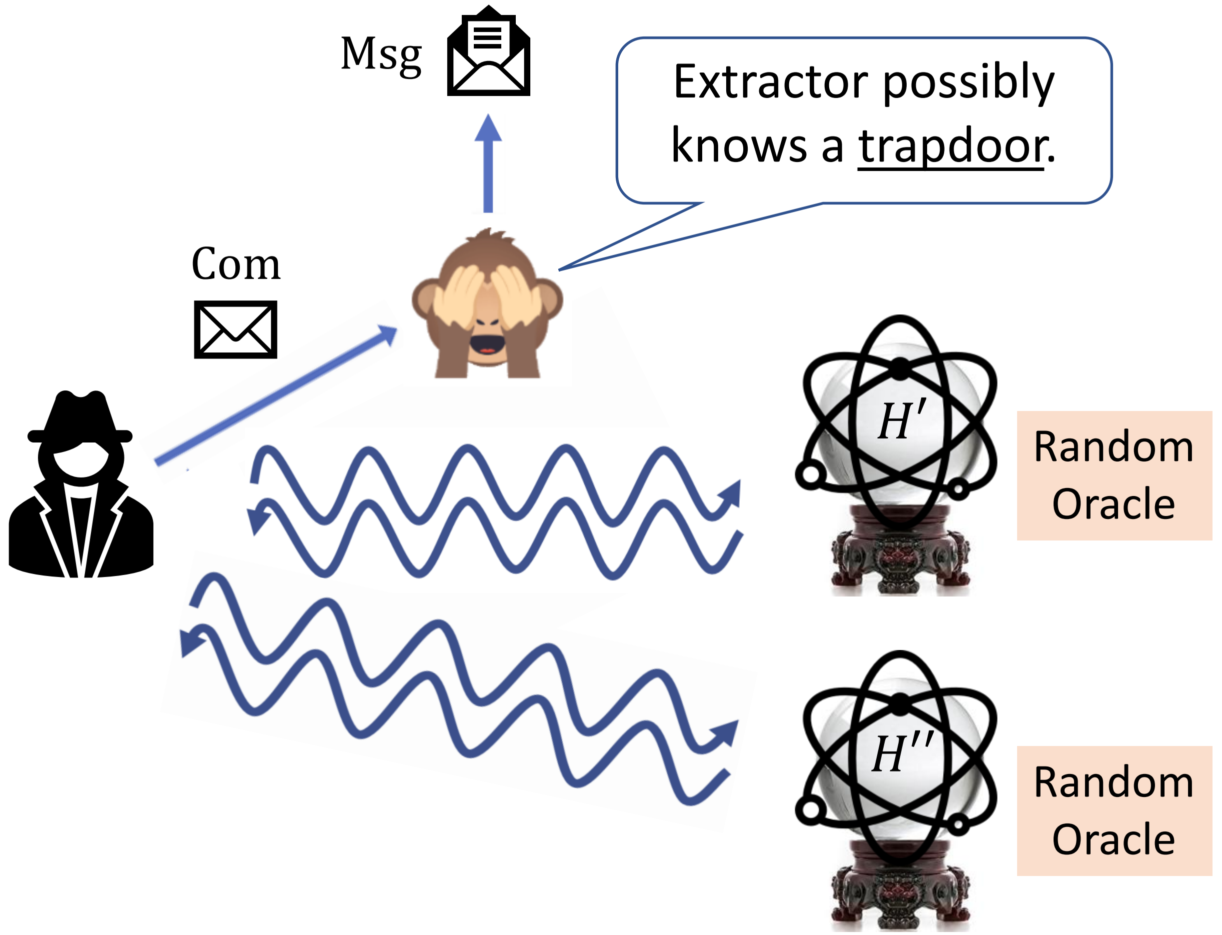
Extractable Commitments in NO QROM

“Textbook” hash-based commitment:

$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)\end{aligned}$$

$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

<u>Same</u> domain and co-domain required for extraction.



Extractable Commitments in NO QROM

"Textbook" hash-based commitment:

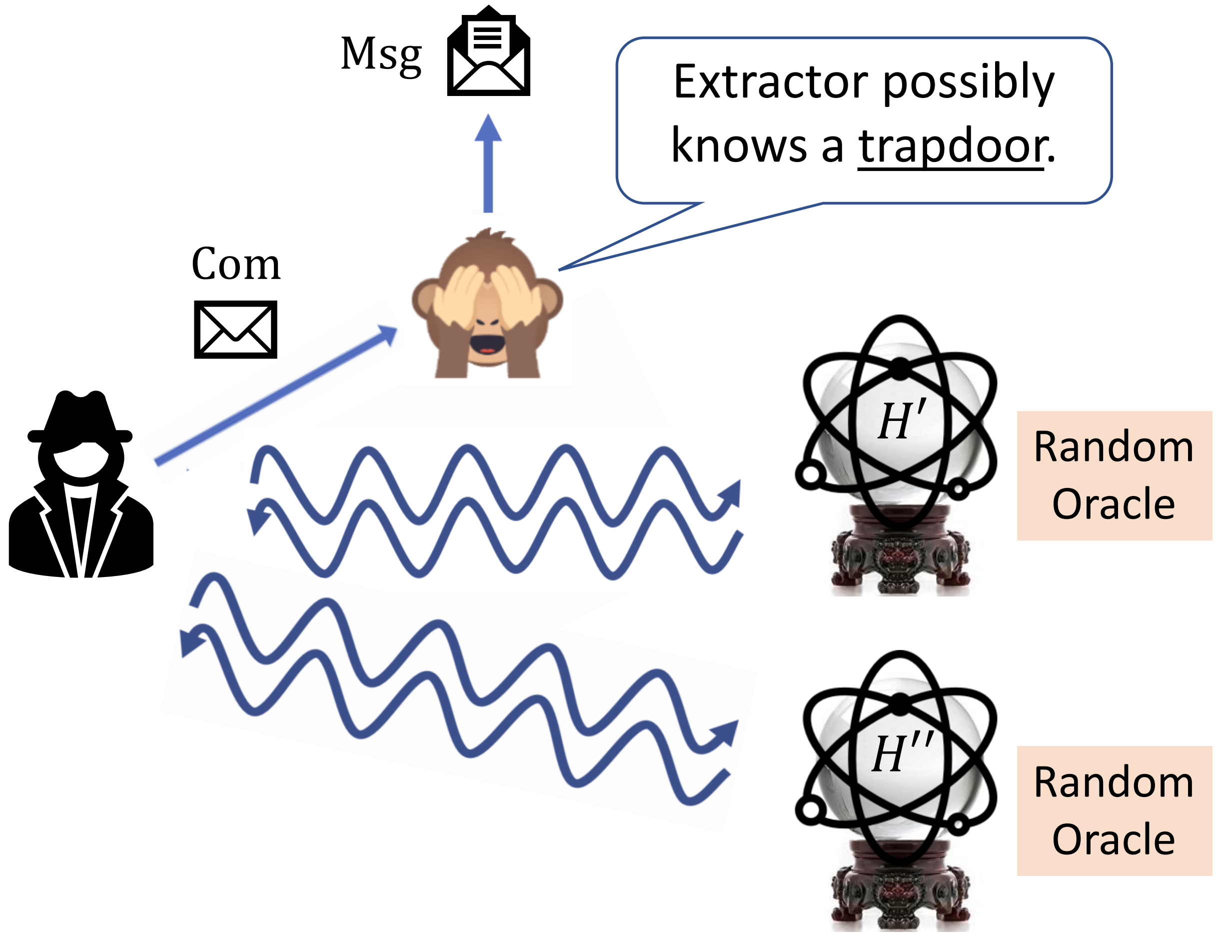
$$\mathrm{Com} = H(\mathrm{Msg}, r)$$
$$= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)$$

$$H' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$$

$$H'' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$$

Same domain and co-domain required for extraction.

Required for (statistical) binding.



Extractable Commitments in NO QROM

"Textbook" hash-based commitment:

$$\mathrm{Com} = H(\mathrm{Msg}, r)$$
$$= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)$$

$H' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Random Oracle

Random Oracle

Same domain and co-domain required for extraction.

Required for (statistical) binding.

Setup phase

Extractable Commitments in NO QROM

"Textbook" hash-based commitment:

$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r)\,||\,H''(\mathrm{Msg}, r)\end{aligned}$$

$H'\colon \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H''\colon \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Same domain and co-domain required for extraction.

Required for (statistical) binding.

Makes at-most q queries to H'.

Random Oracle

Random Oracle

Setup phase

Extractable Commitments in NO QROM

"Textbook" hash-based commitment:

$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)\end{aligned}$$

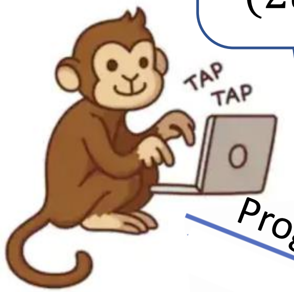
$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Same domain and co-domain required for extraction.

Required for (statistical) binding.

Makes at-most q queries to H'.



Replace H' with a random polynomial F of degree $(2q-1)$ over $\mathbb{F}_{2^{|\mathrm{Msg}|+|r|}}$.

Program H'

Random Oracle

Random Oracle

Setup phase

Extractable Commitments in NO QROM

“Textbook” hash-based commitment:

$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)\end{aligned}$$

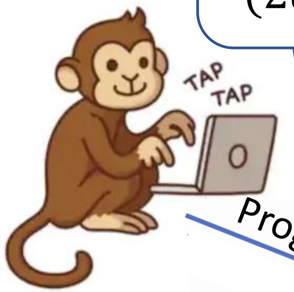
$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

<u>Same</u> domain and co-domain required for extraction.

Required for (statistical) <u>binding</u>.

Replace H' with a random polynomial F of degree $(2q-1)$ over $\mathbb{F}_{2^{|\mathrm{Msg}|+|r|}}$.



Program H'

<u>Perfect</u> indistinguishability of H' and F follows from [Zhandry’12a].

Makes at-most q queries to H'.

Random Oracle

Random Oracle

Setup phase

Extractable Commitments in NO QROM

"Textbook" hash-based commitment:

$$\mathrm{Com} = H(\mathrm{Msg}, r)$$
$$= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)$$

$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

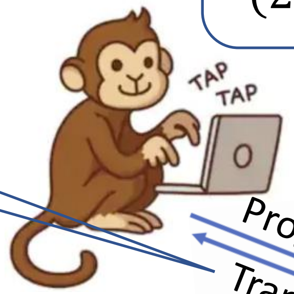
<u>Same</u> domain and co-domain required for extraction.

$H'': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Required for (statistical) <u>binding</u>.

Replace H' with a random polynomial F of degree $(2q-1)$ over $\mathbb{F}_{2^{|\mathrm{Msg}|+|r|}}$.

Polynomial F.



Program H'

Trapdoor

Makes at-most q queries to H'.

<u>Perfect</u> indistinguishability of H' and F follows from [Zhandry'12a].

Random Oracle

Random Oracle

Setup phase

Extractable Commitments in NO QROM

“Textbook” hash-based commitment:

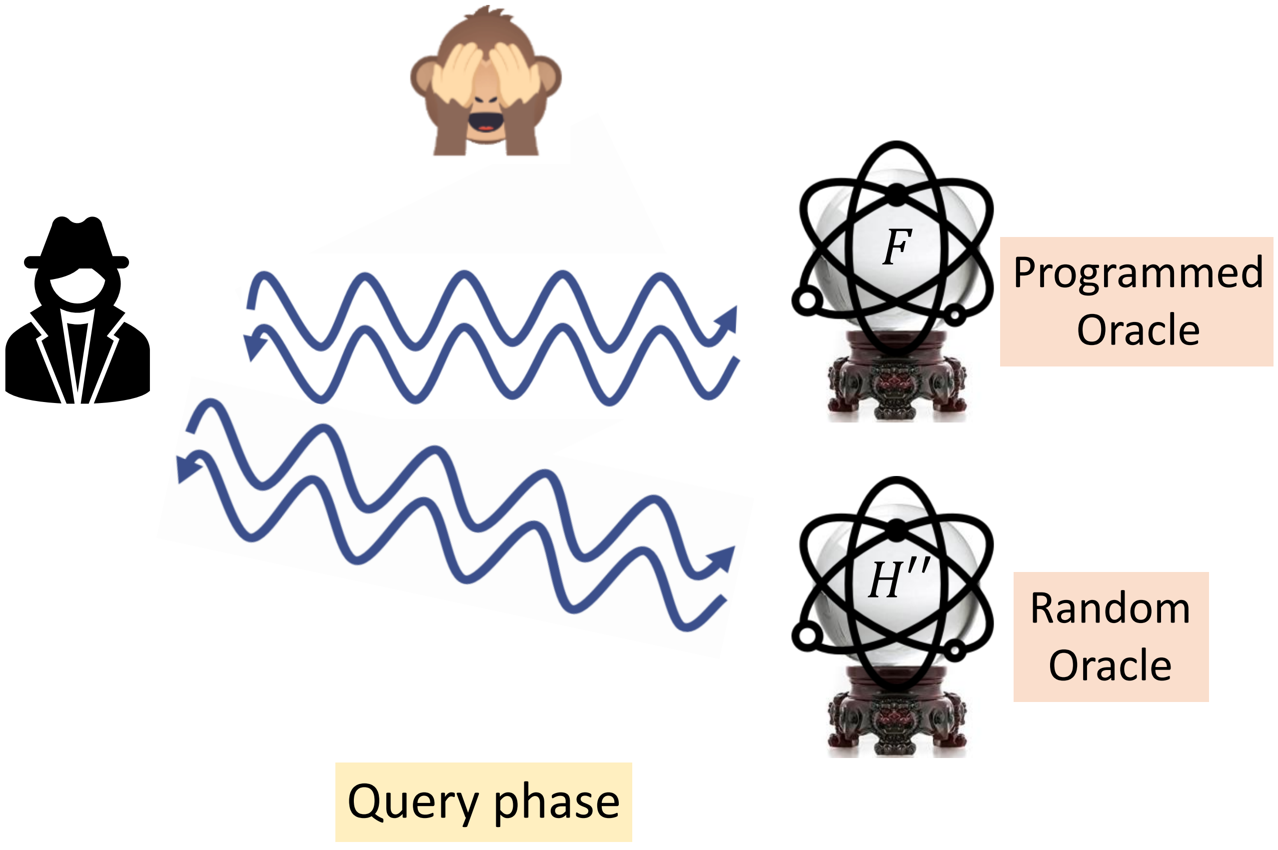
$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r) \\ &= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)\end{aligned}$$

$H' \colon \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

<u>Same</u> domain and co-domain required for extraction.

$H'' \colon \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Required for (statistical) <u>binding</u>.



Extractable Commitments in NO QROM

$$\mathrm{Com} = F(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)$$

"Textbook" hash-based commitment:

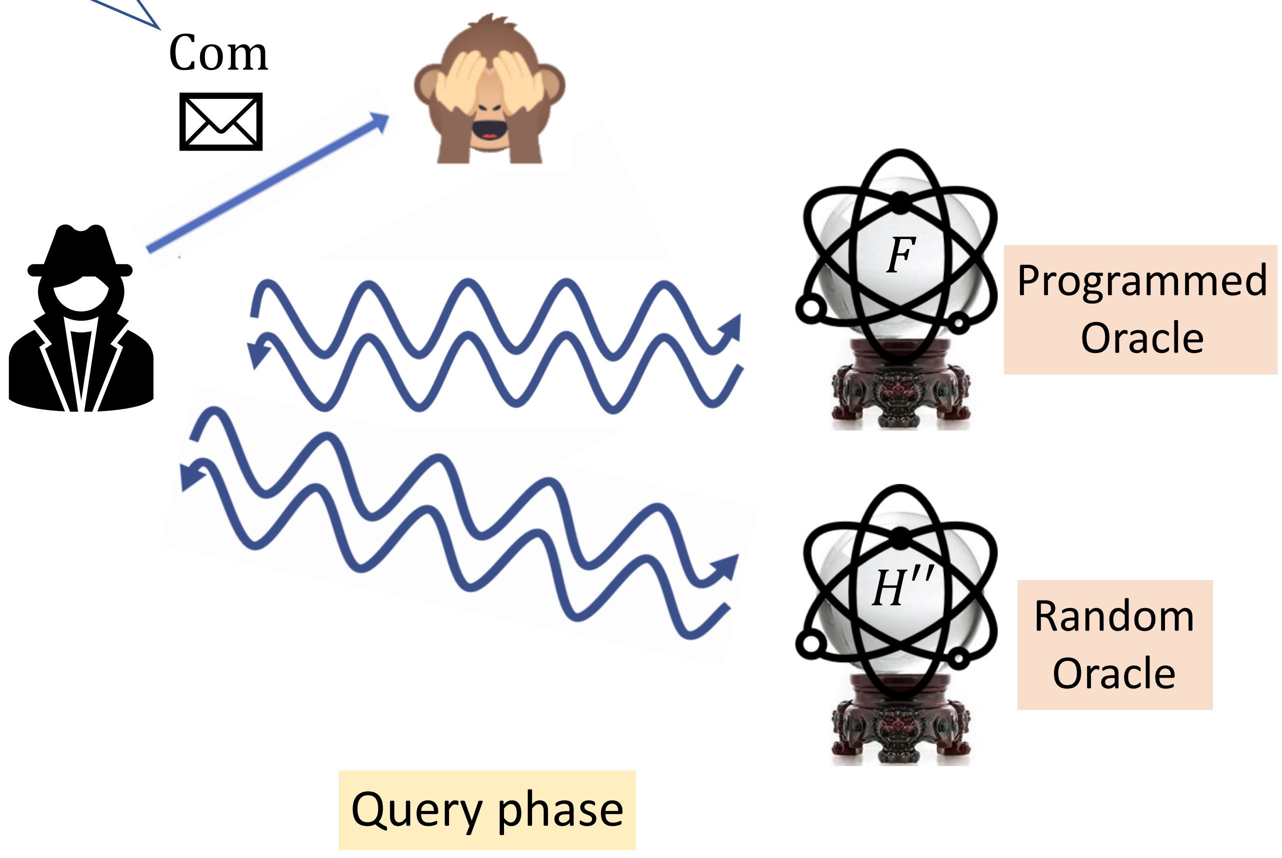
$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r) \\ &= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)\end{aligned}$$

$H' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Same domain and co-domain required for extraction.

Required for (statistical) binding.



Extractable Commitments in NO QROM

$\mathrm{Com} = F(x)||H''(x)$

“Textbook” hash-based commitment:

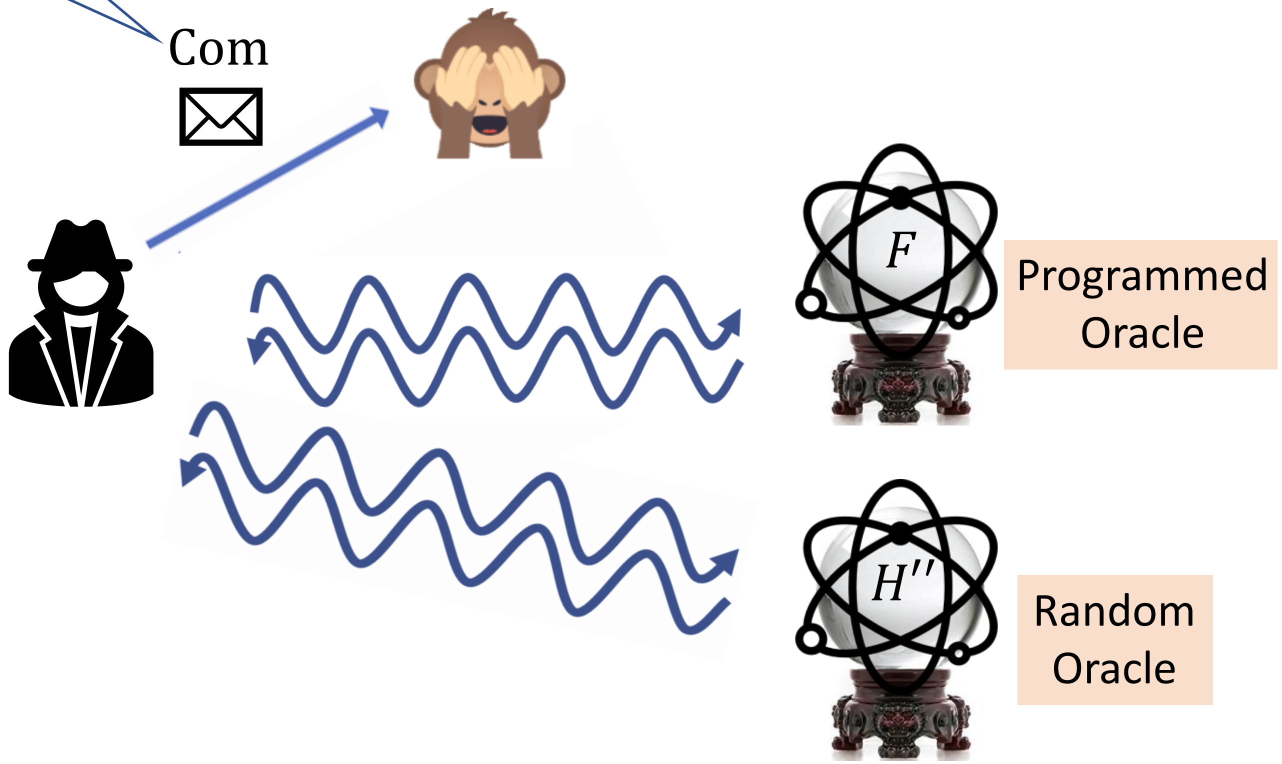
$$\mathrm{Com} = H(\mathrm{Msg}, r)$$
$$= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)$$

$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

<u>Same</u> domain and co-domain required for extraction.

Required for (statistical) <u>binding</u>.



Query phase

Extractable Commitments in NO QROM

$$\mathrm{Com} = \underbrace{F(x)}_{y_1} || \underbrace{H''(x)}_{y_2}$$

“Textbook” hash-based commitment:

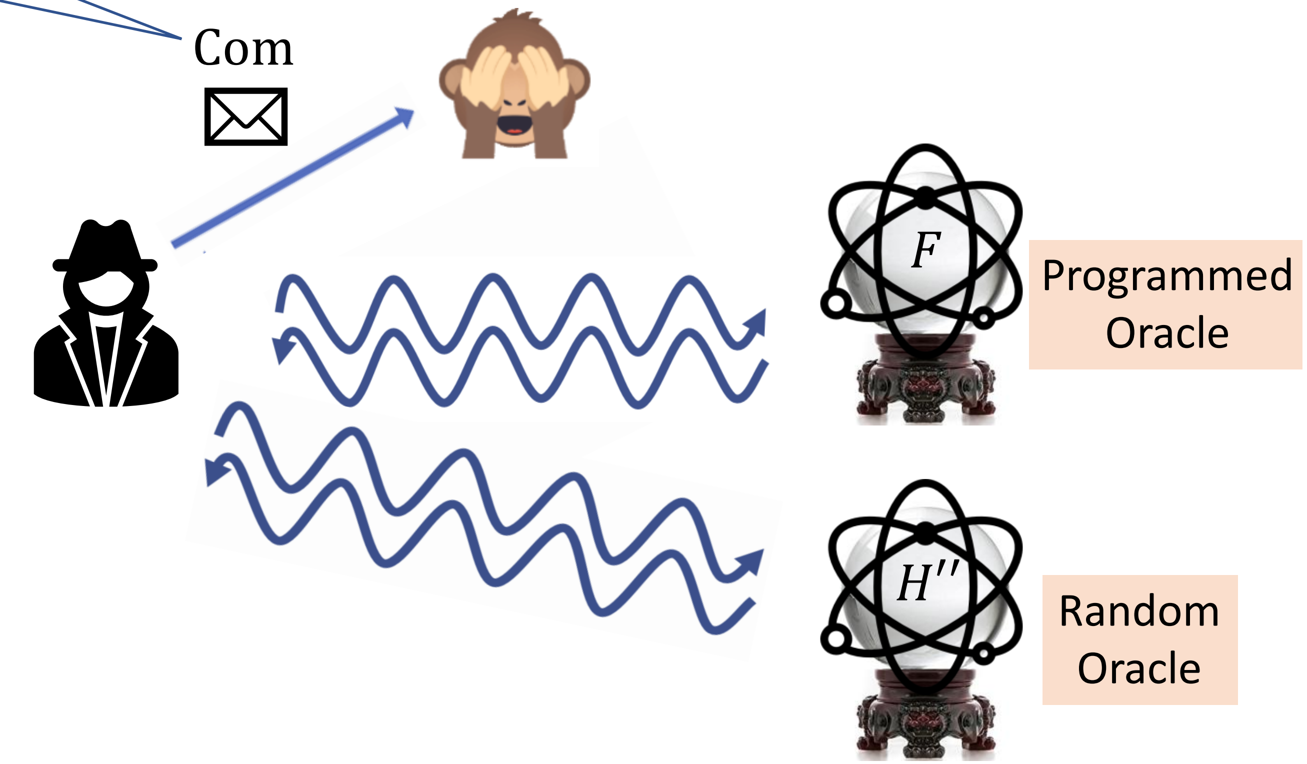
$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r) \\ &= H'(\mathrm{Msg}, r) || H''(\mathrm{Msg}, r)\end{aligned}$$

$H' : \{0,1\}^{|\mathrm{Msg}|+|r|} \rightarrow \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'' : \{0,1\}^{|\mathrm{Msg}|+|r|} \rightarrow \{0,1\}^{\omega(\log \lambda)}$

<u>Same</u> domain and co-domain required for extraction.

Required for (statistical) <u>binding</u>.



Query phase

Extractable Commitments in NO QROM

$$\mathrm{Com} = \underbrace{F(x)}_{y_1}||\underbrace{H''(x)}_{y_2}$$

Computes roots of polynomial $F(X) - y_1$.

"Textbook" hash-based commitment:

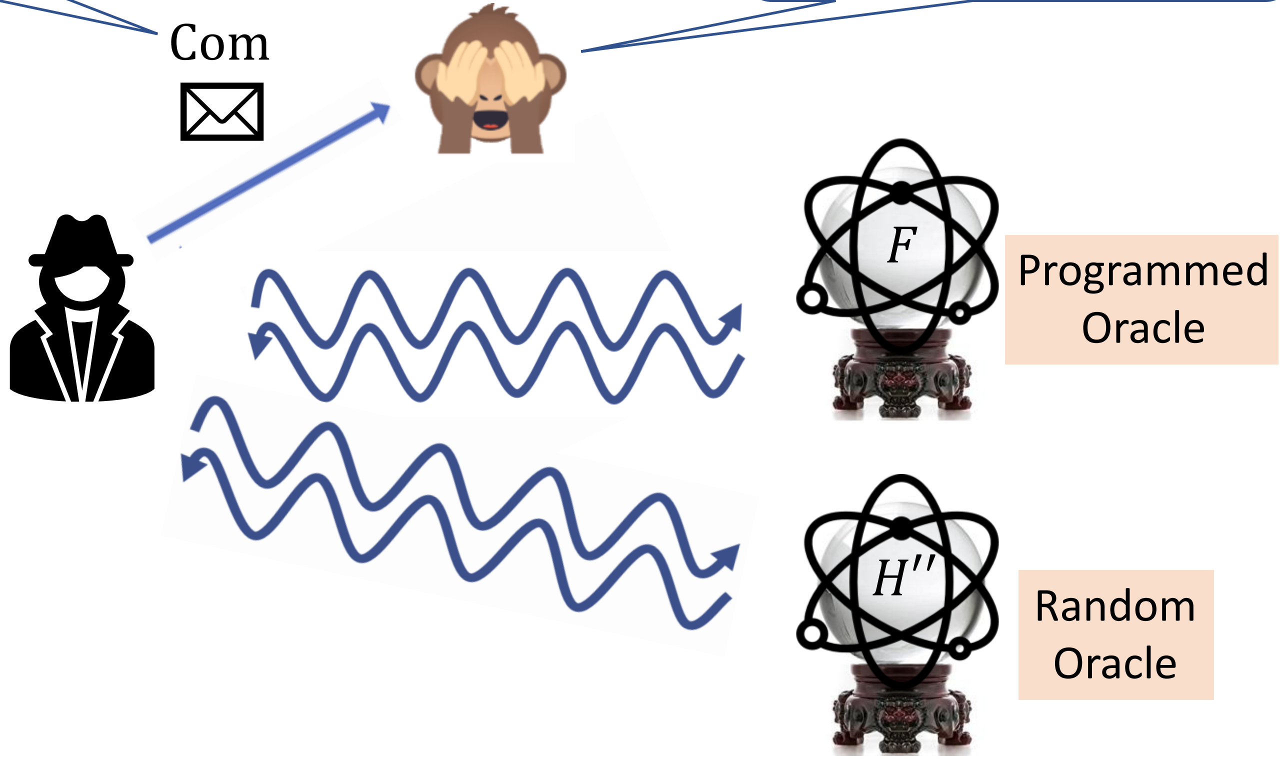
$$\mathrm{Com} = H(\mathrm{Msg}, r)$$
$$= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)$$

$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$

Same domain and co-domain required for extraction.

Required for (statistical) binding.



Query phase

Extractable Commitments in NO QROM

$$\mathrm{Com} = \underbrace{F(x)}_{y_1}||\underbrace{H''(x)}_{y_2}$$

"Textbook" hash-based commitment:

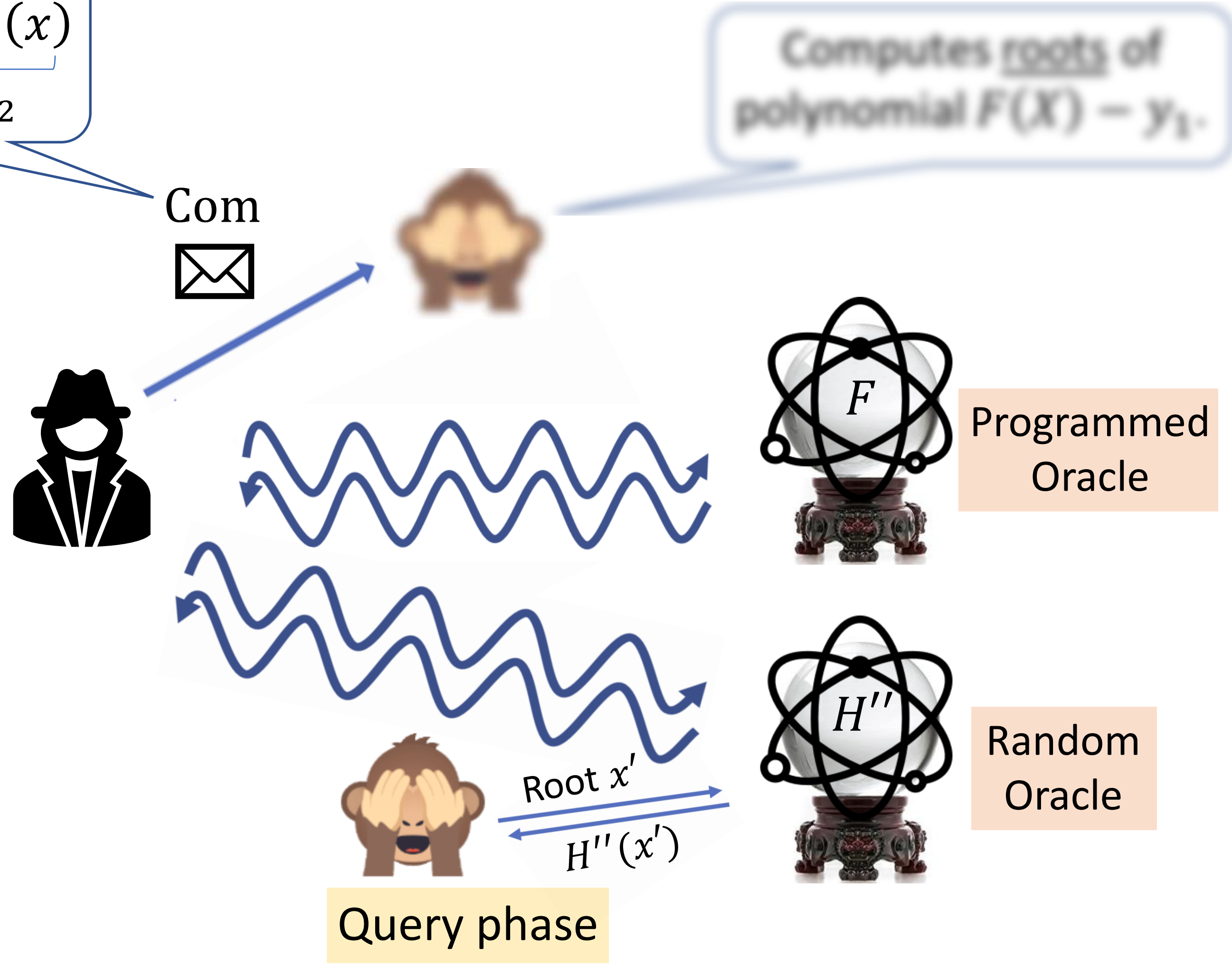
$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)\end{aligned}$$

$$H' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$$

$$H'' : \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log \lambda)}$$

Same domain and co-domain required for extraction.

Required for (statistical) binding.



Extractable Commitments in NO QROM

$$\mathrm{Com} = \underbrace{F(x)}_{y_1}||\underbrace{H''(x)}_{y_2}$$

"Textbook" hash-based commitment:

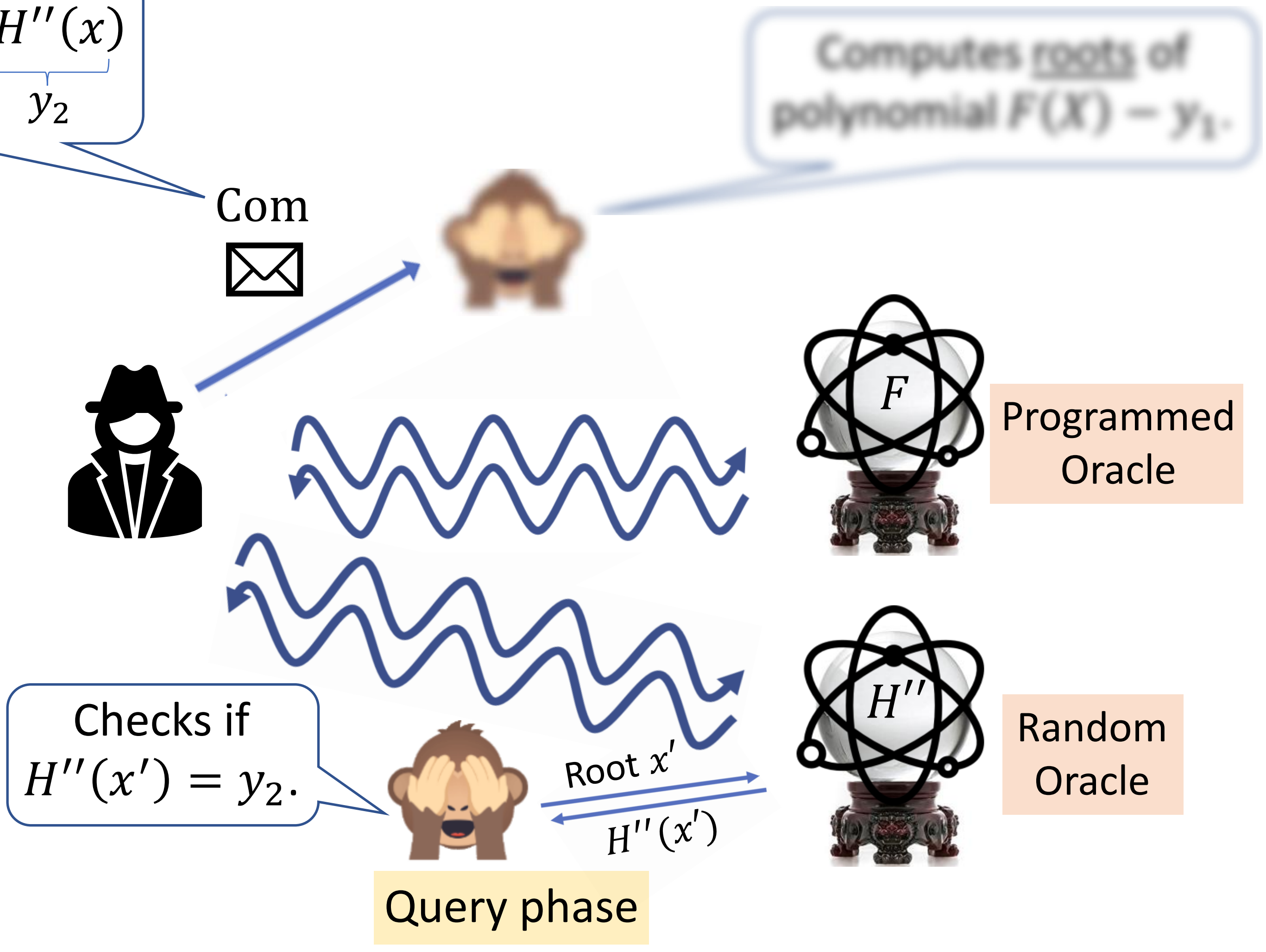
$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r)\\ &= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)\end{aligned}$$

$H': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

$H'': \{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log\lambda)}$

Same domain and co-domain required for extraction.

Required for (statistical) binding.



Extractable Commitments in NO QROM

$$\mathrm{Com} = \underbrace{F(x)}_{y_1}||\underbrace{H''(x)}_{y_2}$$

"Textbook" hash-based commitment:

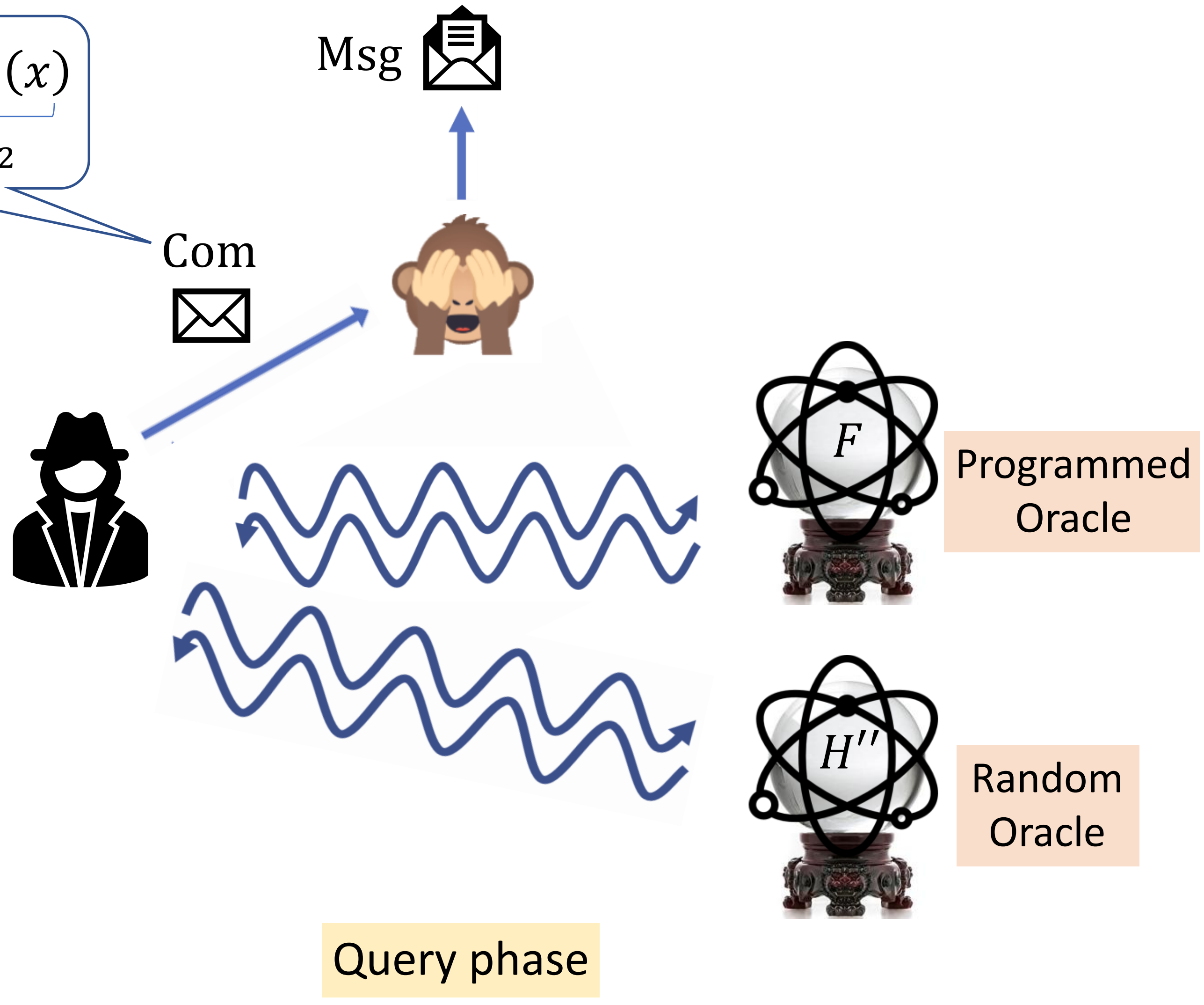
$$\begin{aligned}\mathrm{Com} &= H(\mathrm{Msg}, r) \\ &= H'(\mathrm{Msg}, r)||H''(\mathrm{Msg}, r)\end{aligned}$$

$H'\colon\{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{|\mathrm{Msg}|+|r|}$

<u>Same</u> domain and co-domain required for extraction.

$H''\colon\{0,1\}^{|\mathrm{Msg}|+|r|} \to \{0,1\}^{\omega(\log\lambda)}$

Required for (statistical) <u>binding</u>.



Extractable Commitments in NO QROM

$$\text{Com} = \underbrace{F(x)}_{y_1} || \underbrace{H''(x)}_{y_2}$$

"Textbook" hash-based commitment:

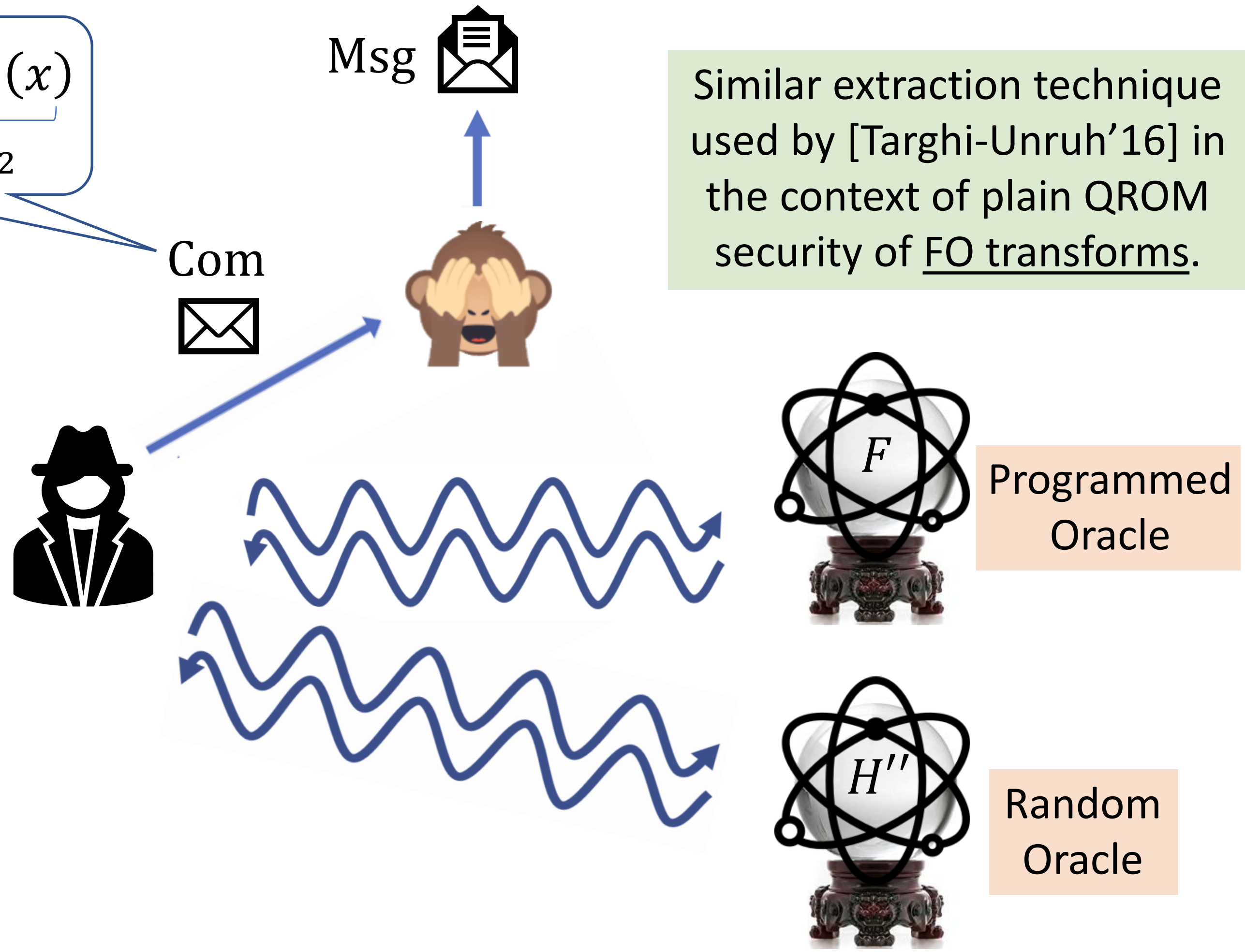
$$\begin{aligned}\text{Com} &= H(\text{Msg}, r)\\ &= H'(\text{Msg}, r) || H''(\text{Msg}, r)\end{aligned}$$

$H' : \{0,1\}^{|\text{Msg}|+|r|} \rightarrow \{0,1\}^{|\text{Msg}|+|r|}$

<u>Same</u> domain and co-domain required for extraction.

$H'' : \{0,1\}^{|\text{Msg}|+|r|} \rightarrow \{0,1\}^{\omega(\log \lambda)}$

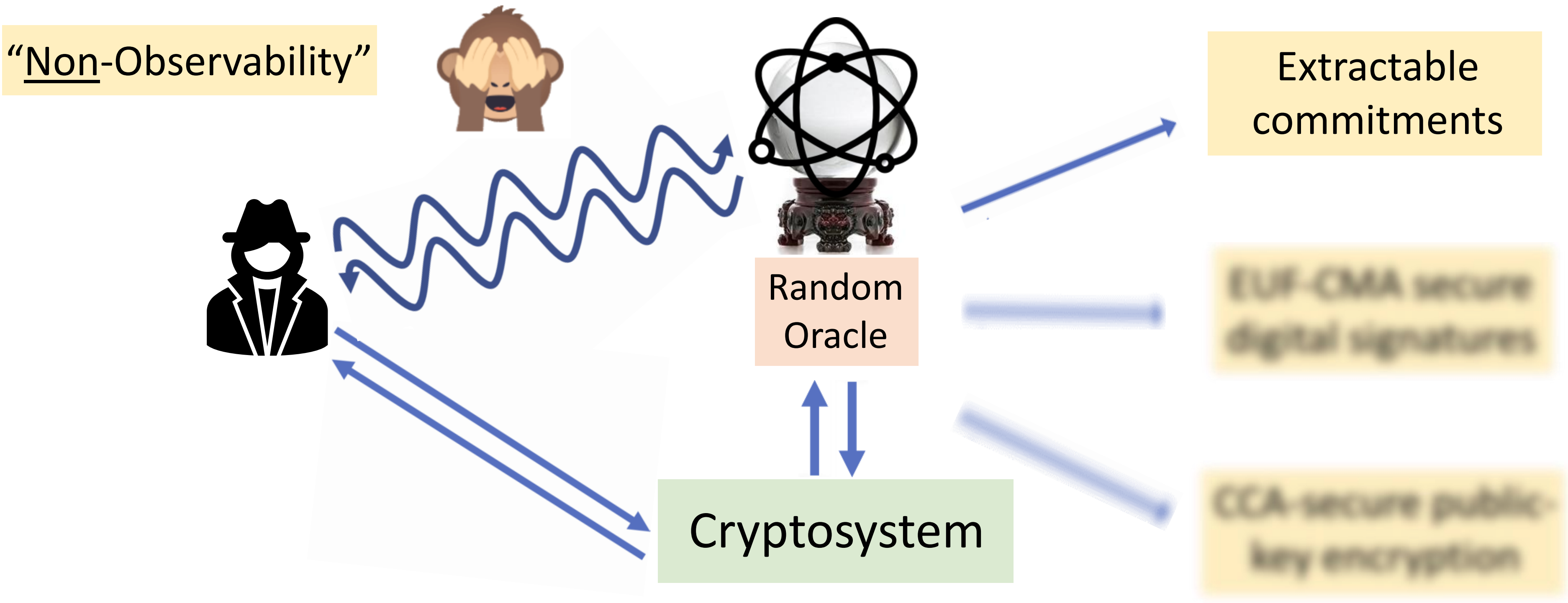
Required for (statistical) <u>binding</u>.



Similar extraction technique used by [Targhi-Unruh'16] in the context of plain QROM security of <u>FO transforms</u>.

Query phase

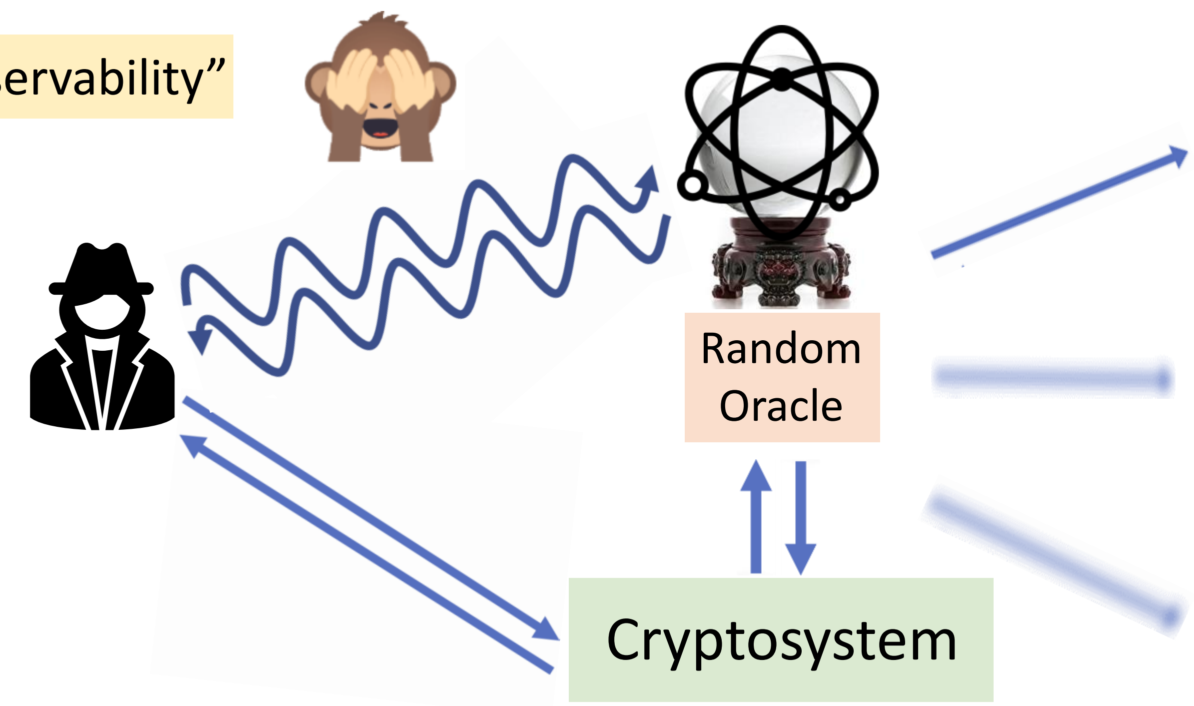
Non-Observable QROM (NO QROM)



Formalized by [Alamati-Maram-Masny’23].

Non-Observable QROM (NO QROM)

"Non-Observability"



Extractable commitments

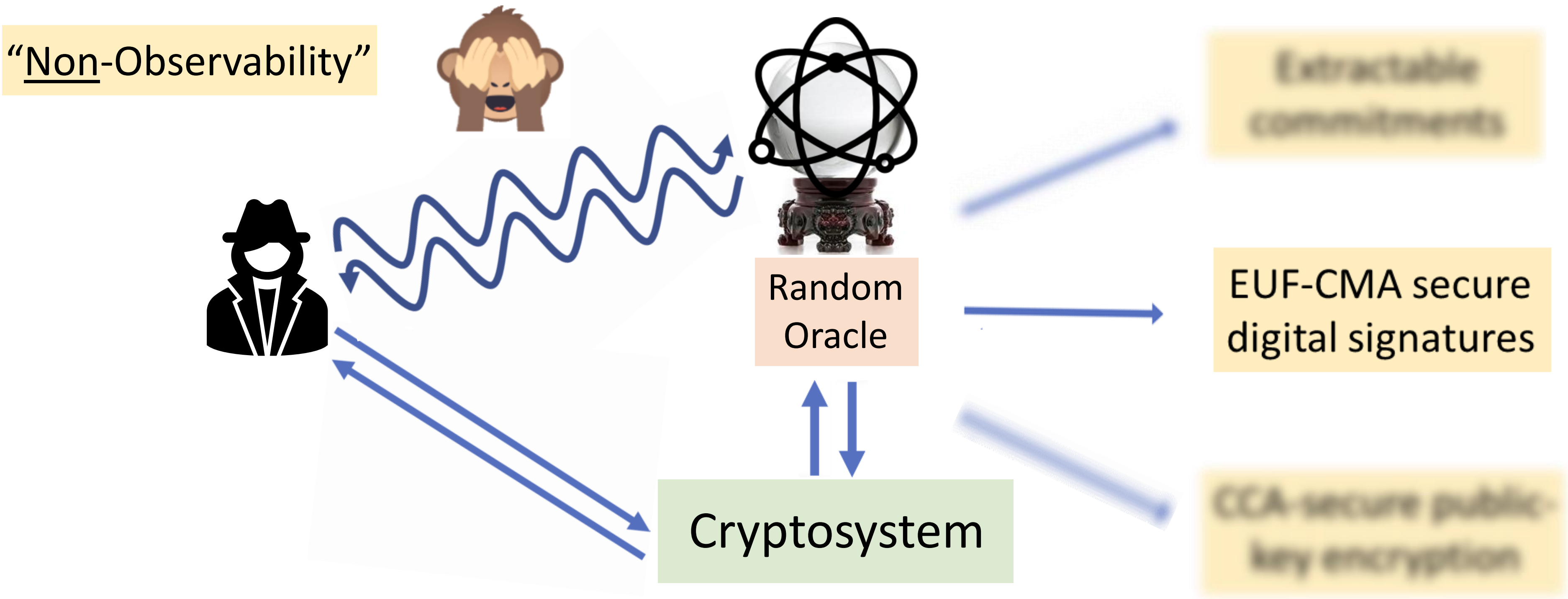
EUF-CMA secure digital signatures

CCA-secure public-key encryption

- Obtained shorter commitments using "small-range distribution" technique of [Zhandry'12b]
  - However, requires superpolynomial extractors.
- Showed hiding property of our commitments via the notion of non-malleability.

Formalized by [Alamati-Maram-Masny'23].

Non-Observable QROM (NO QROM)



Formalized by [Alamati-Maram-Masny’23].

EUF-CMA Secure Signatures in NO QROM

Full-Domain Hash (FDH) Signature

Formalized by [Bellare-Rogaway'93].

EUF-CMA Secure Signatures in NO QROM

Trapdoor Permutation (TDP)

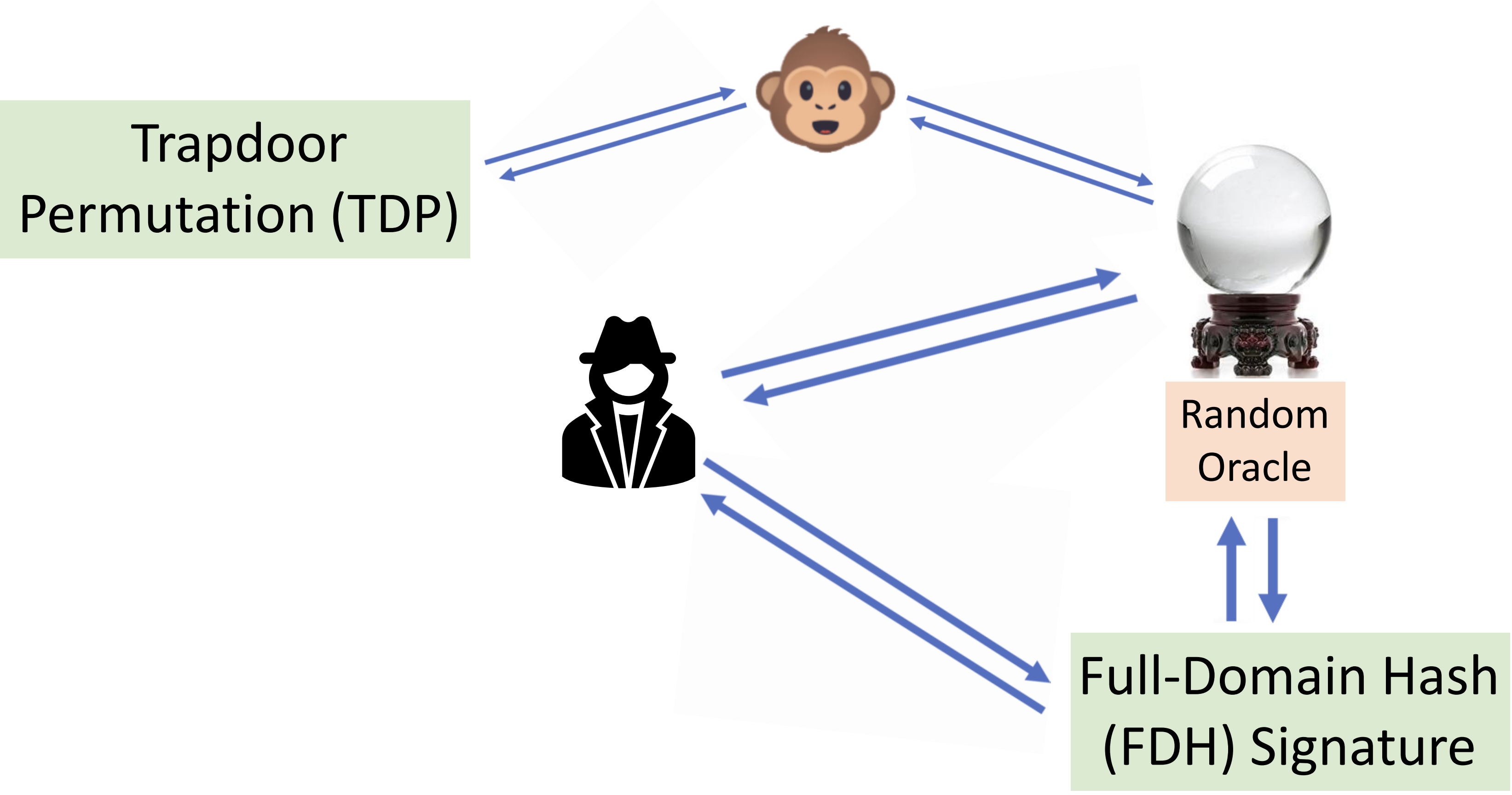
+

Random Oracle

Full-Domain Hash (FDH) Signature

Formalized by [Bellare-Rogaway'93].

EUF-CMA Secure Signatures in NO QROM

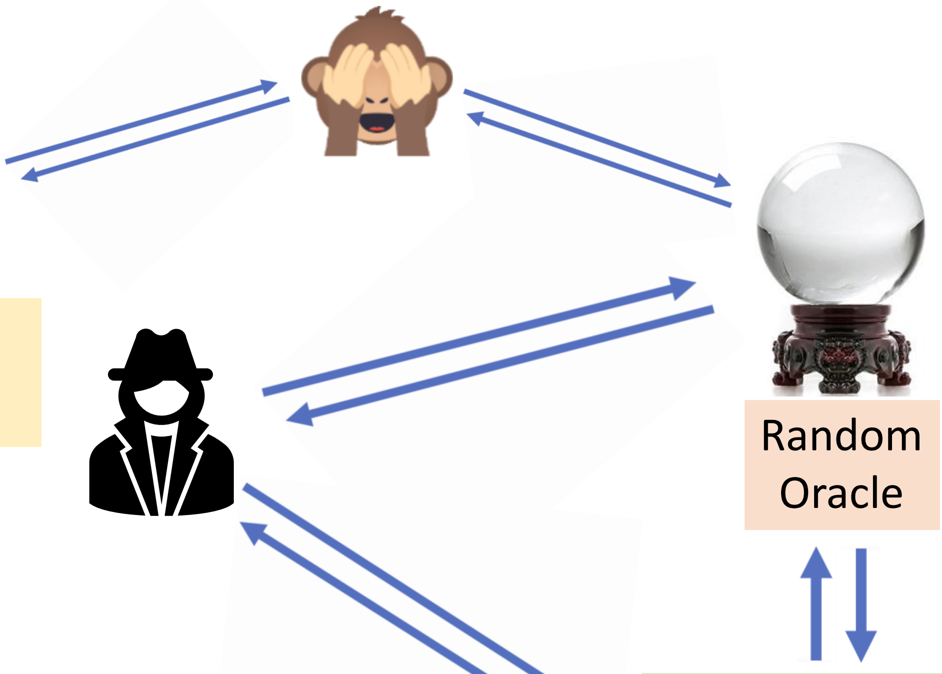


Formalized by [Bellare-Rogaway’93].

EUF-CMA Secure Signatures in NO QROM

Trapdoor Permutation (TDP)

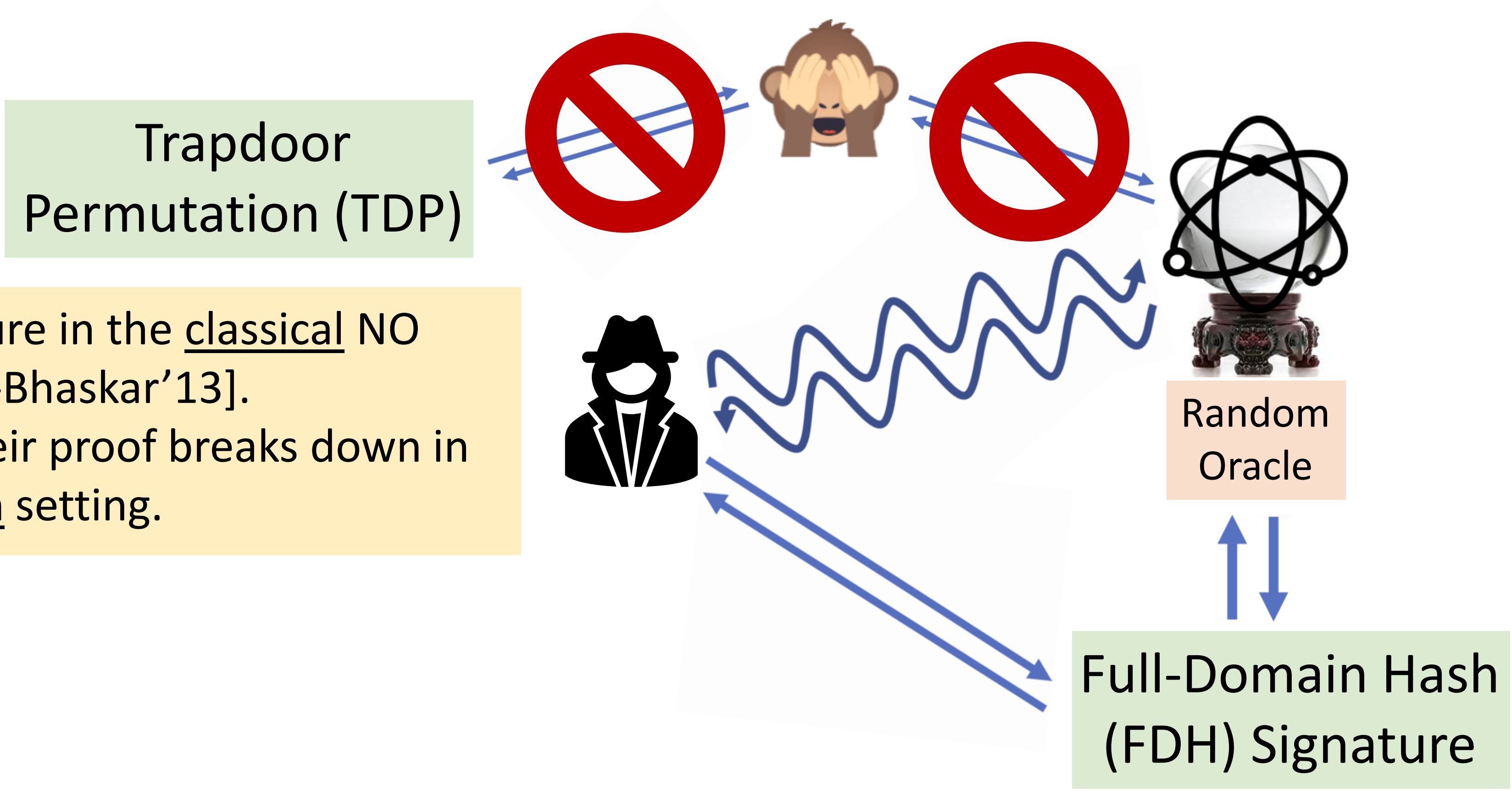
- Shown to be secure in the <u>classical</u> NO ROM by [Ananth-Bhaskar’13].



Full-Domain Hash (FDH) Signature

Formalized by [Bellare-Rogaway’93].

EUF-CMA Secure Signatures in NO QROM



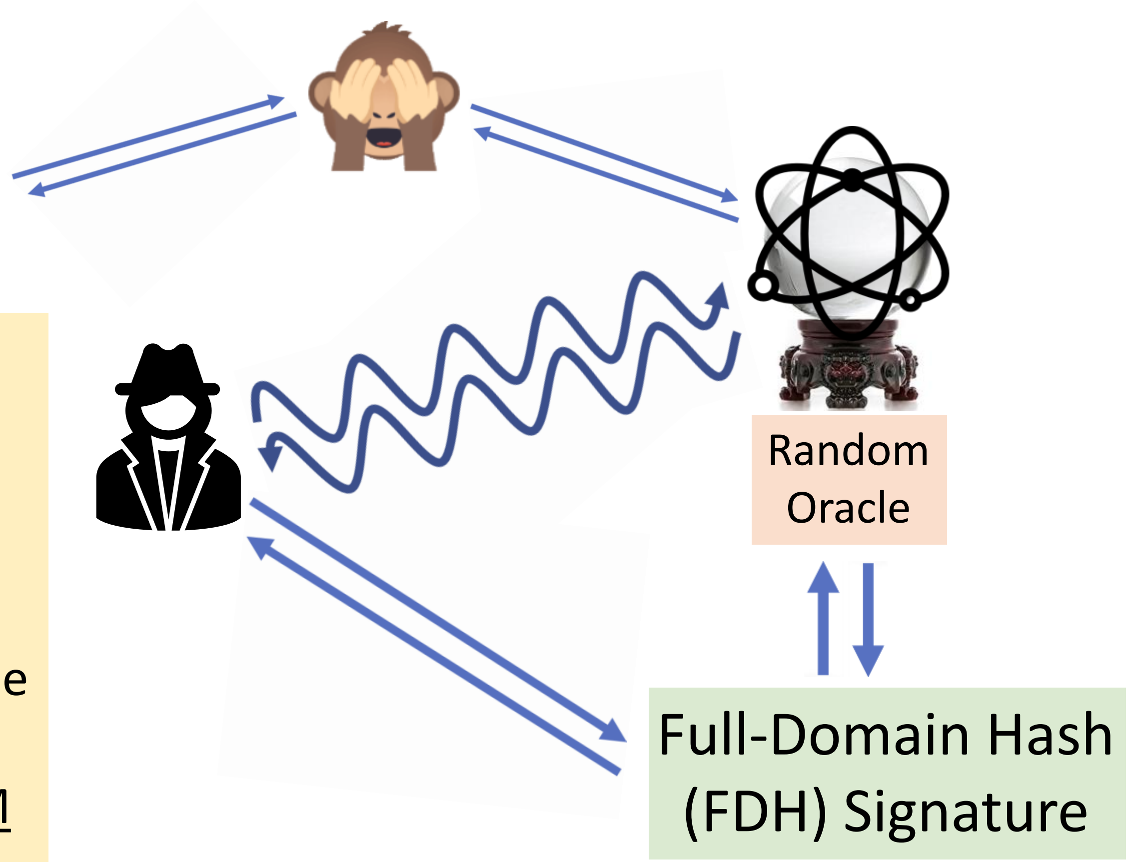
- Shown to be secure in the <u>classical</u> NO ROM by [Ananth-Bhaskar'13].
    - However, their proof breaks down in the <u>quantum</u> setting.

Formalized by [Bellare-Rogaway'93].

EUF-CMA Secure Signatures in NO QROM

Trapdoor Permutation (TDP)

- Shown to be secure in the classical NO ROM by [Ananth-Bhaskar'13].
  - However, their proof breaks down in the quantum setting.
- We prove security of FDH signatures in the NO QROM [Alamati-Maram-Masny'23].
  - Adapted [Zhandry'12a]'s plain QROM security proof.

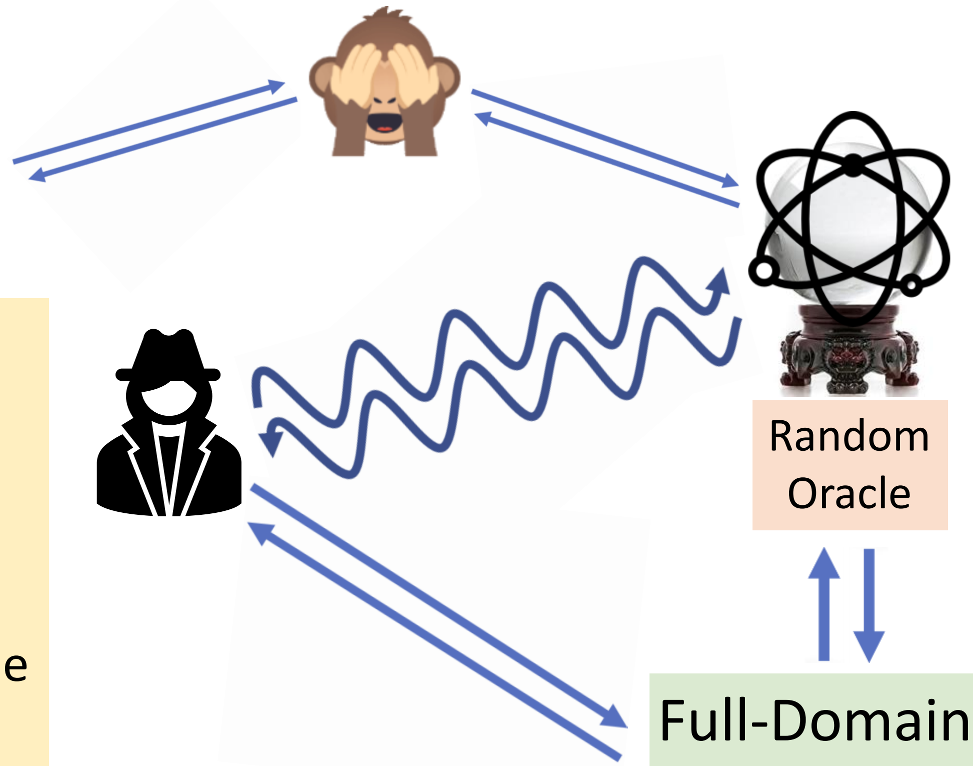


Formalized by [Bellare-Rogaway'93].

EUF-CMA Secure Signatures in NO QROM

Quantum-secure?

Trapdoor Permutation (TDP)



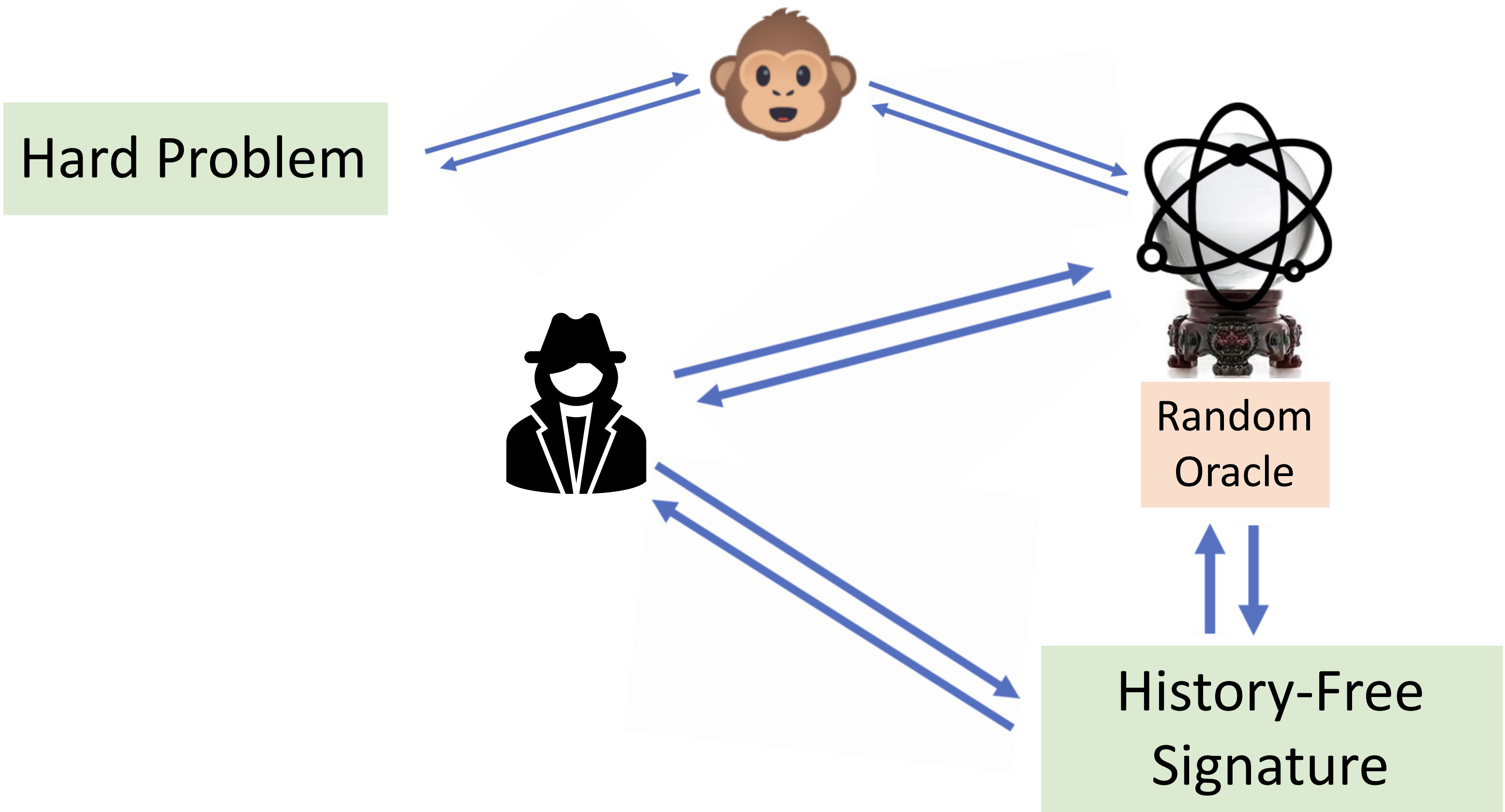
Random Oracle

Full-Domain Hash (FDH) Signature

Formalized by [Bellare-Rogaway'93].

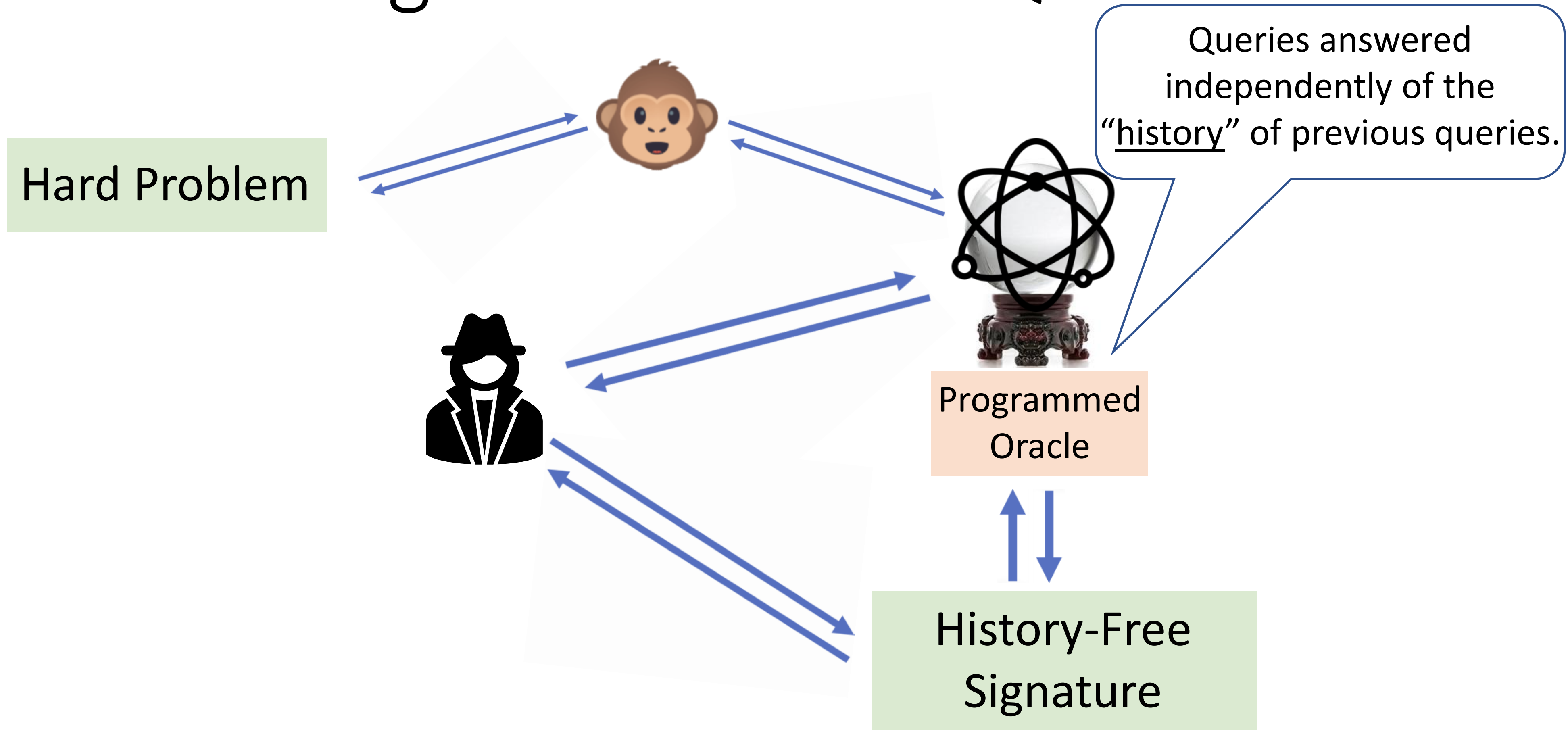
- Shown to be secure in the <u>classical</u> NO ROM by [Ananth-Bhaskar'13].
  - However, their proof breaks down in the <u>quantum</u> setting.
- We prove security of FDH signatures in the <u>NO QROM</u> [Alamati-Maram-Masny'23].
  - Adapted [Zhandry'12a]'s <u>plain QROM</u> security proof.
- However, <u>no concrete instantiations</u> of post-quantum TDPs known.

EUF-CMA Secure Signatures in NO QROM



Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

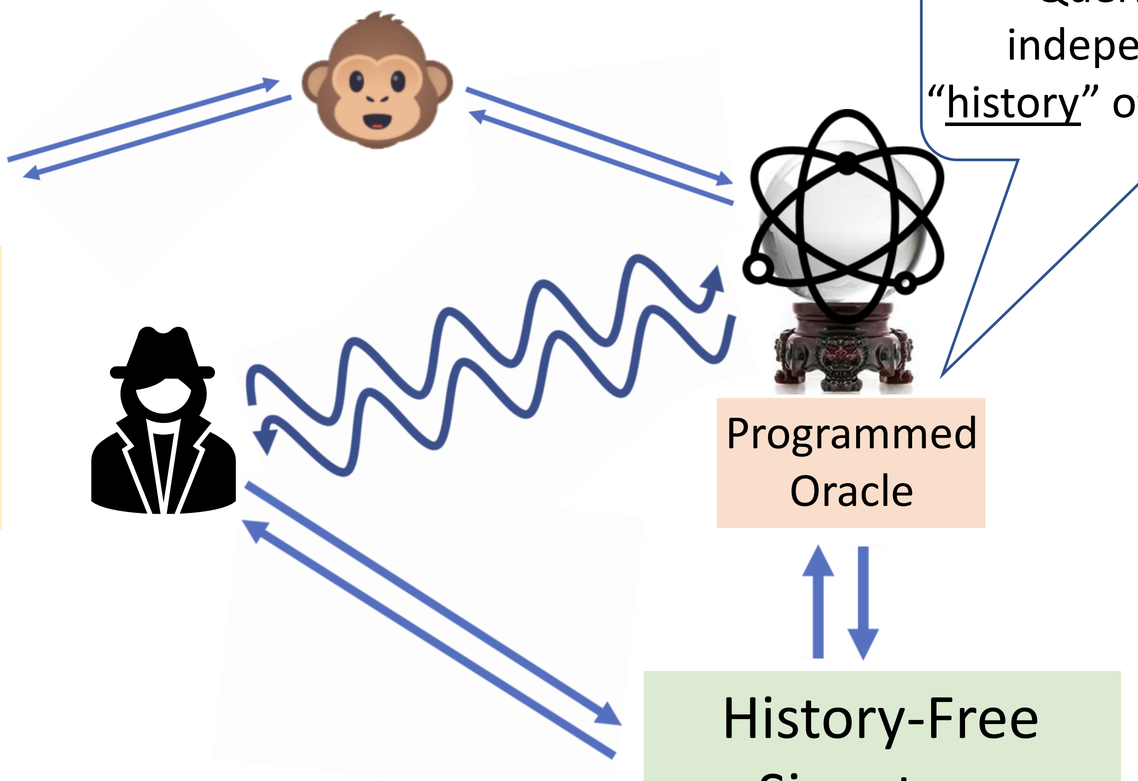
EUF-CMA Secure Signatures in NO QROM



Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

EUF-CMA Secure Signatures in NO QROM

Hard Problem

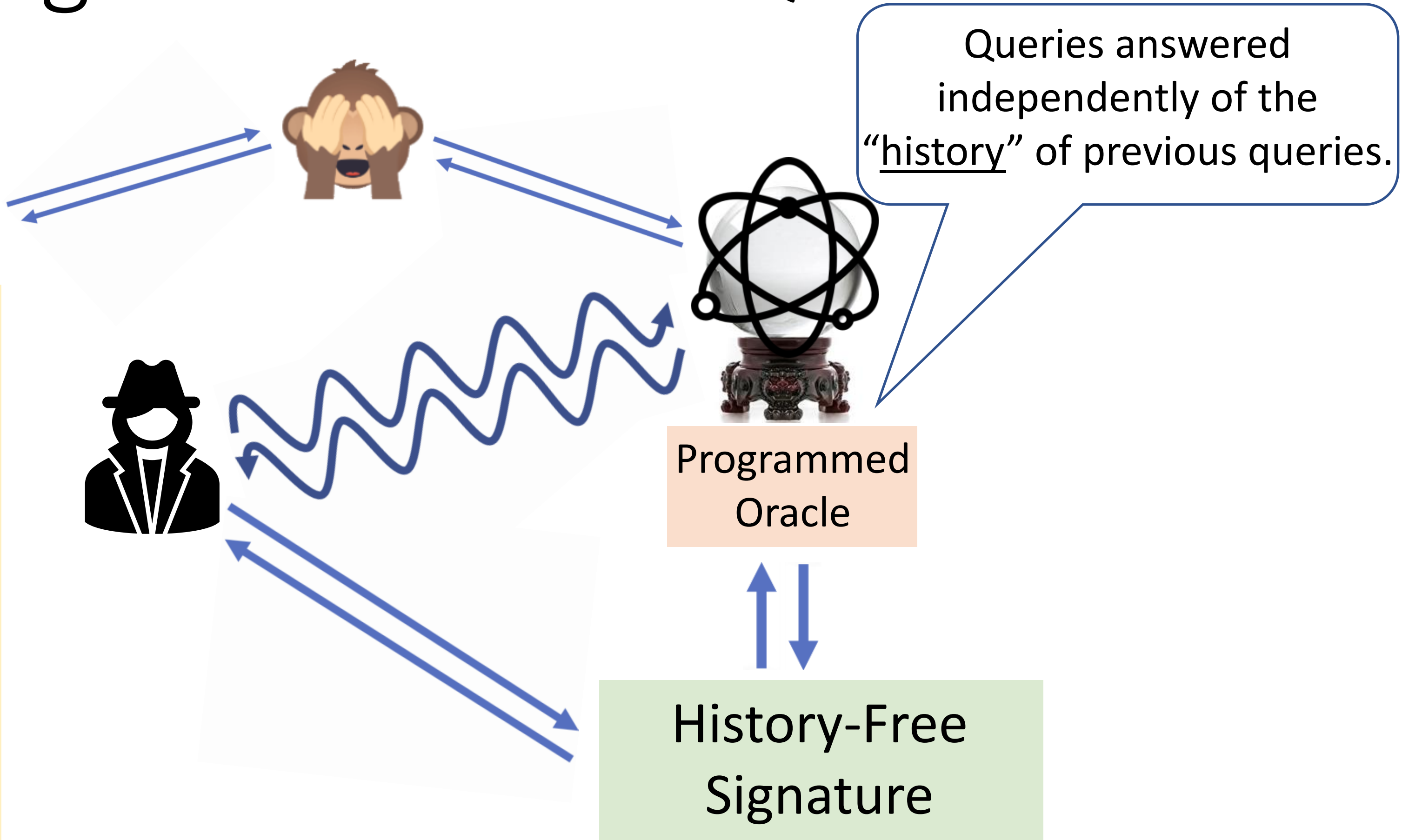


- ROM security proof of history-free signatures can be lifted to (plain) QROM [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

EUF-CMA Secure Signatures in NO QROM

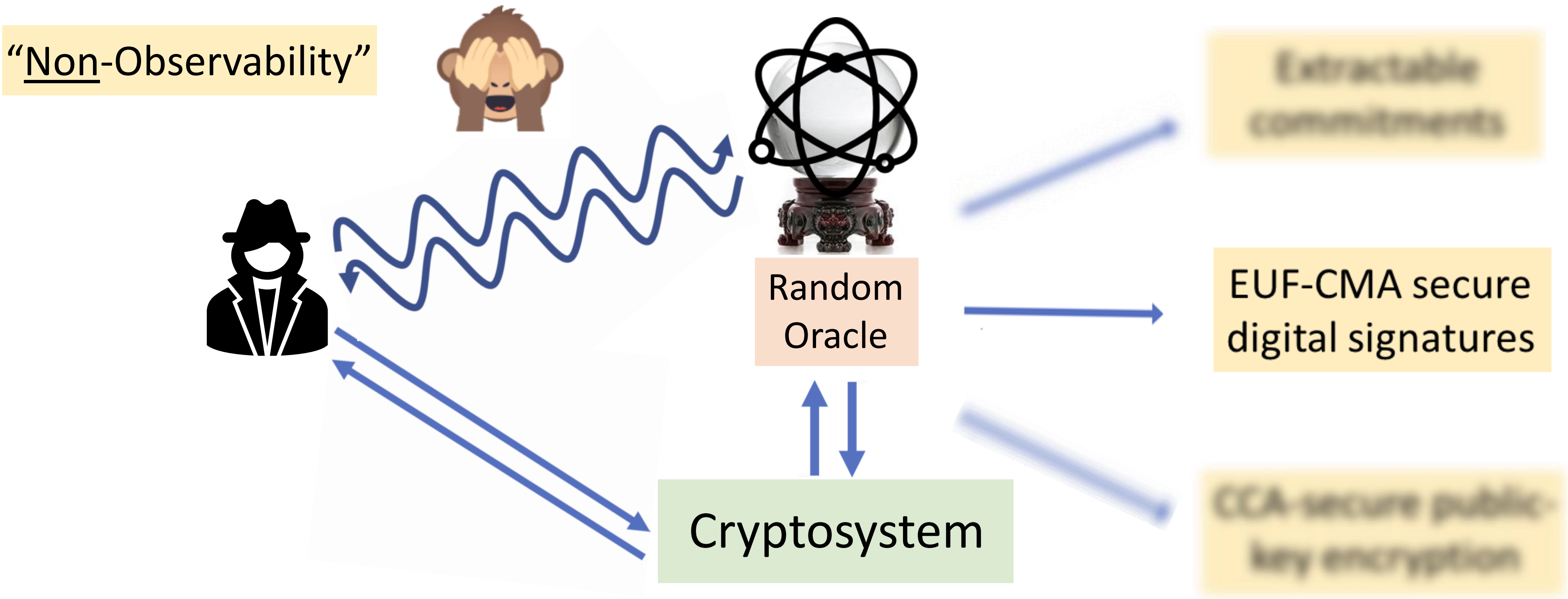
Hard Problem



- ROM security proof of history-free signatures can be lifted to (plain) QROM [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].
- We extend the above result to show security in the NO QROM [Alamati-Maram-Masny'23].
- Lattice-based signatures of [Gentry-Peikert-Vaikuntanathan'08] and Fiat-Shamir signatures in [Kiltz-Lyubashevsky-Schaffner'18] are history-free.

Formalized by [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Zhandry'11].

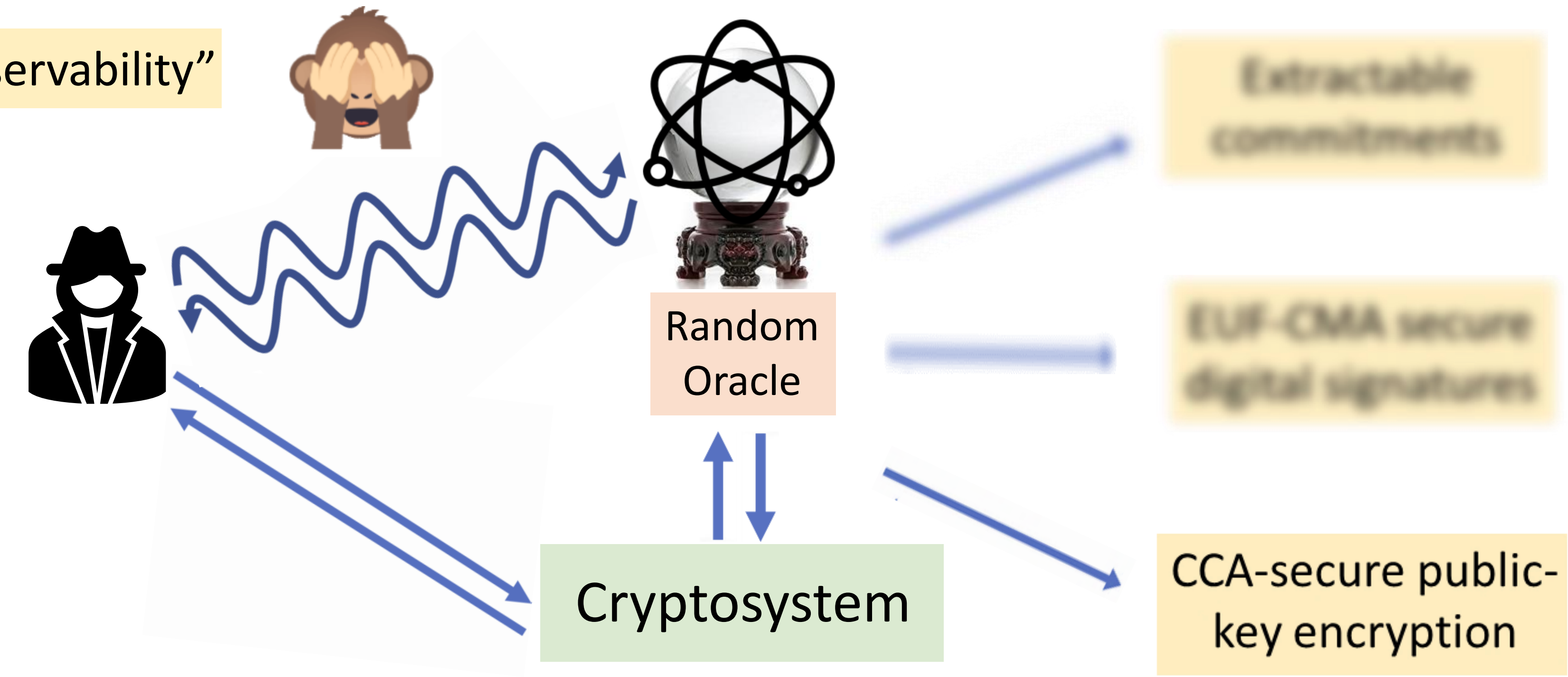
Non-Observable QROM (NO QROM)



Formalized by [Alamati-Maram-Masny'23].

Non-Observable QROM (NO QROM)

"Non-Observability"



Formalized by [Alamati-Maram-Masny'23].

CCA-Secure Public-Key Encryption in NO QROM

CCA-Secure PKE

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

Random Oracle

+

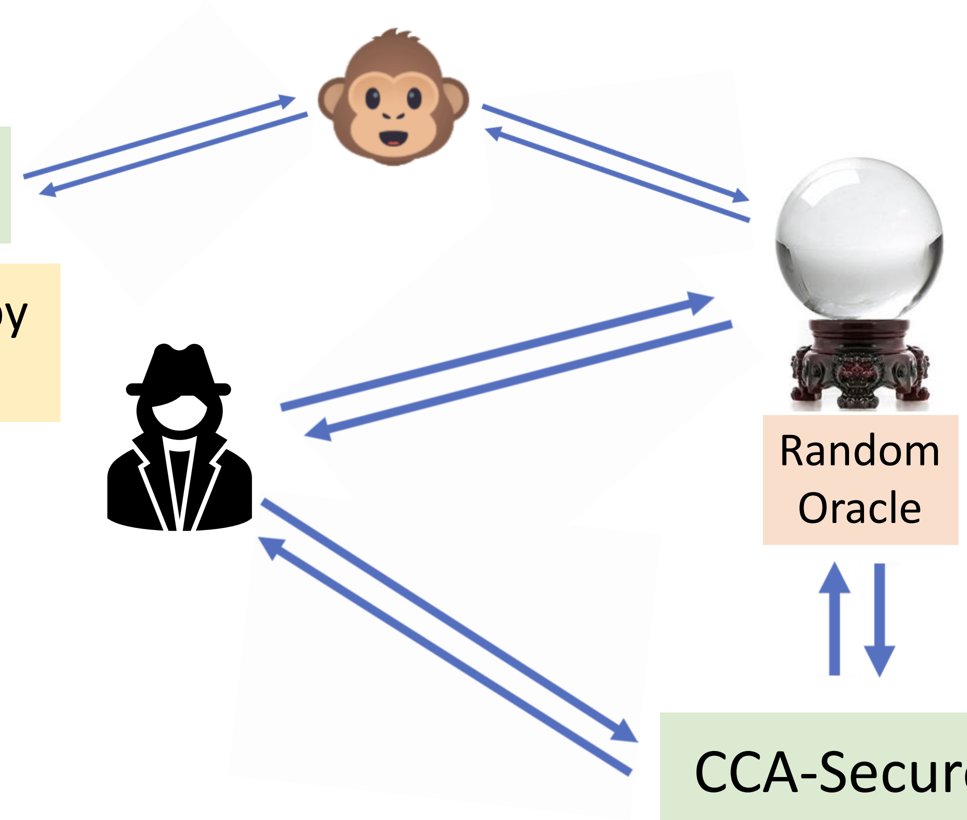
CCA-Secure PKE

Transformation introduced by [Fujisaki-Okamoto’99].

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

- Shown to be secure in the <u>classical ROM</u> by [Fujisaki-Okamoto'99].

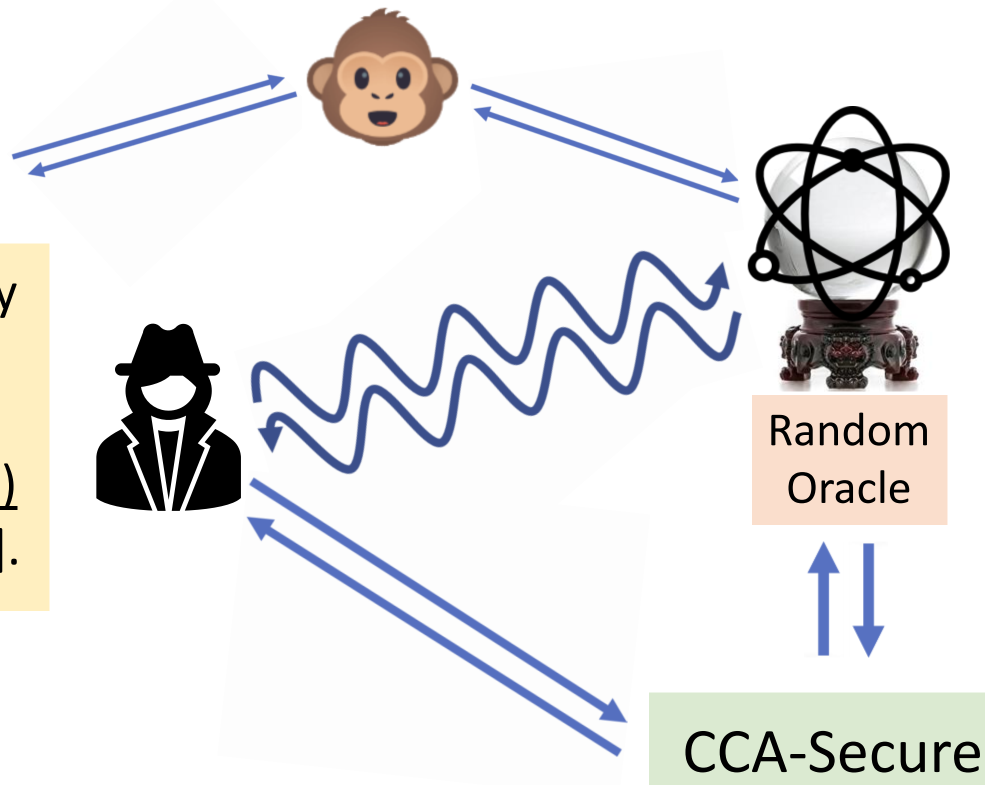


CCA-Secure PKE

Transformation introduced by [Fujisaki-Okamoto'99].

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE



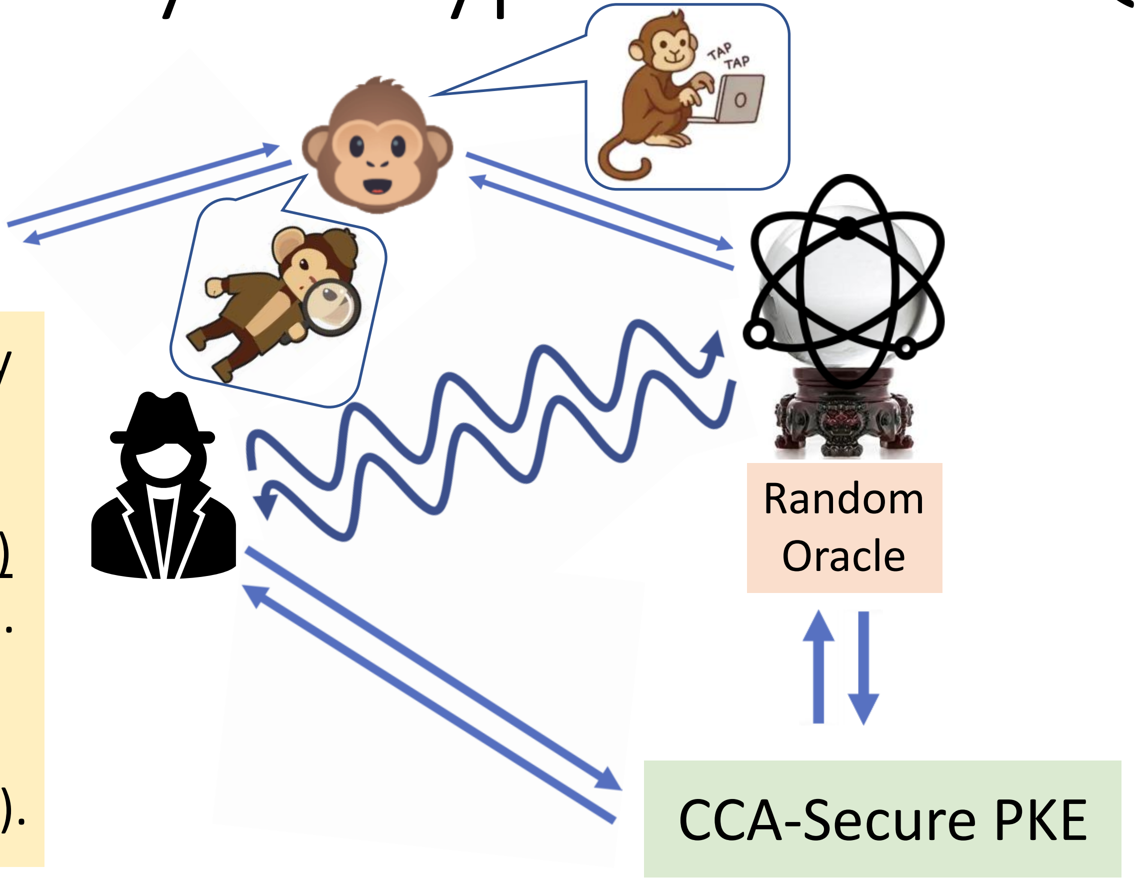
- Shown to be secure in the <u>classical ROM</u> by [Fujisaki-Okamoto’99].
- Was later proven to be secure in the <u>(plain) QROM</u> by [Don-Fehr-Majenz-Schaffner’22].

CCA-Secure PKE

Transformation introduced by [Fujisaki-Okamoto’99].

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

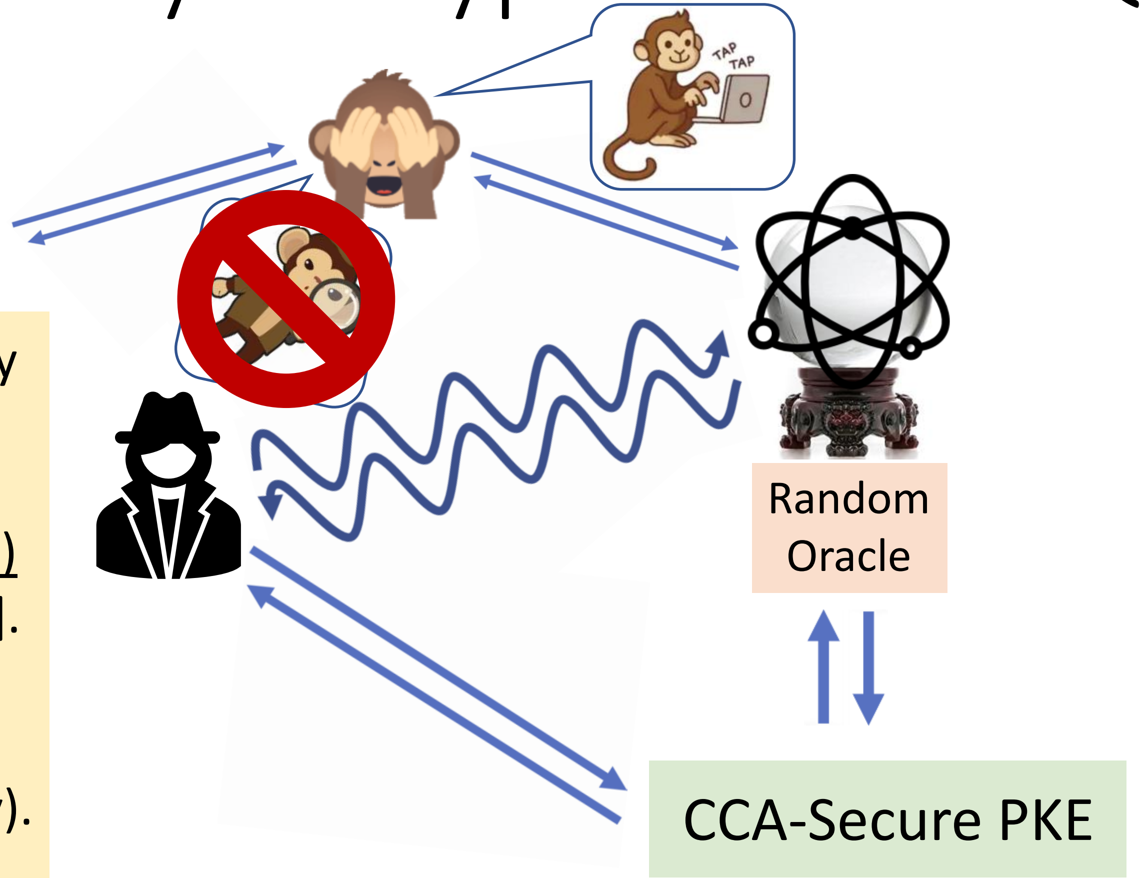


- Shown to be secure in the <u>classical ROM</u> by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the <u>(plain) QROM</u> by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on <u>observability</u> (and programmability).

Transformation introduced by [Fujisaki-Okamoto'99].

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

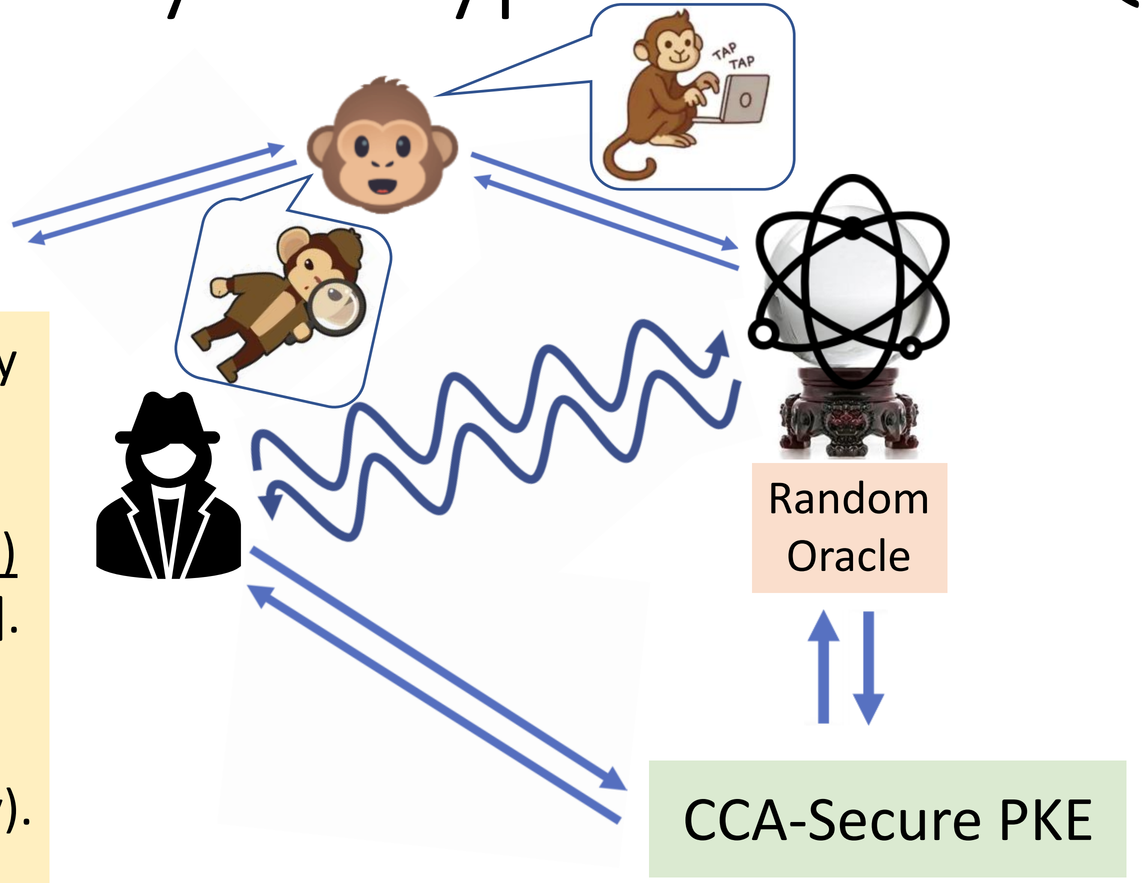


- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.

Transformation introduced by [Alamati-Maram-Masny'23]

CCA-Secure Public-Key Encryption in NO QROM

Msg Ctxt CPA-Secure PKE



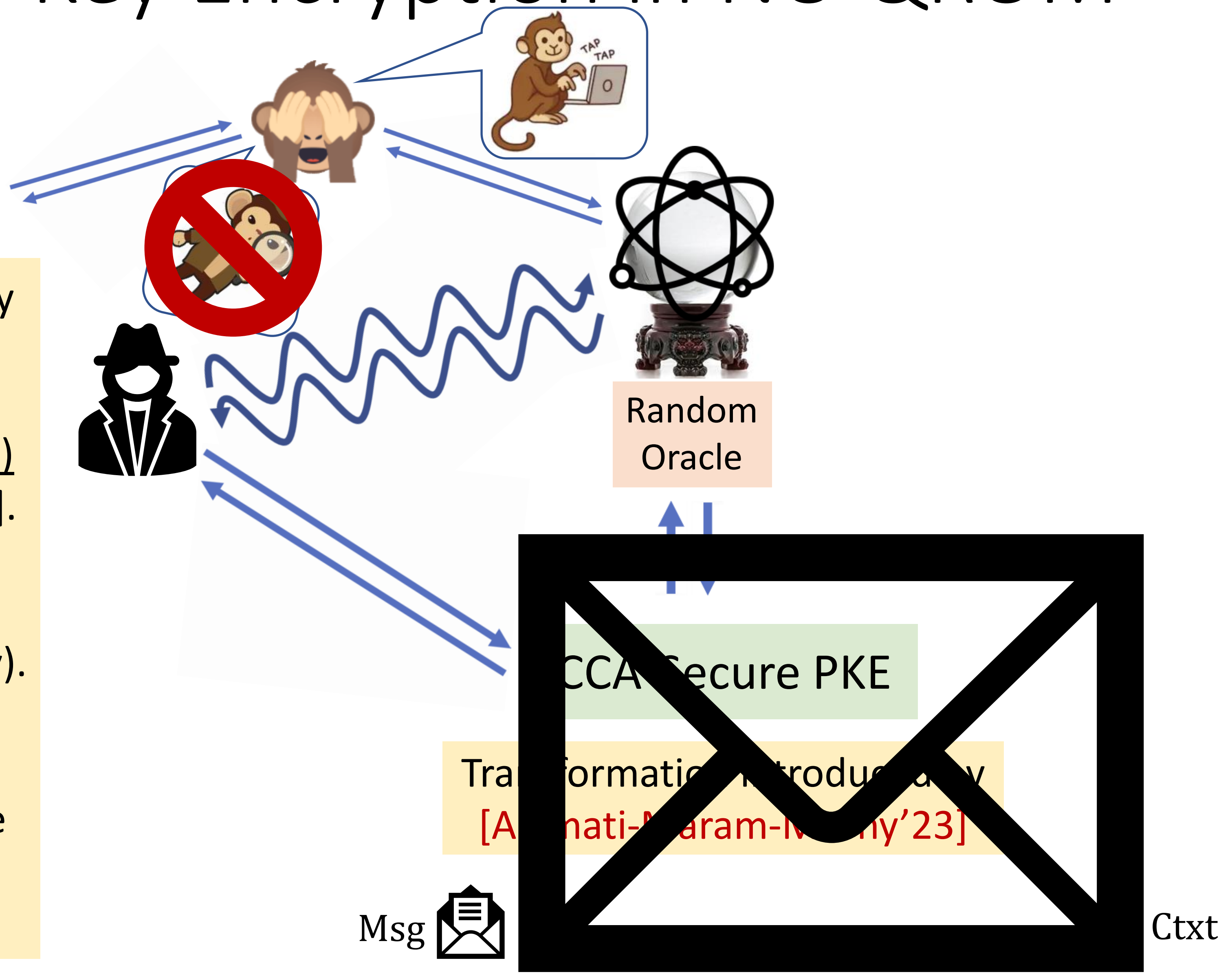
- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.

Transformation introduced by [Fujisaki-Okamoto'99].

Msg Ctxt

CCA-Secure Public-Key Encryption in NO QROM

- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.



CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.

+

"Hinting" PRG

CCA-Secure PKE

Construction by [Koppula-Waters'19].

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.

+

"Hinting" PRG

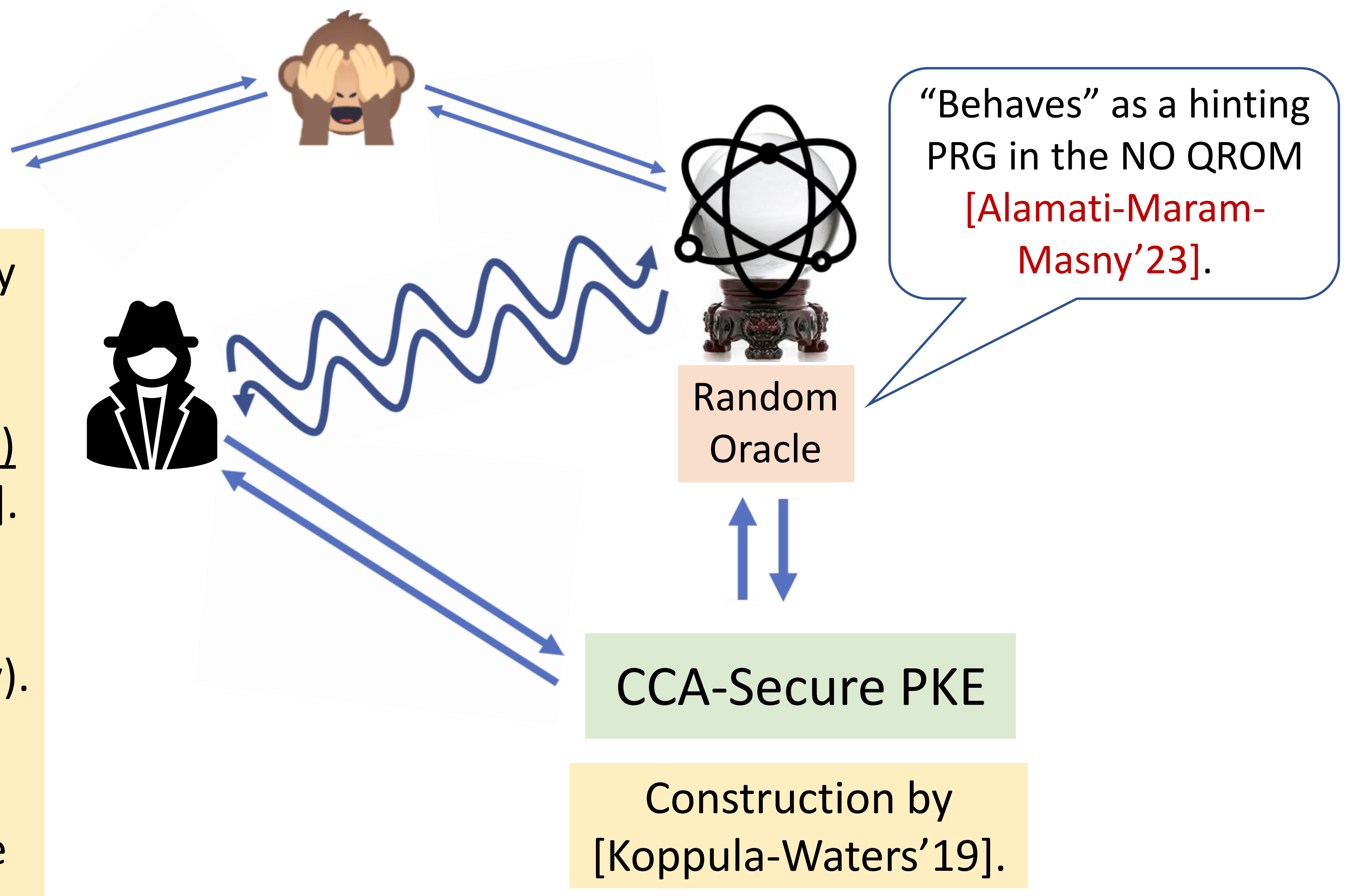
PRG with a stronger security guarantee.

CCA-Secure PKE

Construction by [Koppula-Waters'19].

CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

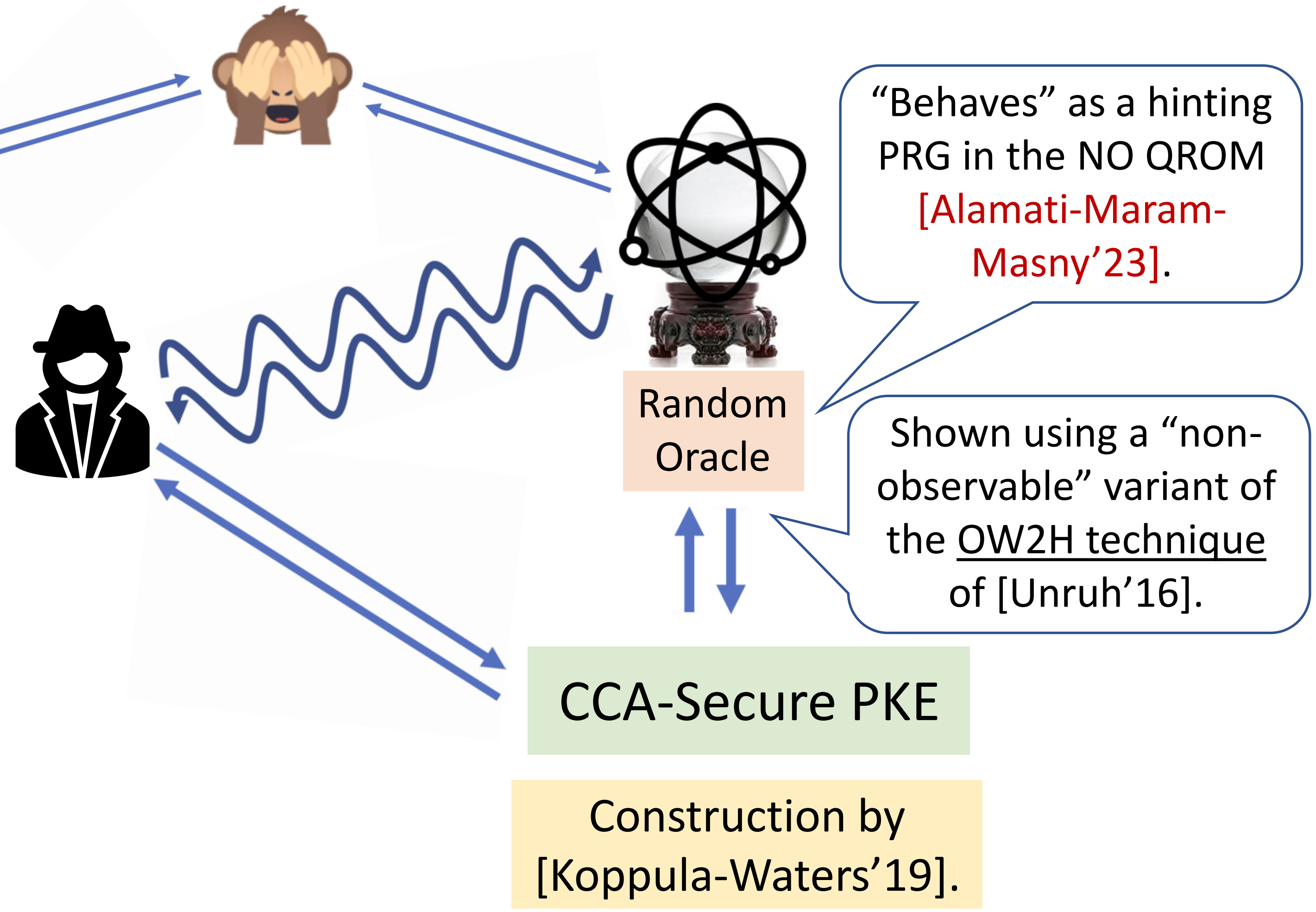


- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.

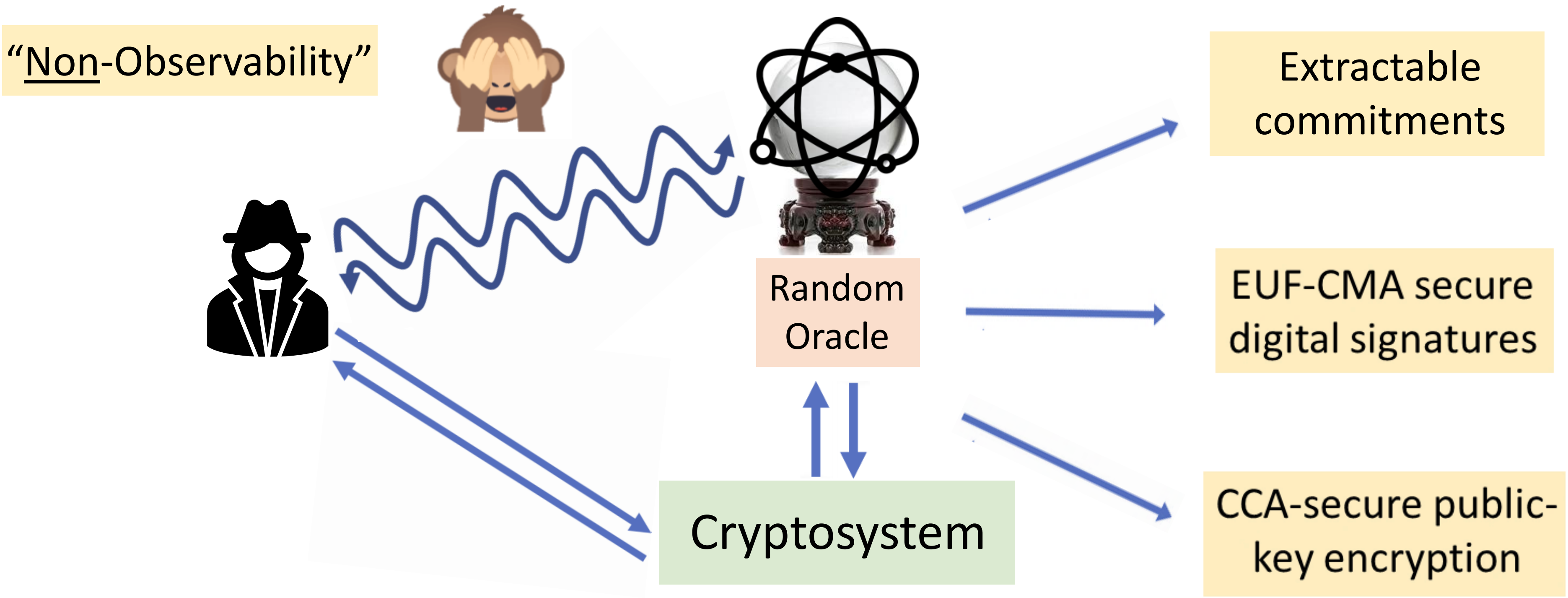
CCA-Secure Public-Key Encryption in NO QROM

CPA-Secure PKE

- Shown to be secure in the classical ROM by [Fujisaki-Okamoto'99].
- Was later proven to be secure in the (plain) QROM by [Don-Fehr-Majenz-Schaffner'22].
- However, above security proofs crucially rely on observability (and programmability).
- We provide an alternative "CPA → CCA" transform that can be proven secure in the NO QROM…[Alamati-Maram-Masny'23]
  - … but at the expense of efficiency.



Non-Observable QROM (NO QROM)



Formalized by [Alamati-Maram-Masny'23].