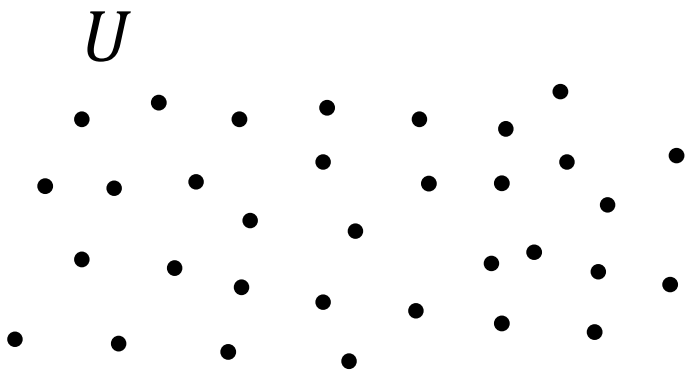
Bet-or-Pass: Adversarially Robust Bloom Filters

Moni Naor and Noa Oved

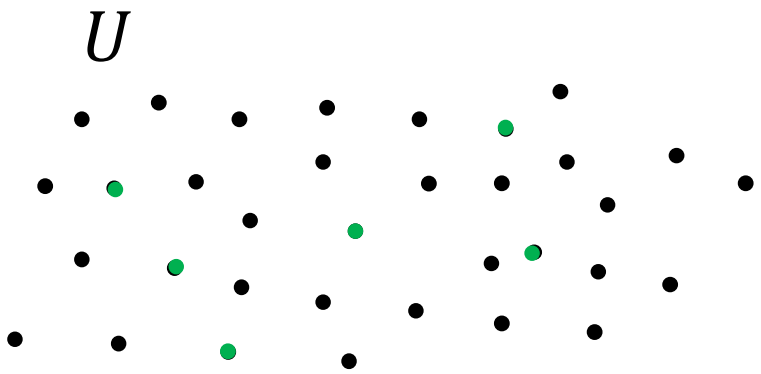
Weizmann Institute of Science

TCC 2022

Bloom Filters [Bloom70]



Bloom Filters [Bloom70]

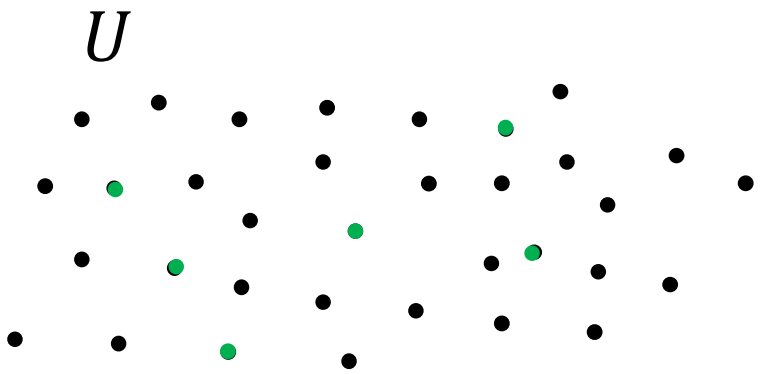


Static set S

$|S| = n$

$|U| \gg |S|$

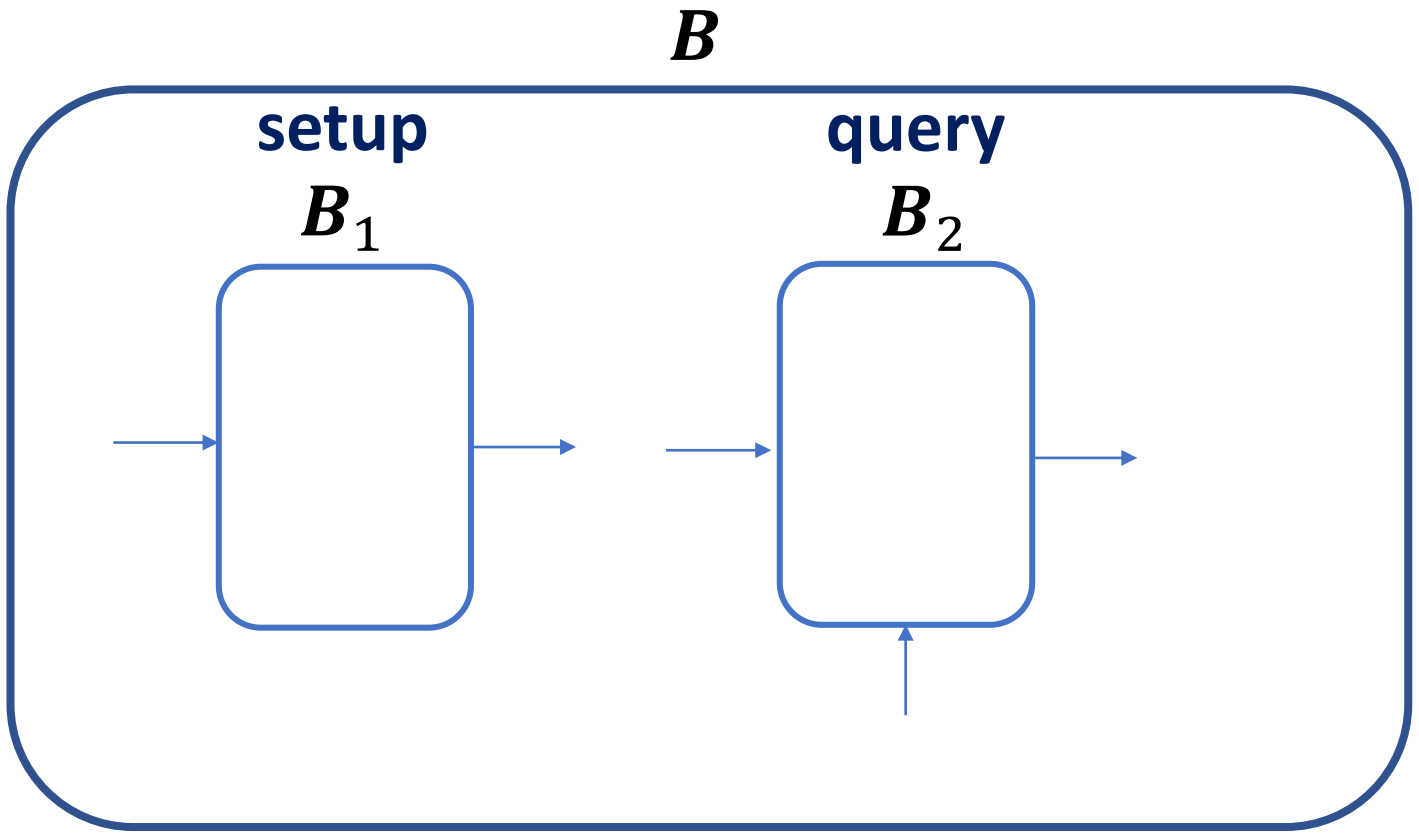
Bloom Filters [Bloom70]



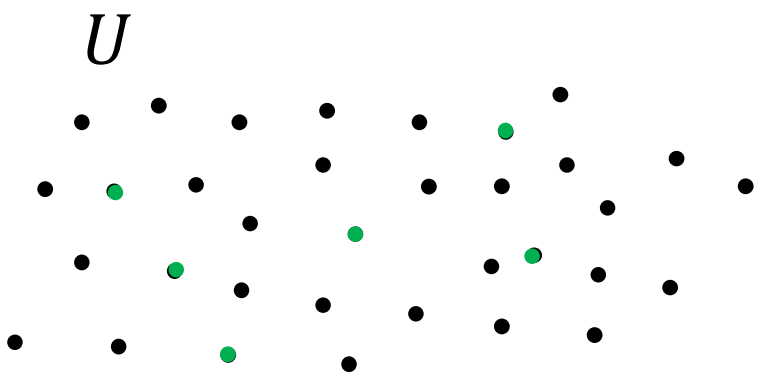
Static set S

$|S| = n$

$|U| \gg |S|$



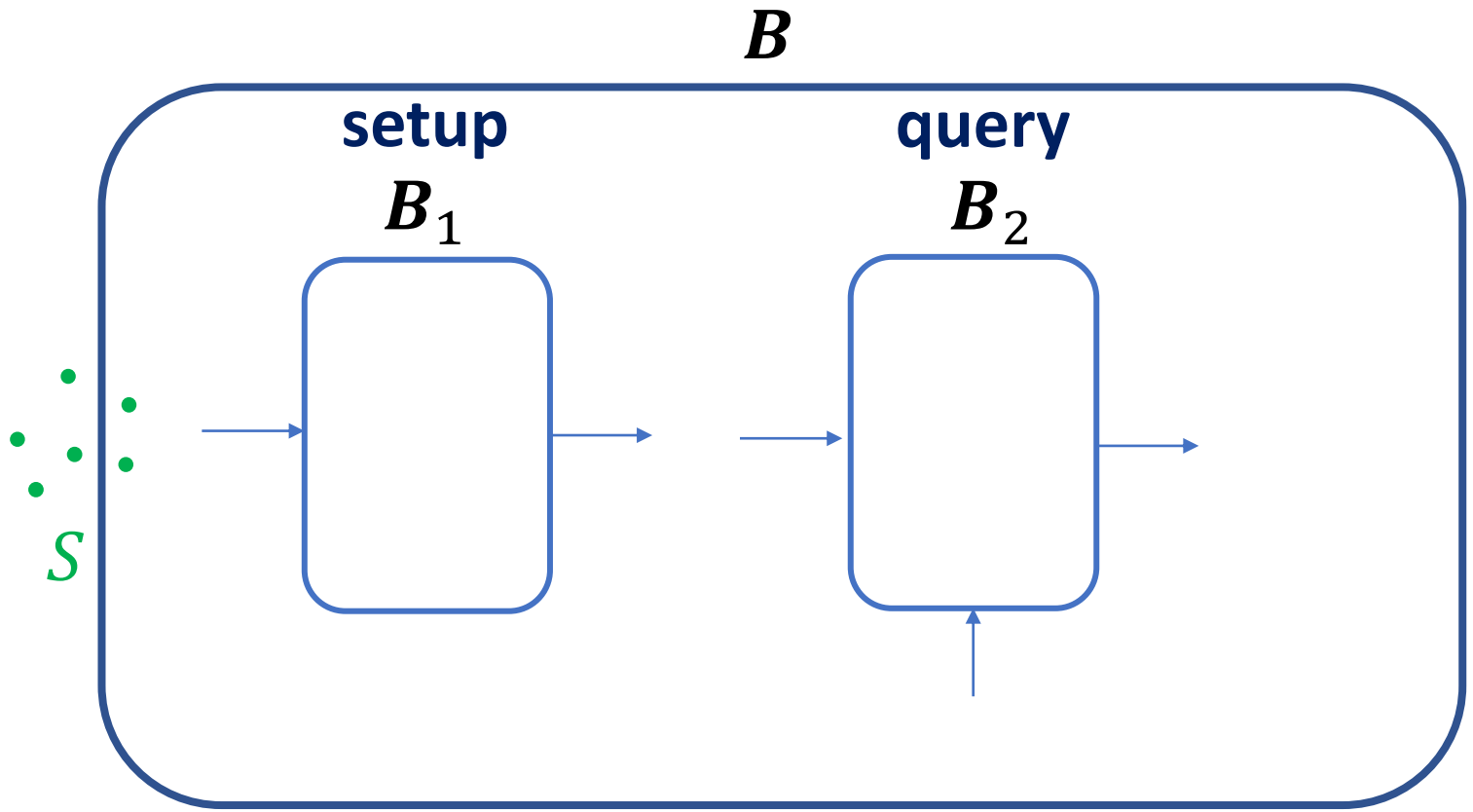
Bloom Filters [Bloom70]



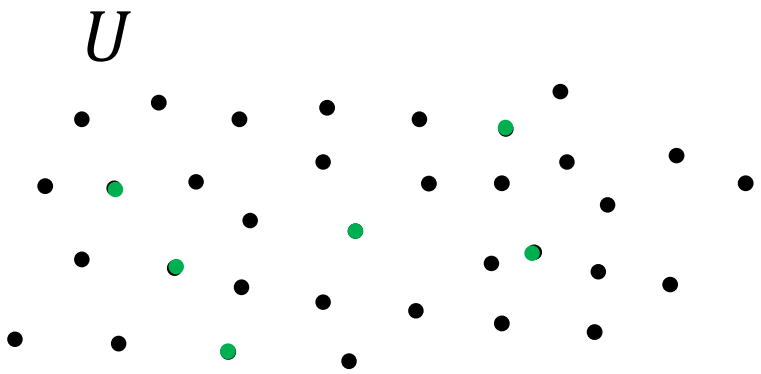
Static set S

$|S| = n$

$|U| \gg |S|$



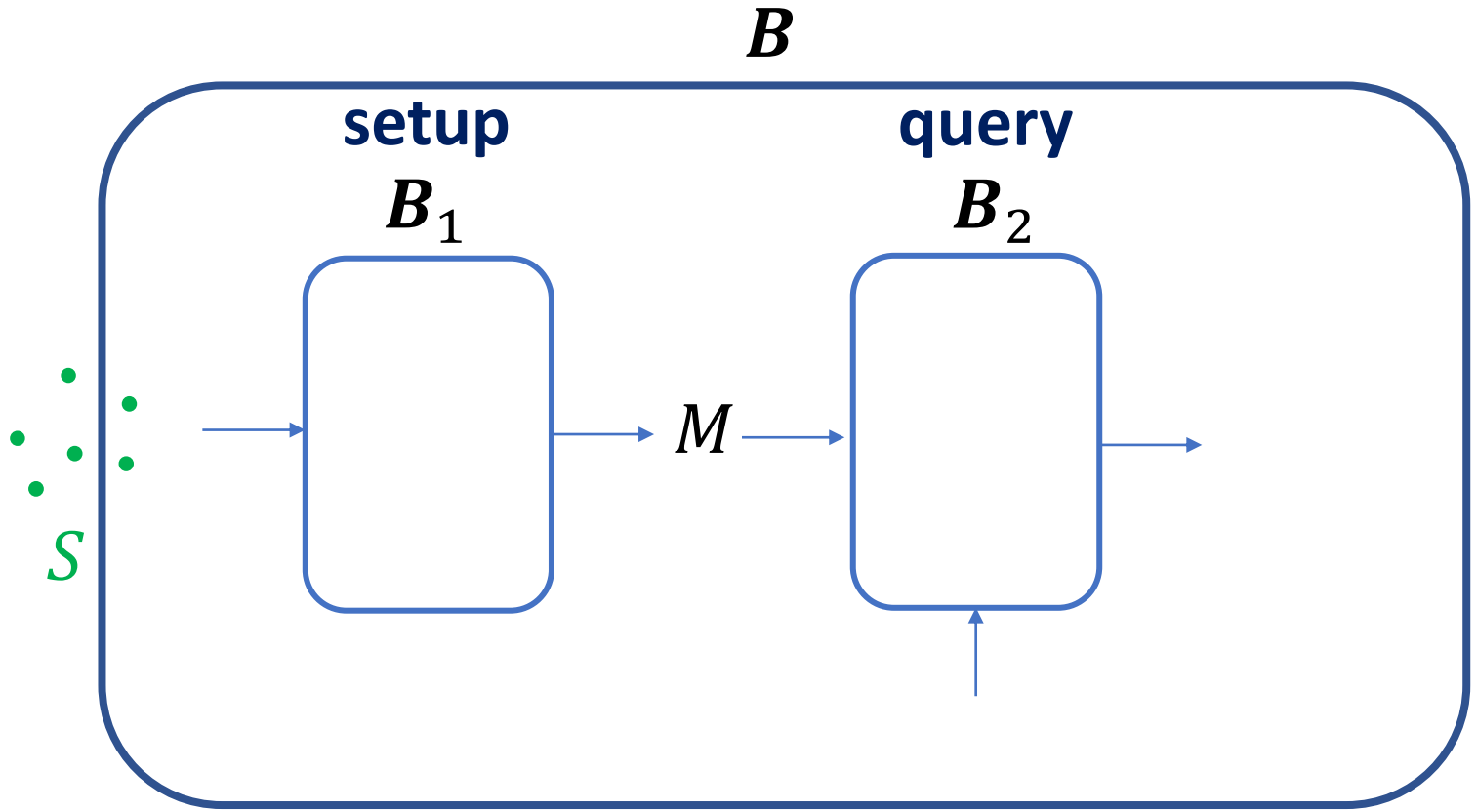
Bloom Filters [Bloom70]



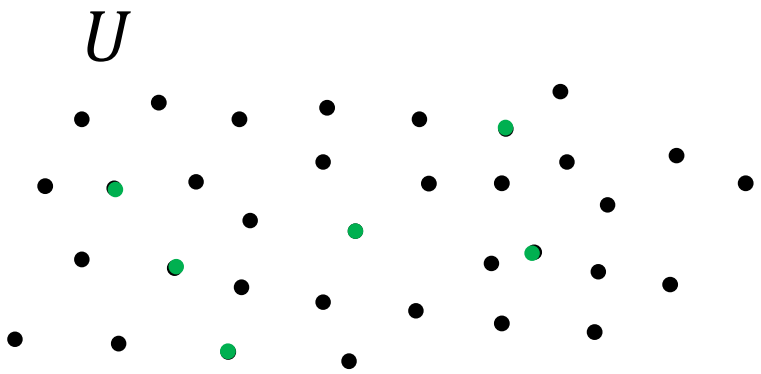
Static set S

$|S| = n$

$|U| \gg |S|$



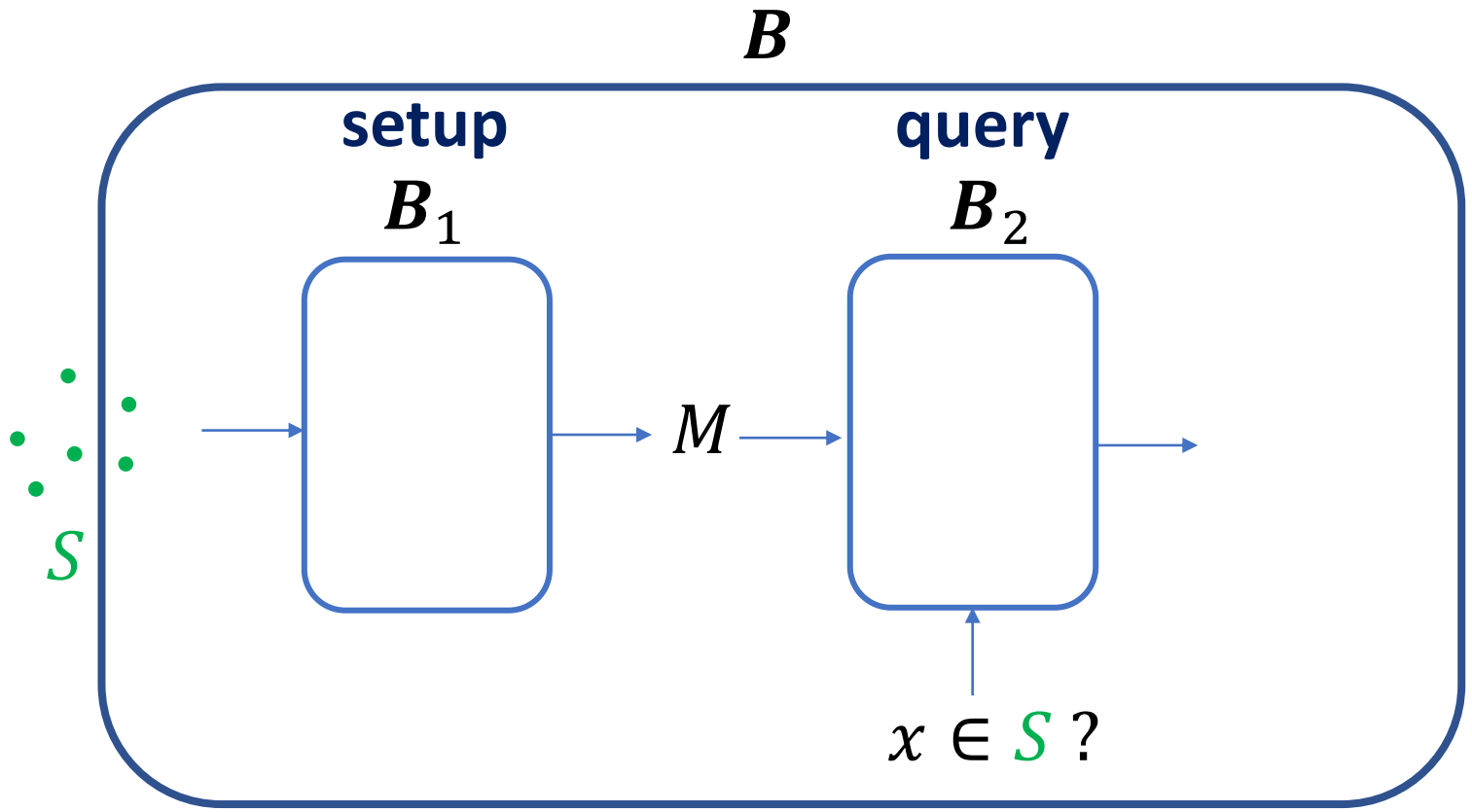
Bloom Filters [Bloom70]



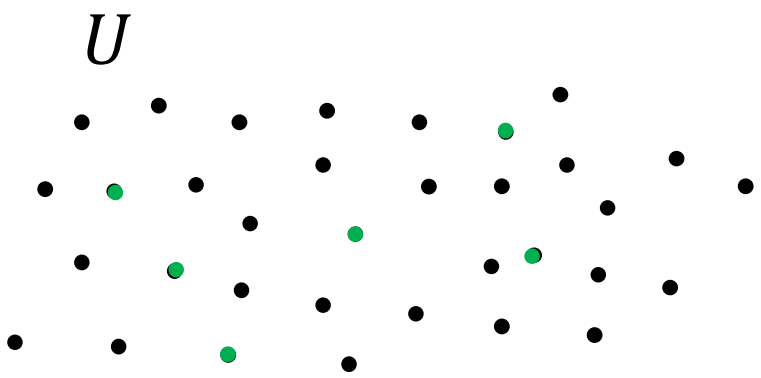
Static set S

$|S| = n$

$|U| \gg |S|$

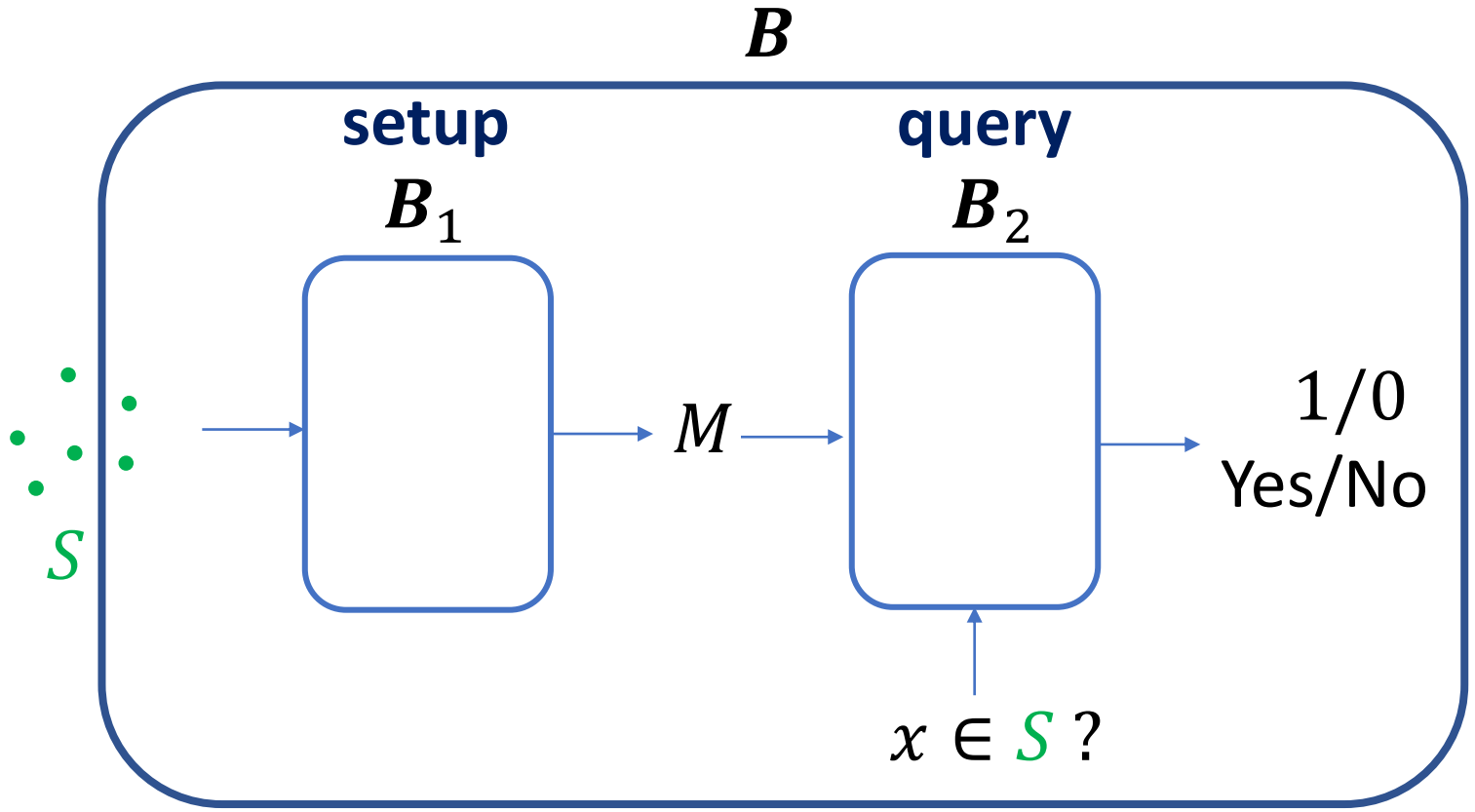


Bloom Filters [Bloom70]



Static set S
$|S| = n$

$|U| \gg |S|$



Bloom Filters

Definition:

$\boldsymbol{B_{n,\varepsilon}}$ satisfies that for all sets S of size n:

- For any $x \in S$: $\boldsymbol{B_{n,\varepsilon}}$ outputs “Yes”
- For any $x \notin S$: $\Pr[\boldsymbol{B_{n,\varepsilon}}(x)$ outputs “Yes” $] \leq \varepsilon$

Bloom Filters

Definition:

$\boldsymbol{B_{n,\varepsilon}}$ satisfies that for all sets S of size n:

- For any $x \in S$: $\boldsymbol{B_{n,\varepsilon}}$ outputs "Yes"
- For any $x \notin S$: $\Pr[\boldsymbol{B_{n,\varepsilon}}(x)$ outputs "Yes" $] \leq \varepsilon$

Memory Lower Bound [CFG+78]: $n \log \frac{1}{\varepsilon} \leq memory \ll |S|$

set representation

Bloom Filters

Definition:

$\boldsymbol{B_{n,\varepsilon}}$ satisfies that for all sets S of size n:

- For any $x \in S$: $\boldsymbol{B_{n,\varepsilon}}$ outputs "Yes"
- For any $x \notin S$: $\Pr[\boldsymbol{B_{n,\varepsilon}}(x)$ outputs "Yes" $] \leq \varepsilon$

non-negligible

Memory Lower Bound [CFG+78]: $n \log \frac{1}{\varepsilon} \leq memory \ll |S|$

set representation

Goal

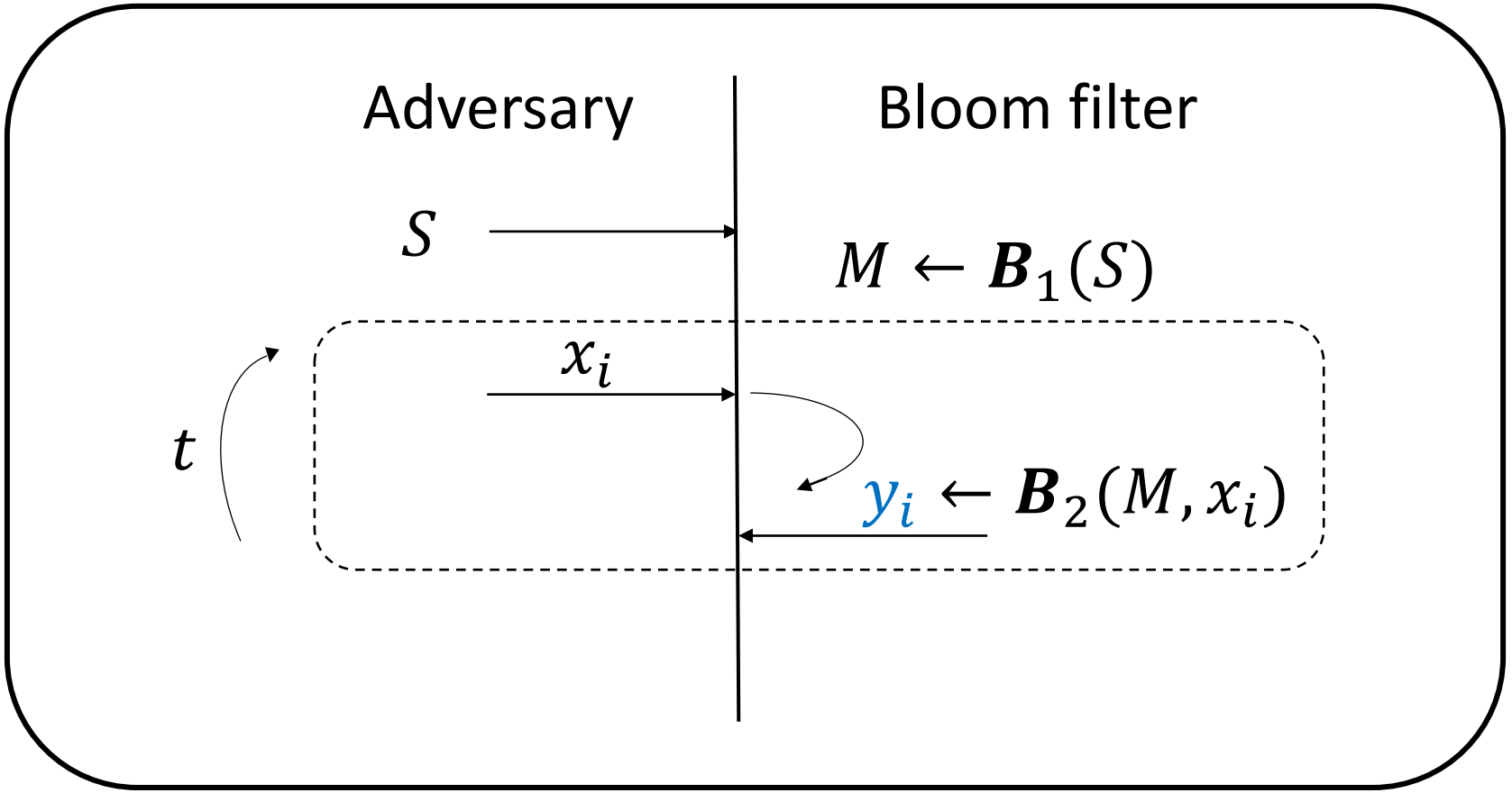
Find a fundamental definition for **robust Bloom filter**

Previous work: [NY15],[BFG+18]

Settings

λ: security parameter

Adaptive Game [based on NY15]



Robust Bloom filter

Wishful thinking:

Robust Bloom filter ≈ truly unpredictable ε-biased coin

$$(y_1, \ldots, y_t) \approx (\$_1, \ldots, \$_t)$$

Robust Bloom filter

Wishful thinking:

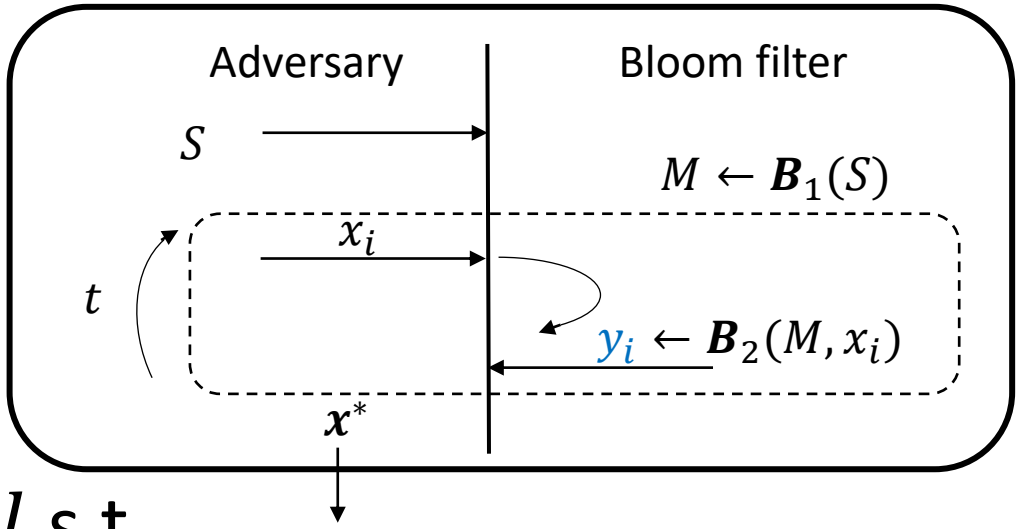
Robust Bloom filter ≈ truly unpredictable ε-biased coin

$$(y_1, \dots, y_t) \approx (\$_1, \dots, \$_t)$$

Motivation: avoid clusters of false positives

$$0001111111001 \qquad ,1 = \mathrm{FP}$$

Previous Work [NY15]

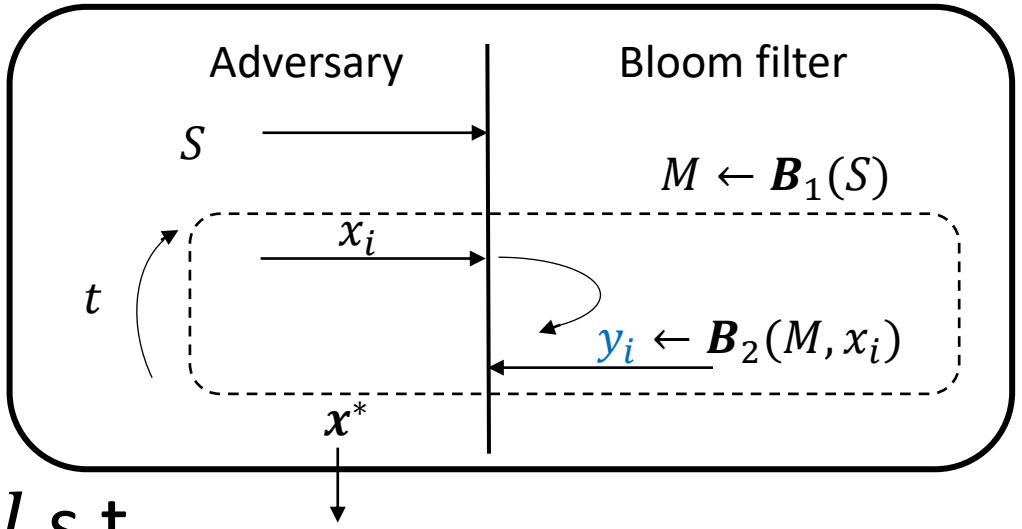


(informal) Definition [NY15]:

$\boldsymbol{B}_{\boldsymbol{n},\boldsymbol{\varepsilon}}$ satisfies **NY15** if ∀ PPT $\mathcal{A}$ ∃ $negl$ s.t.

$$\Pr[x^* \; is \; false \; positive] \leq \varepsilon + negl(\lambda)$$

Previous Work [NY15]



(informal) Definition [NY15]:

$\boldsymbol{B}_{\boldsymbol{n},\boldsymbol{\varepsilon}}$ satisfies **NY15** if ∀ PPT $\mathcal{A}$ ∃ $negl$ s.t.

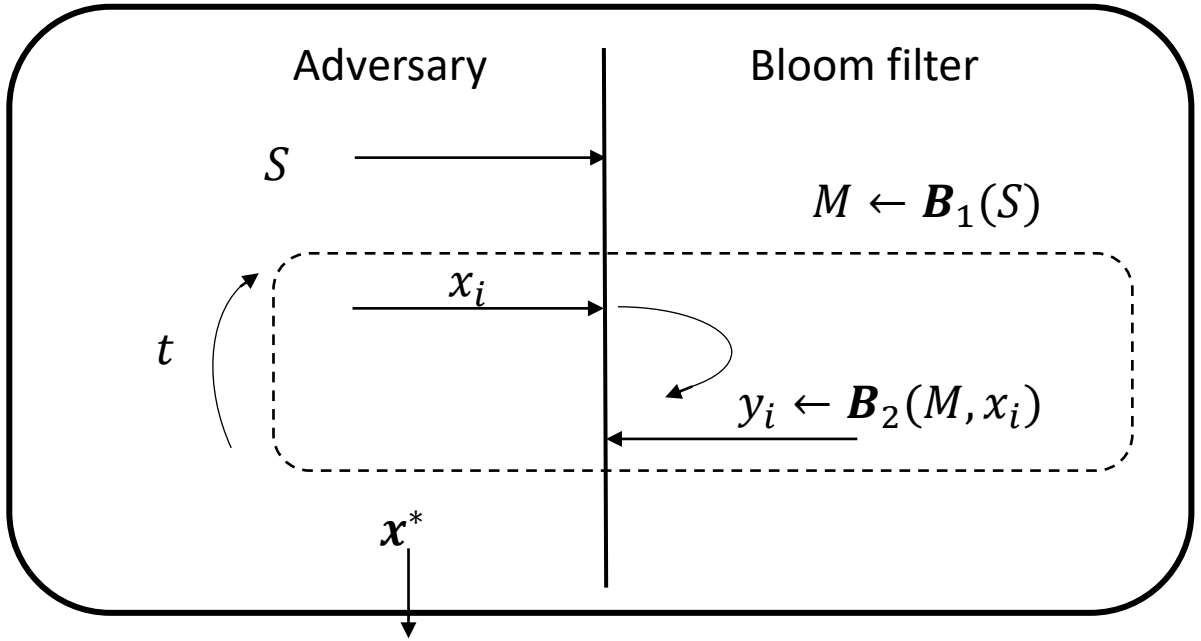
$$\Pr[x^* \; is \; false \; positive] \leq \varepsilon + negl(\lambda)$$

NY15 **does not** satisfies our wishful thinking:

$$(y_1, \ldots, y_t) \not\approx (\$_1, \ldots, \$_t)$$

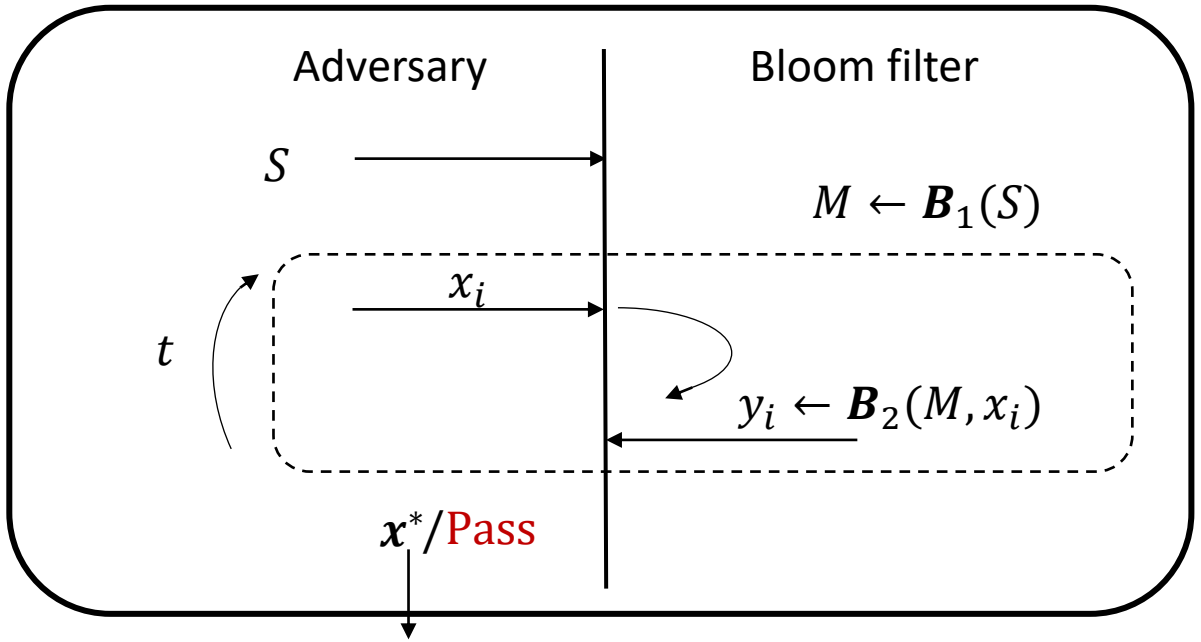
Main Result

Introduce *Bet-or-Pass* (BP), we allow the adversary to Pass



Main Result

Introduce *Bet-or-Pass* (BP), we allow the adversary to Pass



Main Result

Adversary Profit:

$$Profit_{\mathcal{A}} = \begin{cases} 1/\varepsilon & if\ \mathcal{A}\ outputs\ a\ false\ positive \\ -1/(1-\varepsilon) & if\ \mathcal{A}\ outputs\ \boldsymbol{not}\ a\ false\ \ positive \\ 0 & if\ \mathcal{A}\ passes \end{cases}$$

Note: The expected profit of ε-biased coin is 0

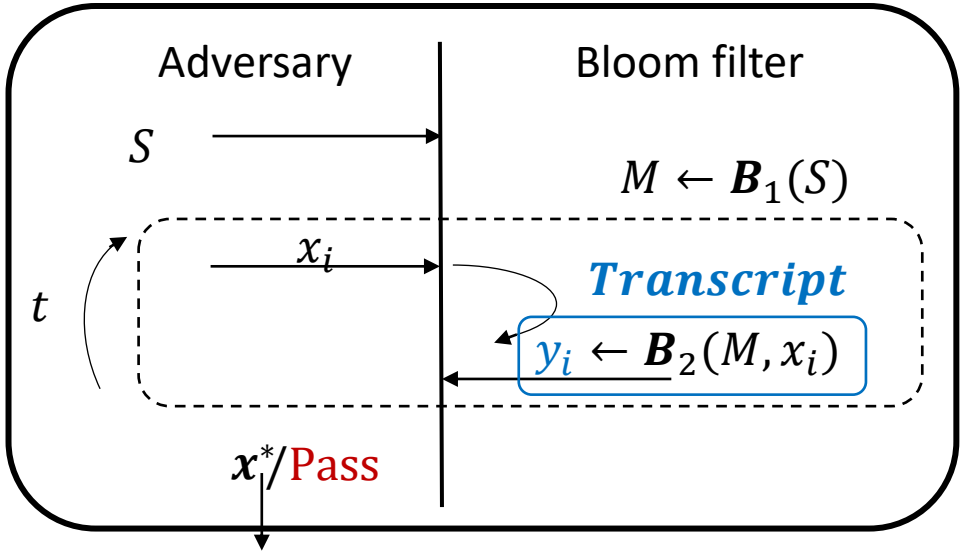
(informal) Definition:

$\boldsymbol{B_{n,\varepsilon}}$ satisfies **Bet-or-Pass** (**BP**) if $\forall$ PPT $\mathcal{A}$ $\exists\ negl$ s.t.

$$\mathbb{E}[Profit_{\mathcal{A}}] \leq 0 + negl(\lambda)$$

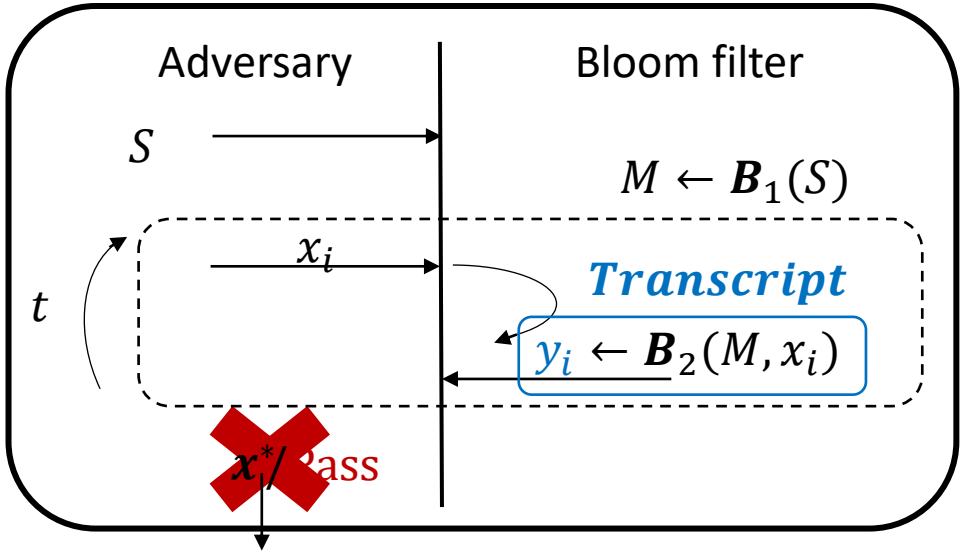
Formalize Wishful Thinking

Monotone Test

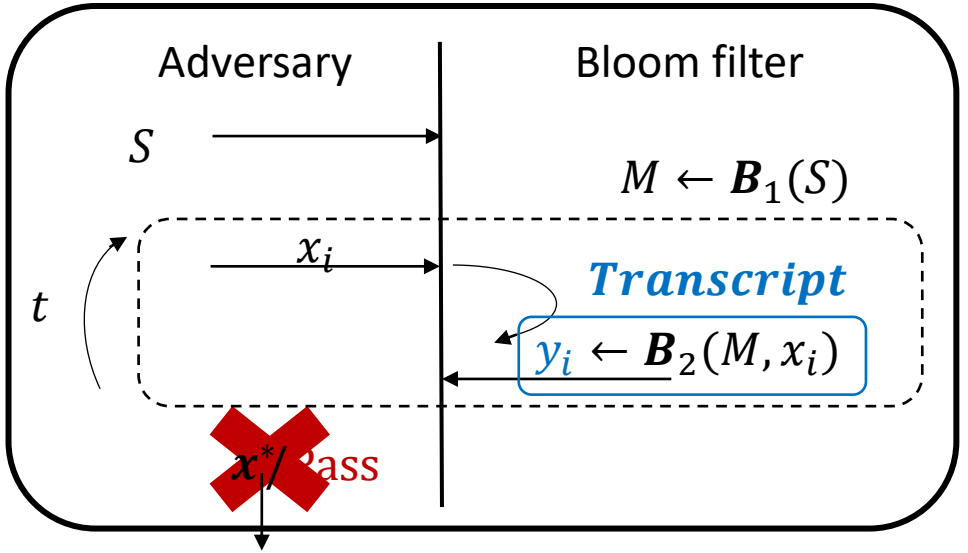


Formalize Wishful Thinking

Monotone Test

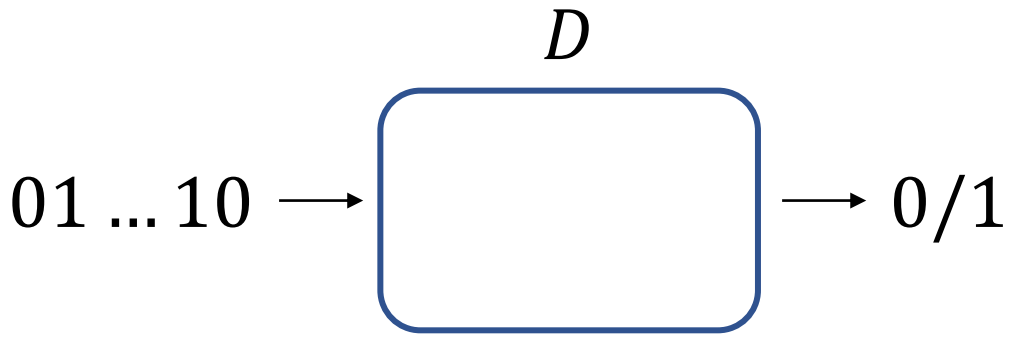


Formalize Wishful Thinking

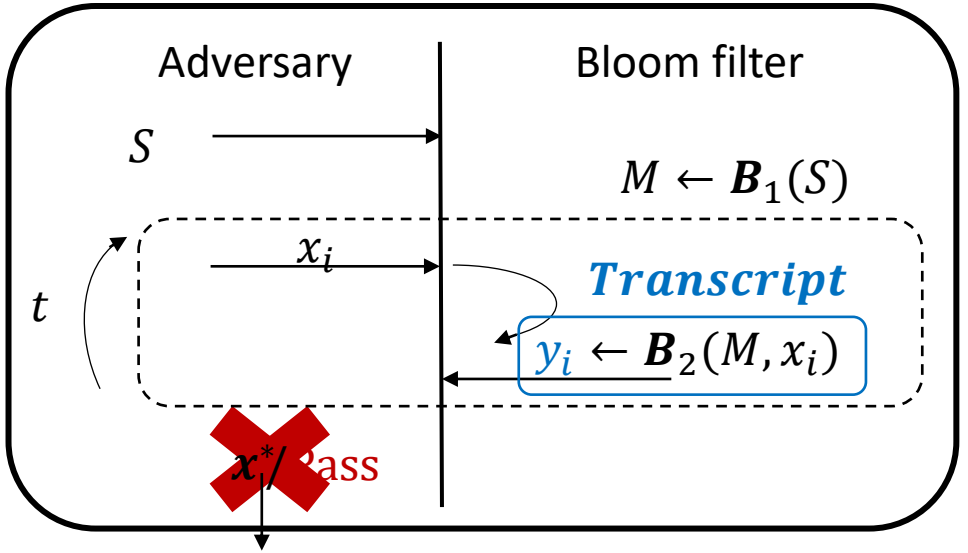


Monotone Test

Distinguisher:

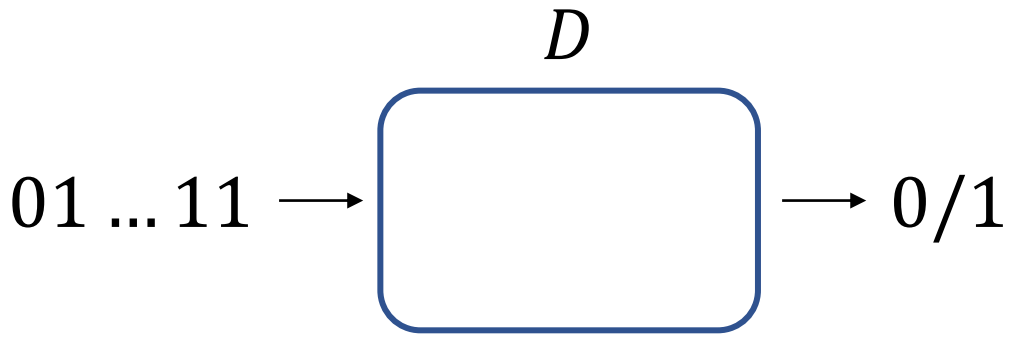


Formalize Wishful Thinking

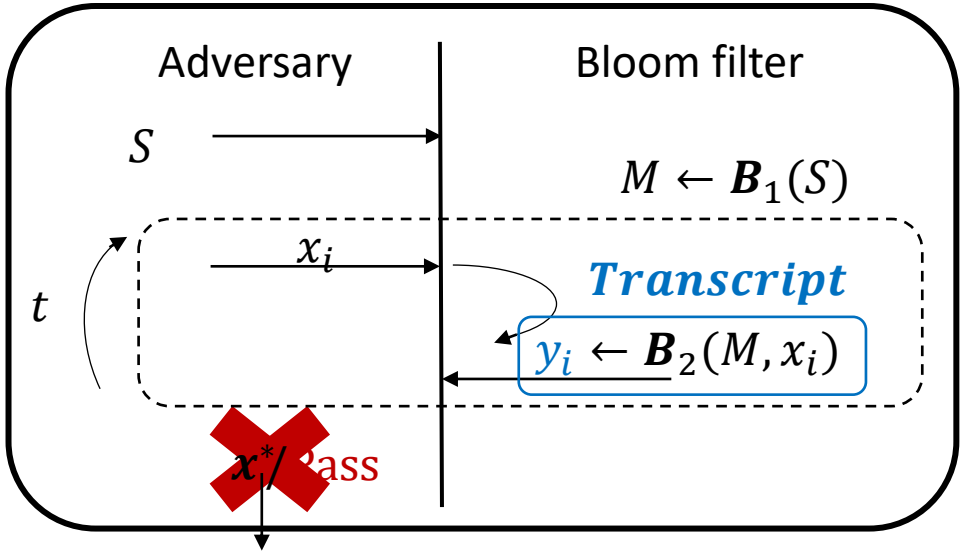


Monotone Test

Distinguisher:

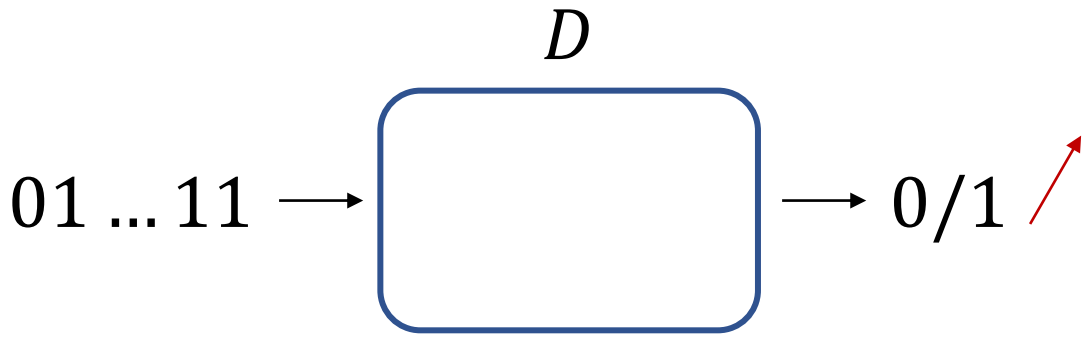


Formalize Wishful Thinking

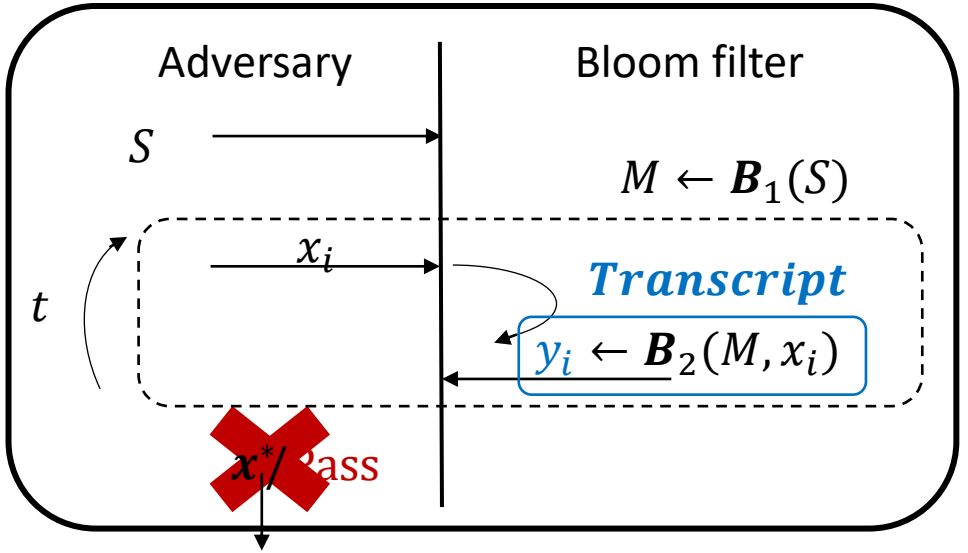


Monotone Test

Distinguisher:

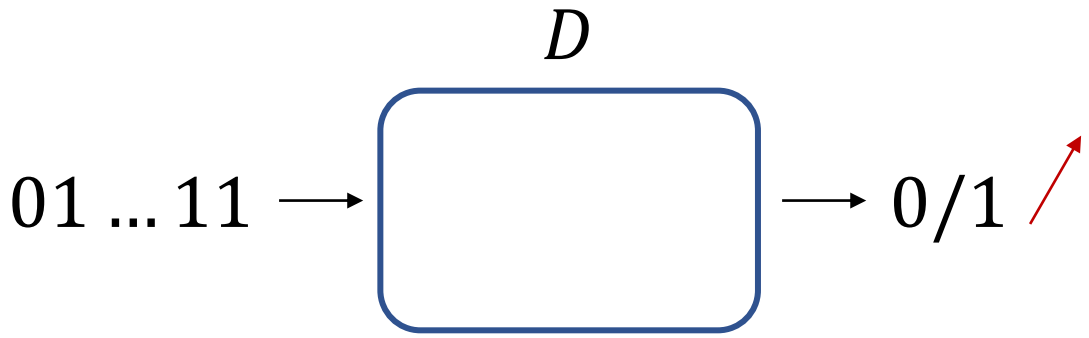


Formalize Wishful Thinking



Monotone Test

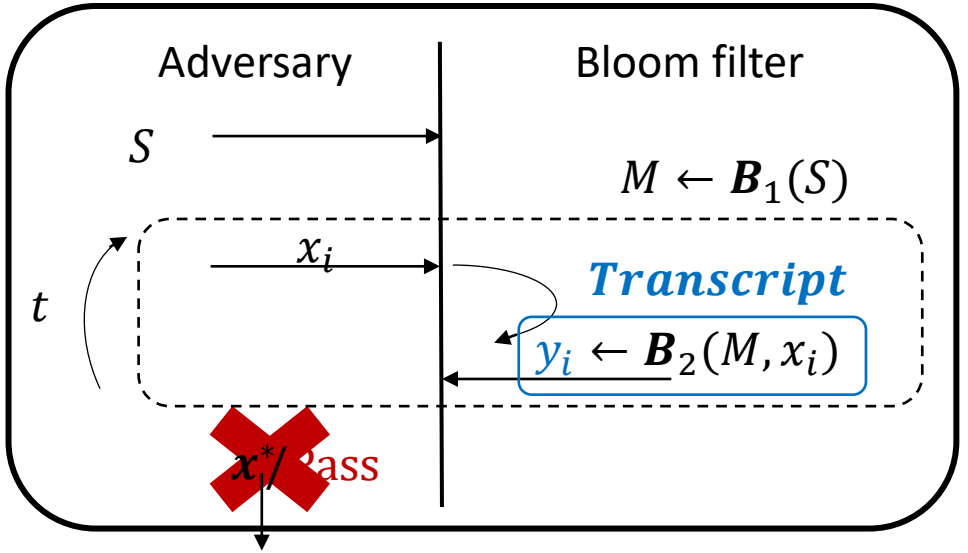
Distinguisher:



Example:

- **Cluster**: outputs 1 iff the sequence contains w consecutive 1's.

Formalize Wishful Thinking



Monotone Test

(informal) Definition:

$\boldsymbol{B}_{\boldsymbol{n},\boldsymbol{\varepsilon}}$ satisfies **Monotone Test** if ∀ Monotone PPT distinguisher D and ∀ PPT $\mathcal{A}$ ∃ $negl$ s.t.

$$\Pr_{\mathcal{S}\in Transcript}[D(\mathcal{S}) = 1] - \Pr_{\mathcal{S}\in \$_{\varepsilon}}[D(\mathcal{S}) = 1] \leq negl(\lambda)$$

Main Result

Let $0 < \varepsilon < 1$ and $\mathrm{n} \in N$. Let $\boldsymbol{B_{n,\varepsilon}}$ be **BP** test resilient Bloom filter. Then $\boldsymbol{B_{n,\varepsilon}}$ is also **monotone** test resilient.

Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch

- Proof by contradiction
- We show how we can take $\mathcal{A}$ and D and use them when building an adversary that can predict when it's best to bet.
- Hybrid argument

Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch

Theorem: BP $\Longrightarrow$ monotone

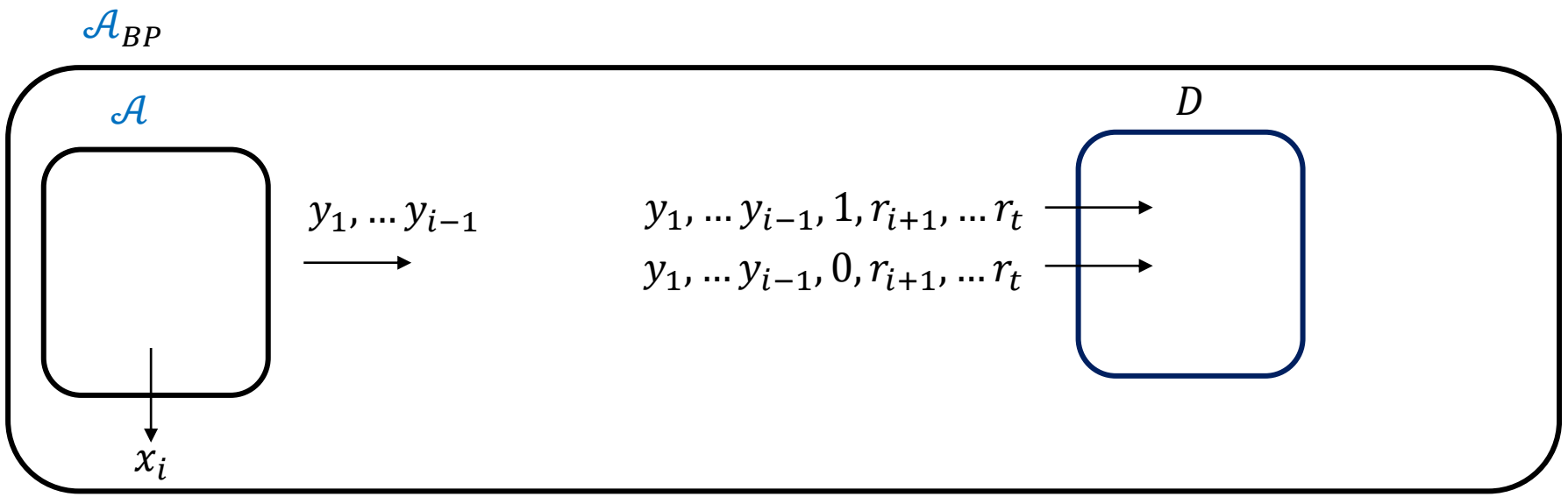
Main Theorem: Proof Sketch

Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch

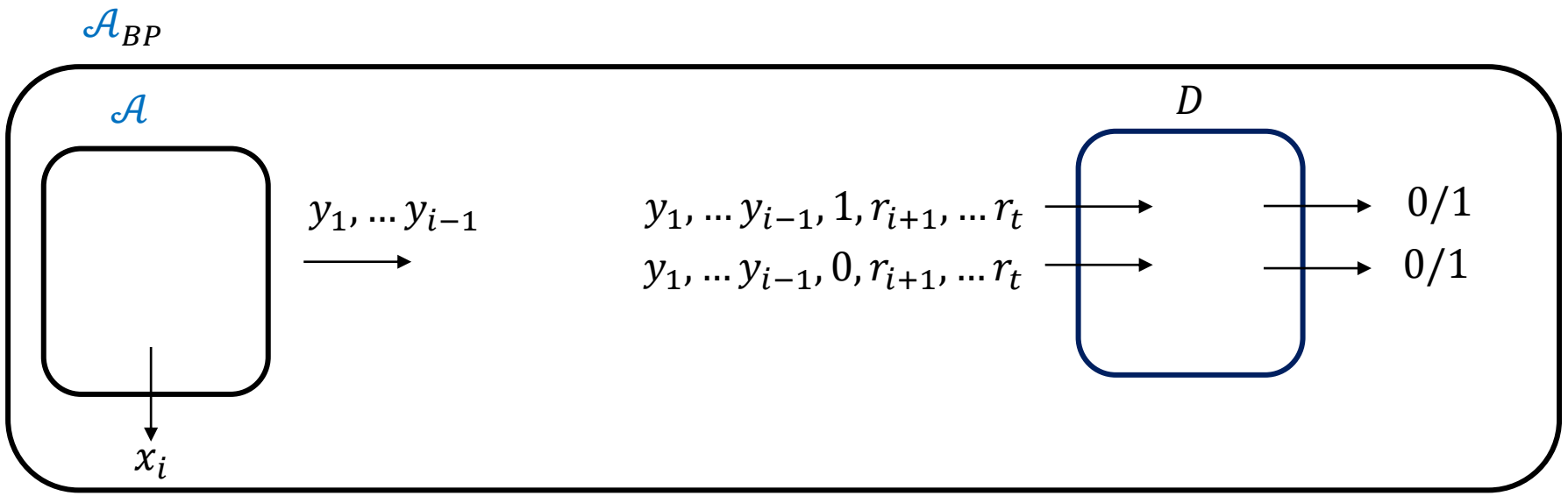
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



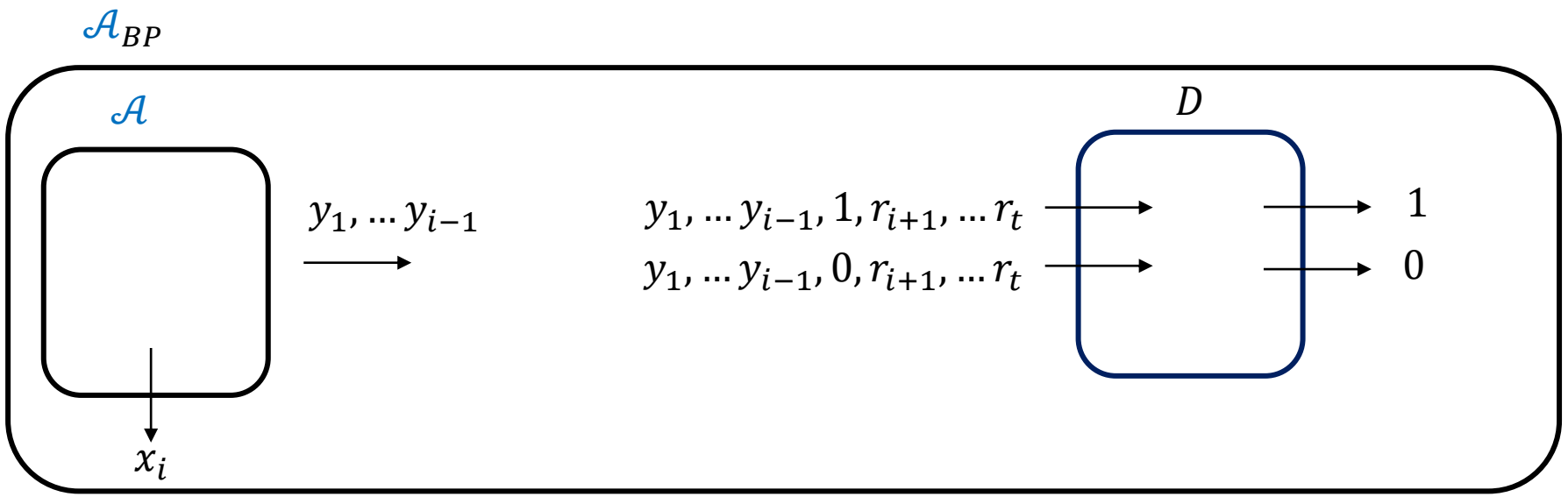
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



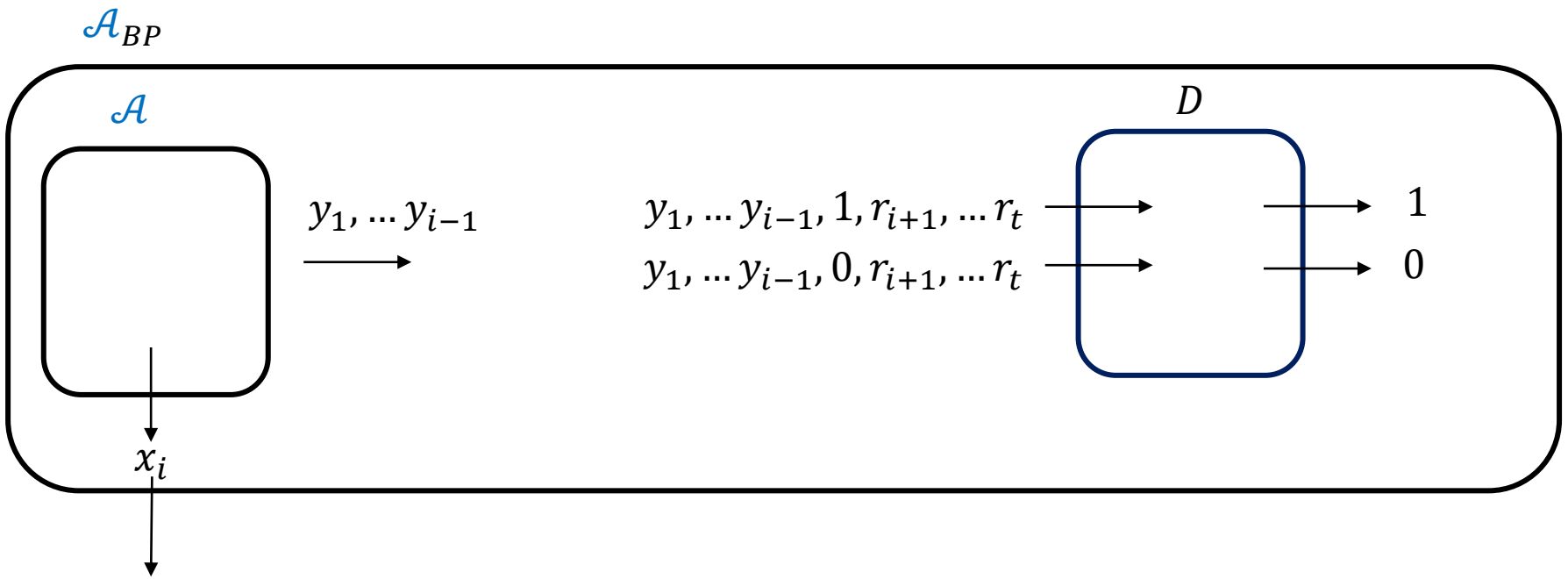
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



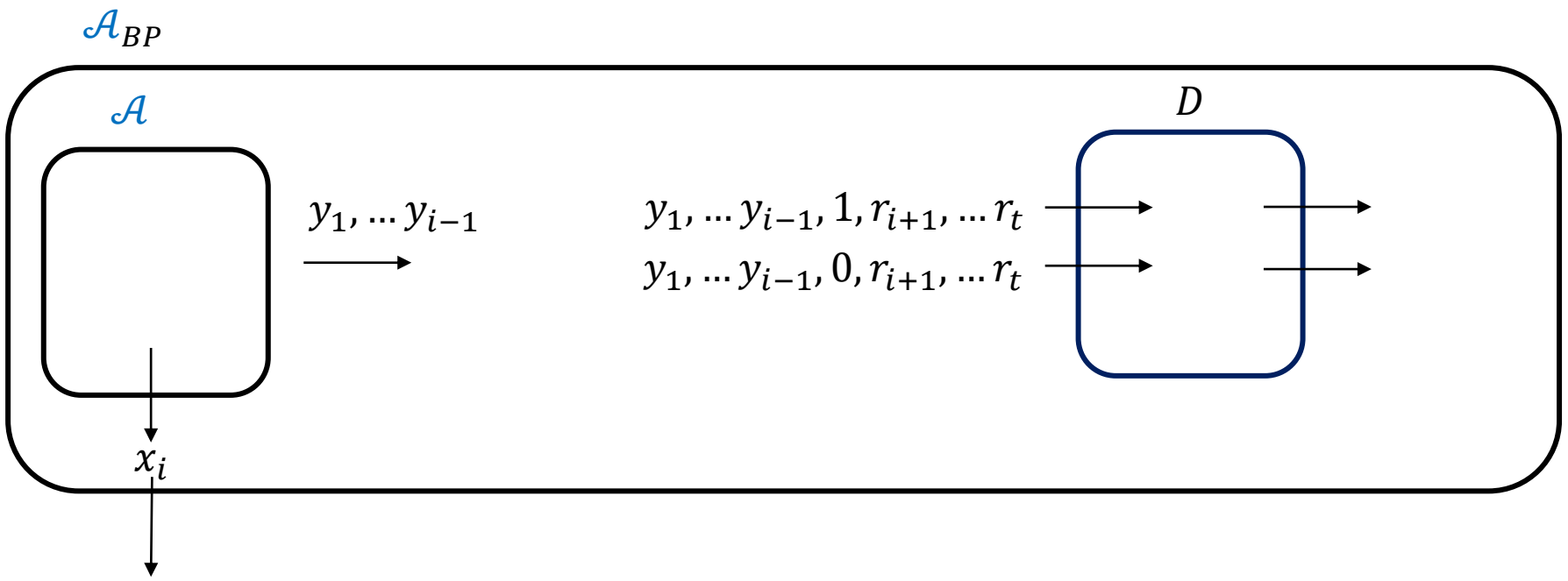
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



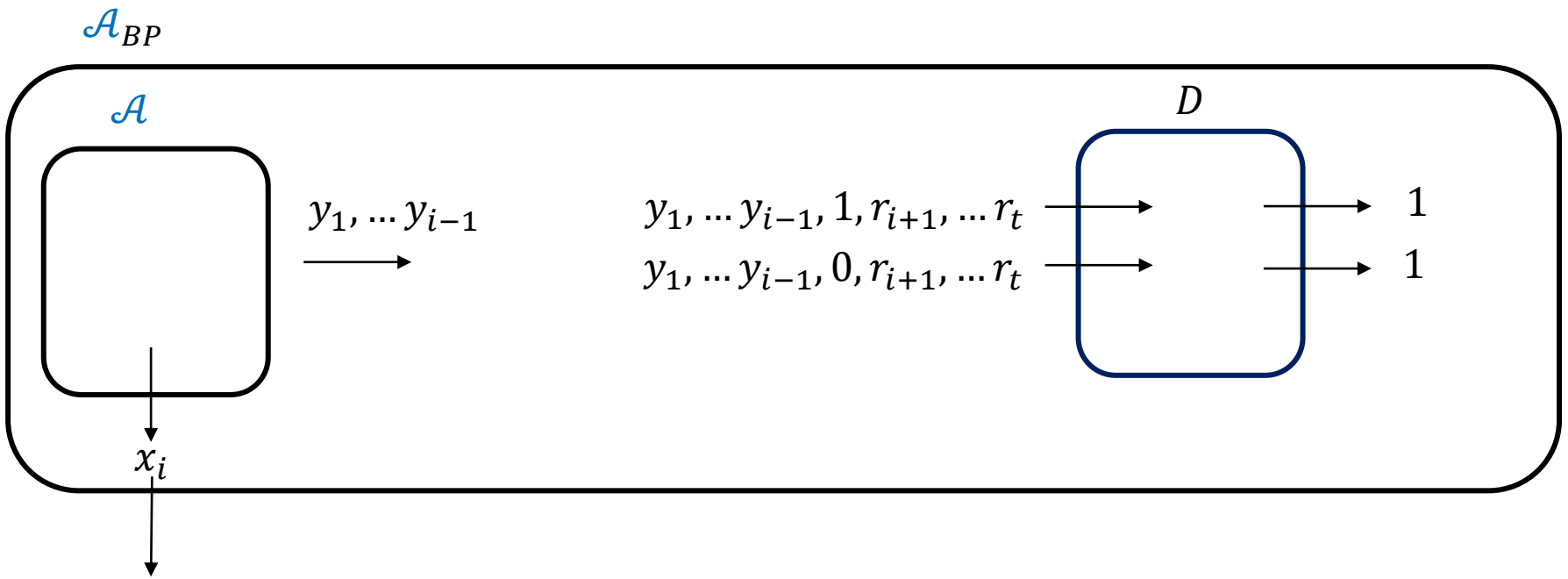
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



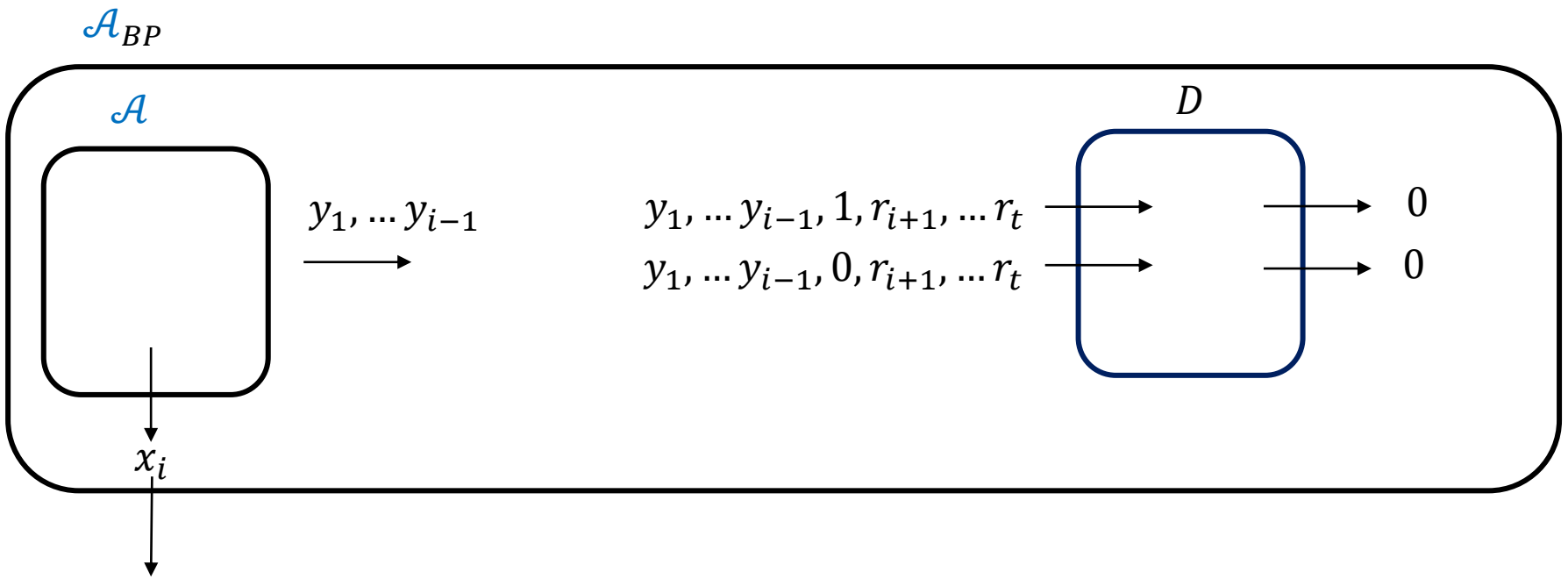
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



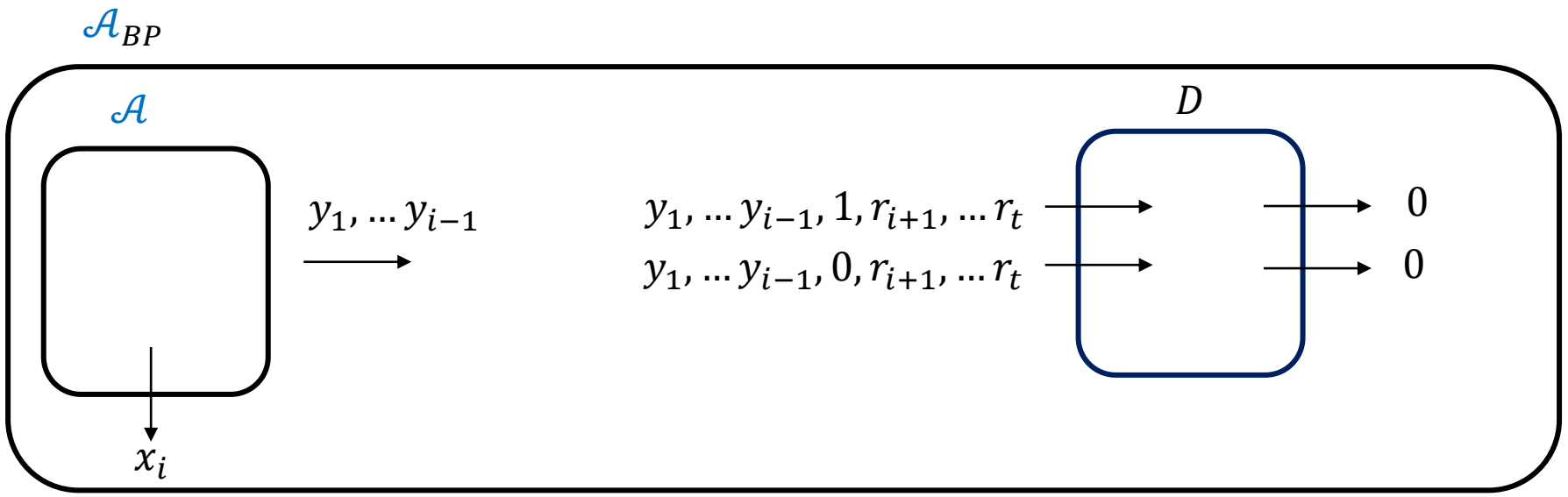
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



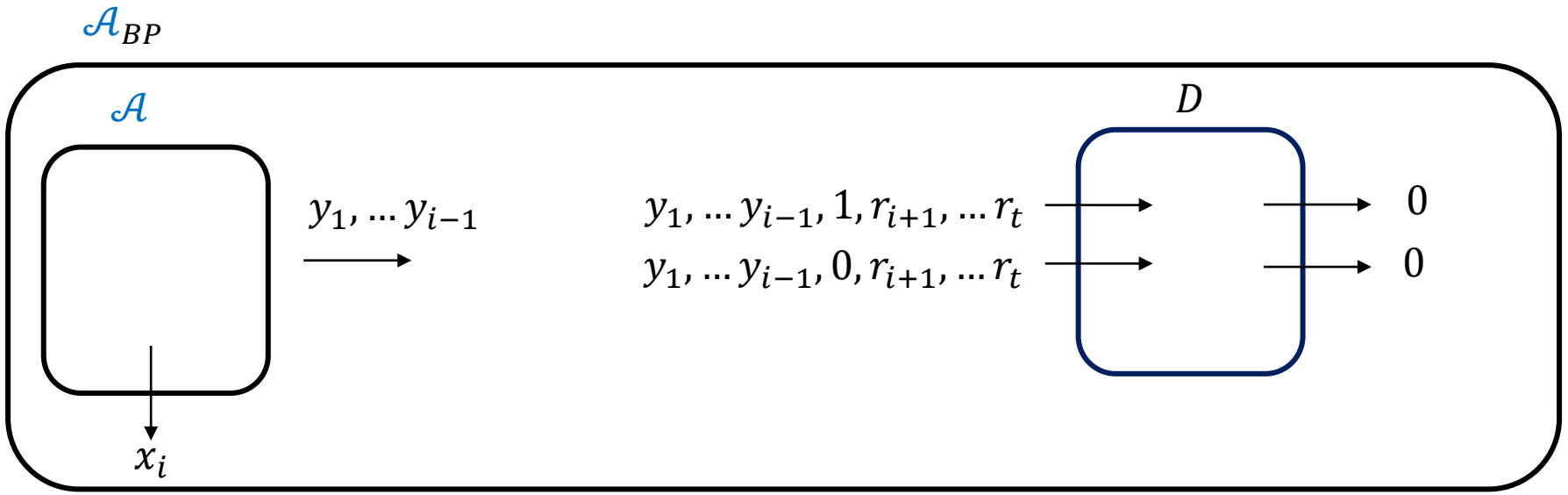
Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



Theorem: BP $\Longrightarrow$ monotone

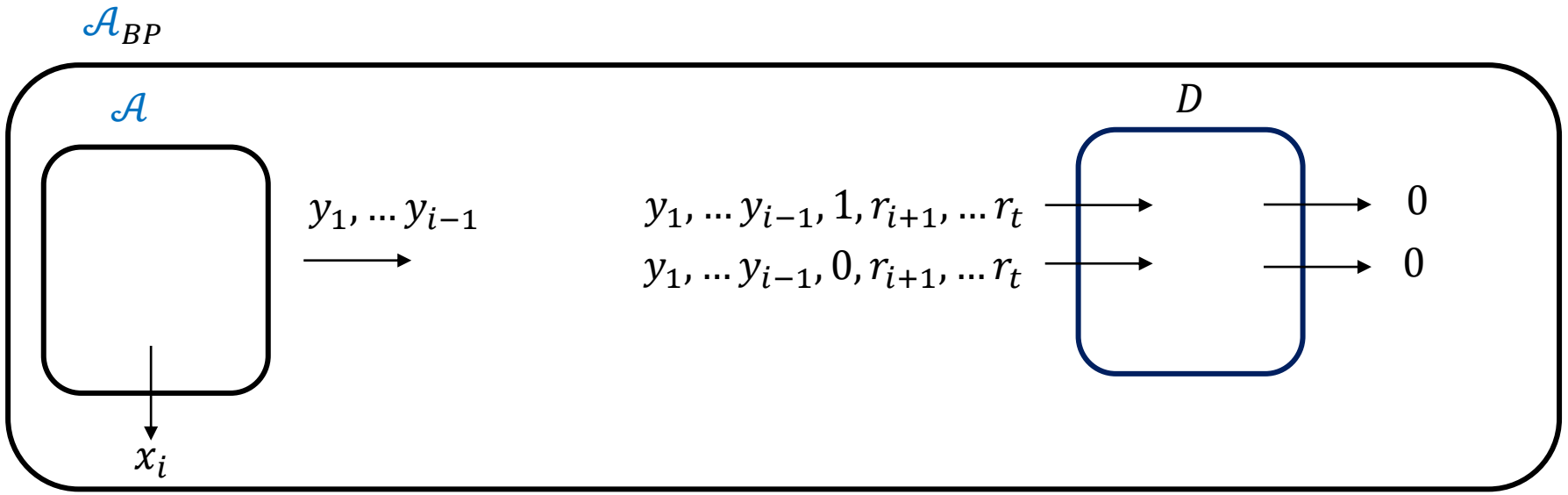
Main Theorem: Proof Sketch



$\Pr[bet] > 0$ and $\Pr[x_i \; is \; FP \mid bet] > \varepsilon \Longrightarrow \mathbb{E}[Profit_{\mathcal{A}_{BP}}] > 0$

Theorem: BP $\Longrightarrow$ monotone

Main Theorem: Proof Sketch



$\Pr[bet] > 0$ and $\Pr[x_i \text{ is } FP \mid bet] > \varepsilon \Longrightarrow \mathbb{E}[Profit_{\mathcal{A}_{BP}}] > 0$

■

Summary and More

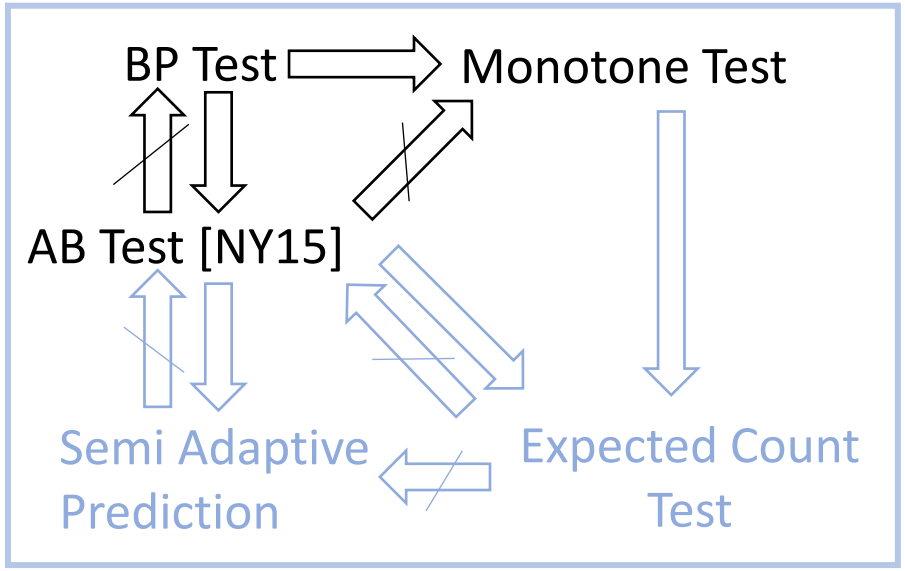
Paper:
Bet-or-Pass: Adversarially Robust Bloom Filters
Moni Naor and Noa Oved

- Highlight the notion of *Bet-or-Pass*
  - Construction based on OWF
  - More (weaker) notions

Summary and More

- Highlight the notion of *Bet-or-Pass*
  - Construction based on OWF
  - More (weaker) notions

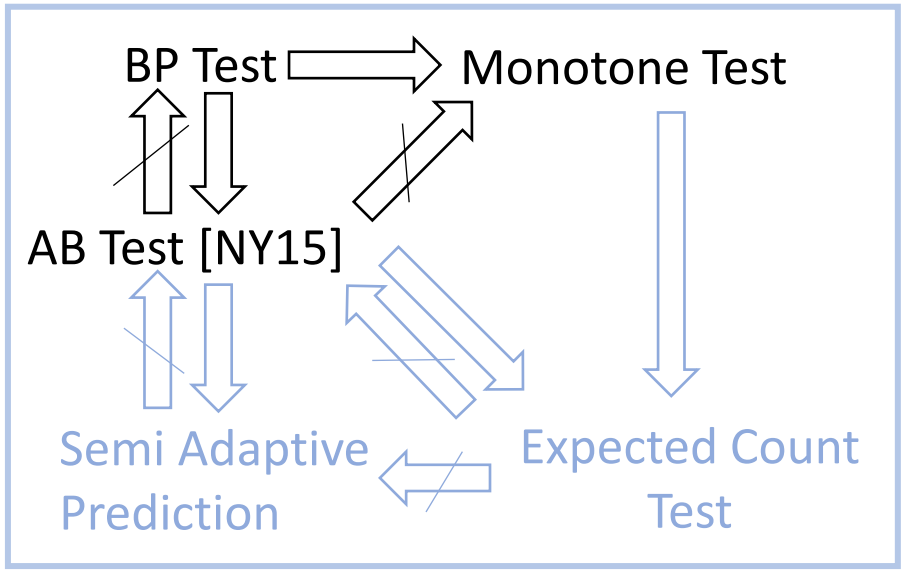
Paper:
Bet-or-Pass: Adversarially Robust Bloom Filters
Moni Naor and Noa Oved



Summary and More

- Highlight the notion of *Bet-or-Pass*
  - Construction based on OWF
  - More (weaker) notions
- Open Questions:
  - Monotone Test Resilience implies BP Test Resilience?
  - Allowing repetitions [BFG+18]
  - And more

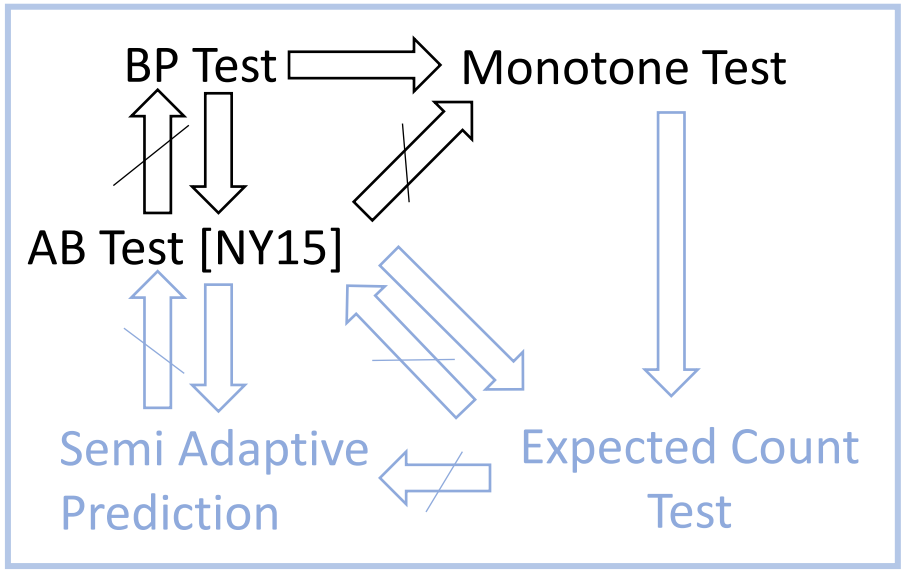
Paper:
Bet-or-Pass: Adversarially Robust Bloom Filters
Moni Naor and Noa Oved



Summary and More

Paper:
Bet-or-Pass: Adversarially Robust Bloom Filters
Moni Naor and Noa Oved

- Highlight the notion of *Bet-or-Pass*
  - Construction based on OWF
  - More (weaker) notions
- Open Questions:
  - Monotone Test Resilience implies BP Test Resilience?
  - Allowing repetitions [BFG+18]
  - And more



Thank You!