Verifiable Private Information Retrieval

Shany Ben-David
Tel-Aviv University
→ Bar-Ilan University

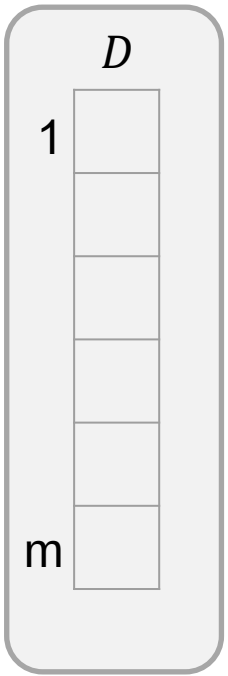
Joint work with:
Yael Tauman Kalai (Microsoft Research and MIT)
Omer Paneth (Tel-Aviv University)

Private Information Retrieval (PIR)

Private Information Retrieval (PIR)

Client: $i \in [m]$

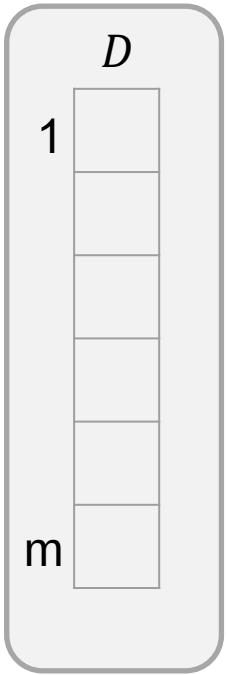
Server: D



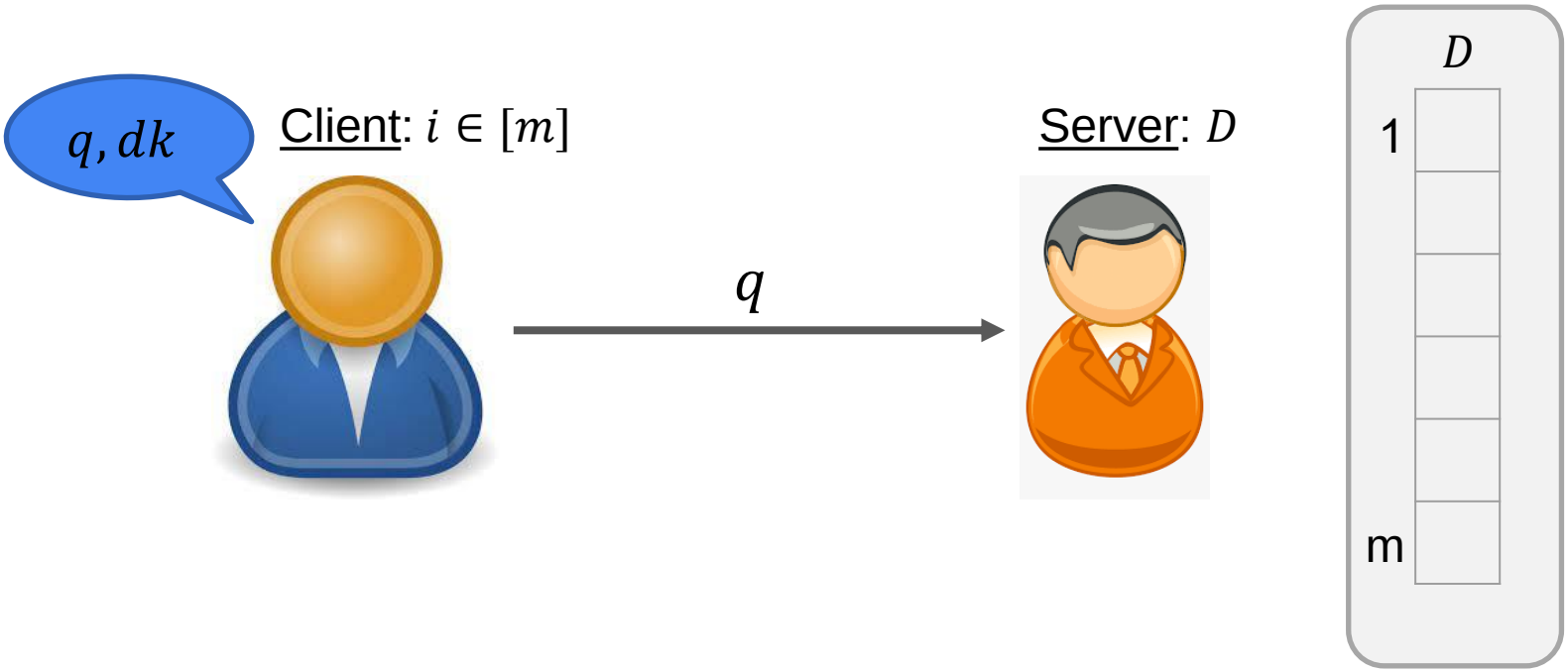
Private Information Retrieval (PIR)

Client: $i \in [m]$

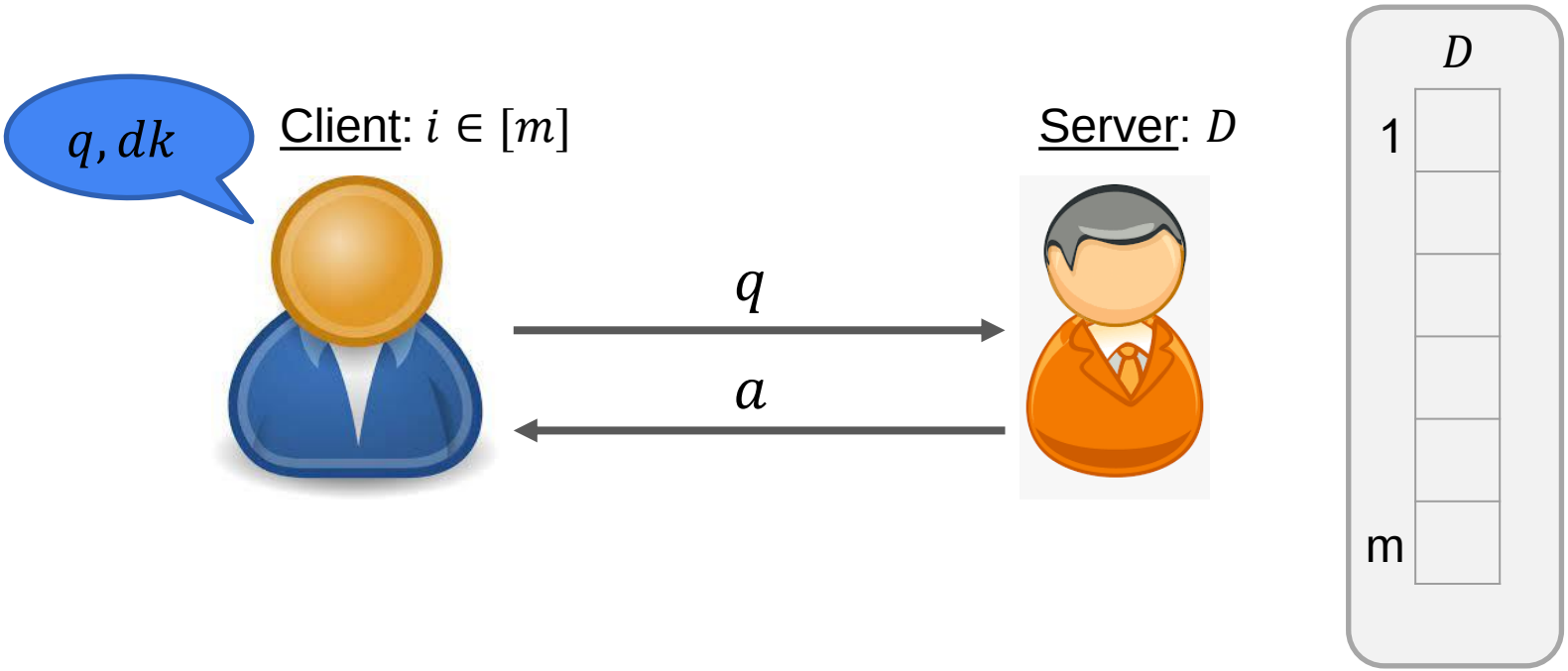
Server: D



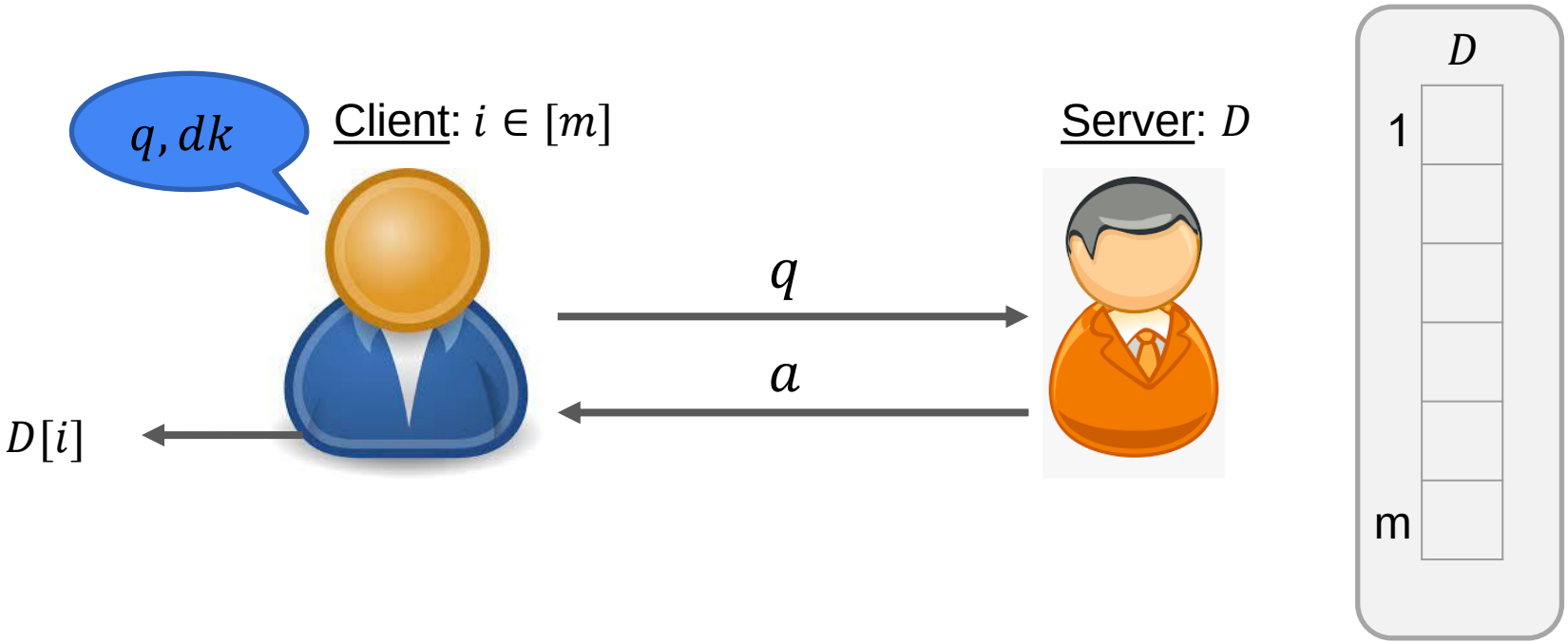
Private Information Retrieval (PIR)



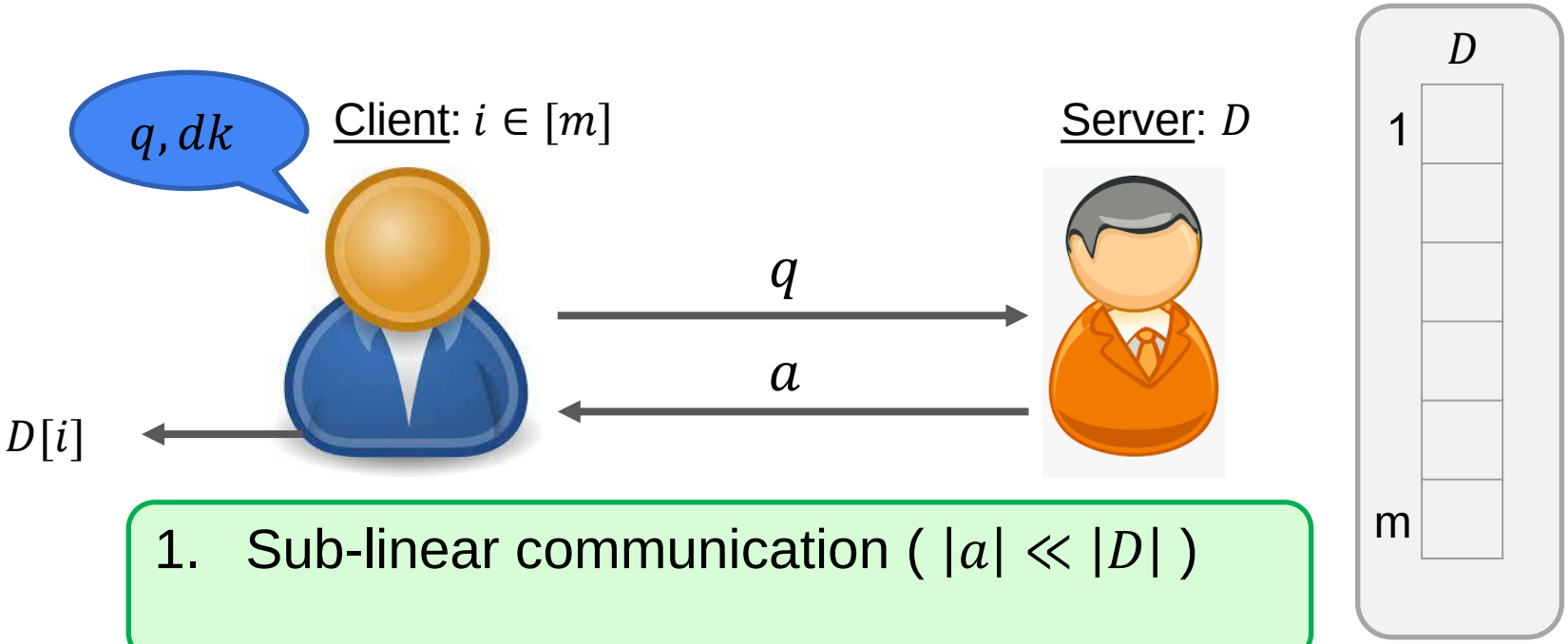
Private Information Retrieval (PIR)



Private Information Retrieval (PIR)

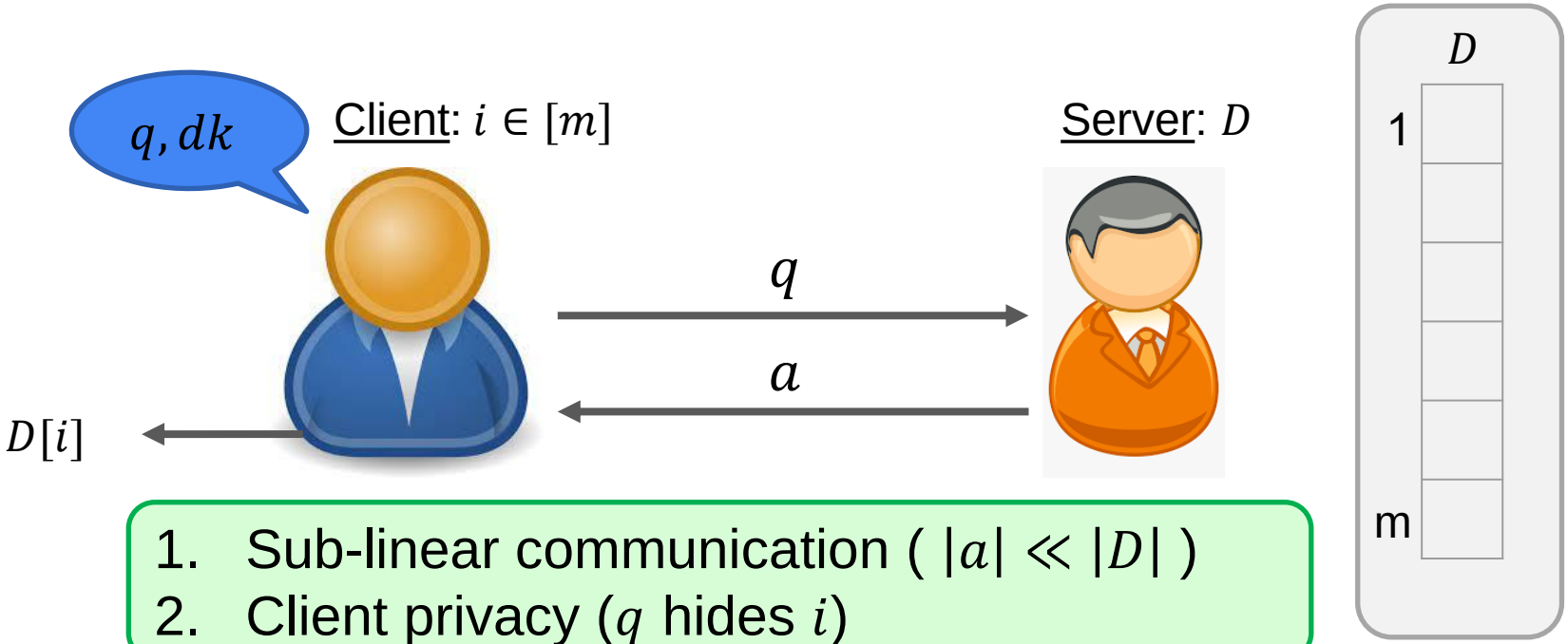


Private Information Retrieval (PIR)



1. Sub-linear communication ($|a| \ll |D|$)

Private Information Retrieval (PIR)



1. Sub-linear communication ($|a| \ll |D|$)
2. Client privacy (q hides i)

Example

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal
Recent changes
Upload file

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Wikidata item

Print/export
Download as PDF
Printable version

Moon landing

From Wikipedia, the free encyclopedia

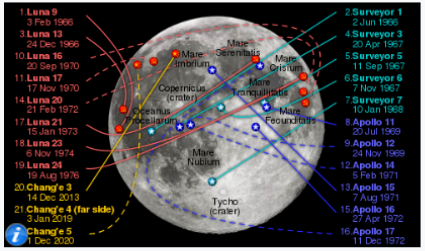
This article is about the general topic of landing on the moon. For the first crewed Moon landing, see Apollo 11 and Apollo program. For other uses, see Moon landing (disambiguation). "Race to the Moon" redirects here. For the Cold War topic, see Space Race.

A **Moon landing** is the arrival of a spacecraft on the surface of the Moon. This includes both crewed and robotic missions. The first human-made object to touch the Moon was the Soviet Union's Luna 2, on 13 September 1959.[3]

The United States' Apollo 11 was the first crewed mission to land on the Moon, on 20 July 1969.[4] There were six crewed U.S. landings between 1969 and 1972, and numerous uncrewed landings, with no soft landings happening between 22 August 1976 and 14 December 2013.

The United States is the only country to have successfully conducted crewed missions to the Moon, with the last departing the lunar surface in December 1972. All soft landings took place on the near side of the Moon until 3 January 2019, when the Chinese Chang'e 4 spacecraft made the first landing on the far side of the Moon.[5]

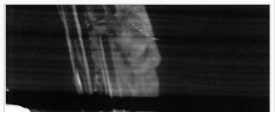
Contents [hide]



Clickable map of the locations of all successful soft landings on the near side of the Moon to date (top).

Luna programme (USSR) Surveyor program (US)
Chang'e program (China) Apollo program (US)

Dates are landing dates in Coordinated Universal Time. Except for the Apollo program, all soft landings were uncrewed.



Example

Moon landing

From Wikipedia, the free encyclopedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal
Recent changes
Upload file

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Wikidata item

Print/export
Download as PDF
Printable version

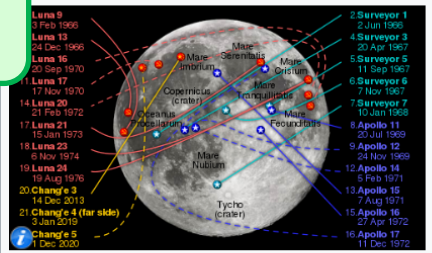
PIR protects client's privacy

Moon landing (disambiguation).

and 1972, and numerous uncrewed landings, with no soft landings happening between 22 August 1976 and 14 December 2013.

The United States is the only country to have successfully conducted crewed missions to the Moon, with the last departing the lunar surface in December 1972. All soft landings took place on the near side of the Moon until 3 January 2019, when the Chinese Chang'e 4 spacecraft made the first landing on the far side of the Moon.[5]

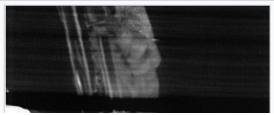
Contents [hide]



Clickable map of the locations of all successful soft landings on the near side of the Moon to date (top).

Luna programme (USSR) Surveyor program (US)
Chang'e program (China) Apollo program (US)

Dates are landing dates in Coordinated Universal Time. Except for the Apollo program, all soft landings were uncrewed.



Example

Moon landing conspiracy theories

From Wikipedia, the free encyclopedia

PIR protects client's privacy

What about fake news?

Much third-party evidence for the landings exists, and detailed rebuttals to the hoax claims have been made.[1] Since the late 2000s, high-definition photos taken by the Lunar Reconnaissance Orbiter (LRO) of the Apollo landing sites have captured the Lunar Module descent stages and the tracks left by the astronauts.[2][3] In 2012,

Astronauts Buzz Aldrin and Neil Armstrong in NASA's training mockup of the Moon and the Apollo Lunar Module. Conspiracy theorists say that the films of the missions were made using sets similar to this training mockup.

Example

Moon landing conspiracy theories

From Wikipedia, the free encyclopedia

PIR protects client's privacy

How to protect the client from a malicious server using a "bad" DB?

Astronauts Buzz Aldrin and Neil Armstrong in NASA's training mockup of the Moon and the Apollo Lunar Module. Conspiracy theorists say that the films of the missions were made using sets similar to this training mockup.

Example 1 – Wikipedia Server Serving a Bad Article

Example 1 – Wikipedia Server Serving a Bad Article

What is a good\bad DB?

Example 1 – Wikipedia Server Serving a Bad Article

What is a good\bad DB?

D

$Article_1$
$Article_2$
$Article_m$

Example 1 – Wikipedia Server Serving a Bad Article

What is a good\bad DB?

D

$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$

Example 1 – Wikipedia Server Serving a Bad Article

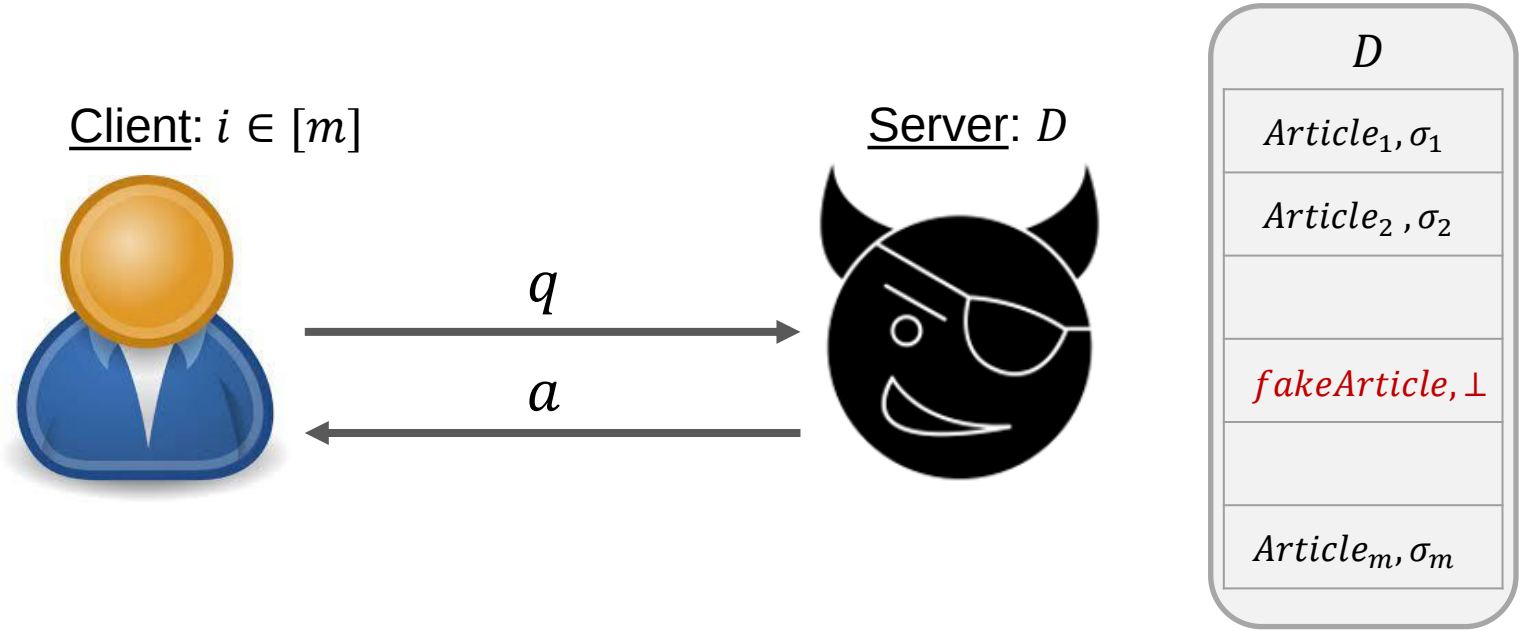
What is a good\bad DB?

D

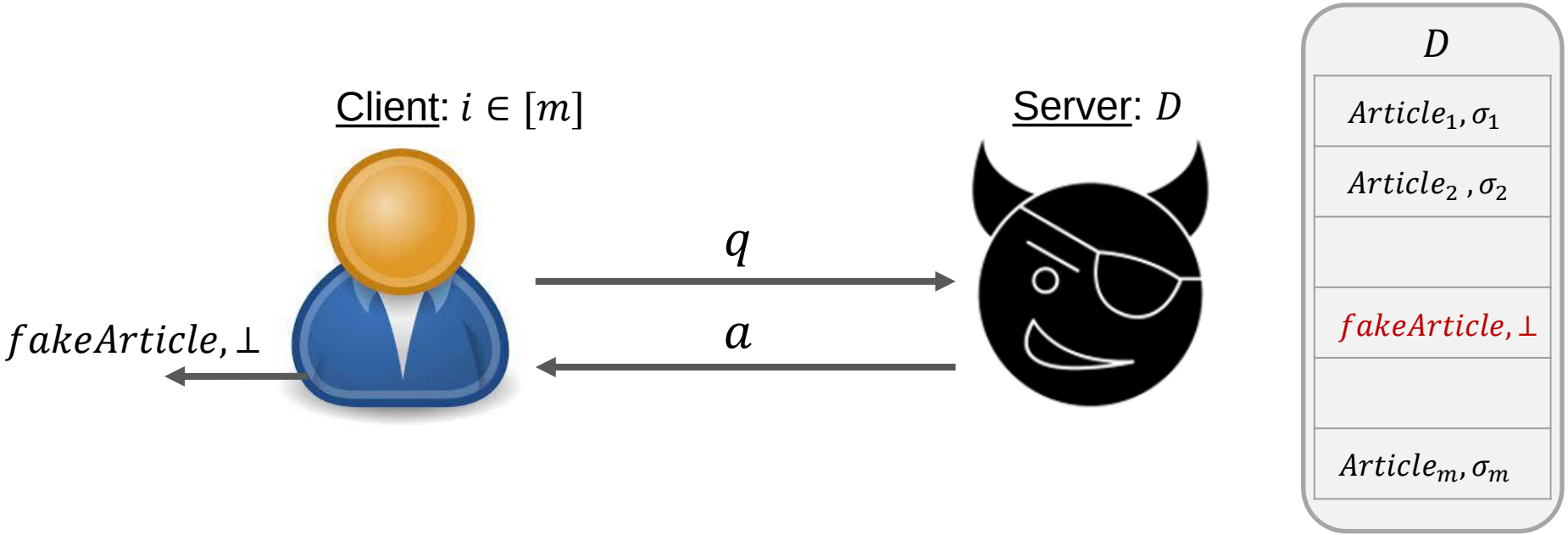
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$

Good DB contains 100% signed articles.

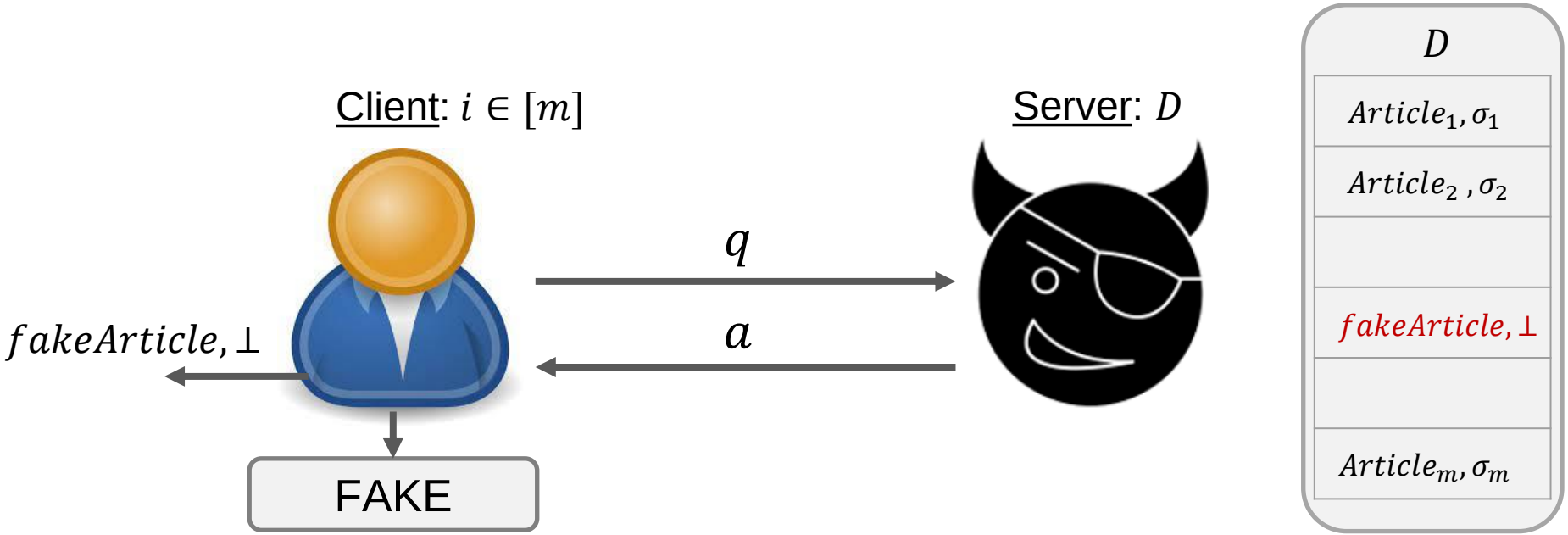
Example 1 – Wikipedia Server Serving a Bad Article



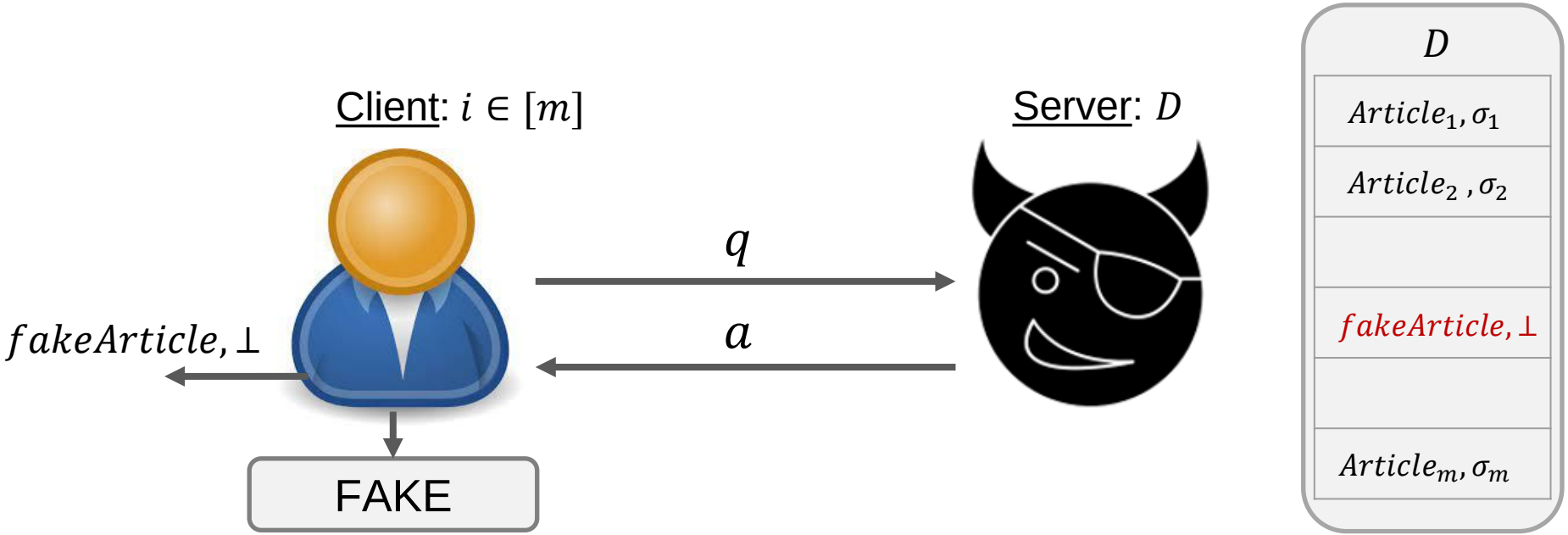
Example 1 – Wikipedia Server Serving a Bad Article



Example 1 – Wikipedia Server Serving a Bad Article



Example 1 – Wikipedia Server Serving a Bad Article



Goal1- Publishing the results of the verification

Example 2 – Wikipedia – 99% Signed

D
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$

Example 2 – Wikipedia – 99% Signed

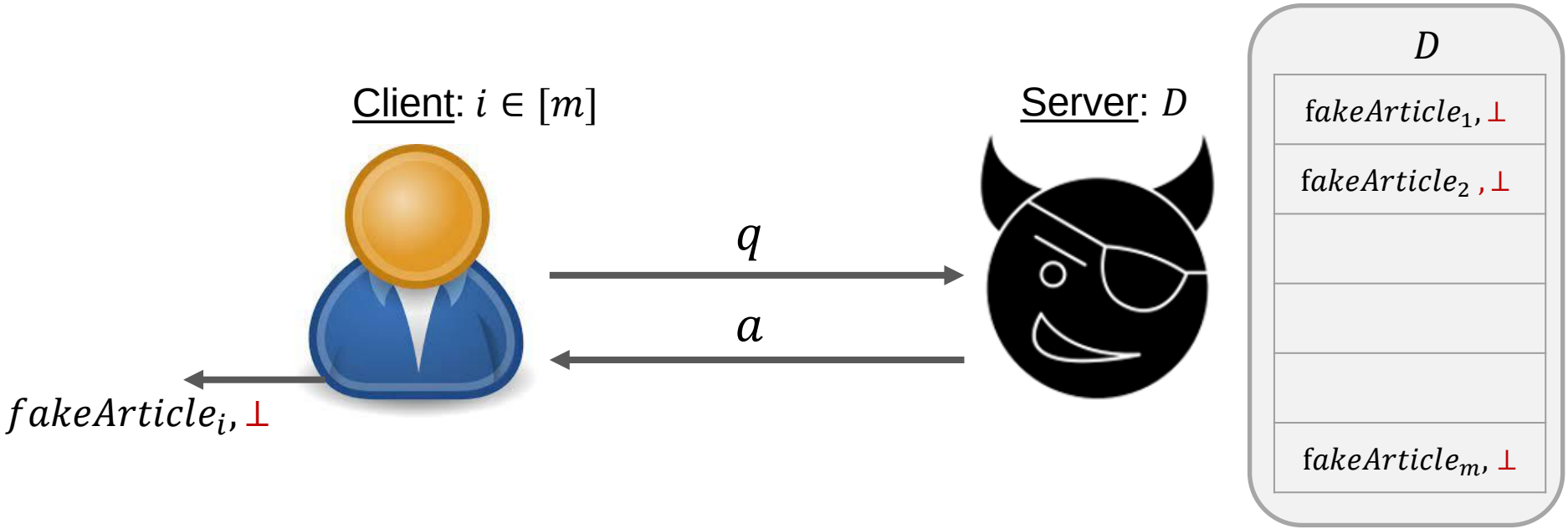
D
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$NewArticle_i, \perp$
$Article_m, \sigma_m$

Example 2 – Wikipedia – 99% Signed

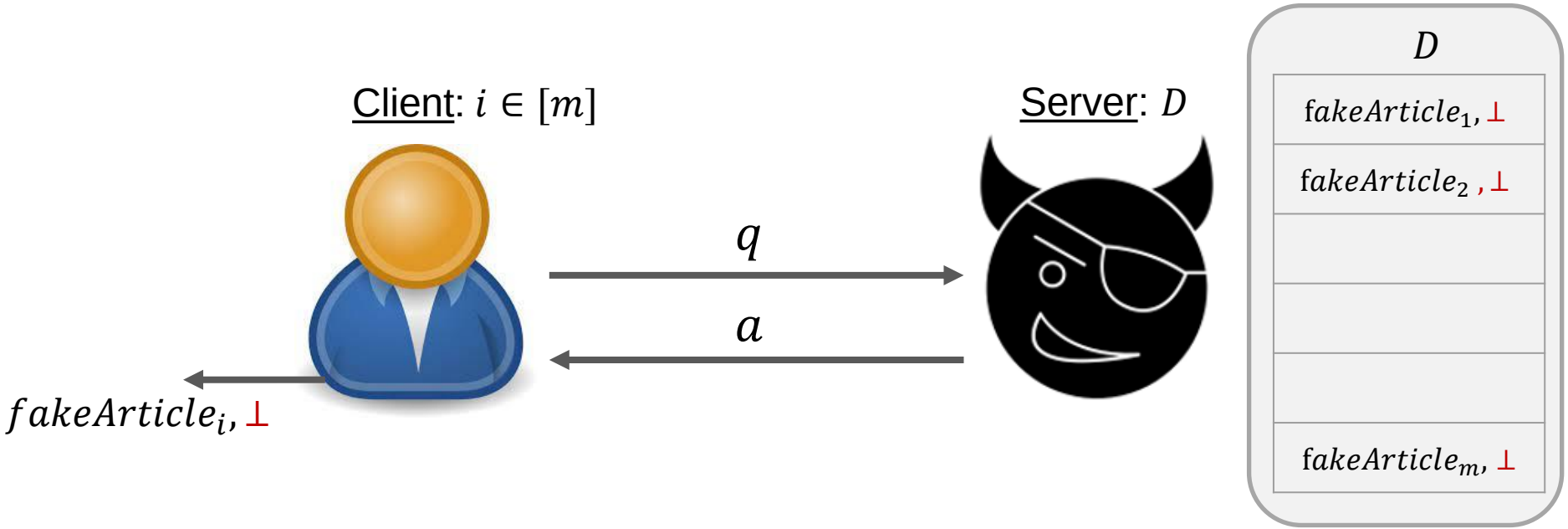
D
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$NewArticle_i, \perp$
$Article_m, \sigma_m$

Good DB contains 99% signed articles.

Example 2 – Wikipedia – 99% Signed



Example 2 – Wikipedia – 99% Signed



Goal2 – Verify global properties of the database

Contribution (in a nutshell)

Contribution (in a nutshell)

1. We introduce a new notion of **verifiable PIR**.

Contribution (in a nutshell)

1. We introduce a new notion of **verifiable PIR**.
2. We give constructions based on **standard assumptions**.

Contribution (in a nutshell)

1. We introduce a new notion of **verifiable PIR**.
2. We give constructions based on **standard assumptions**.

Verifiable Private Information Retrieval (vPIR) – Syntax

Verifiable Private Information Retrieval (vPIR) – Syntax

$P(D) \rightarrow \{0,1\}$

Verifiable Private Information Retrieval (vPIR) – Syntax

$$P(D) \rightarrow \{0,1\}$$

Client: $i \in [m]$

Server: D s.t $P(D) = 1$

Verifiable Private Information Retrieval (vPIR) – Syntax

$P(D) \rightarrow \{0,1\}$

Client: $i \in [m]$

Server: D s.t $P(D) = 1$

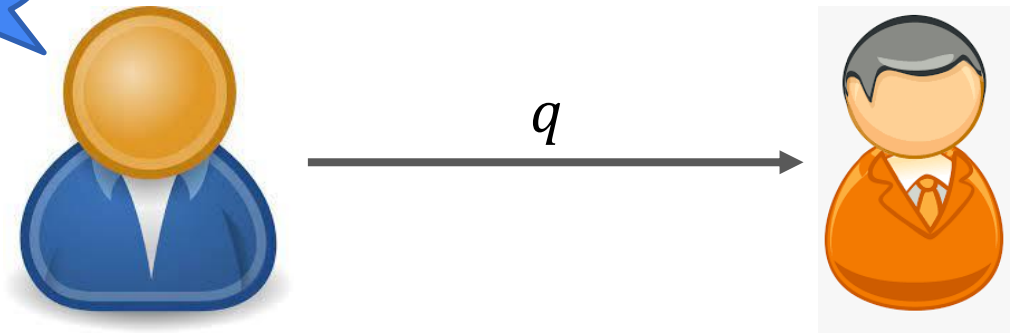
Verifiable Private Information Retrieval (vPIR) – Syntax

$P(D) \rightarrow \{0,1\}$

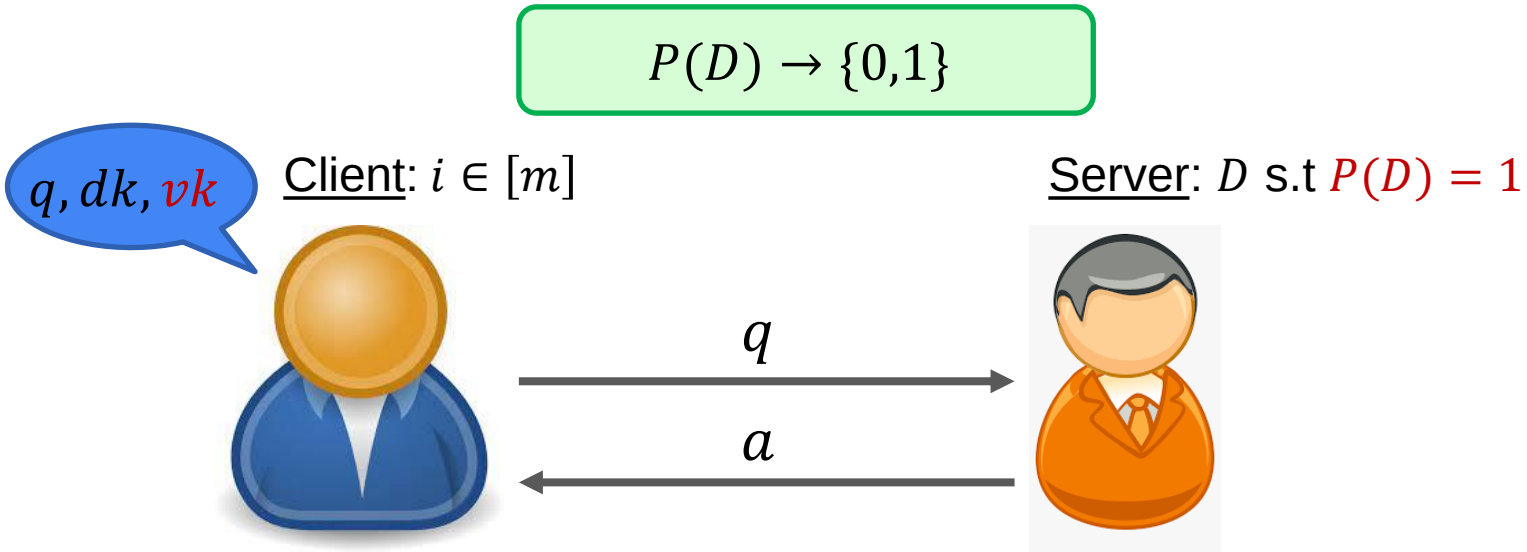
q, dk, vk

Client: $i \in [m]$

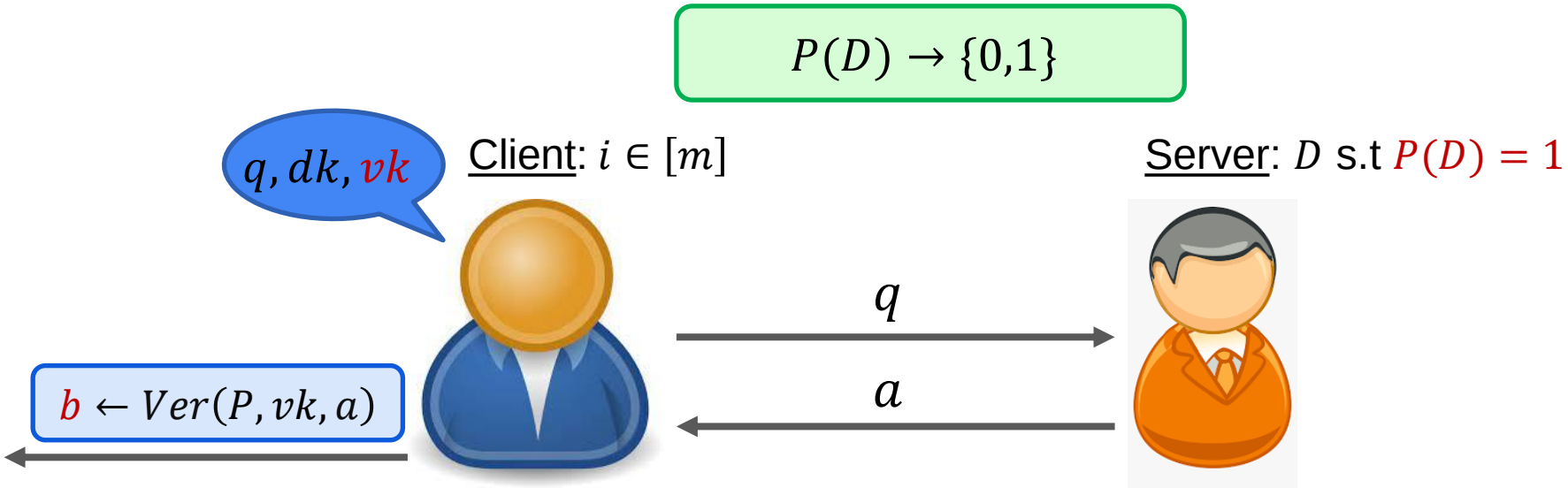
Server: D s.t $P(D) = 1$



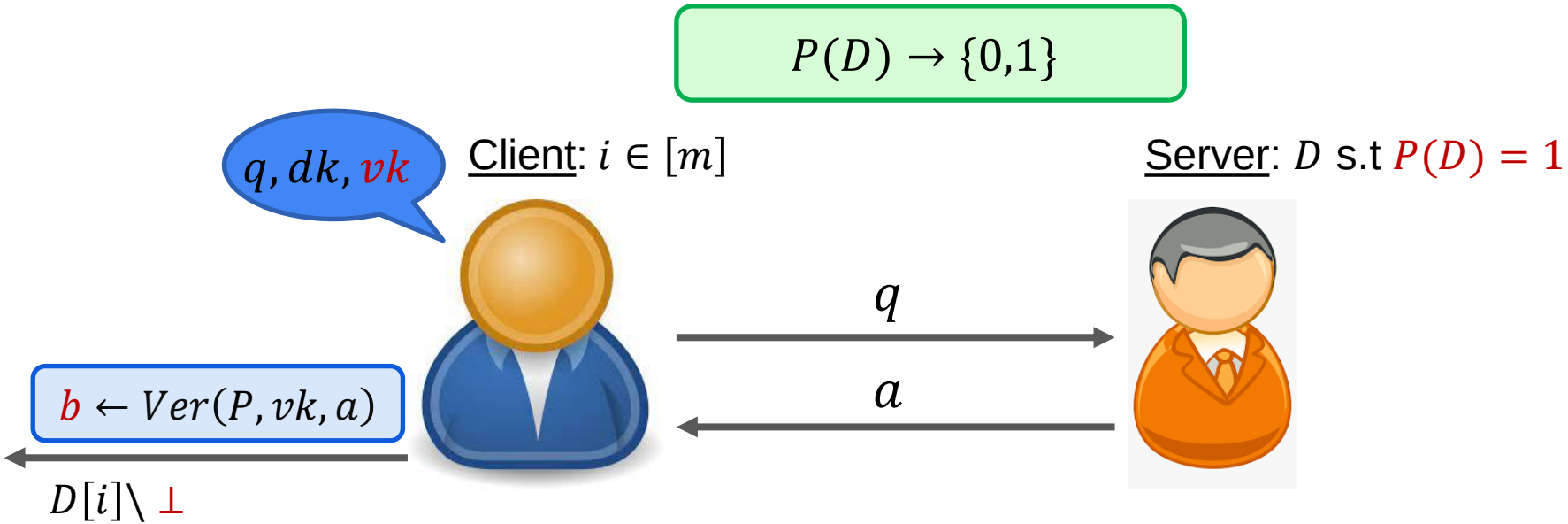
Verifiable Private Information Retrieval (vPIR) – Syntax



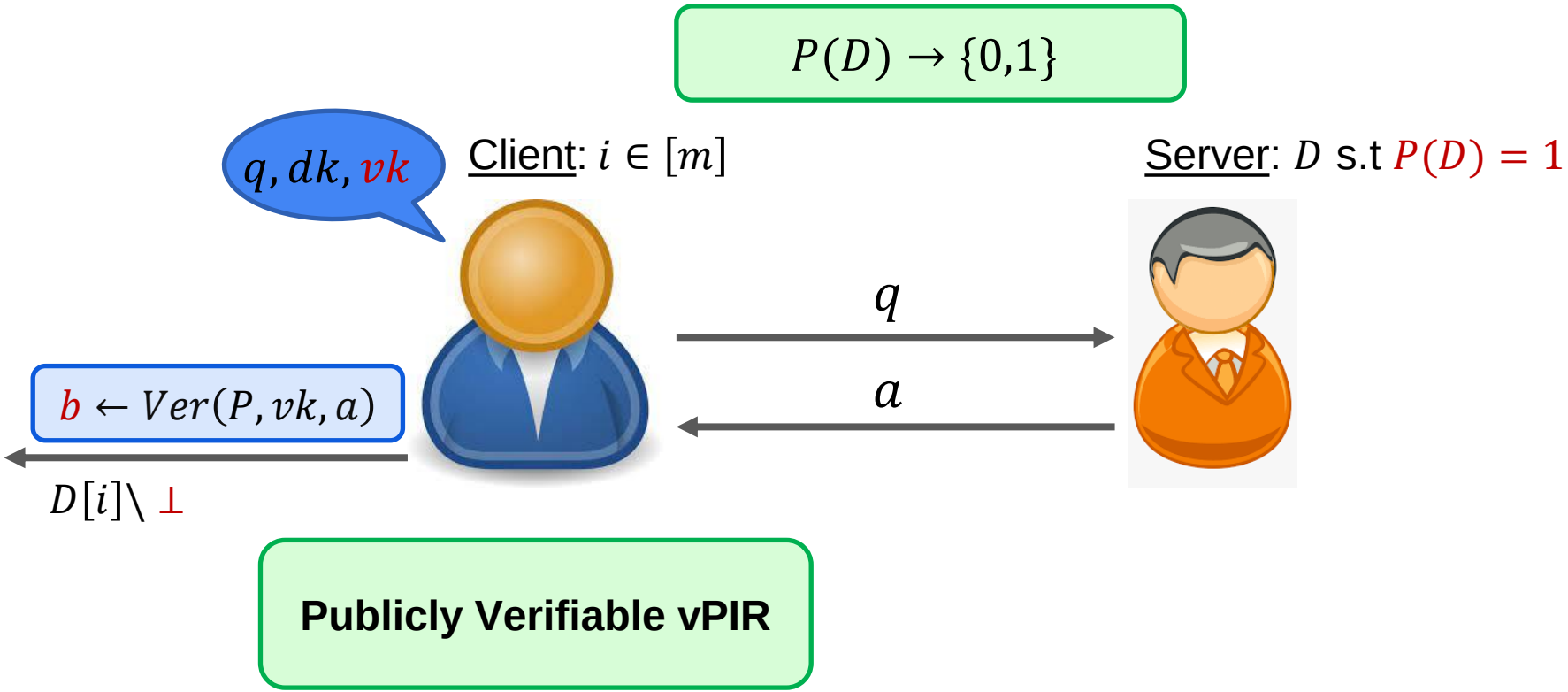
Verifiable Private Information Retrieval (vPIR) – Syntax



Verifiable Private Information Retrieval (vPIR) – Syntax



Verifiable Private Information Retrieval (vPIR) – Syntax



Publicly Verifiable vPIR

Verifiable Private Information Retrieval (vPIR) – Syntax

$P(D) \rightarrow \{0,1\}$

q, dk, vk

Client: $i \in [m]$

Server: D s.t $P(D) = 1$

q

a

$b \leftarrow Ver(P, vk, a)$

$D[i] \setminus \perp$

Publicly Verifiable vPIR

Privately Verifiable vPIR

vPIR – Requirements

vPIR – Requirements

1. Sub-linear communication ($|a| \ll |D|$)

vPIR – Requirements

1. Sub-linear communication ($|a| \ll |D|$)
2. Client privacy (q hides i **even given** $\boldsymbol{vk}$)

vPIR – Requirements

1. Sub-linear communication ($|a| \ll |D|$)
2. Client privacy (q hides i **even given** $\boldsymbol{vk}$)
3. Security ($P(D) = 1$)

Simulation Based Security – Ideal World

Simulation Based Security – Ideal World

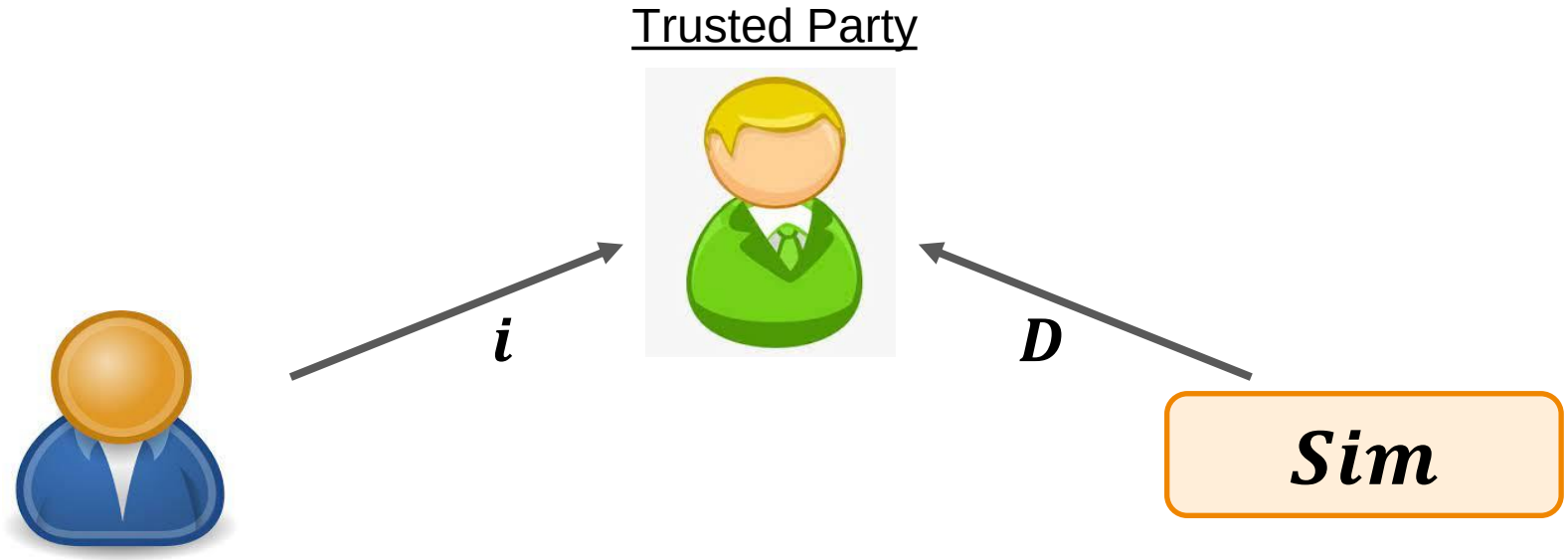
Trusted Party

Simulation Based Security – Ideal World

Trusted Party

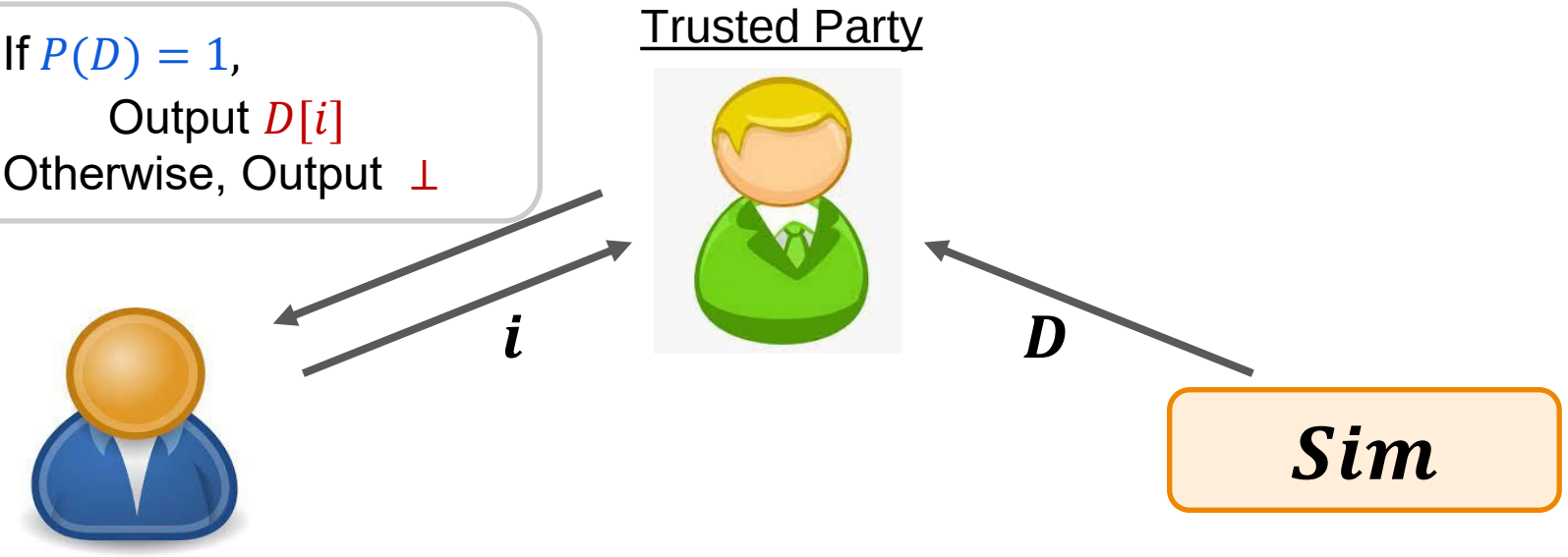
Sim

Simulation Based Security – Ideal World



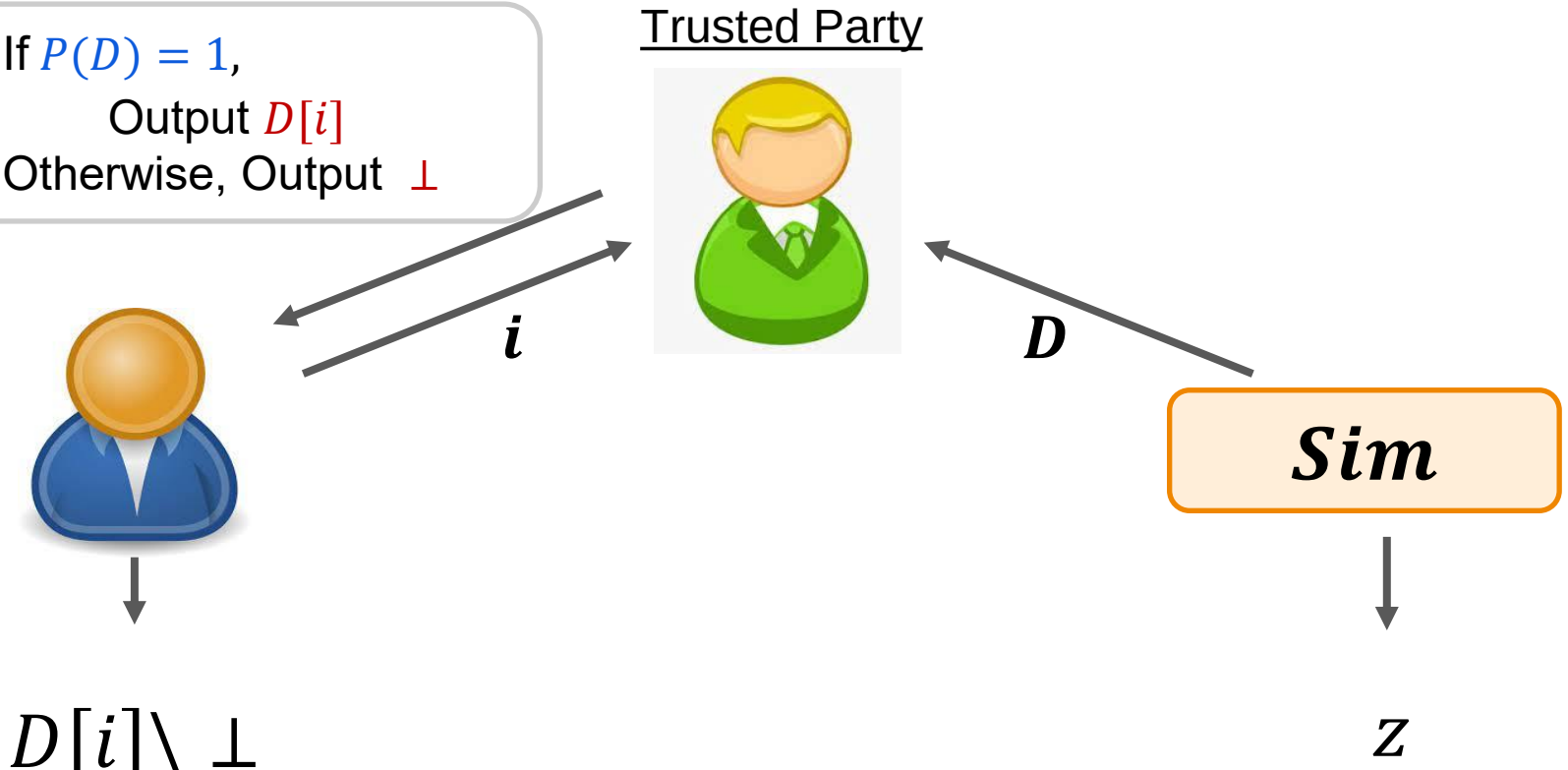
Simulation Based Security – Ideal World

- If $P(D) = 1$,
  Output $D[i]$
- Otherwise, Output $\perp$



Simulation Based Security – Ideal World

- If $P(D) = 1$,
  Output $D[i]$
- Otherwise, Output $\perp$



Simulation Based Security – Ideal World

- If $P(D) = 1$,
  Output $D[i]$
- Otherwise, Output $\perp$

Trusted Party

i

D

Sim

$Ideal_{sim}(i)$

$D[i] \setminus \perp$

z

Simulation Based Security – Ideal World

- If $P(D) = 1$,
  Output $D[i]$
- Otherwise, Output $\perp$

Trusted Party

i

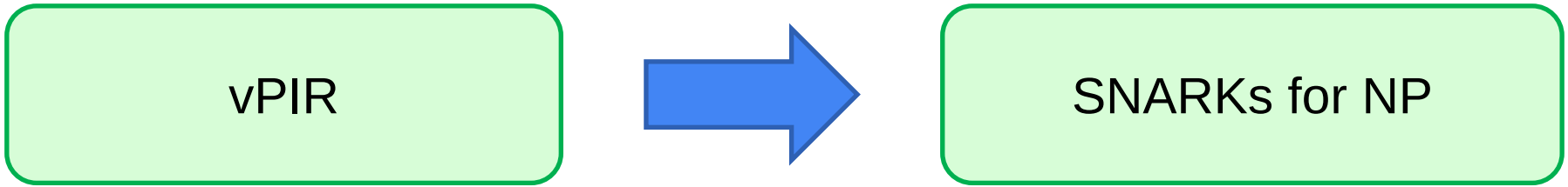
D

Sim

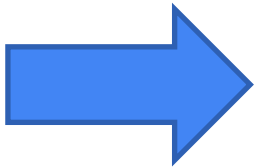
$Ideal_{sim}(i)$

$D[i] \setminus \perp$

z


vPIR
SNARKs for NP

vPIR



SNARKs for NP

We can’t expect to get vPIR from standard assumptions

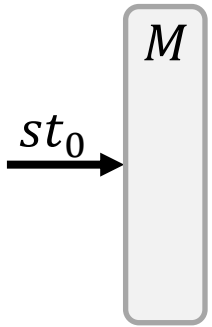
Properties Decidable on a Small State

Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.

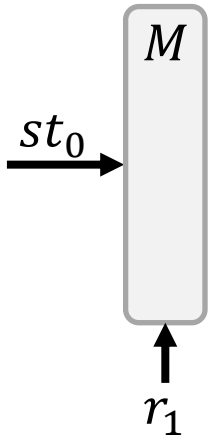
Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.



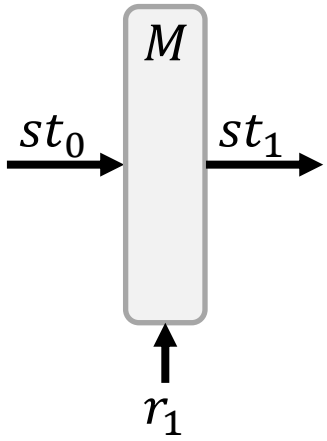
Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.



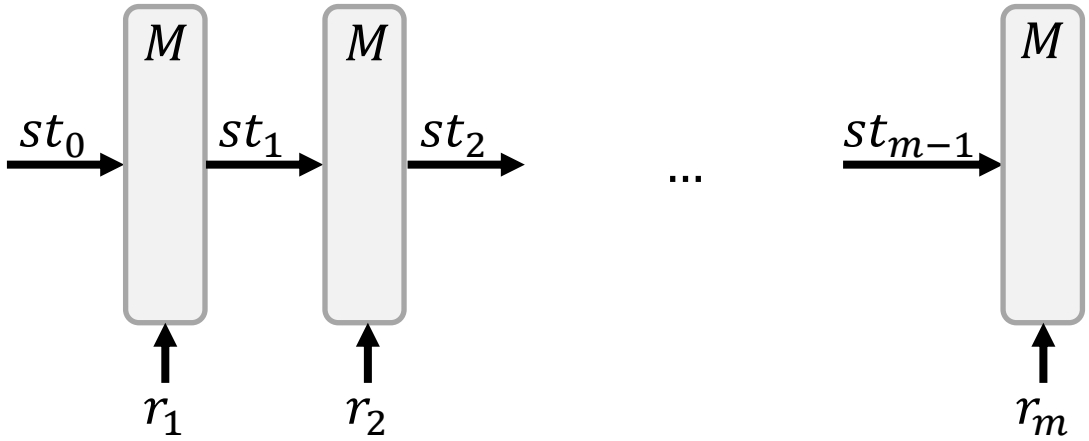
Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.



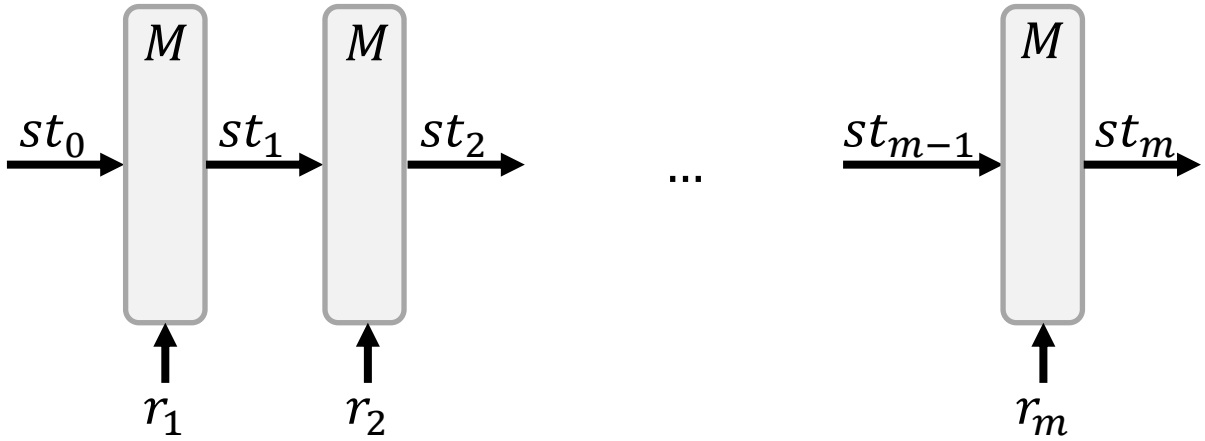
Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.



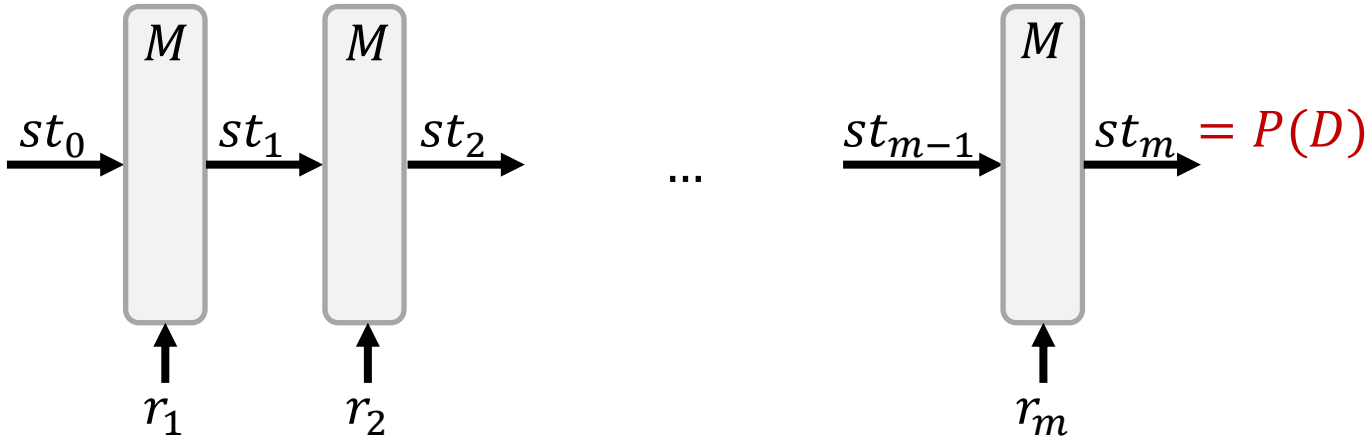
Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.



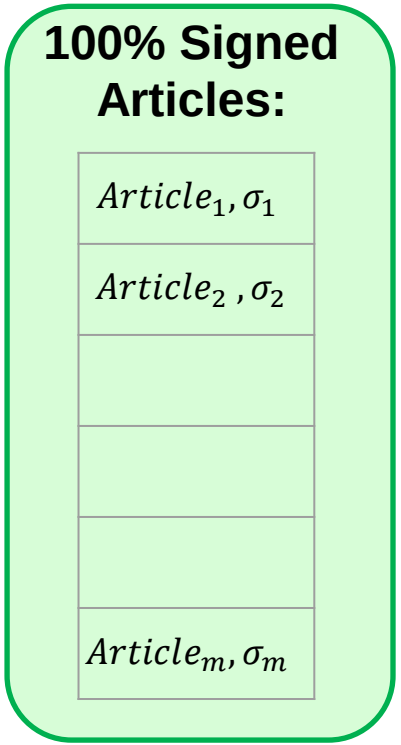
Properties Decidable on a Small State

Property P is decidable with state of size at most ℓ if it is decidable using a Turing machine M that reads the DB once and maintains a state of size ℓ between the rows.

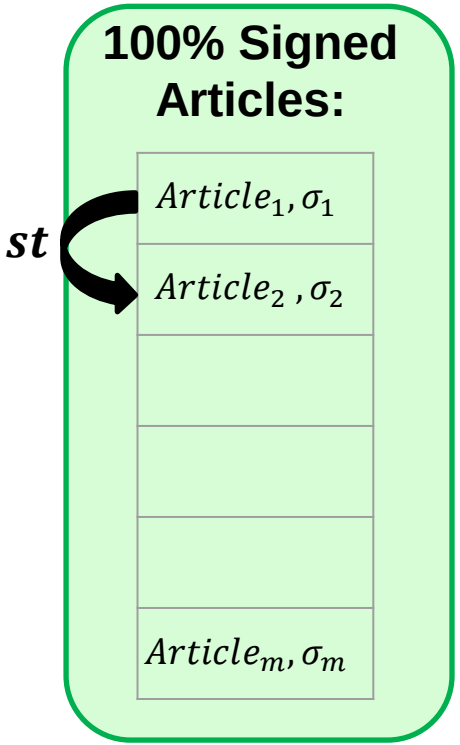


Examples

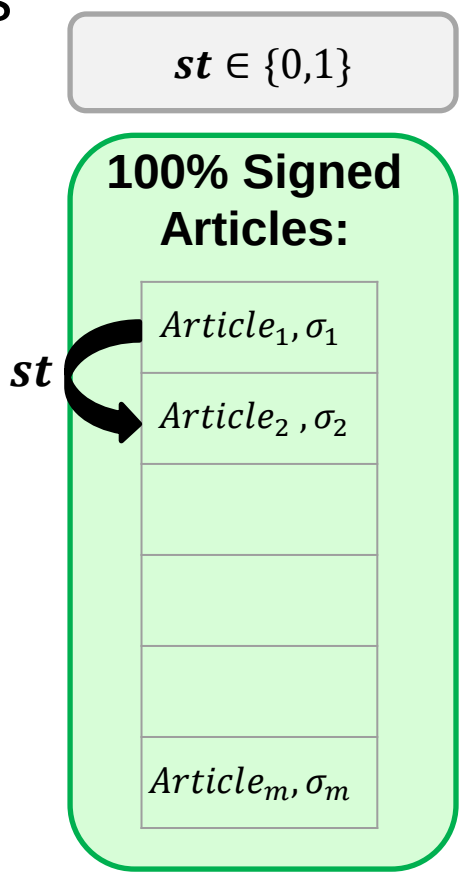
Examples


100% Signed Articles:
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$

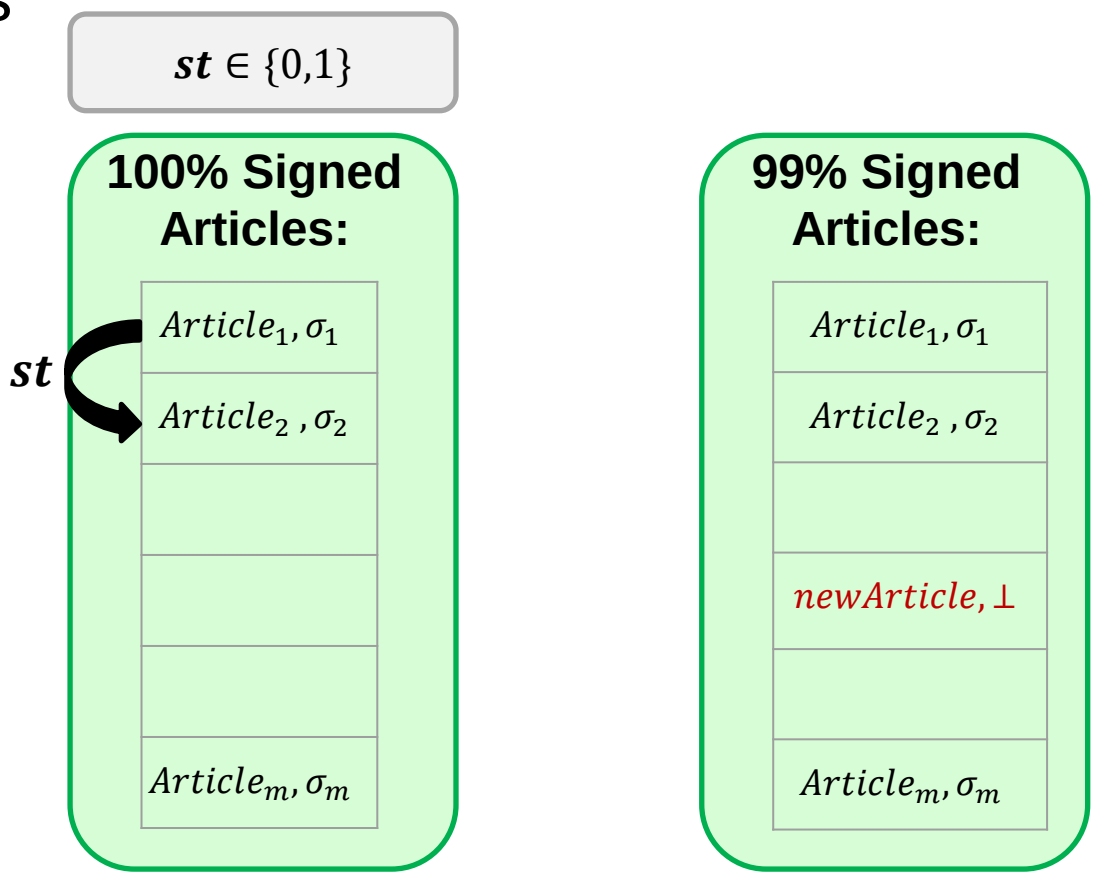
Examples


100% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$

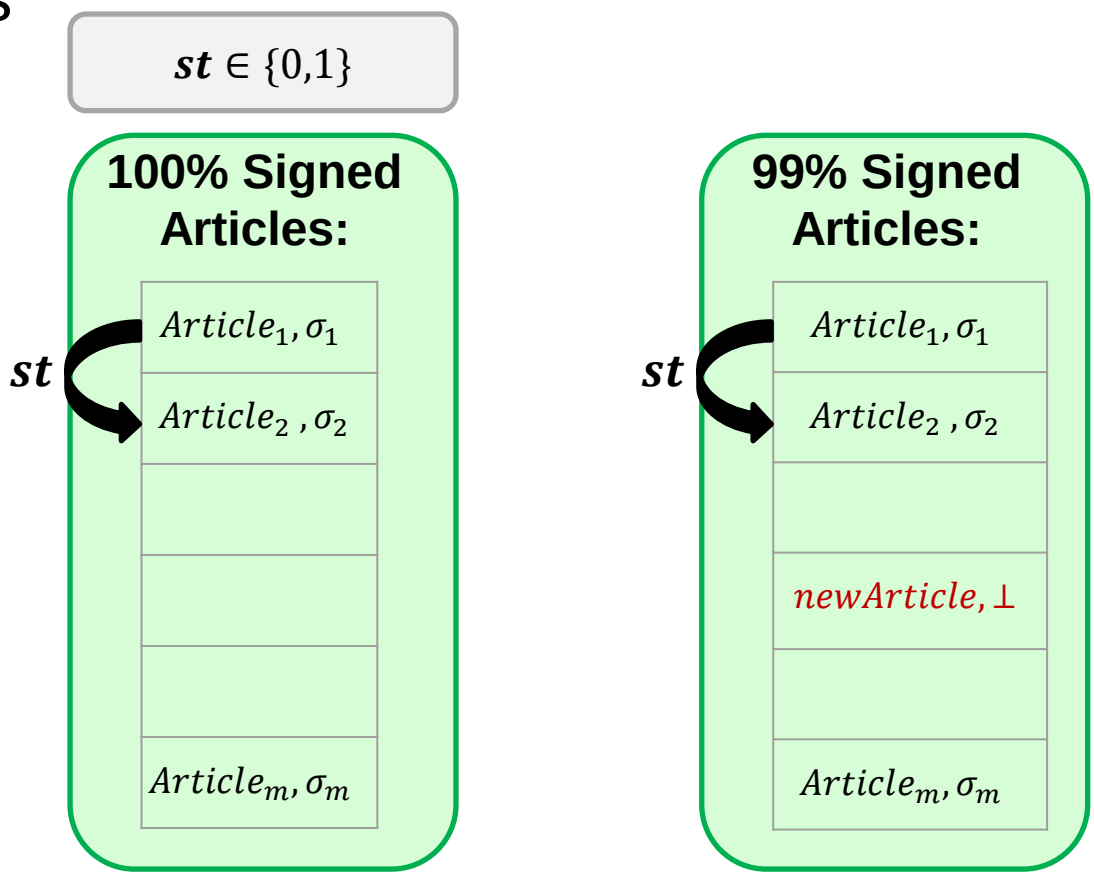
Examples


$st \in \{0,1\}$
100% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$

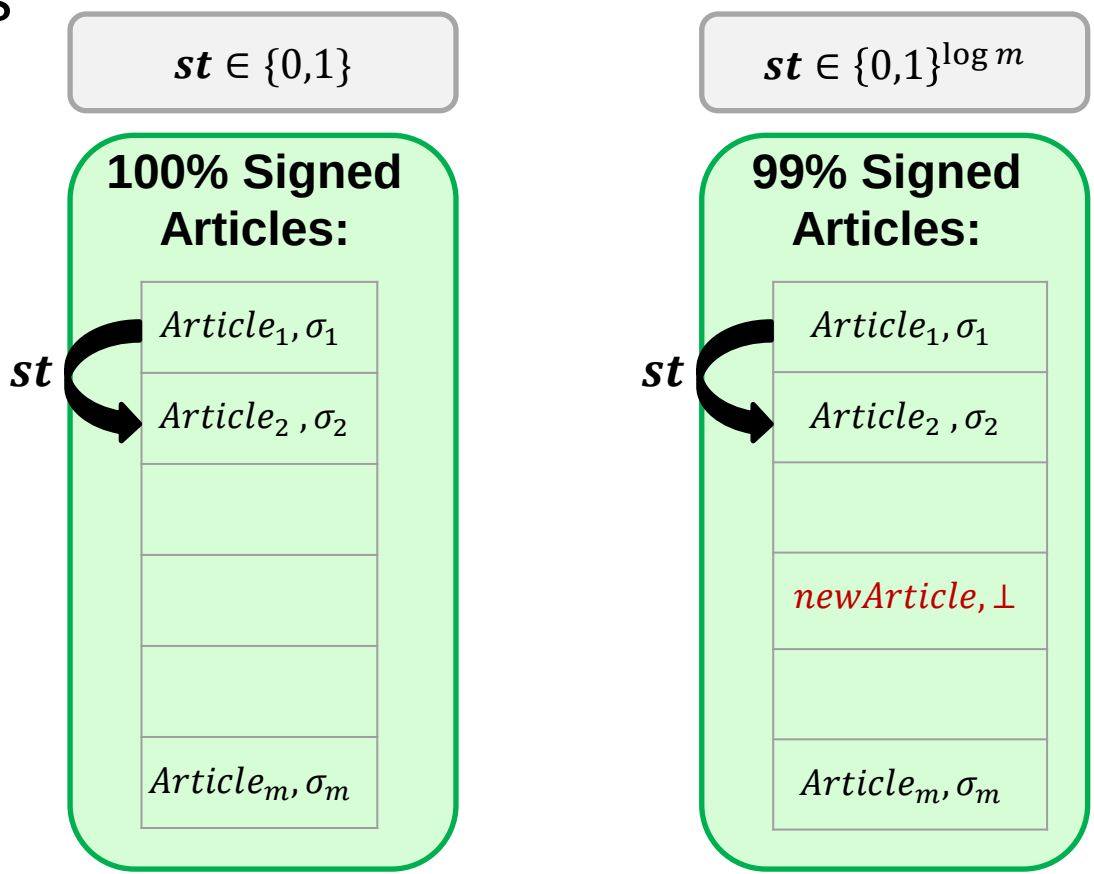
Examples


$st \in \{0,1\}$
100% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$
99% Signed Articles:
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$newArticle, \perp$
$Article_m, \sigma_m$

Examples


$st \in \{0,1\}$
100% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$
99% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$newArticle, \perp$
$Article_m, \sigma_m$

Examples


$st \in \{0,1\}$
100% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$Article_m, \sigma_m$
$st \in \{0,1\}^{\log m}$
99% Signed Articles:
st
$Article_1, \sigma_1$
$Article_2, \sigma_2$
$newArticle, \perp$
$Article_m, \sigma_m$

vPIR – Results

vPIR – Results

Theorem1:
$\forall \ell$, assuming 2^{ℓ}-secure **PIR**, there exists a **privately verifiable vPIR** for every property decidable with state of size at most ℓ, where the simulation running time is $2^{O(\ell)}$.

vPIR – Results

Theorem1:
$\forall \ell$, assuming 2^{ℓ}-secure **PIR**, there exists a **privately verifiable vPIR** for every property decidable with state of size at most ℓ, where the simulation running time is $2^{O(\ell)}$.

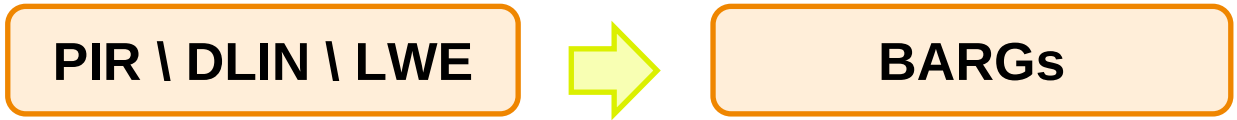
Theorem2:
$\forall \ell$, assuming 2^{ℓ}-hardness of **DLIN/LWE**, there exists a **publicly verifiable vPIR** for every property decidable with state of size at most ℓ where the simulation running time is $2^{O(\ell)}$.

Construction

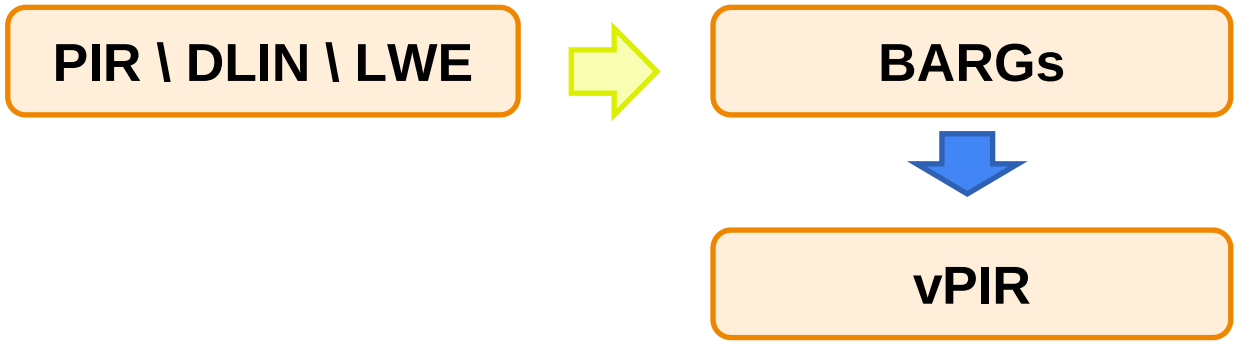
Construction

PIR \ DLIN \ LWE

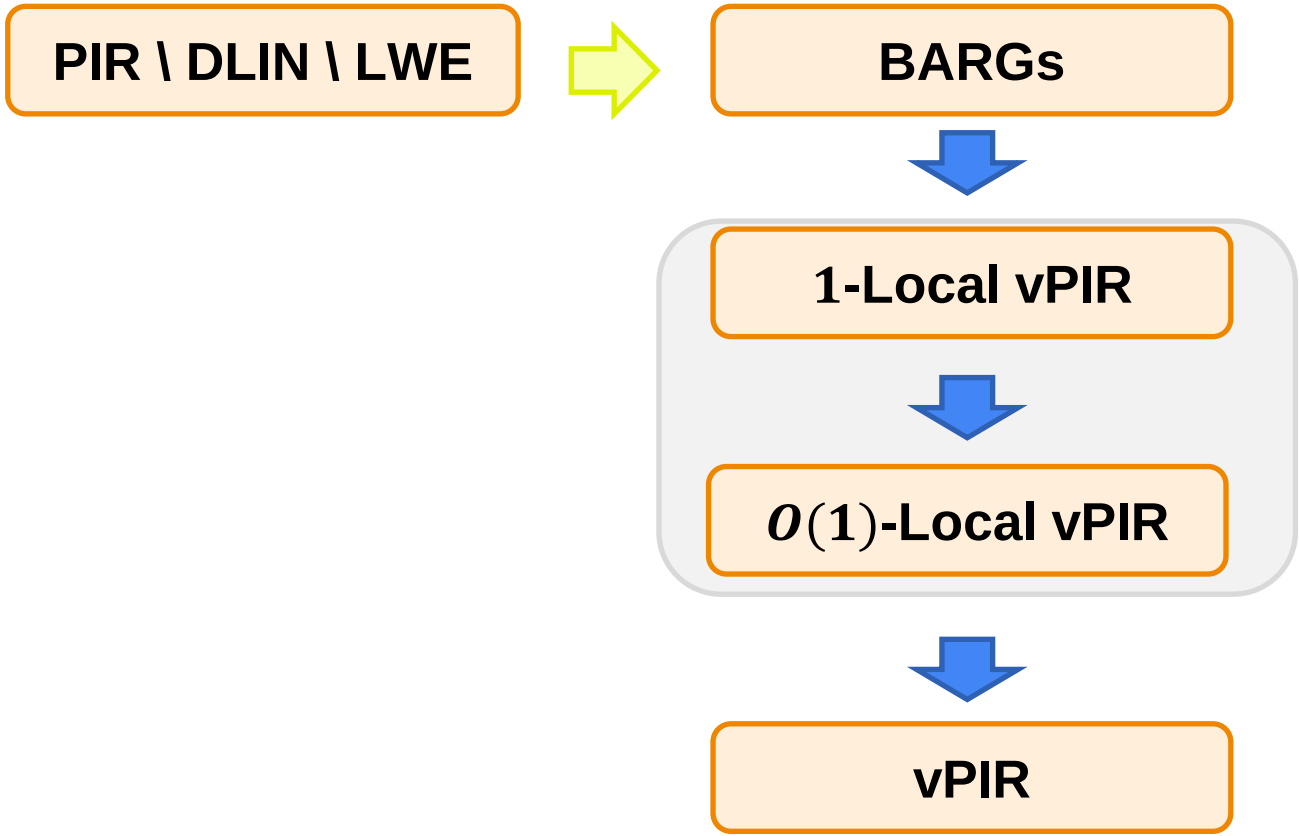
Construction



Construction



Construction



Open Questions

Identify other interesting **class of global properties** that can be proved based on **standard assumptions**.

Open Questions

Identify other interesting **class of global properties** that can be proved based on **standard assumptions**.

Simulate the view of the **client and server** together.