Conditional Disclosure of Secrets

Benny Applebaum
Tel Aviv University

BIU Winter-School of Information-Theoretic Cryptography

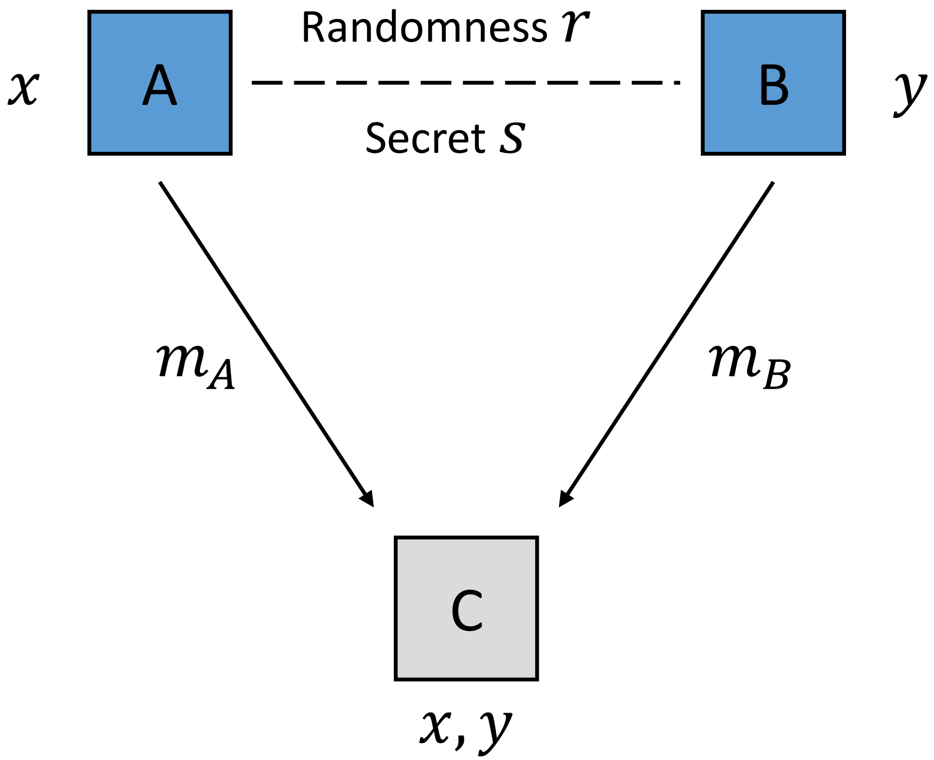
February 2020

Plan

- Definition
- Applications
- General Constructions
  - Direct construction
  - PIR-based construction
  - Amortized CDS
- Few words about Lower-bounds

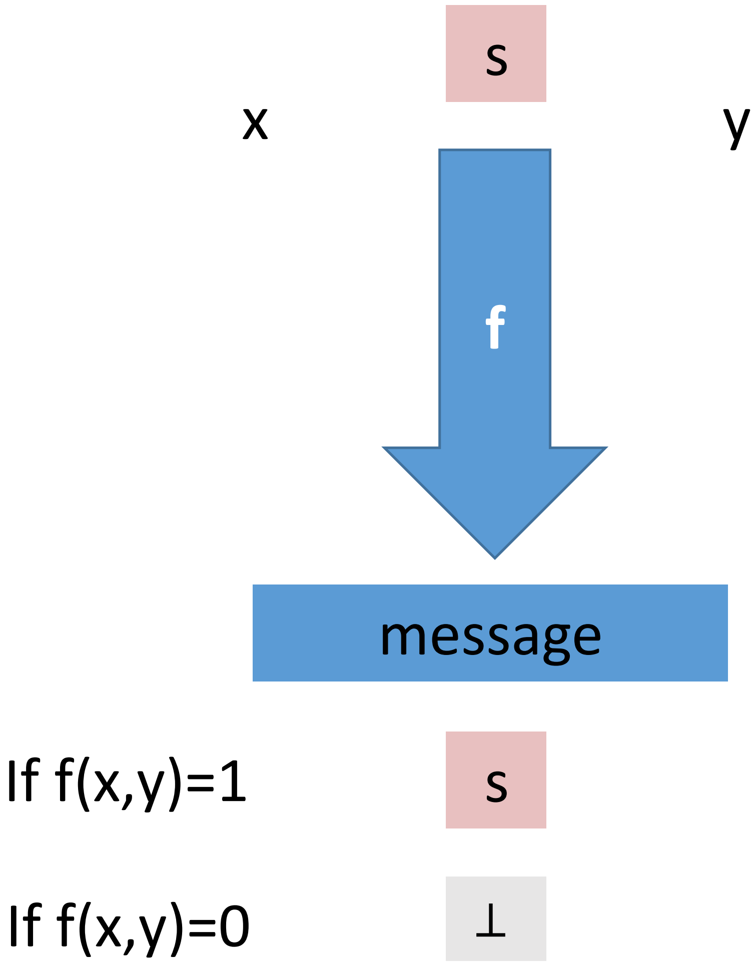
Conditional Disclosure of Secrets [GIKM00]

$f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$



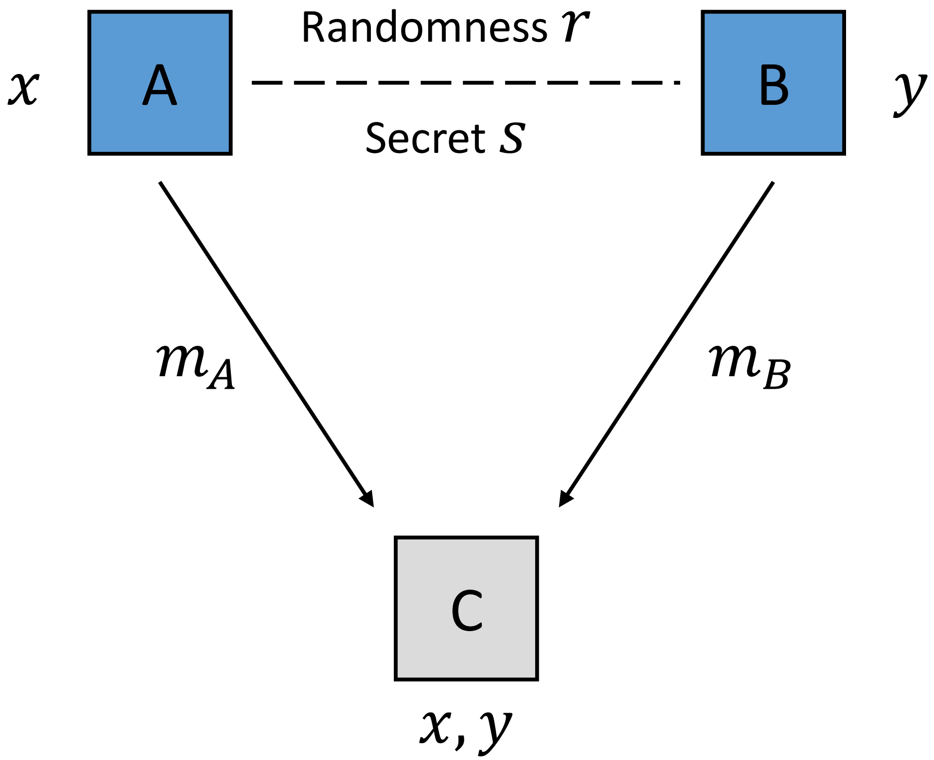
Goal: Charlie learns secret if and only if f(x,y)=1

f-channel



Conditional Disclosure of Secrets [GIKM00]

$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$



Goal: Charlie learns secret if and only if f(x,y)=1

δ-Correctness:

If $f(x,y) = 1$, then for any s,

$$\Pr[C(x,y,m_A,m_B) = s] \geq 1 - \delta$$

ϵ-Privacy:

If $f(x,y) = 0$, then for any s, x, y

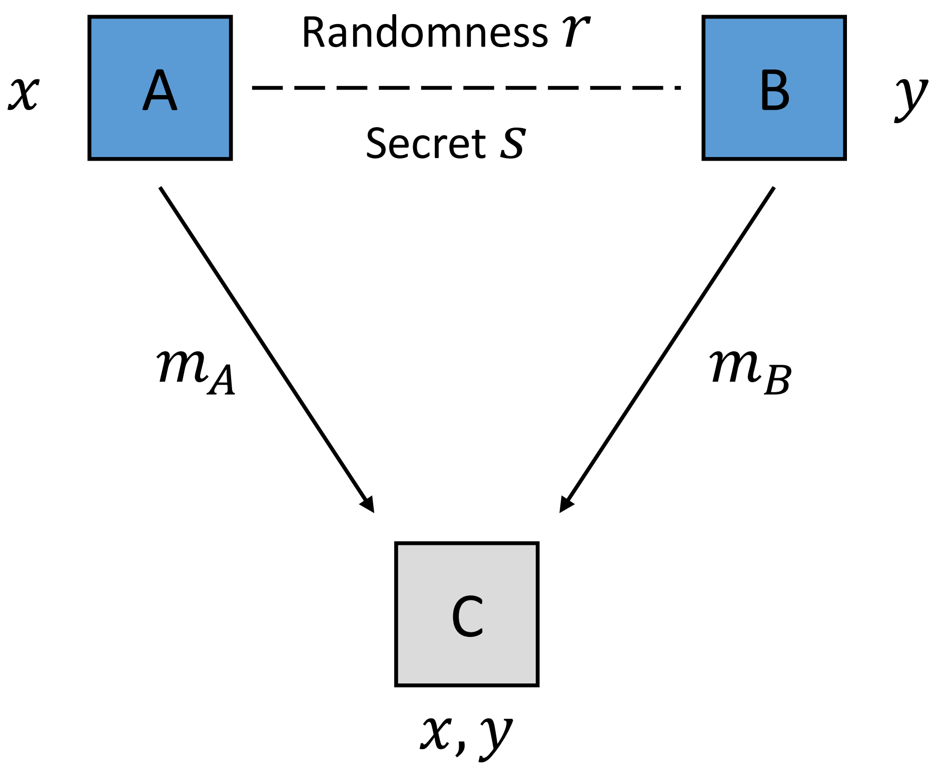
$$\Delta(\ Sim(x,y)\ ;\ (m_A, m_B)\ ) \leq \epsilon$$

Communication: $|m_A| + |m_B|$

Randomness: $|r|$

Conditional Disclosure of Secrets [GIKM00]

$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$



Goal: Charlie learns secret if and only if f(x,y)=1

δ-Correctness:

If $f(x,y) = 1$, then for any s,

$$\Pr[C(x, y, m_A, m_B) = s] \geq 1$$

ϵ-Privacy:

If $f(x,y) = 0$, then for any s, x, y

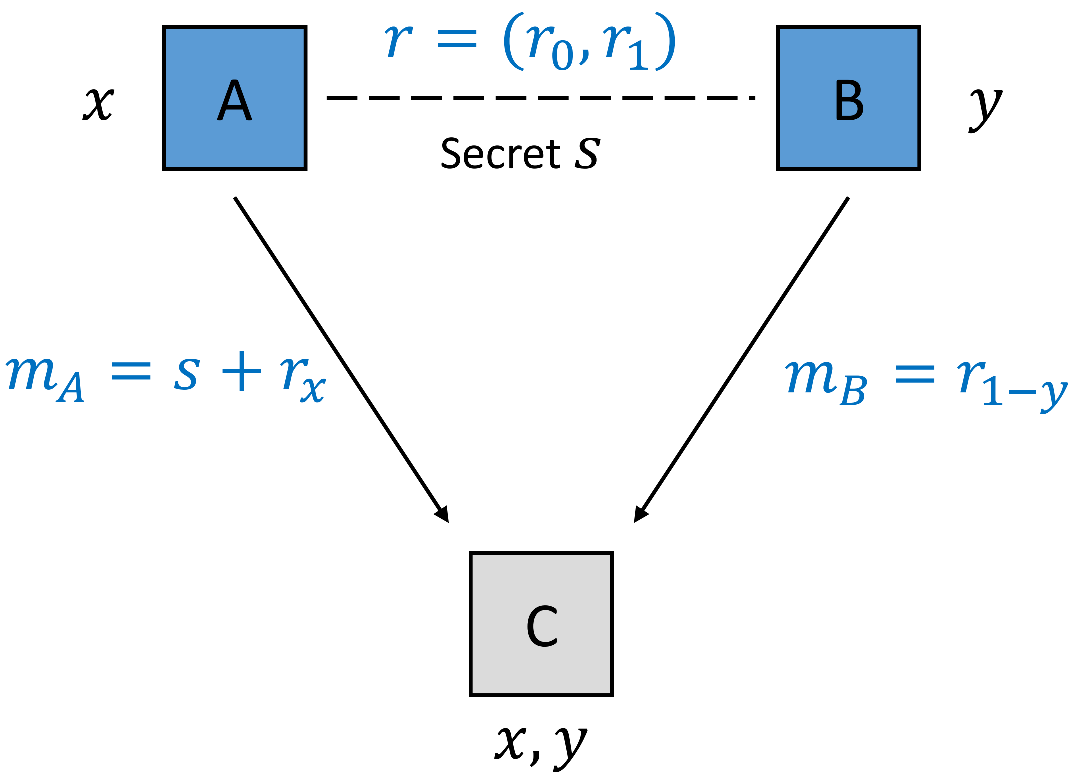
$$\Delta(\, Sim(x,y)\, ;\, (m_A, m_B)\,) \leq 0$$

Communication: $|m_A| + |m_B|$

Randomness: $|r|$

Example: XOR

$$f: \{0,1\}^1 \times \{0,1\}^1 \rightarrow \{0,1\}$$



Goal: Charlie learns secret if and only if f(x,y)=1

Perfect Correctness:

If $f(x,y) = 1$, then for any s,

$$\Pr[m_A + m_B = s] = 1$$

Perfect Privacy:

If $f(x,y) = 0$, then for any s,

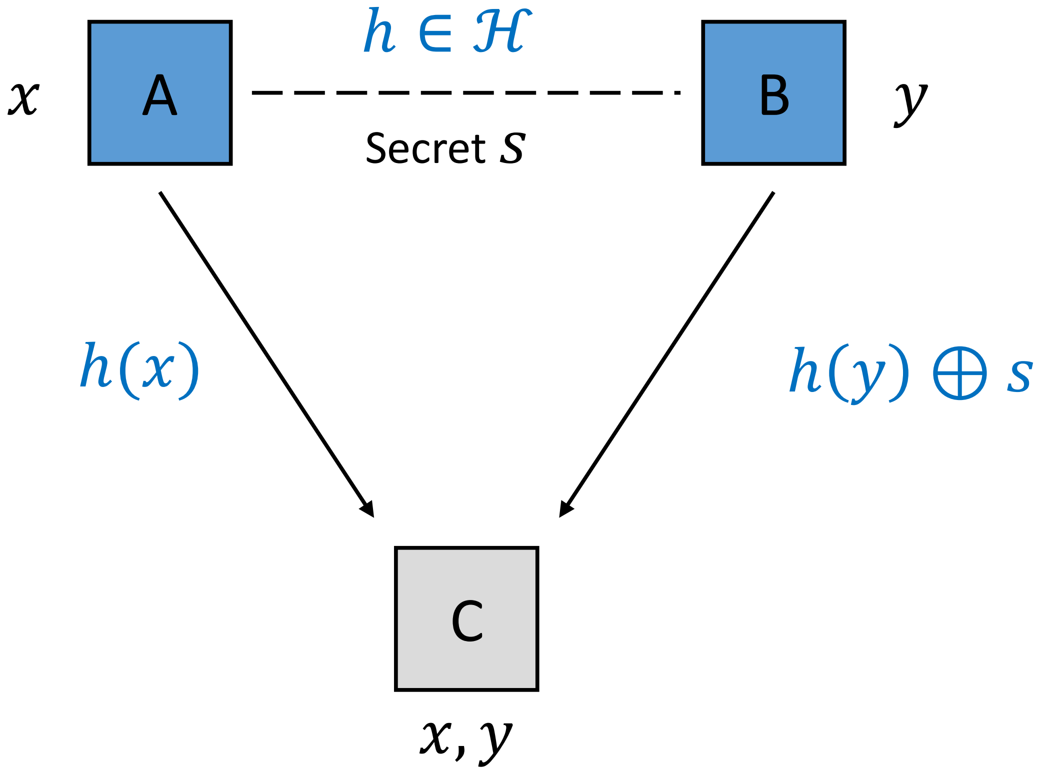
$$(m_A, m_B) \equiv U_2$$

Communication & randomness: 2

Note: This CDS is Linear

Example: Equality

$$f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$



Q: Non-equality?

h is a hash function from a 2-wise independent family $\mathcal{H}$

<u>Perfect Correctness:</u>

If $x = y$, then for any s,

$$s = h(x) \oplus h(y) \oplus s$$

<u>Perfect Privacy:</u>

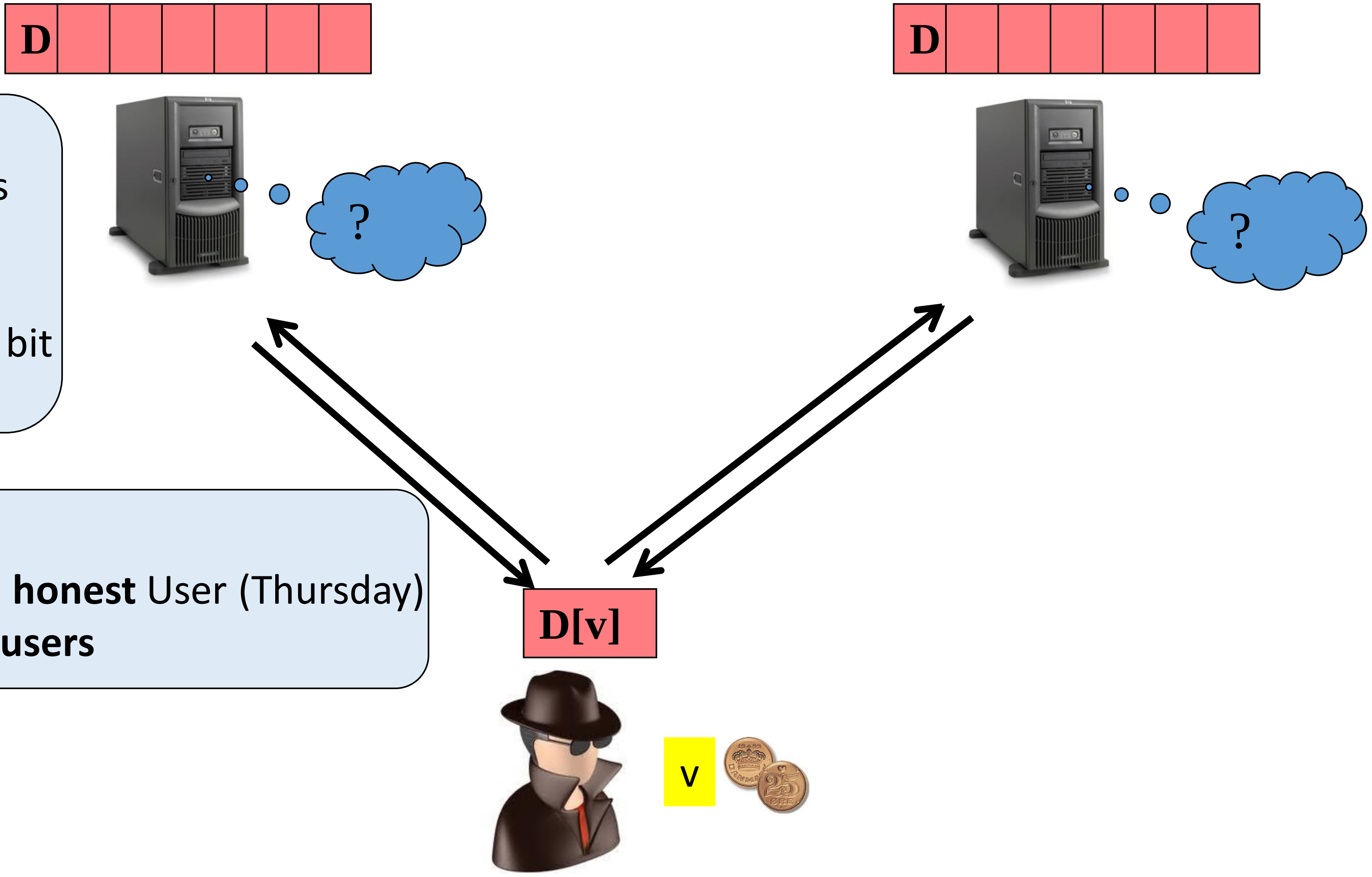
If $x \neq y$, $h(x)$ is a random element independent of $h(y)$

Application: PIR with Data Privacy (SPIR)

[GIKM00]

User's privacy:
v is hidden from servers

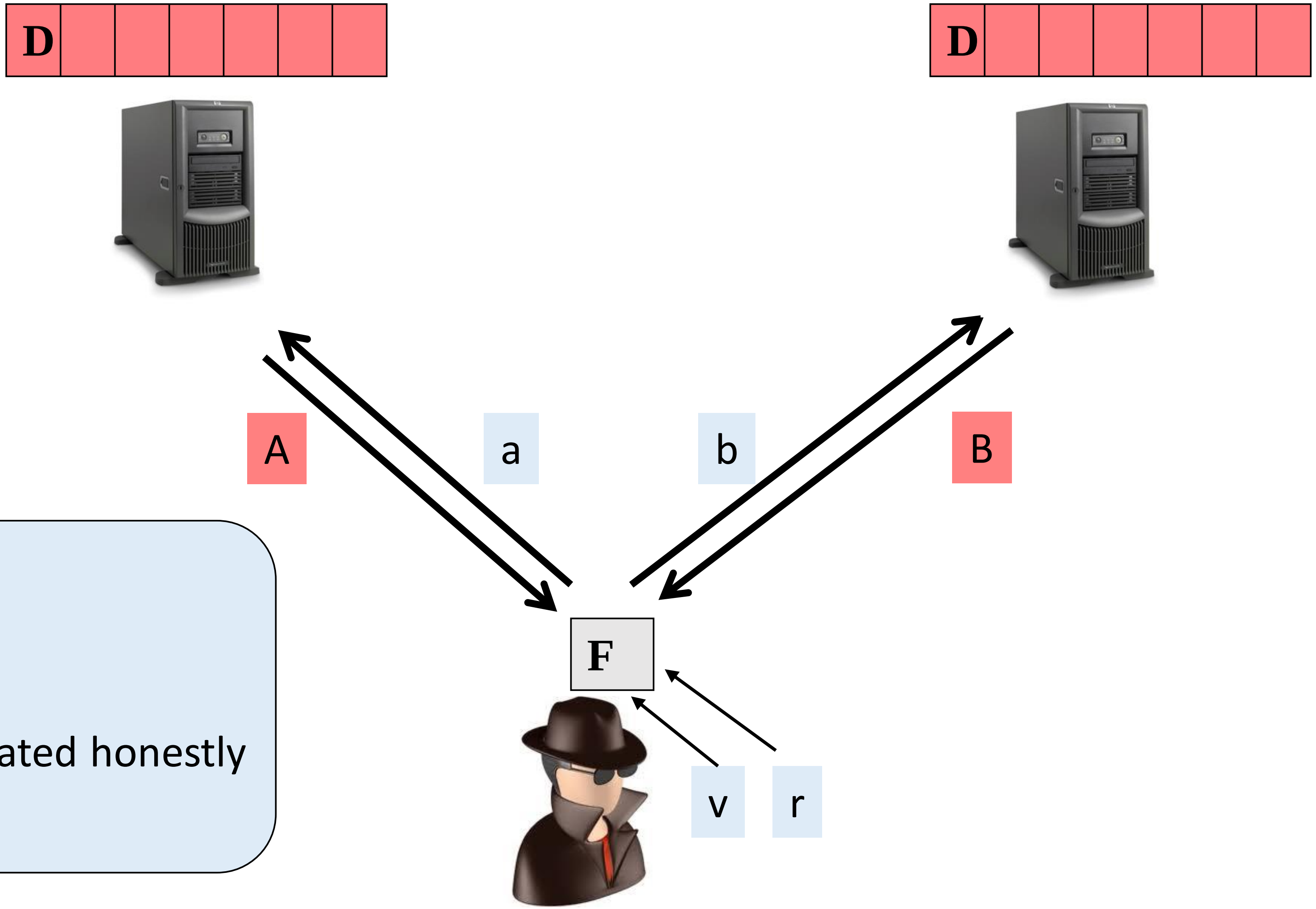
Data privacy:
Users learns **only** single bit



General PIR ⇒ SPIR:

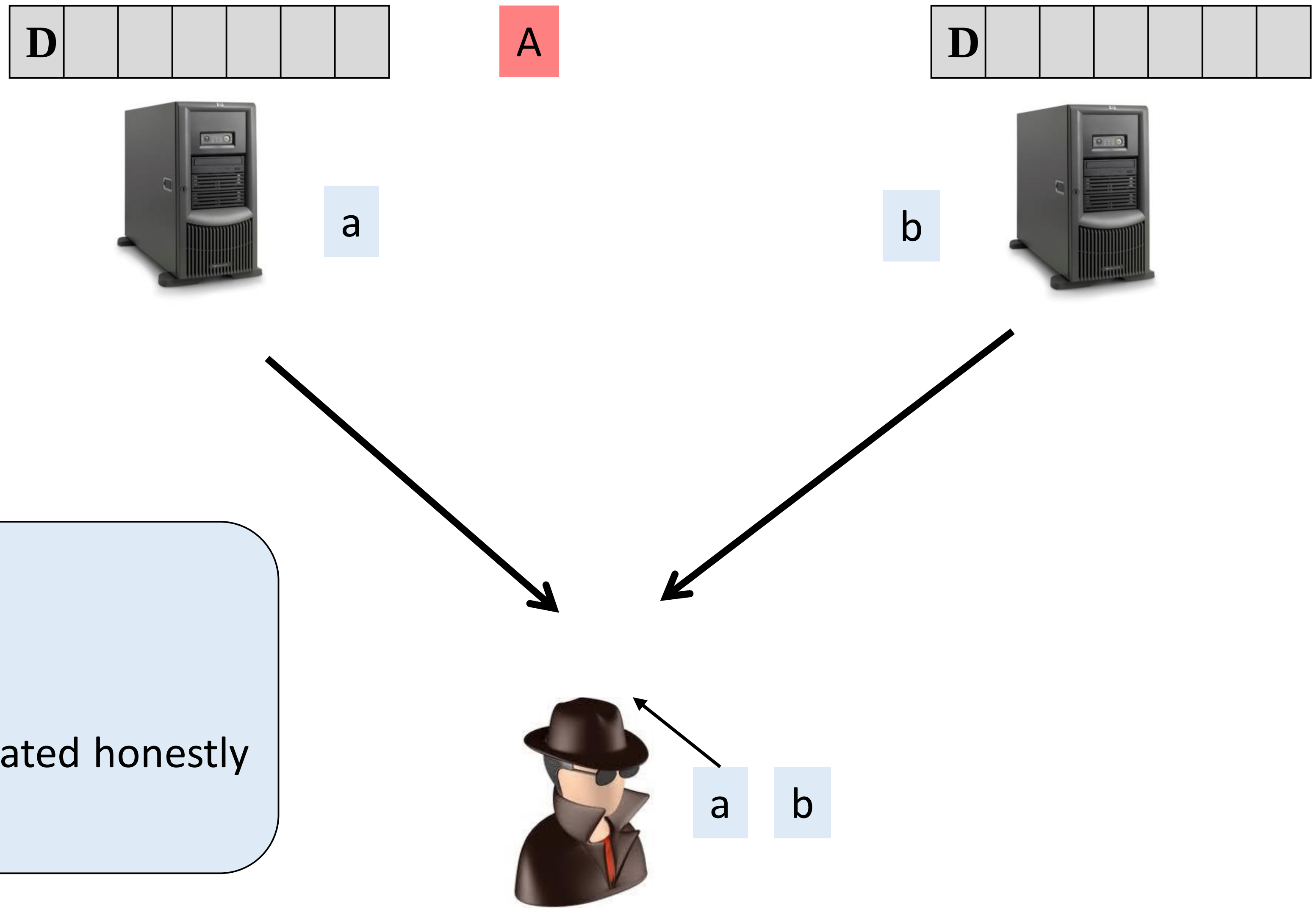
1. Data privacy against **honest** User (Thursday)
2. **Handling malicious users**

Honest-User SPIR $\Rightarrow$ SPIR



IDEA:
Release answers iff
the queries were generated honestly

Honest-User SPIR ⇒ SPIR

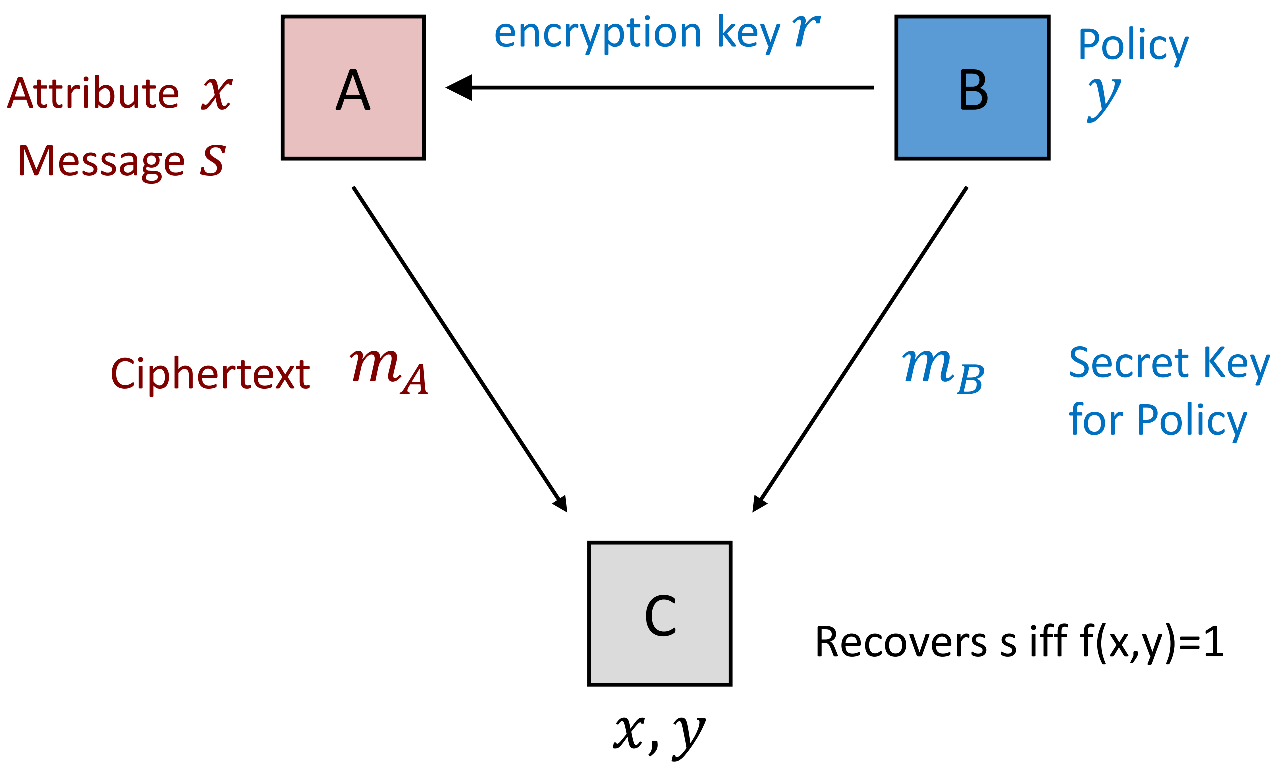


Release A iff
GOOD(a,b)=1

IDEA:
Release answers iff
the queries were generated honestly

CDS as 1-time Symmetric Attribute Based Encryption

$$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$



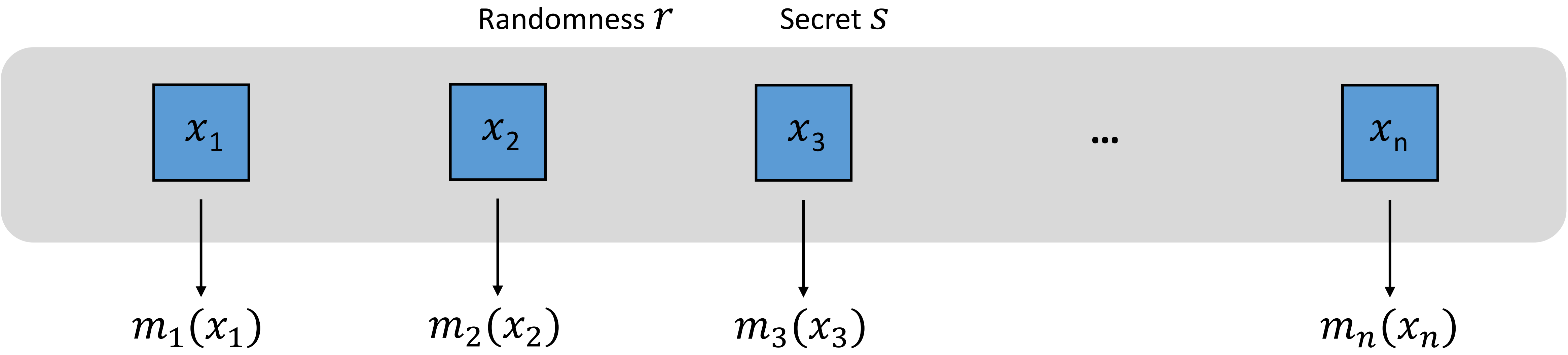
ABE:

- For each policy y, generate secret-key sk(y)
- Encrypt message S under attribute x
- Decryption works iff f(x,y)=1.

Thm: linear-CDS + bilinear groups ⇒ public-key (multi-use) ABE . [Att14,Wee14]

Multiparty (Fully-Decomposable) CDS

$f: \{0,1\}^n \rightarrow \{0,1\}$ n senders each holding a single bit



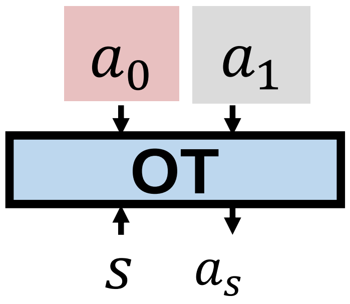
Given $x, m(x) = (m_1(x_1), \ldots, m_n(x_n))$ can recover s iff $f(x) = 1$

Fully Decomposable CDS $\Rightarrow$ Zero-Knowledge over OT

[JawKerOrl13, FredNieOrl15]

$f: \{0,1\}^n \to \{0,1\}$

Verifier



Prover: I know x such that $f(x) = 1$

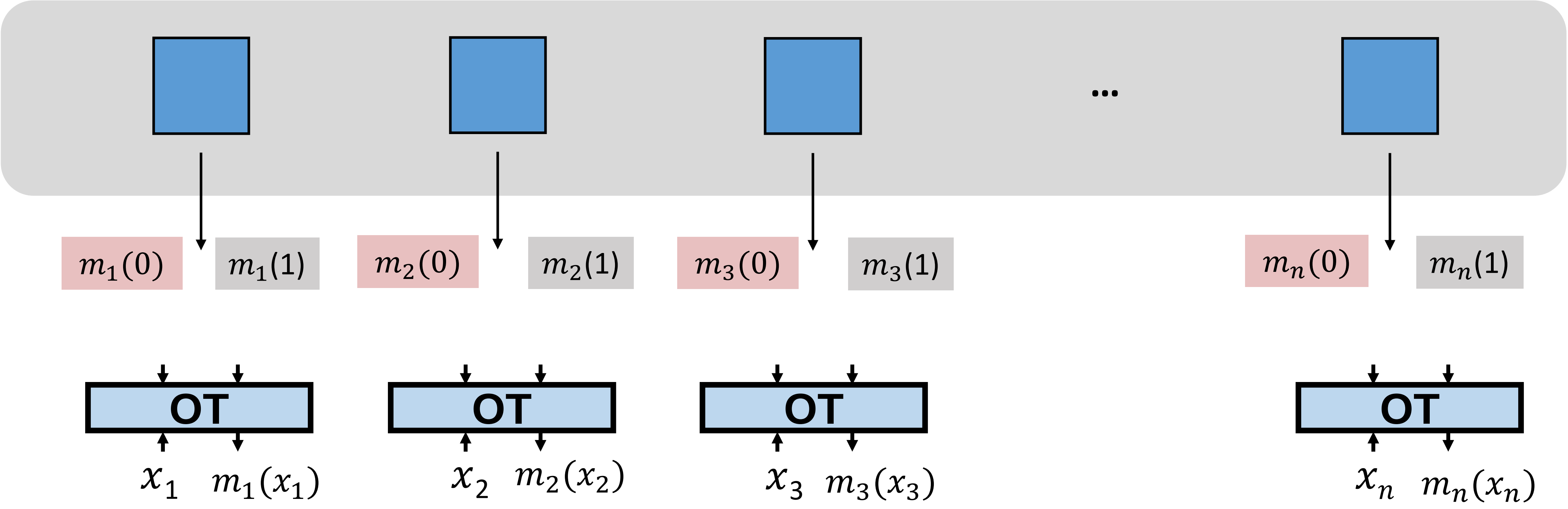
Fully Decomposable CDS ⇒ Zero-Knowledge over OT

[JawKerOrl13, FredNieOrl15]

$f: \{0,1\}^n \rightarrow \{0,1\}$

Verifier

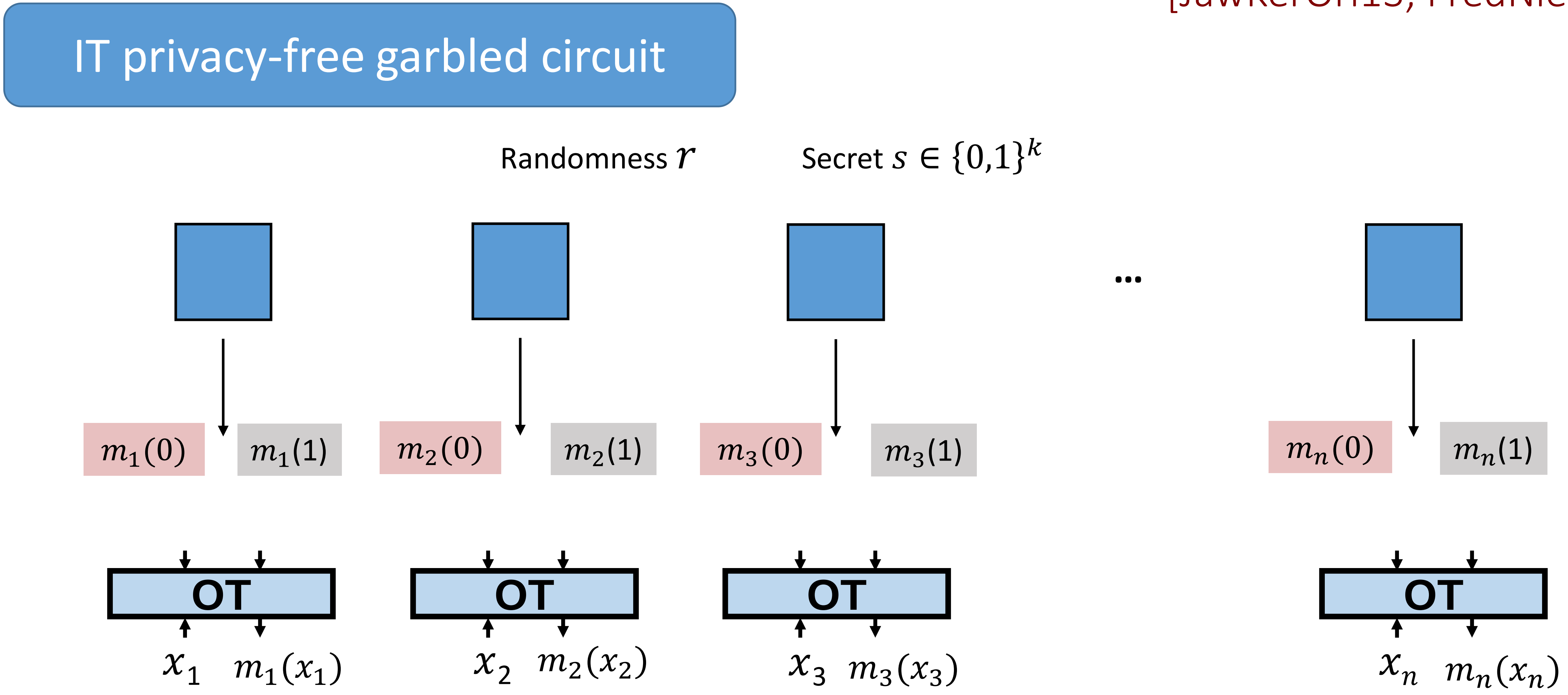
Randomness r **Secret** $\boldsymbol{s} \in \{0,1\}^k$



Prover: I know x such that $f(x) = 1$ **Sends** $\boldsymbol{s}$ as a certificate

Fully Decomposable CDS ⇒ Zero-Knowledge over OT

[JawKerOrl13, FredNieOrl15]



Remark: ZK against **honest** verifier (can be upgraded to malicious verifier via commitment)

The Crypto Tower

Obfustopia

Secure Computation

Public-Key

Symmetric

Information Theoretic

Witness Encryption
[GGSW 2013]

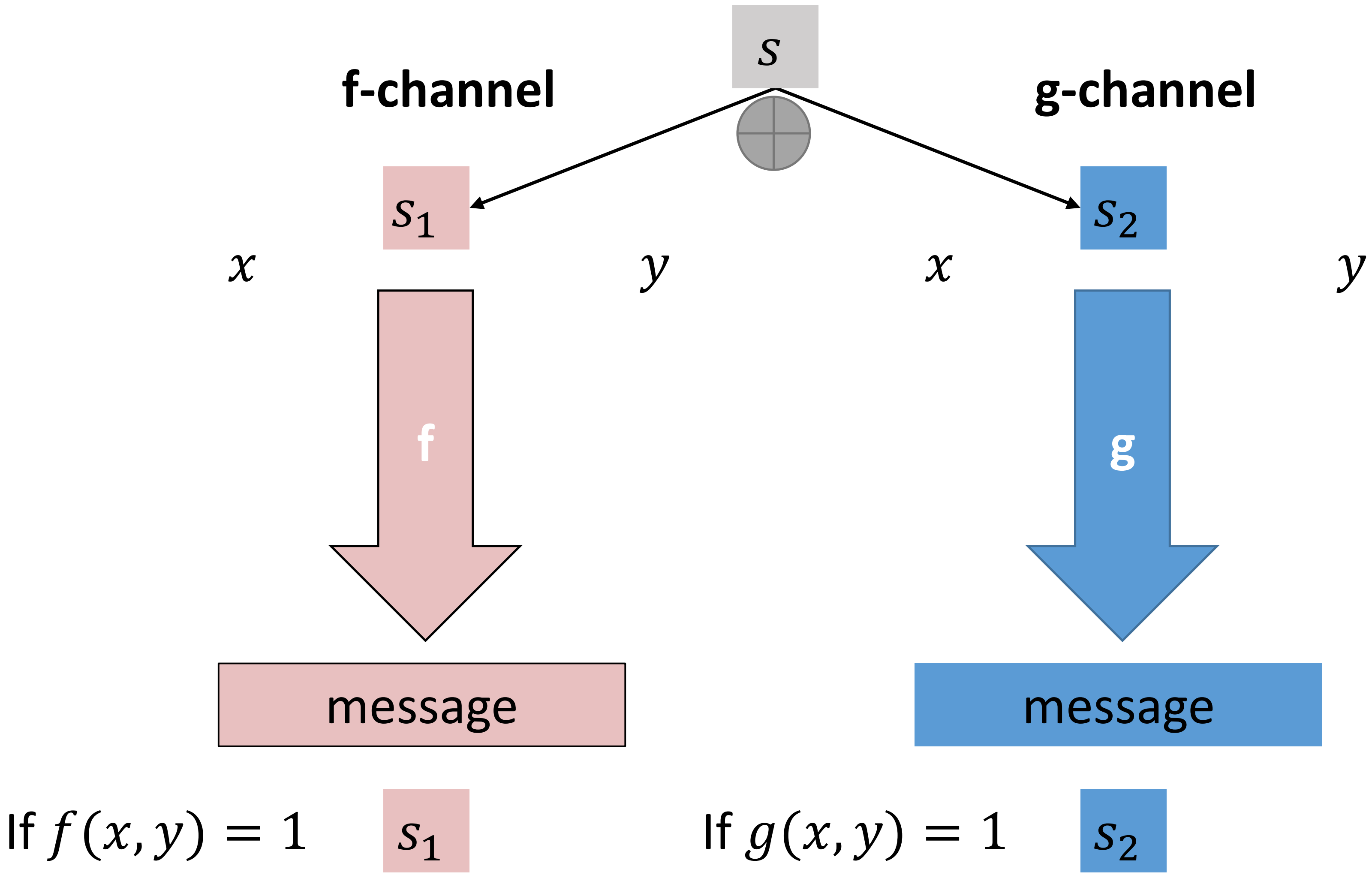
Attribute-Based Encryption
[SW04,GPSW06]

Privacy-free Garbled Circuit
[BHR12]

CDS
[GIKM00]

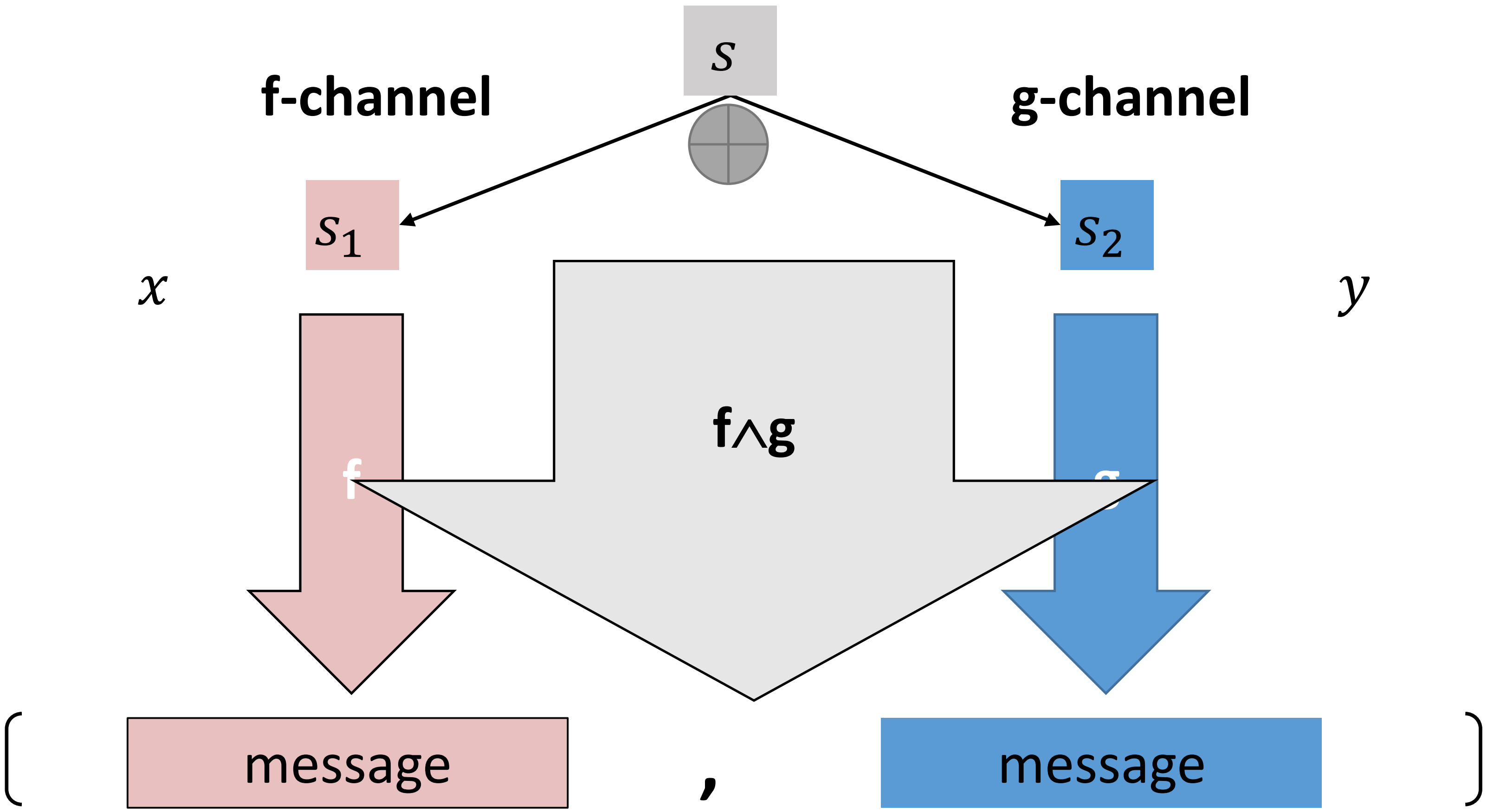
Simple Closure Properties

Closure under AND



Closure under AND

$$\mathrm{CDS}(f \wedge g) \leq \mathrm{CDS}(f) + \mathrm{CDS}(g)$$

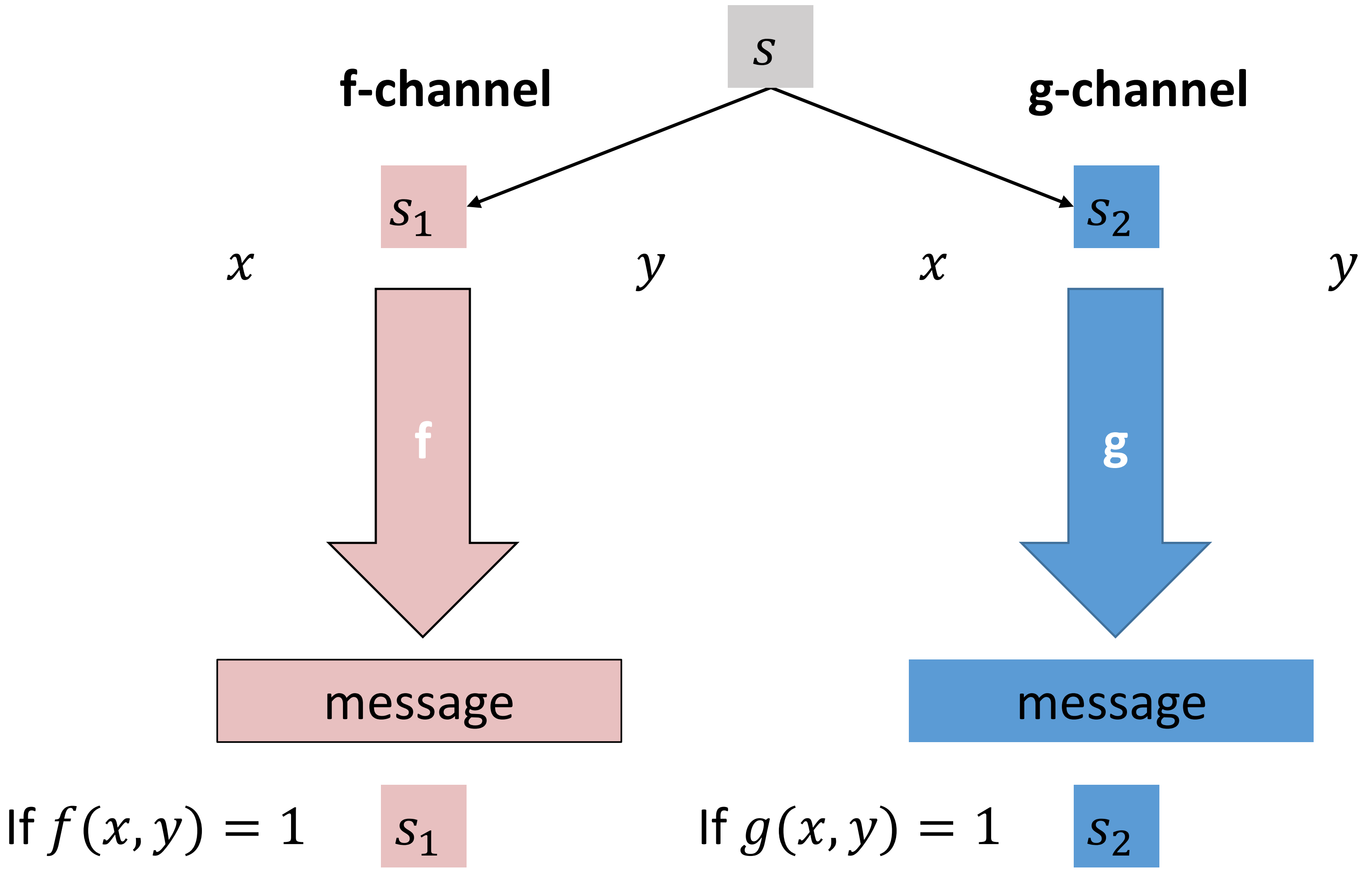


If $f(x,y) = 1$ s_1

If $g(x,y) = 1$ s_2

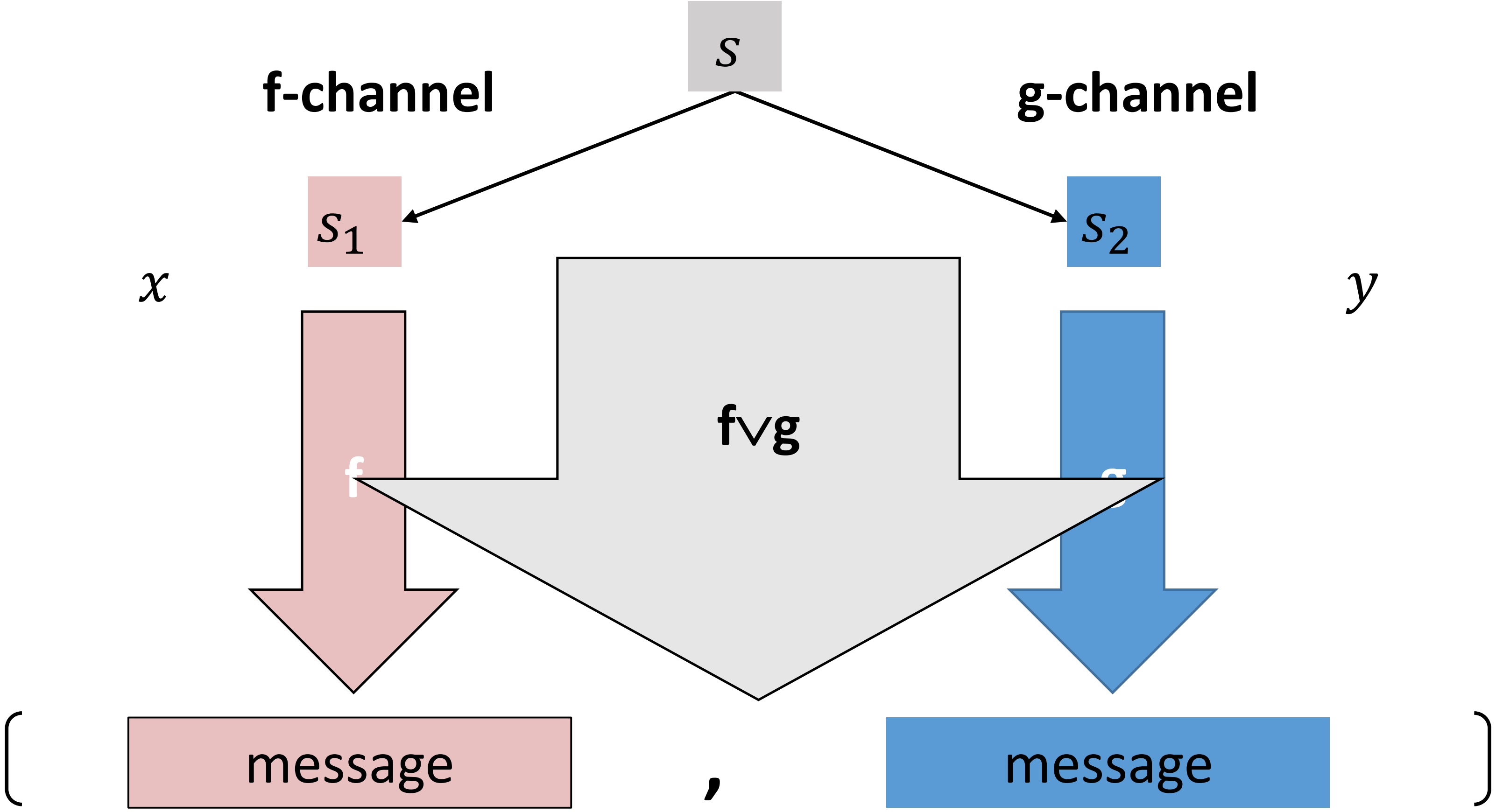
If $(f \wedge g)(x,y)$=1 s

Closure under OR



Closure under OR

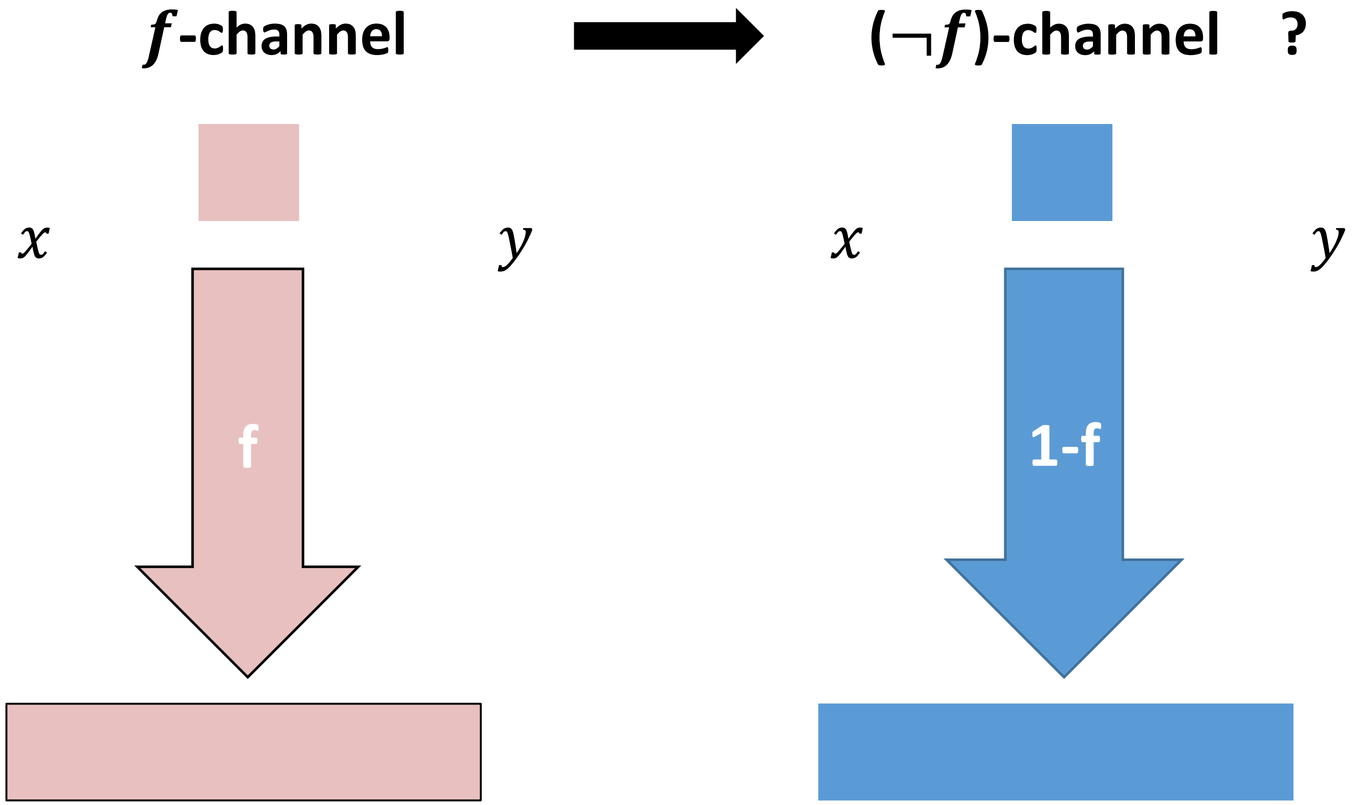
$\mathrm{CDS}(f \vee g) \leq \mathrm{CDS}(f) + \mathrm{CDS}(g)$



If $f(x,y) = 1$ s_1 If $g(x,y) = 1$ s_2

If $(f \vee g)(x,y)$=1 s

Test your intuition: Closure under negation?



YES but with error [A-ArkRayVas17]

Ex: Prove for linear-CDS

Formulas

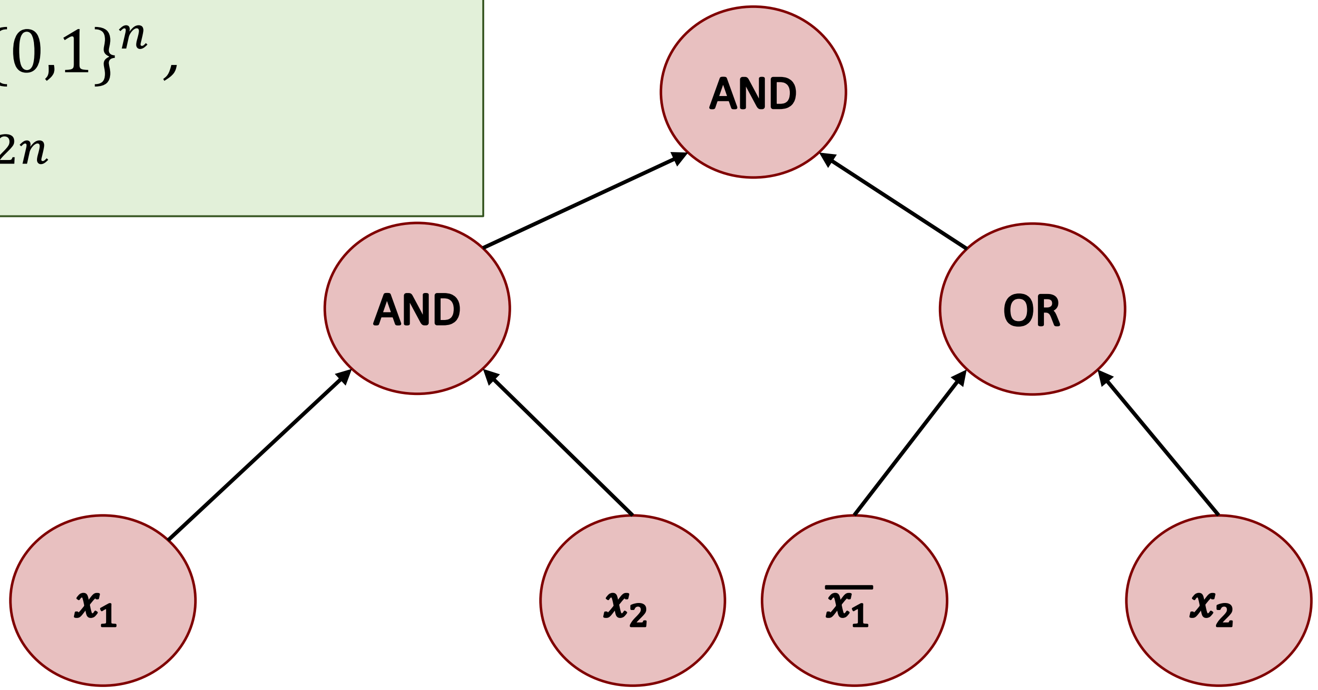
Thm. [GIKRM00] $\mathrm{Lin-CDS}(f) \leq \mathrm{O}(\mathrm{For}mula - size(f))$

Extensions to branching programs/span programs. [GIKM00,IW14,AR16]

Cor. For every $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$,

$$\mathrm{Lin-CDS}(f) \leq 2^{2n}$$

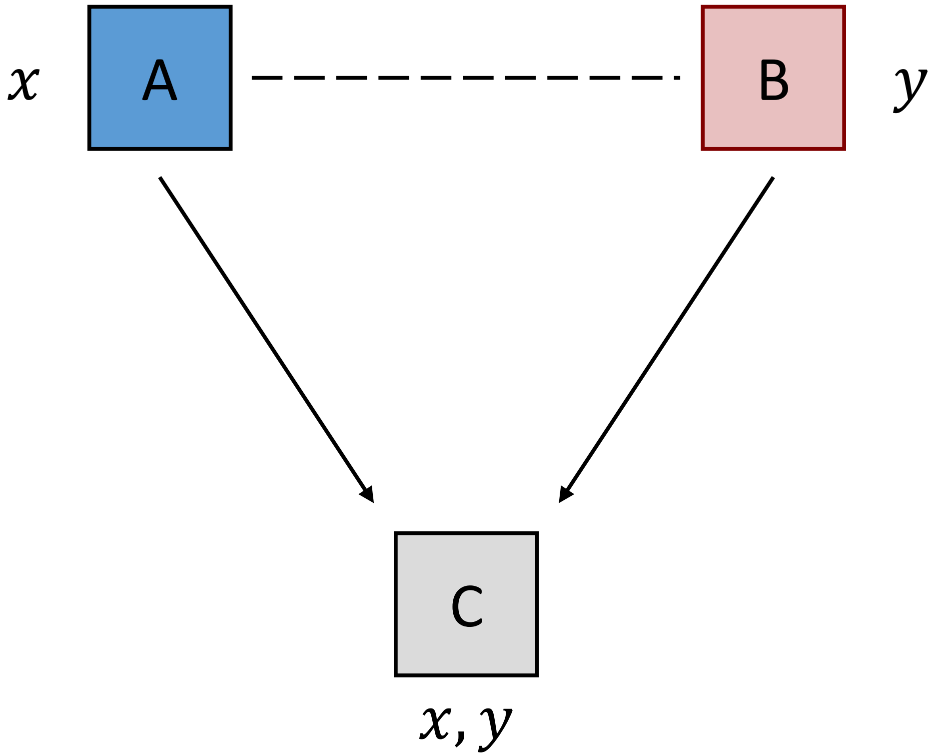
Q: Can we do better?

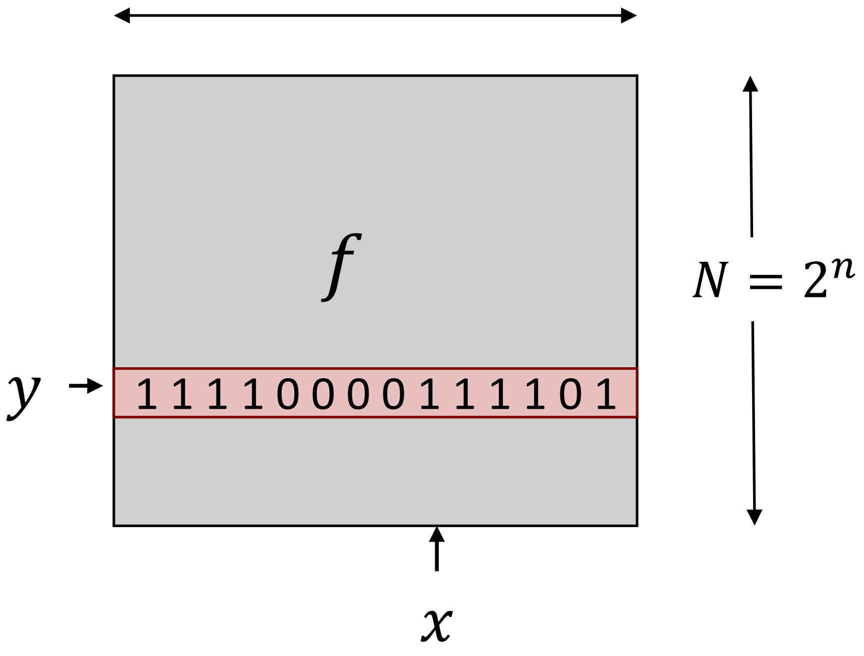


General Functions: Optimal Linear-CDS

CDS for general predicates

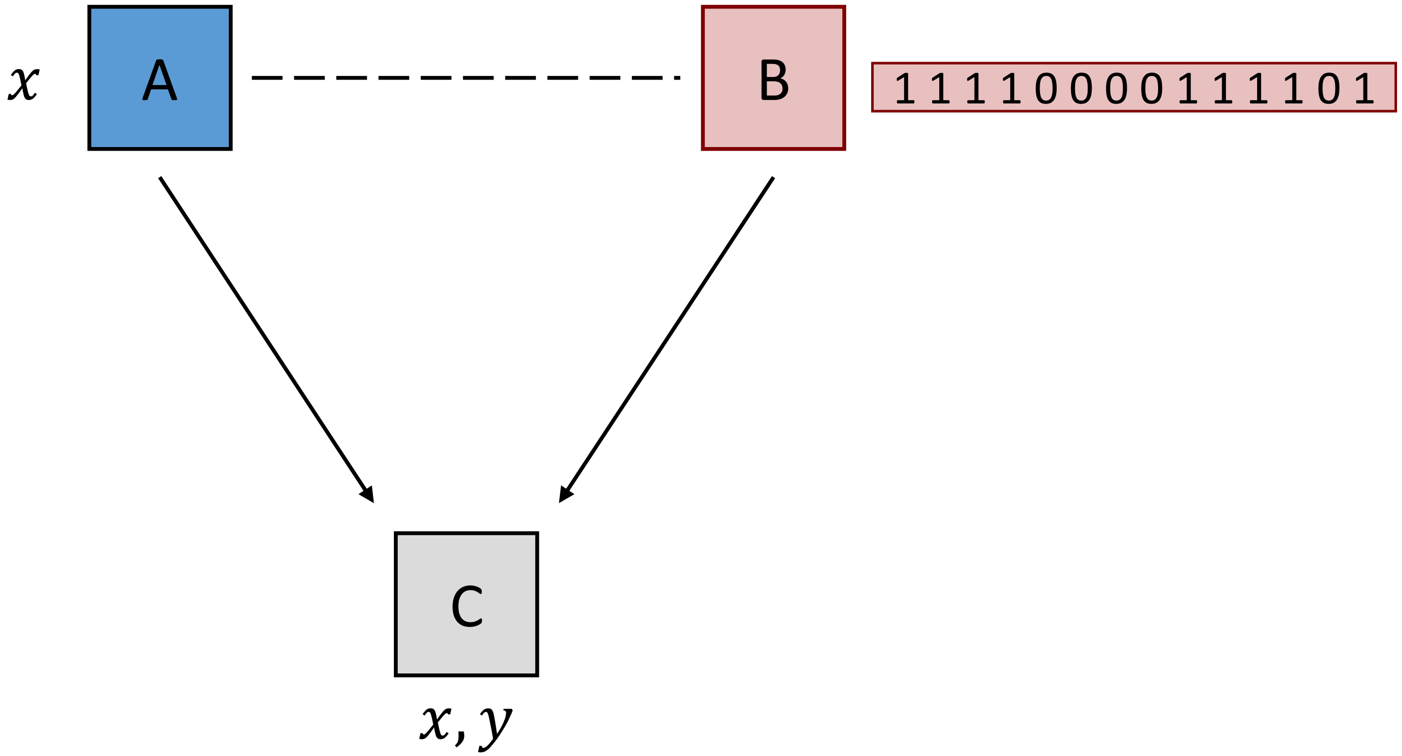
$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

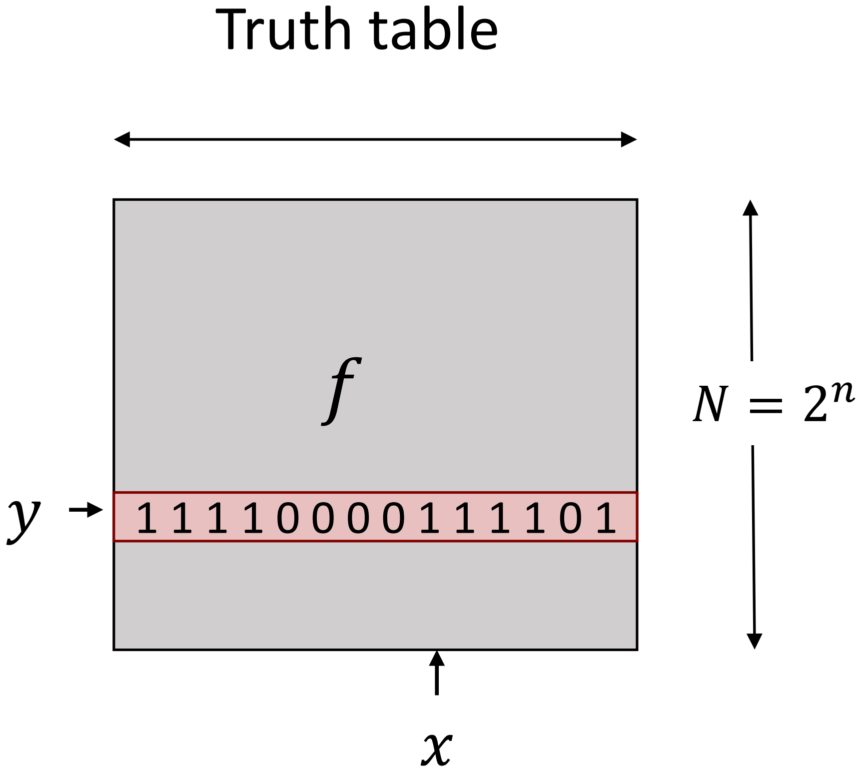




Completeness of the Index function

$Index: [N] \times \{0,1\}^N \to \{0,1\}$

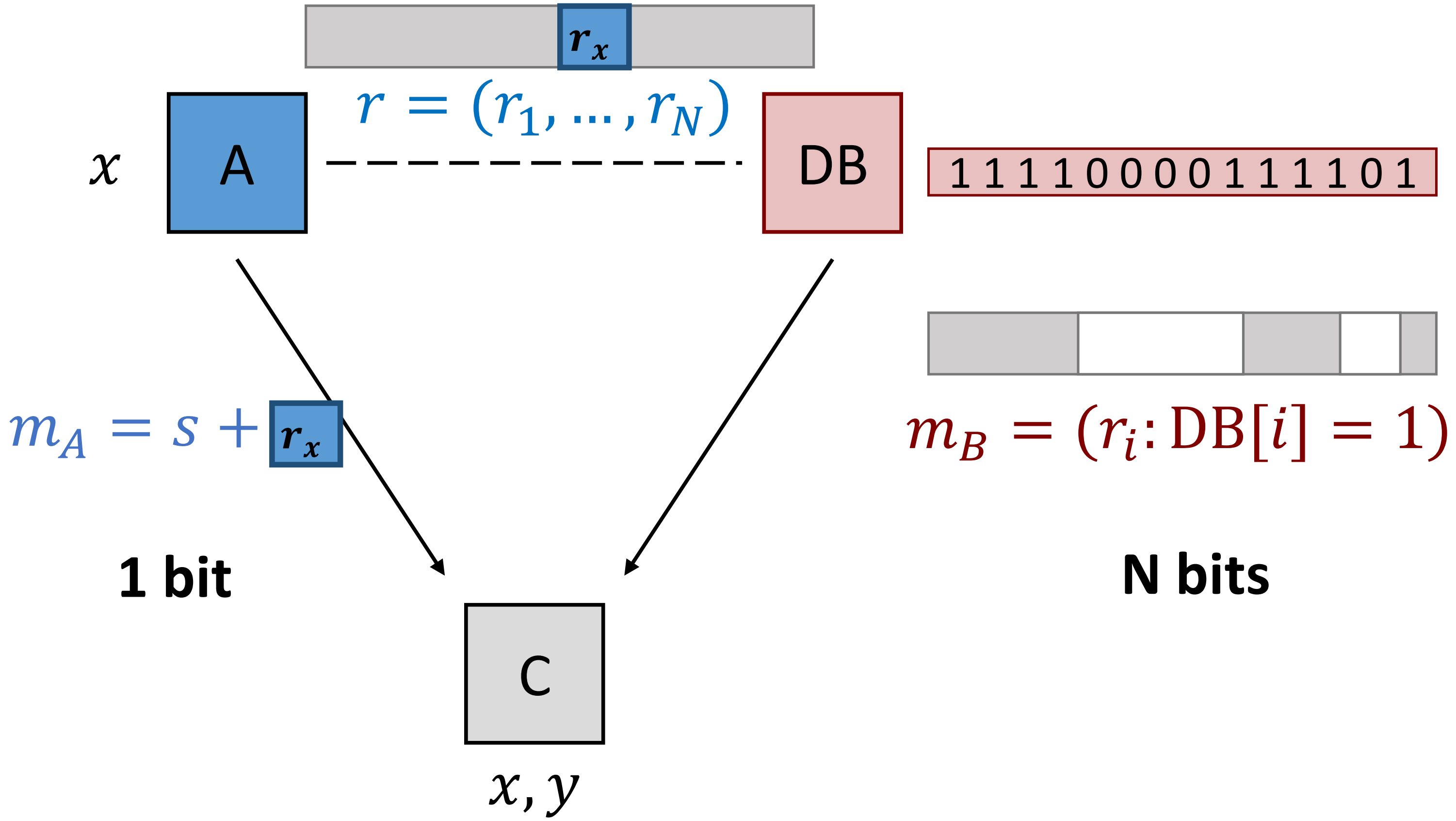




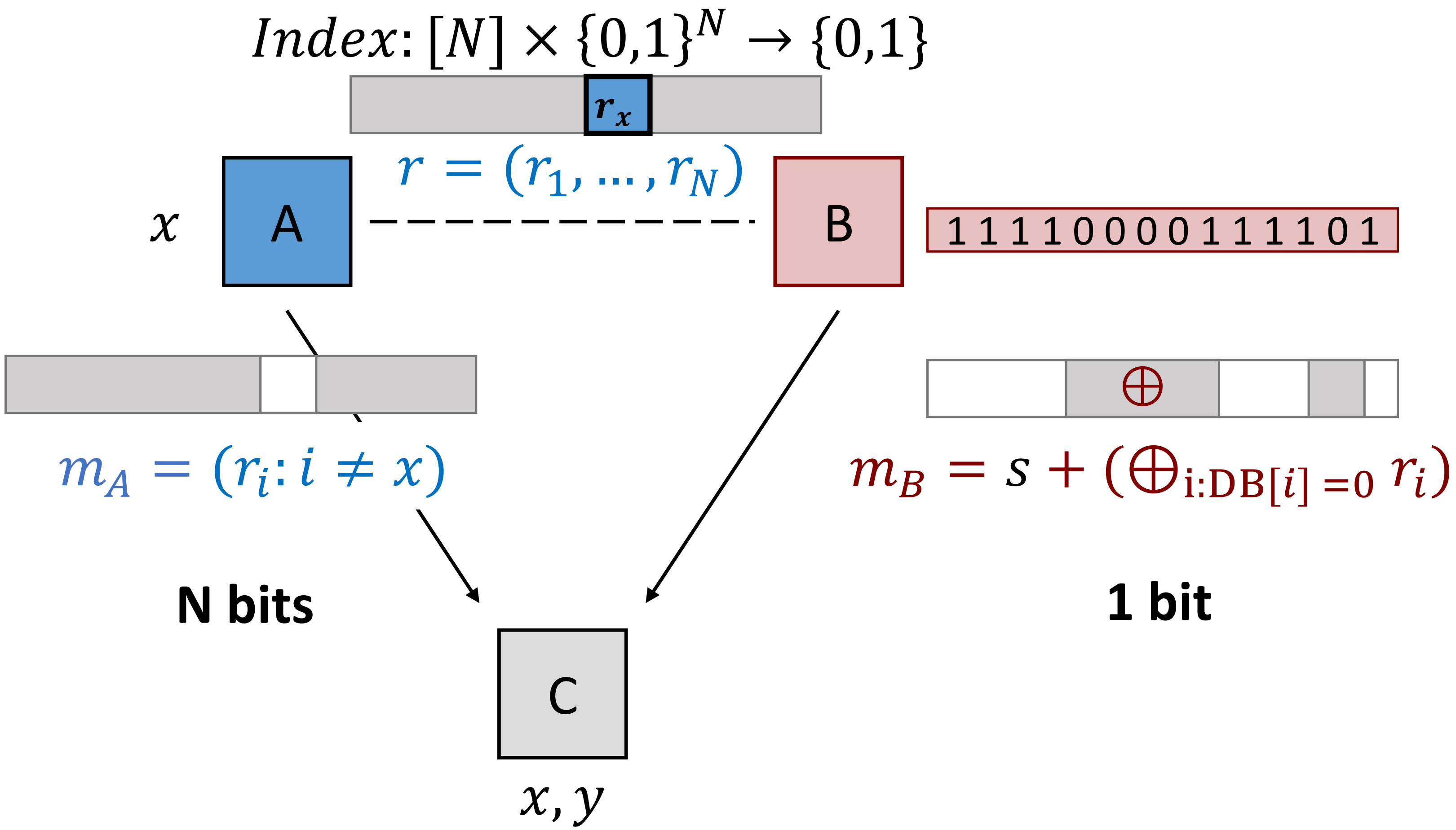
Observation: CDS(f)≤CDS(Index)

Linear CDS for Index

$Index: [N] \times \{0,1\}^N \to \{0,1\}$



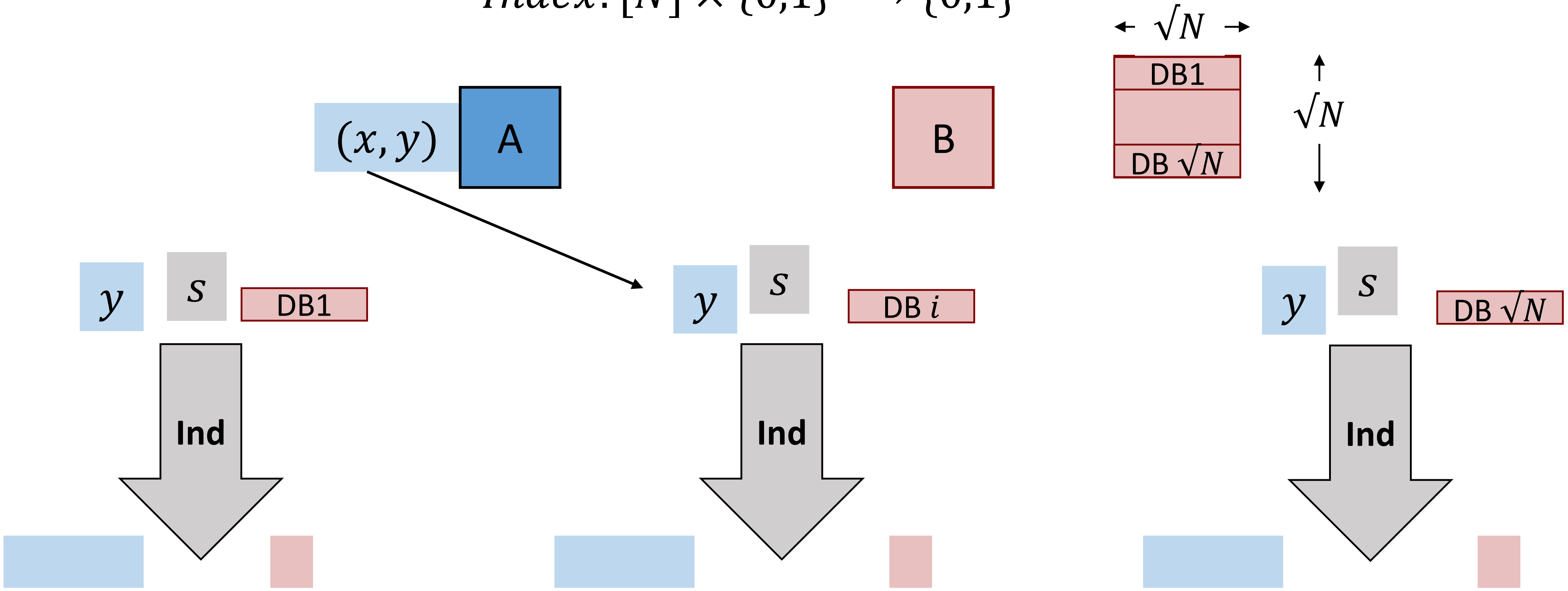
CDS for Index: Dual version?



The missing key participates in encryption iff D[x]=0

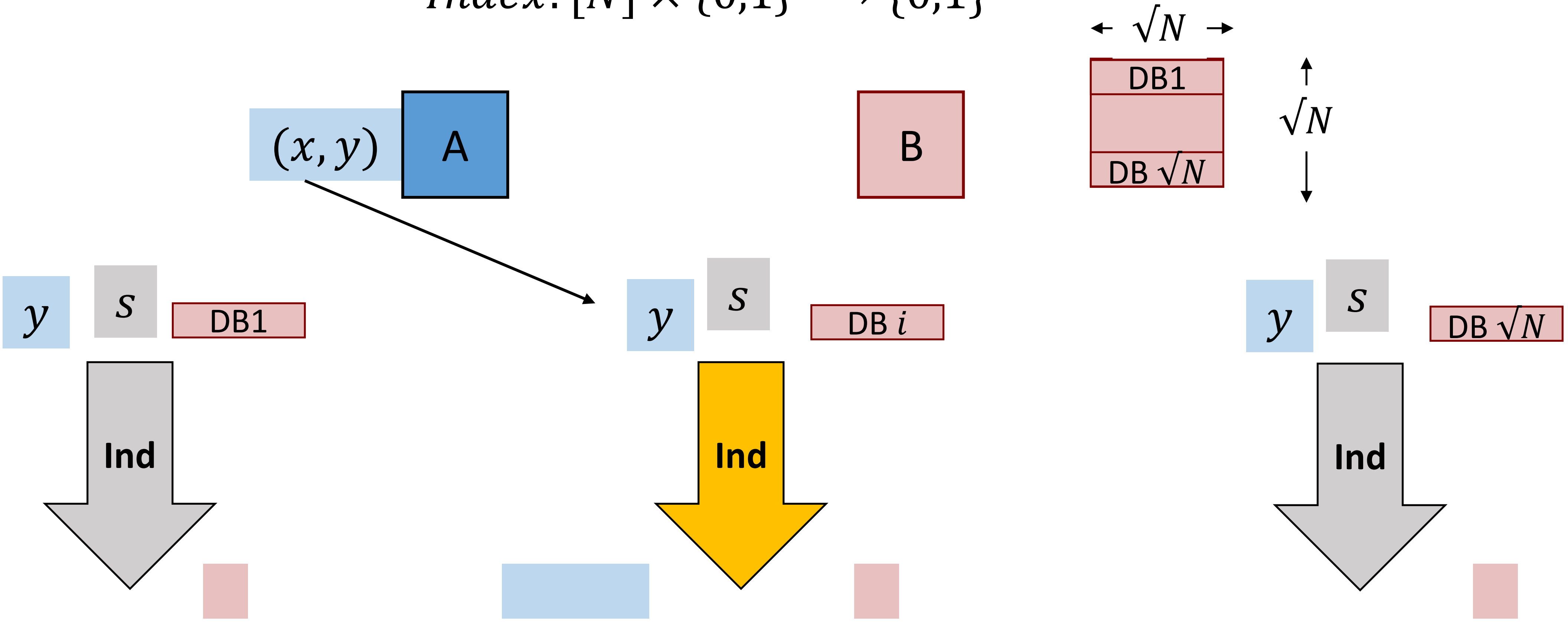
CDS for Index - Balancing

$Index: [N] \times \{0,1\}^N \rightarrow \{0,1\}$



CDS for Index - Balancing

$$Index: [N] \times \{0,1\}^N \to \{0,1\}$$



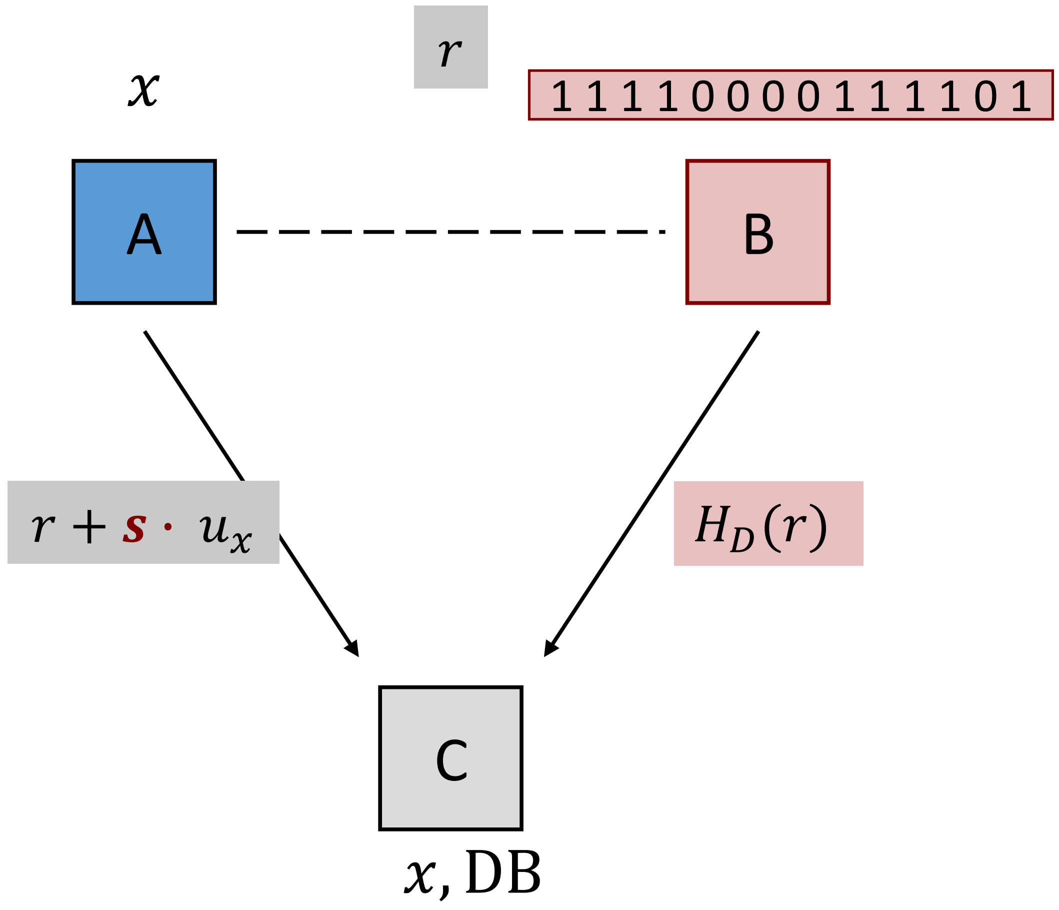
Linear CDS with $\sqrt{N} = 2^{n/2}$ complexity (optimal for linear schemes!)

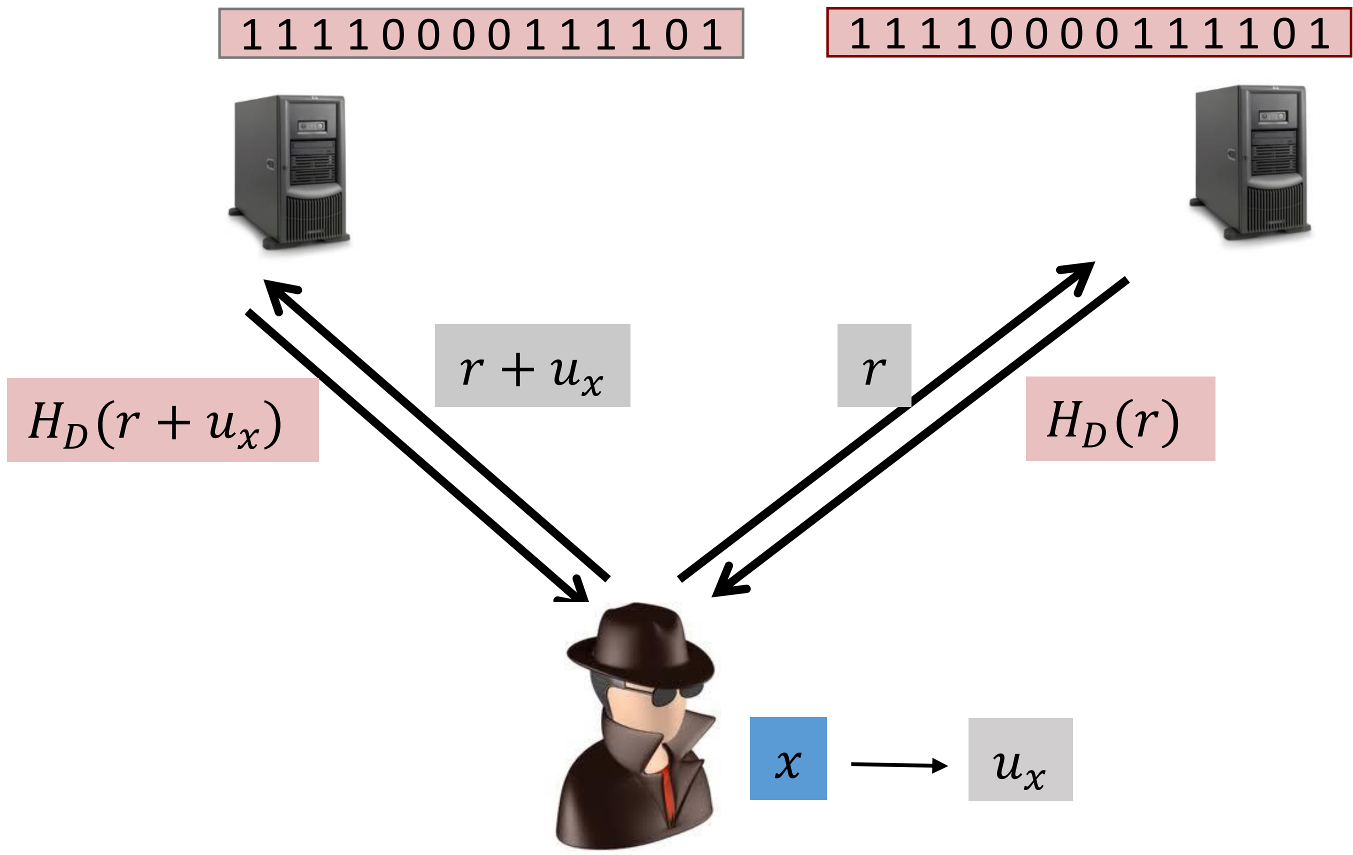
[Bei-Ish-Kum-Kus14, GayKerWee15]

Sub-exponential CDS via Nice-PIR

[Liu-Vai-Wee18]

IDEA: Use Linear-PIR to evaluate $D[x]\cdot s$



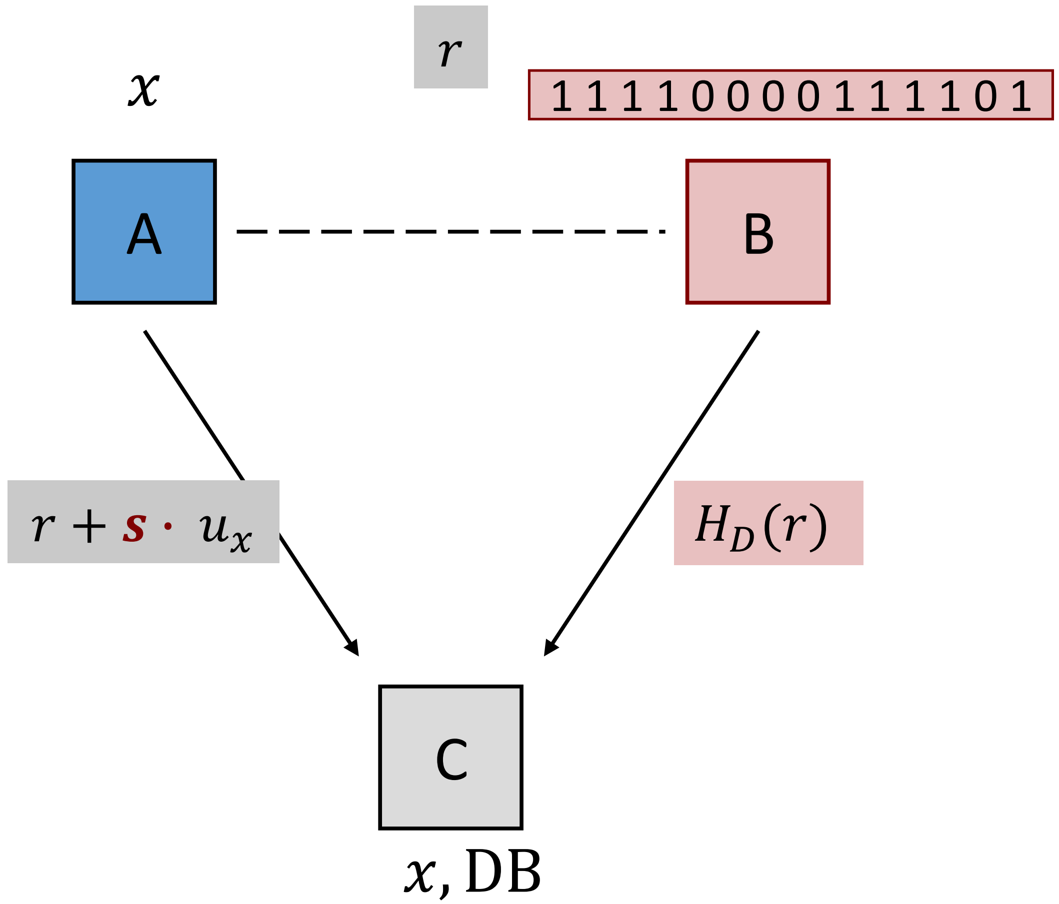


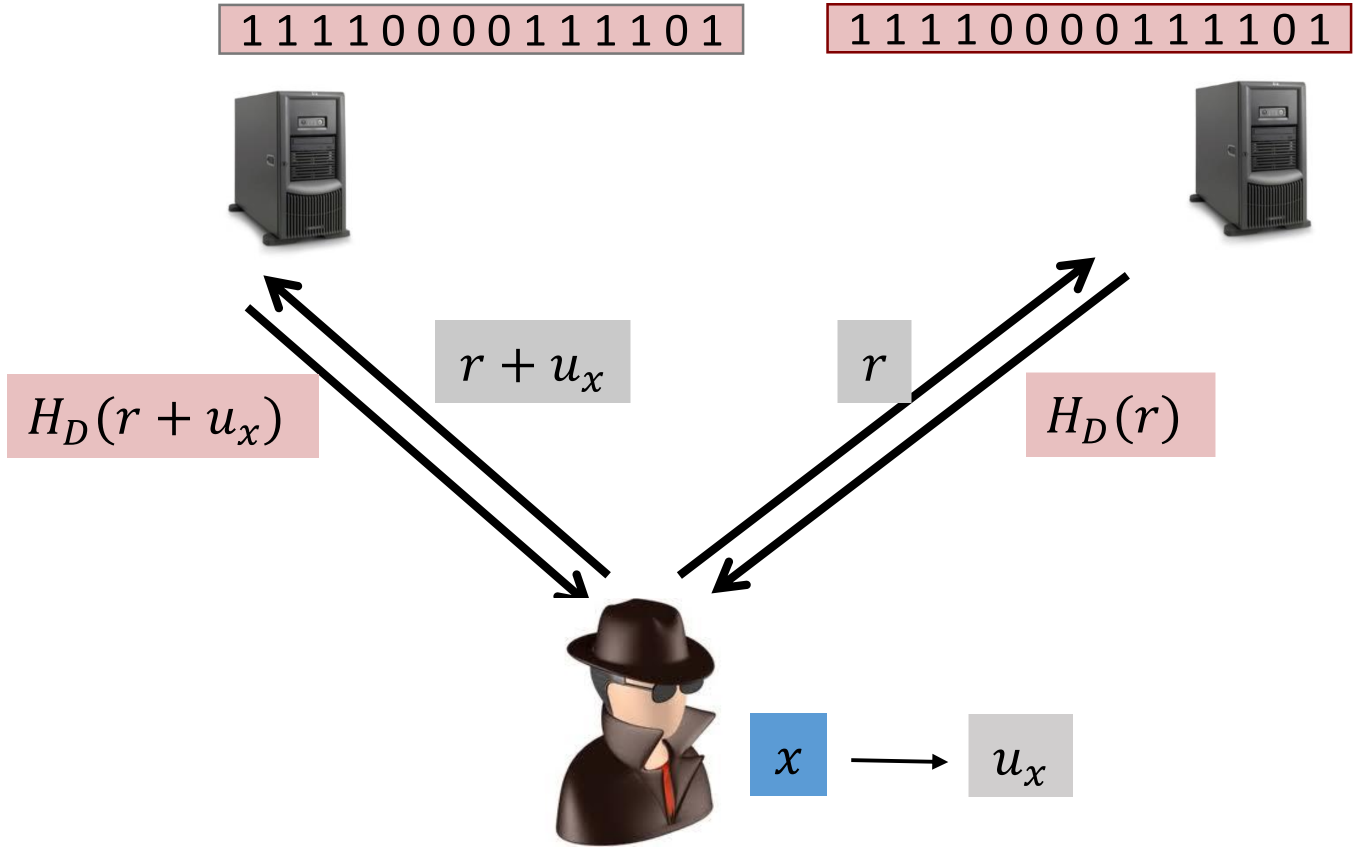
$H_D(r + s \cdot u_x)$ - $H_D(r)$ = $D(x) \cdot s$

$H_D(r + u_x)$ - $H_D(r)$ = $D(x)$

IDEA: Use Linear-PIR to evaluate $D[x] \cdot s$

Correctness: Charlie learns $D[x] \cdot s$



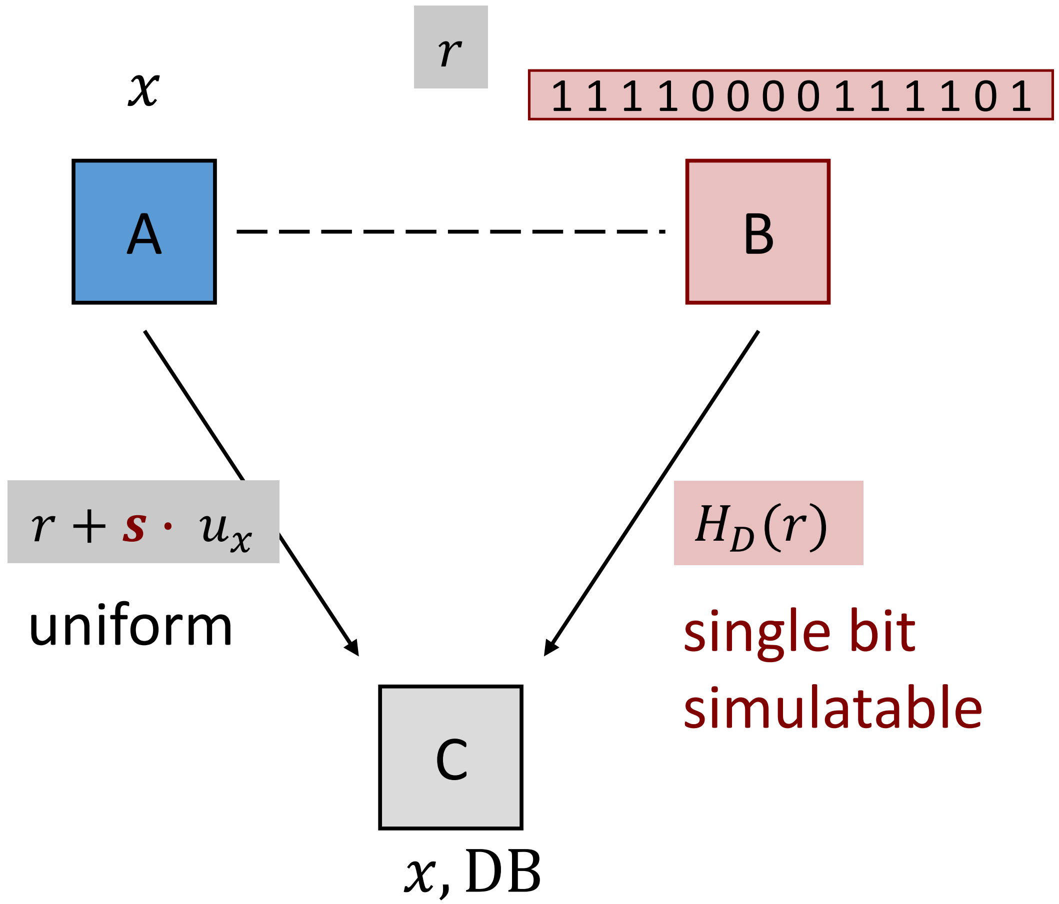


$H_D(r + s \cdot u_x)$ - $H_D(r)$ = $D(x) \cdot s$

$H_D(r + u_x)$ - $H_D(r)$ = $D(x)$

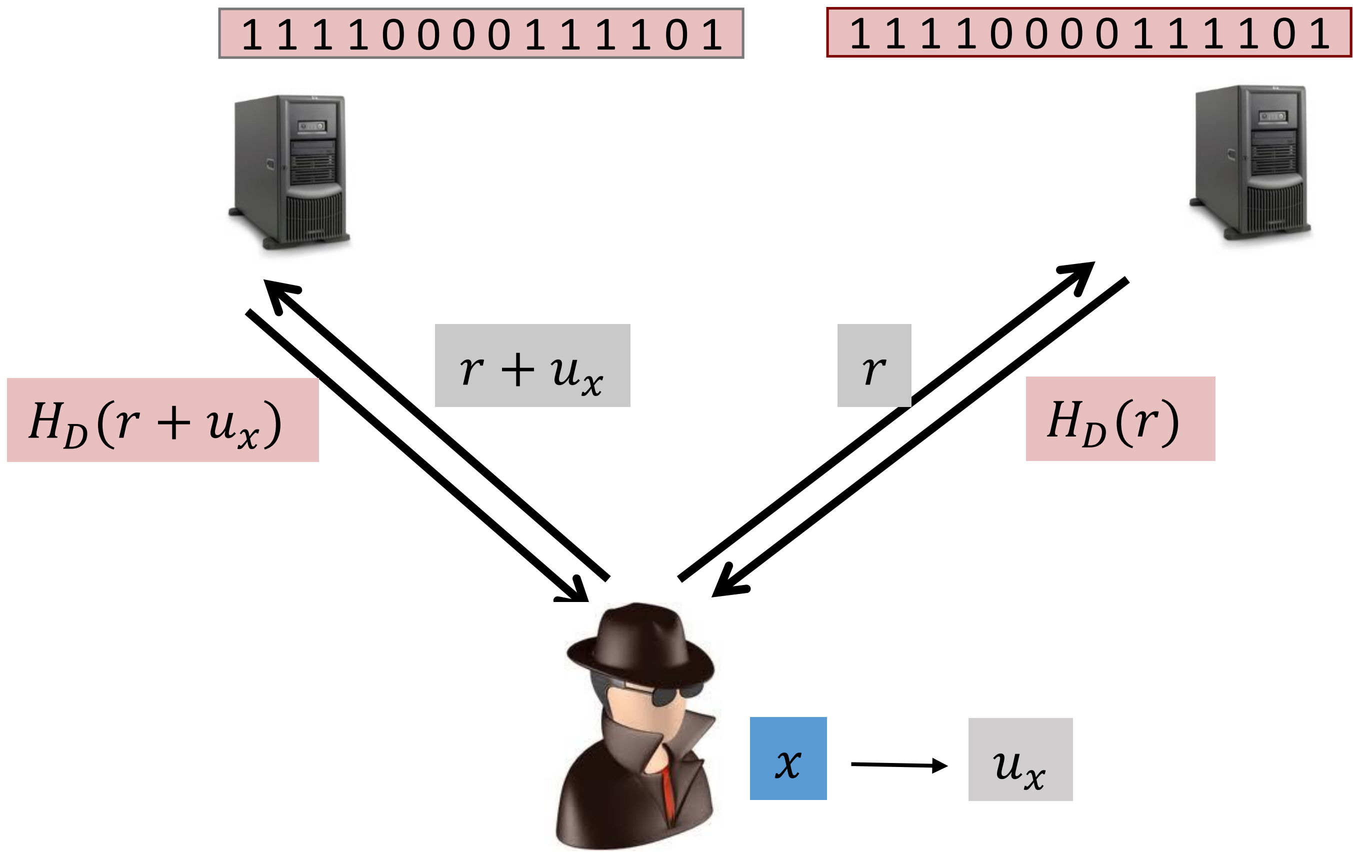
IDEA: Use Linear-PIR to evaluate $D[x]\cdot s$

Privacy: Charlie learns **only** $D[x] \cdot s$



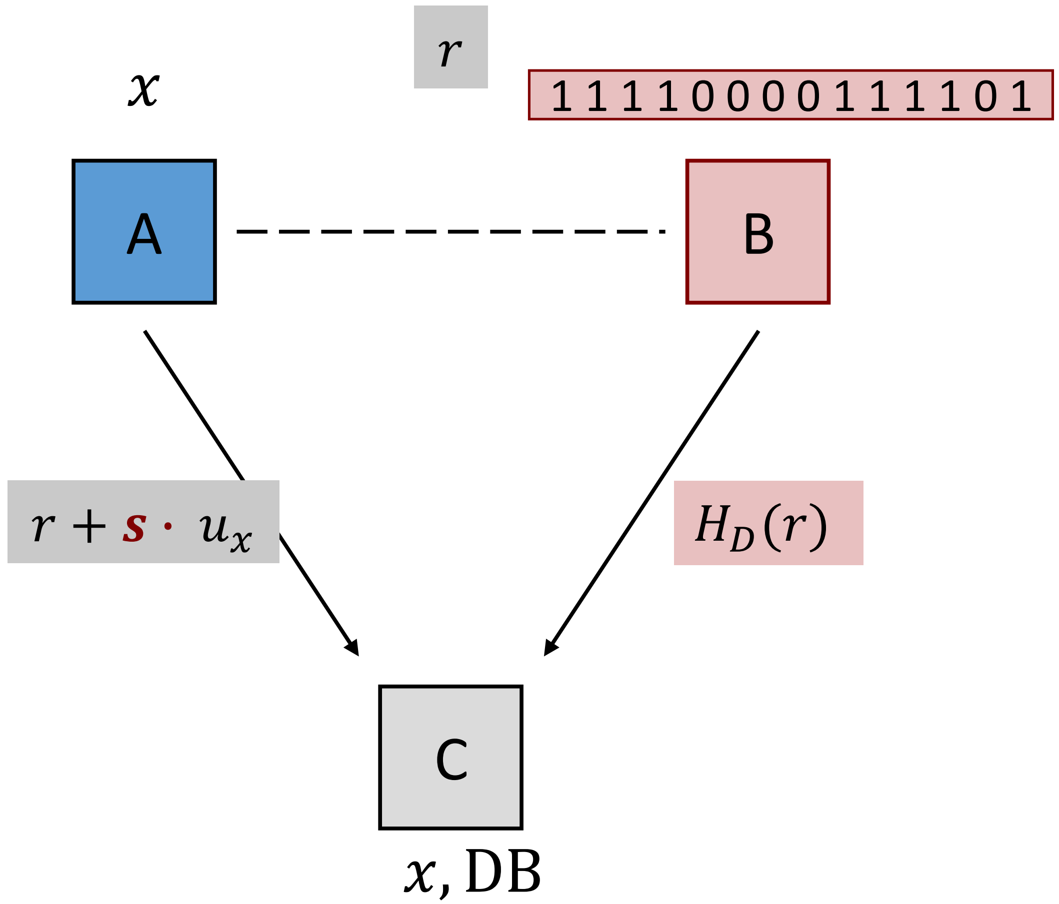
$H_D(r + s \cdot u_x)$ - $H_D(r)$ = $D(x) \cdot s$

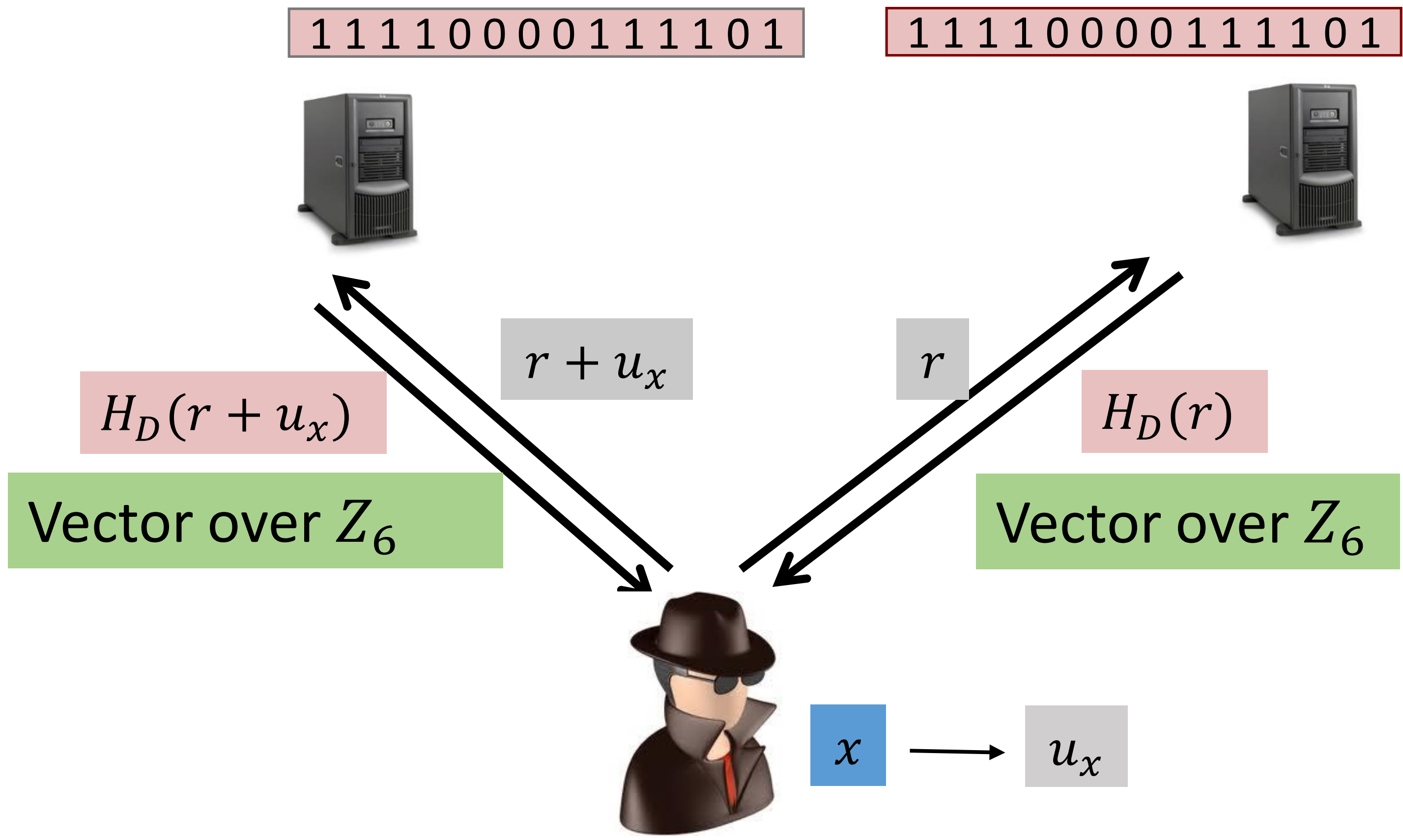
Ex: Instantiate with Hadamard-PIR



$H_D(r + u_x)$ - $H_D(r)$ = $D(x)$

Beyond Linear-PIR (MV-based PIR)

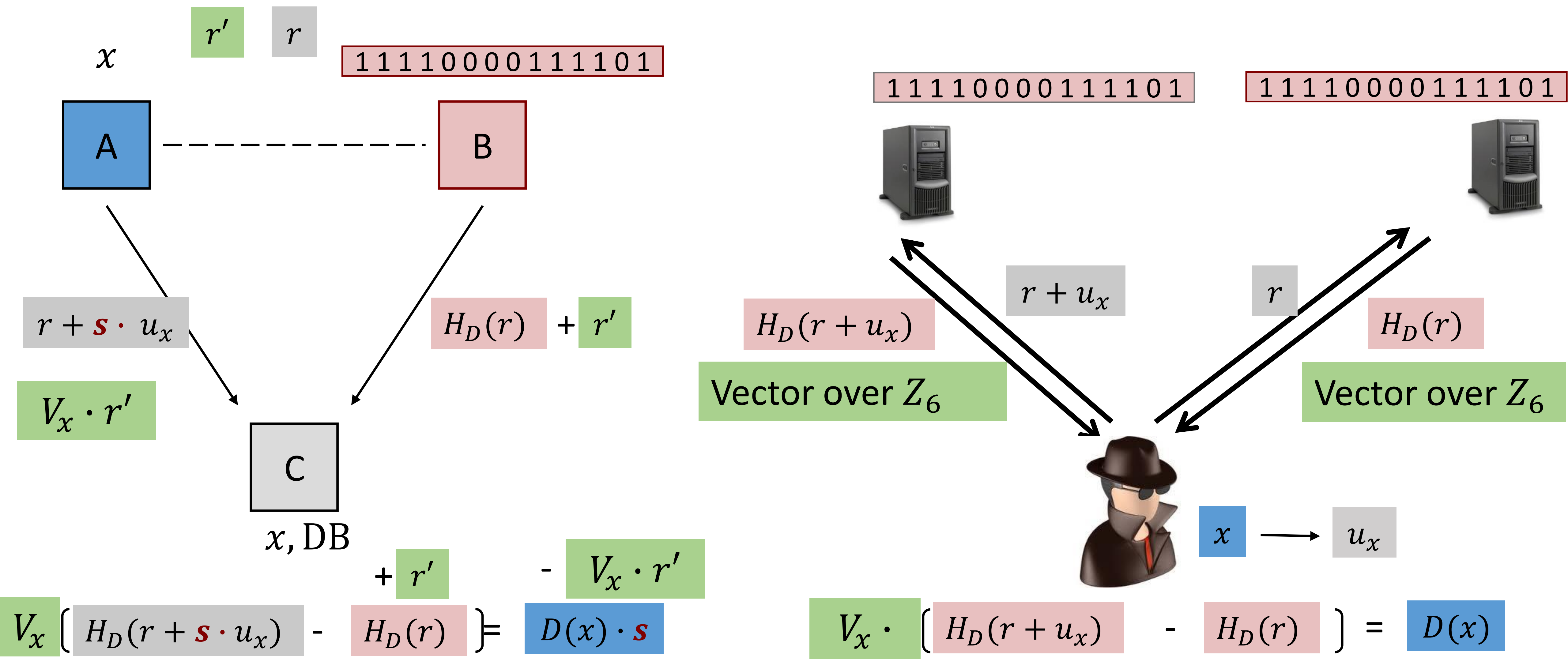




$V_x \left(H_D(r + \mathbf{s} \cdot u_x) - H_D(r) \right) = D(x) \cdot \mathbf{s}$

$V_x \cdot \left(H_D(r + u_x) - H_D(r) \right) = D(x)$

Beyond Linear-PIR (MV-based PIR)



Sub-exponential CDS for general functions

By massaging the 2-server PIR of we get

Thm 1. [LiuVaiWee17] Every $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

has CDS for 1-bit secrets with communication $2^{\sqrt{n \log n}}$

Using "multiparty"-MV-family

Thm 2. [LiuVaiWee18] Every k-party predicate $f: \{0,1\}^{n/k} \times \cdots \times \{0,1\}^{n/k} \to \{0,1\}$

has CDS for 1-bit secrets with communication $2^{\sqrt{n}} \log n$

Amortized CDS for general functions

[A-Ark-Ray-Vas17,A-Ark18]

What if the secret is very long?

Secret S

$\mathrm{CDS}(f,L) \stackrel{\text{def}}{=}$ CDS-communincation of L-bit secret per party

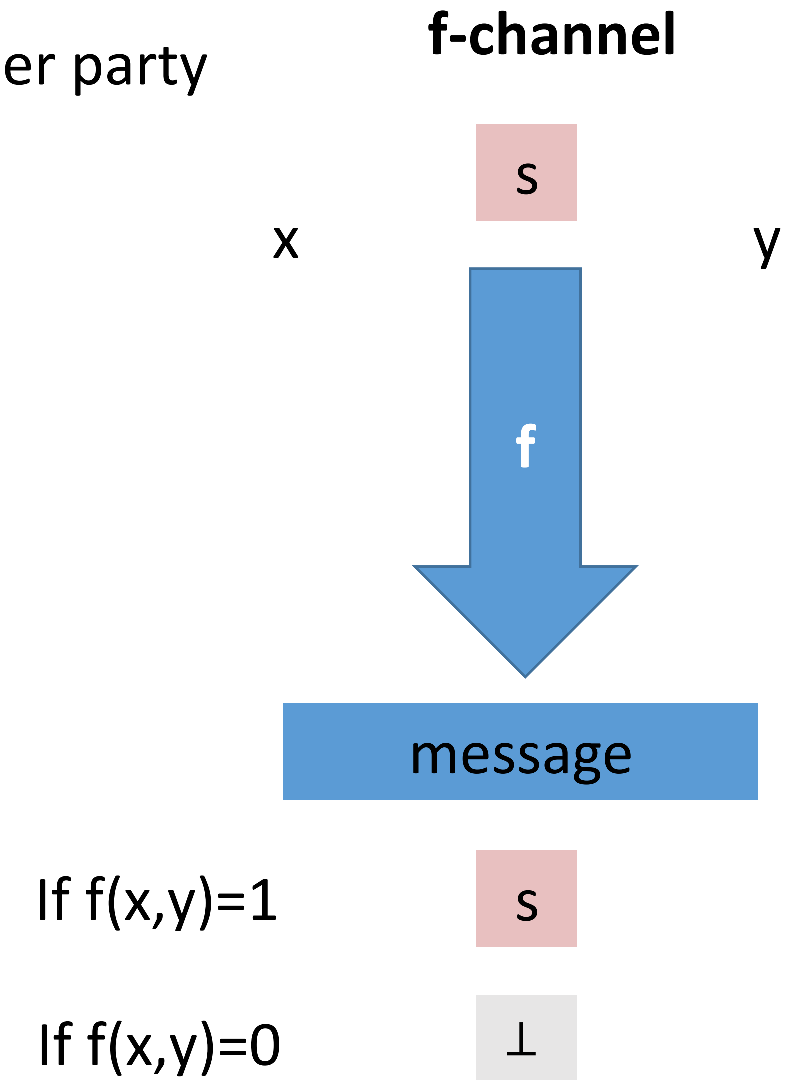
Clearly,

$$L \le \mathrm{CDS}(f,L) \underset{\ll}{\le} L \cdot \mathrm{CDS}(f,1)$$

Can we save?

What is the best achievable rate?

$$\overline{\mathrm{CDS}}(f) \stackrel{\text{def}}{=} \lim_{L\to\infty} \frac{CDS(f,L)}{L}$$



Constant-Rate CDS

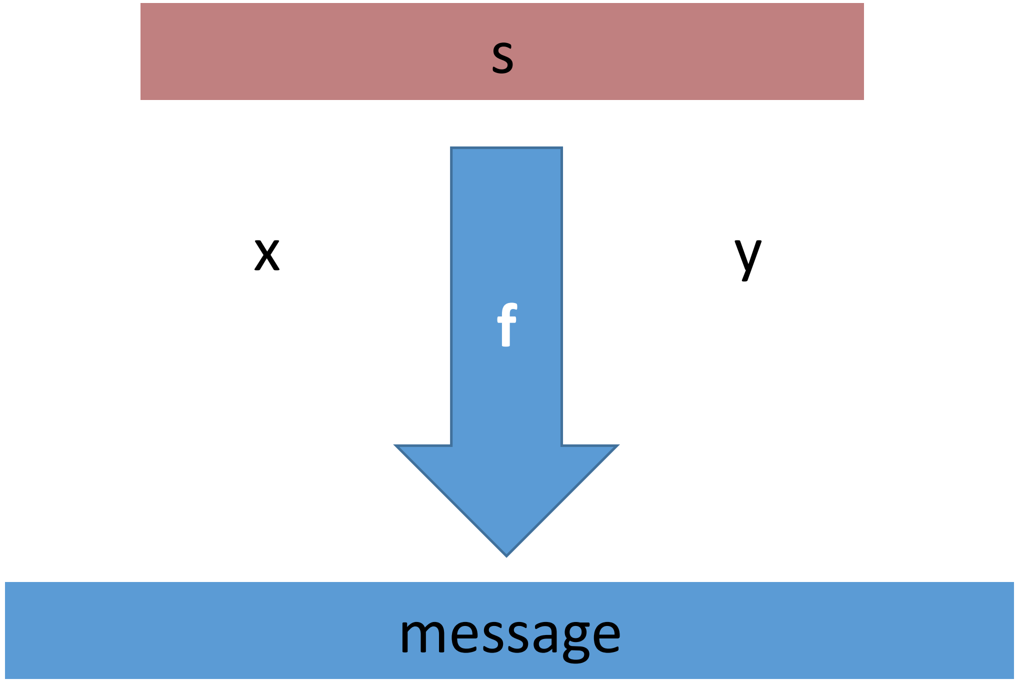
Thm. [AArkRayVas17,AArk18]

For very $f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$$\overline{\mathrm{CDS}}(f) \leq 3$$

- Very long secrets $L \geq \exp(\exp n))$
- Extends to arbitrary number of parties
- Barriers against lower-bounds
  - Entropy-based argument yield $\overline{\mathrm{CDS}}(f)$ LB's

Amortized-CDS=
f-channel for long messages



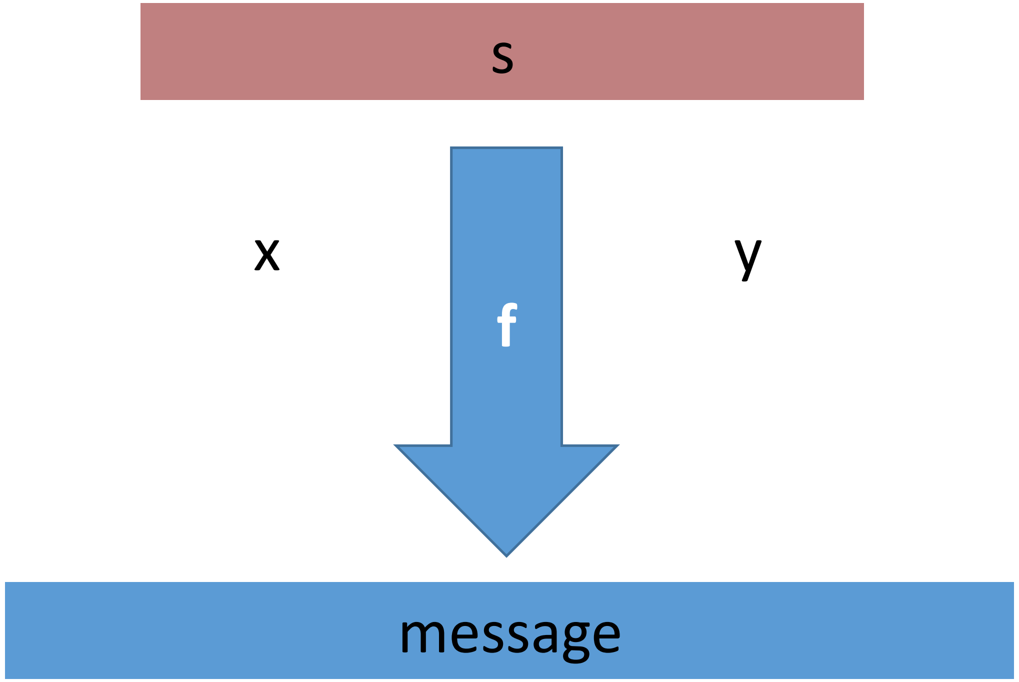
Constant-Rate CDS

Thm. [AArkRayVas17,AArk18]

For very $f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$

$$\overline{\mathrm{CDS}}(f) \leq 3$$

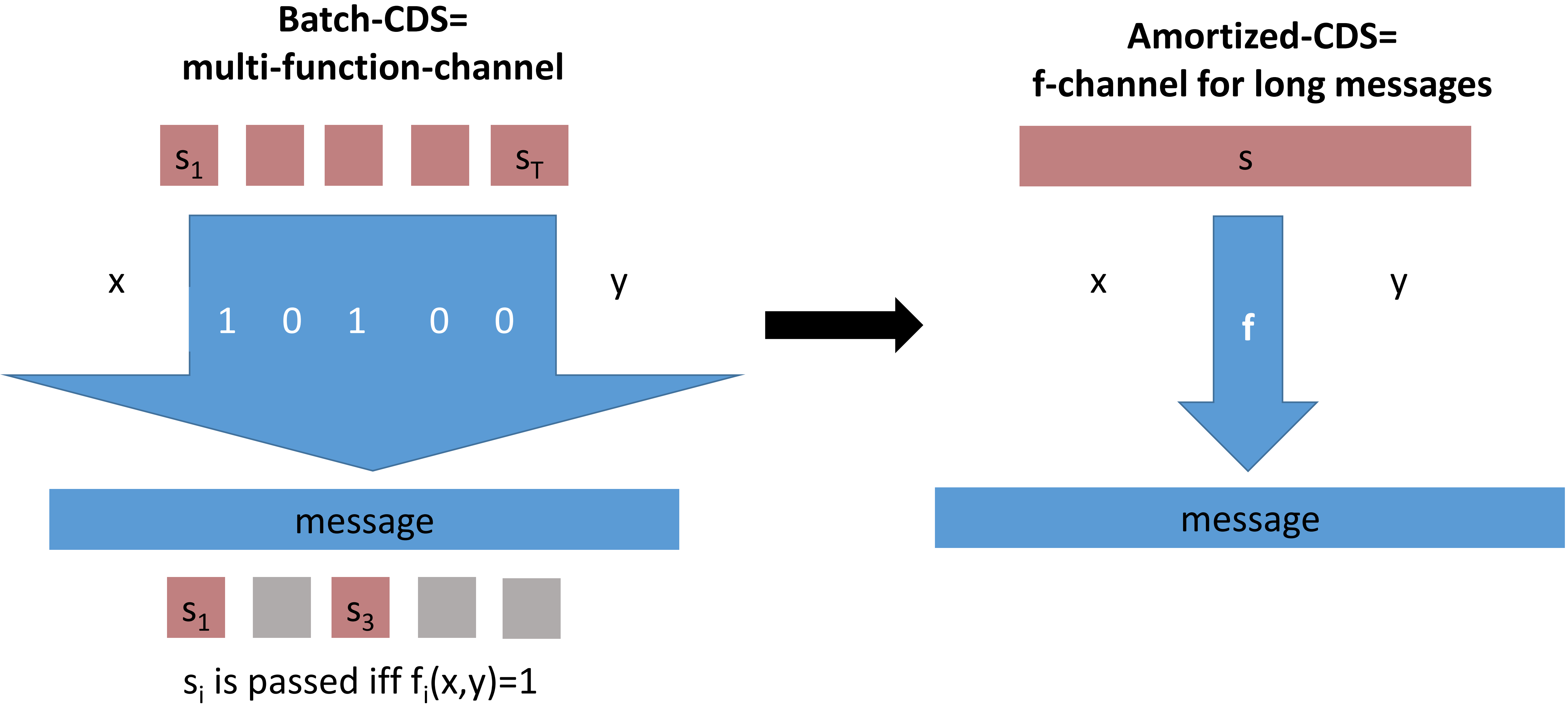
Amortized-CDS=
f-channel for long messages



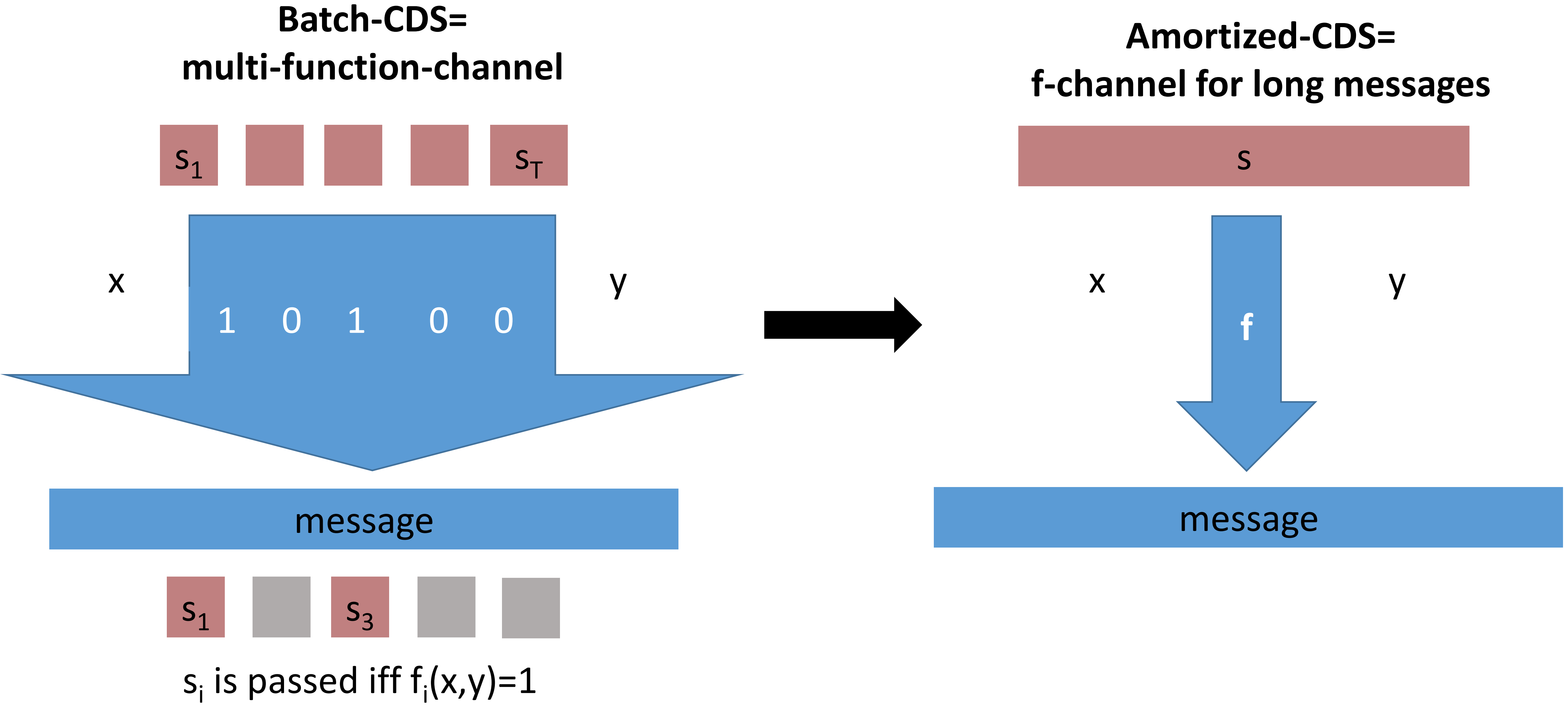
Proof:

1. Construct Batch-CDS
2. From Batch-CDS to Amortized-CDS

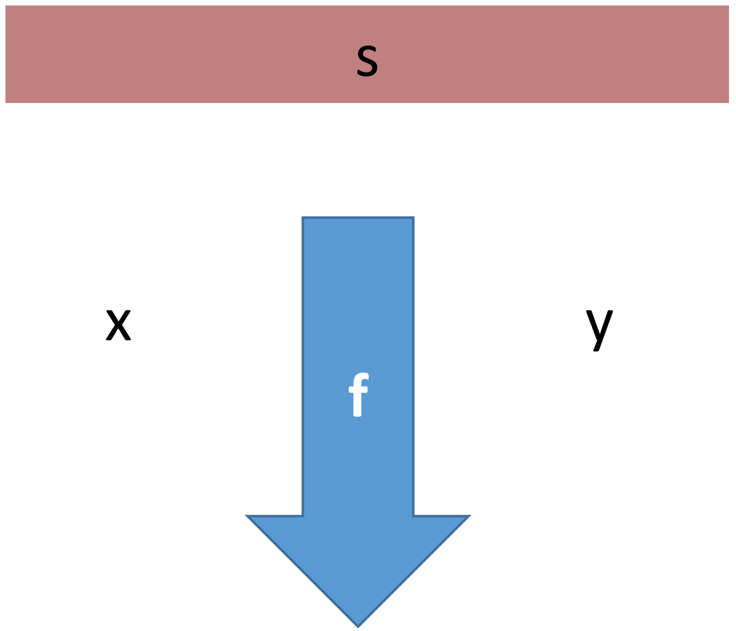
Constructing Amortized CDS



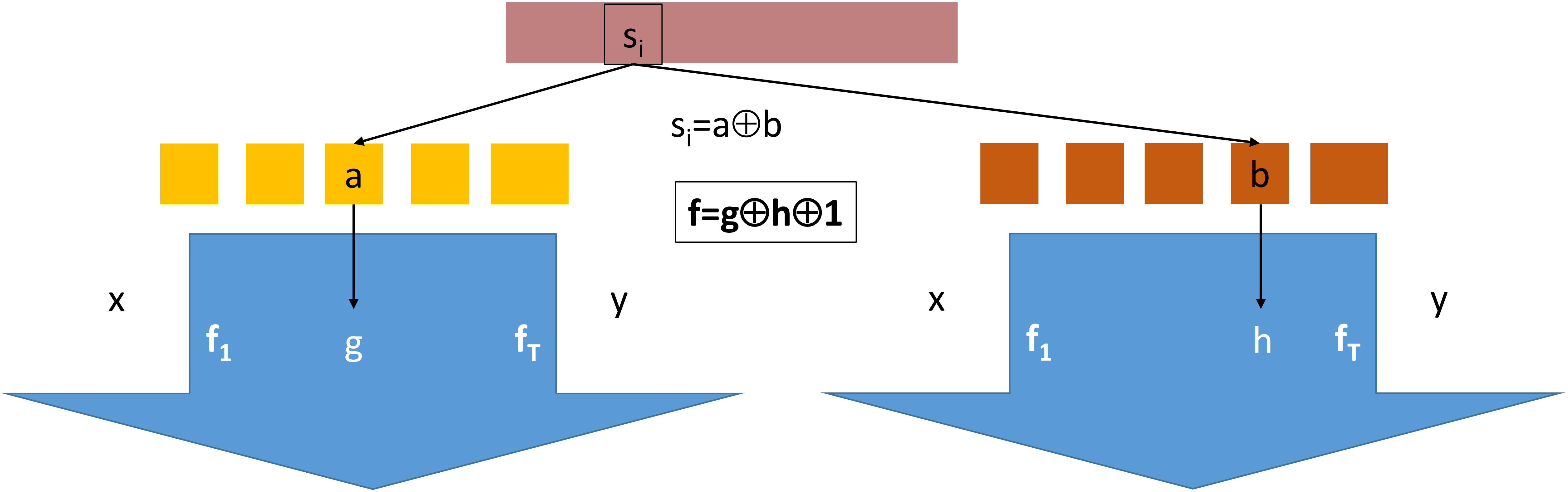
Thm: Batch-CDS for ALL-Functions with blow-up 1.5



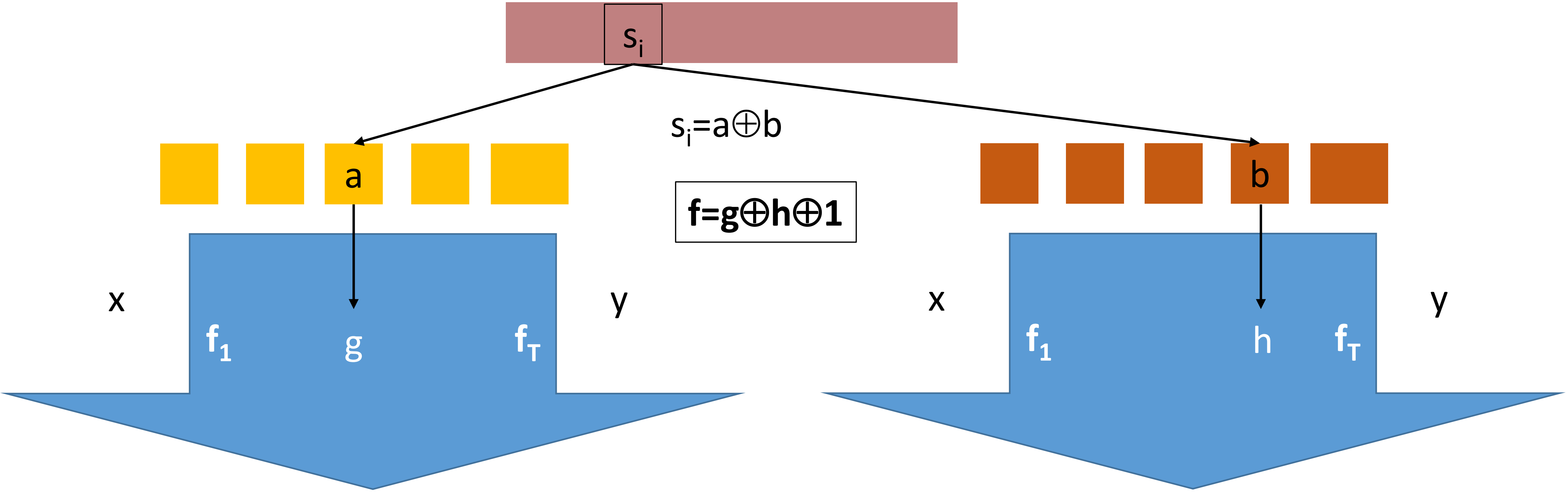
f-channel for long messages



f-channel for long messages



f-channel for long messages



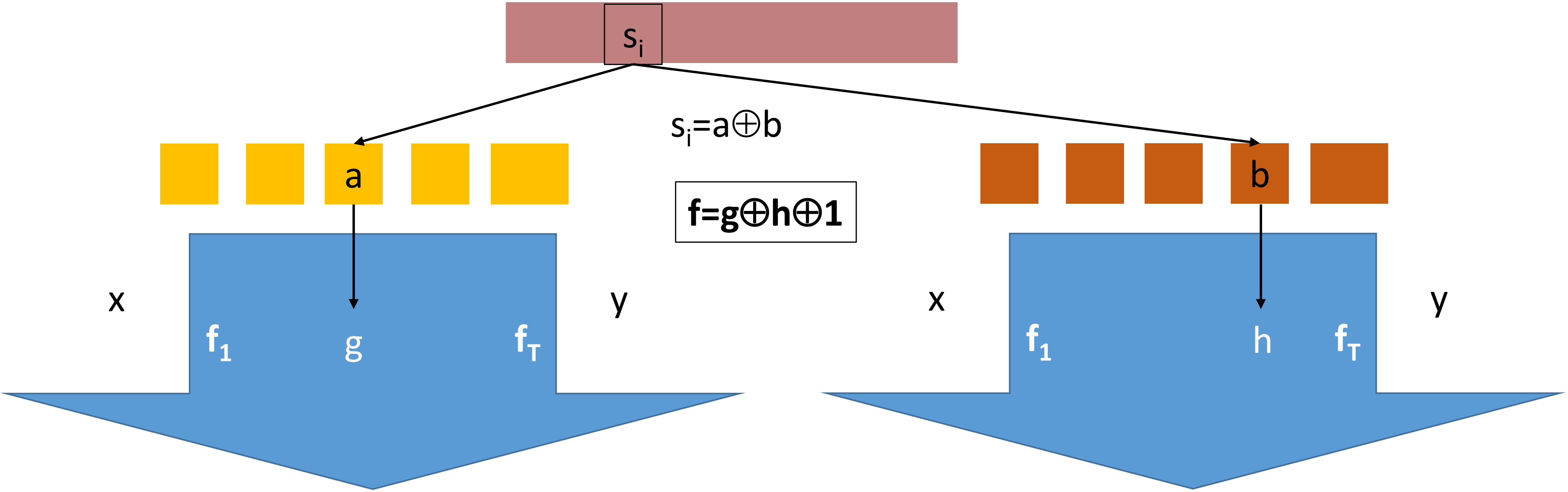
If f(x,y)=0

⇒ Either g=0 or h=0

⇒ One of the shares is hidden

⇒ The channel hides s

f-channel for long messages



If f(x,y)=1

& if g(x,y)=1 ← Happens to half of the functions

$\Rightarrow$ h=1

$\Rightarrow$ Both shares are revealed

$\Rightarrow$ The channel releases s

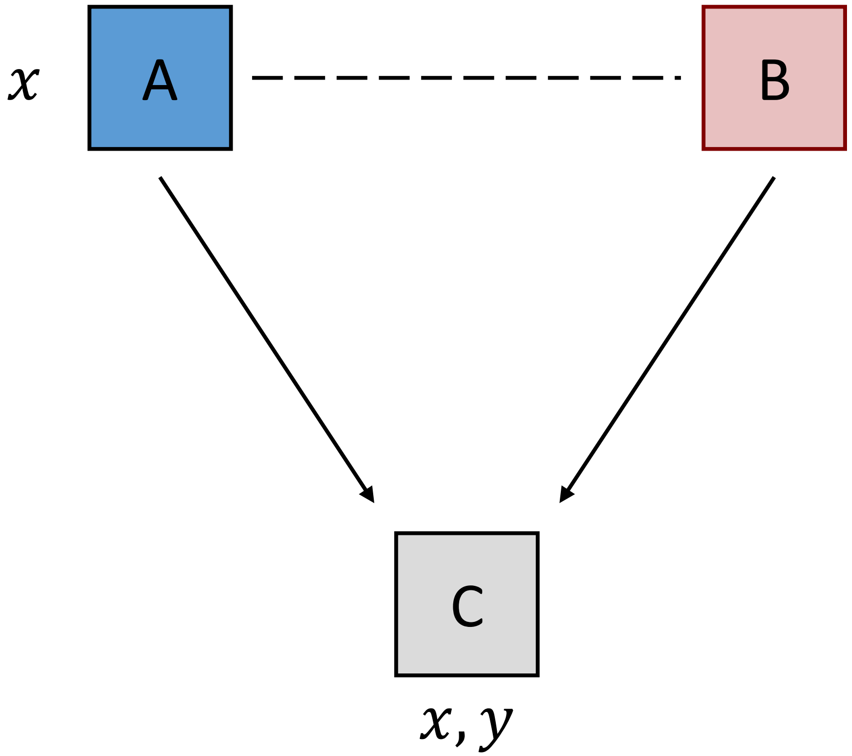
$\Rightarrow$Half of the secrets go through

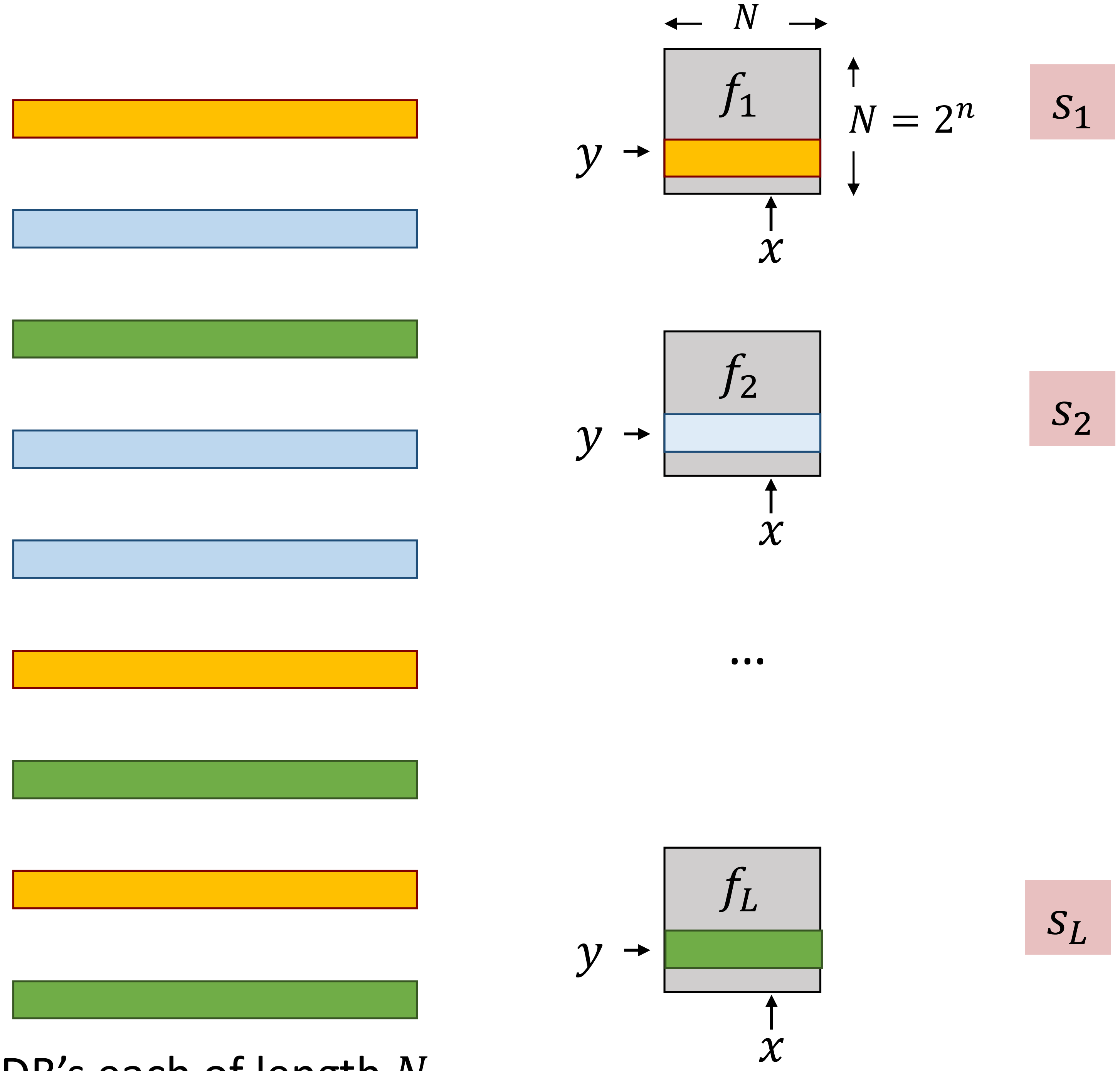
Can get all secrets using pre-coding

duplicate each secret twice & place it on g and 1-g

Constructing Batch CDS

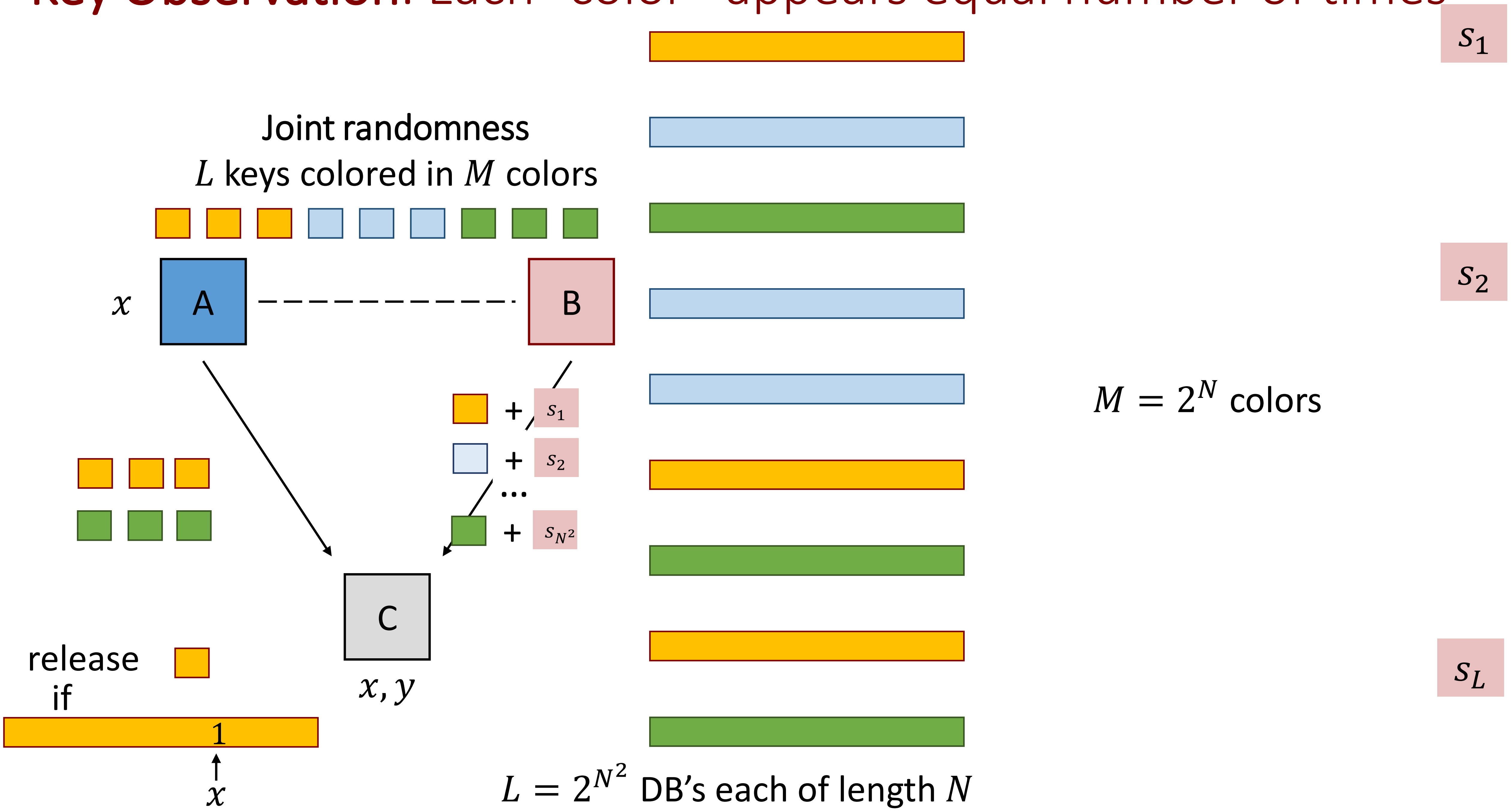
Single Index in Many DB's



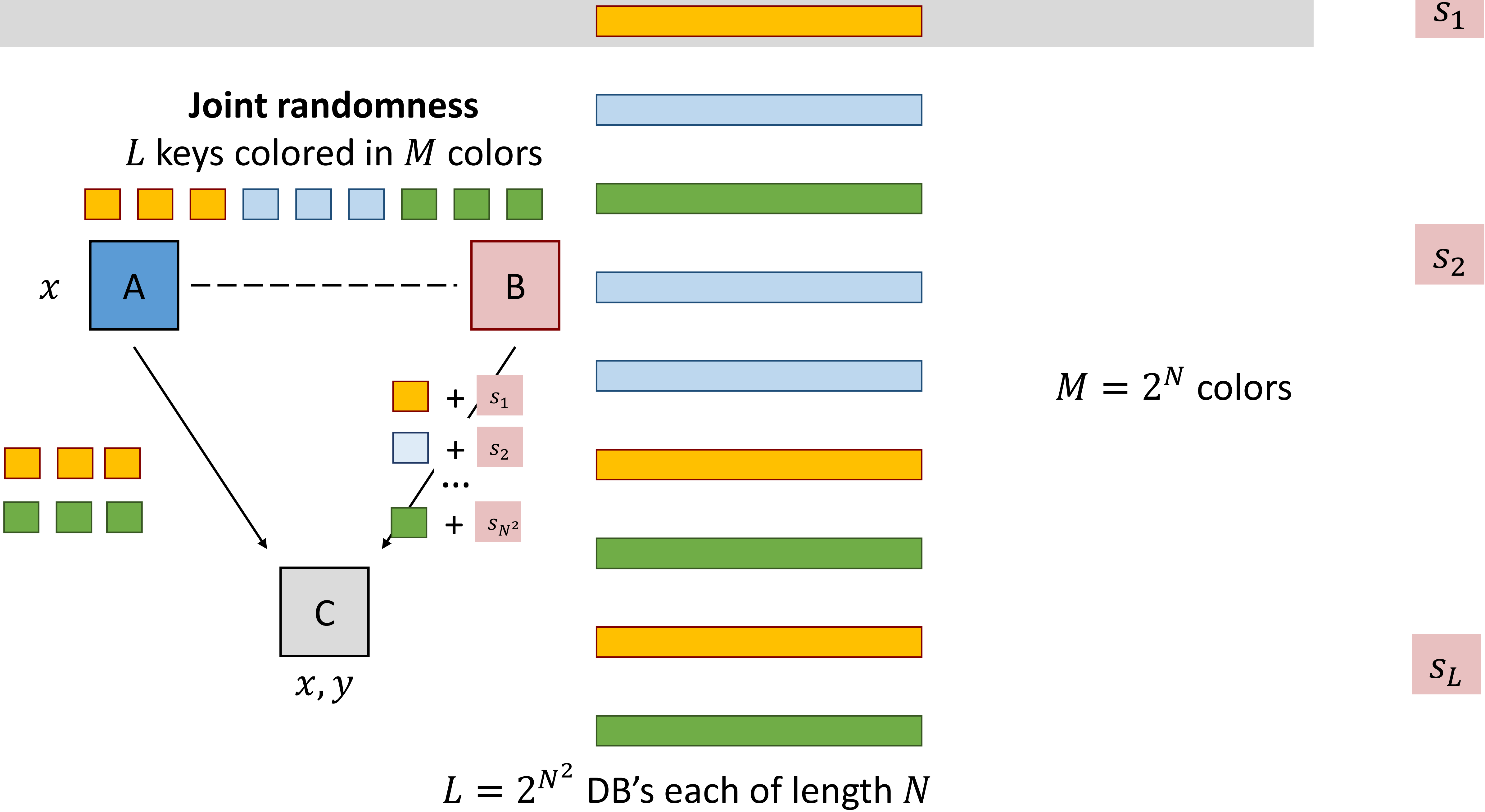


$L = 2^{N^2}$ DB's each of length N

Key Observation: Each "color" appears equal number of times



Communication: Alice $0.5L$, Bob L,



Upper bounds: Summary

Complexity of 2-party CDS:

- **Linear CDS:** $2^{n/2}$ (Tight)
- **General CDS:** $2^{o(n)}$
- **Amortized CDS**: O(1)

OPEN

poly(n)? poly(n) for **circuits**?

Smaller amortization point?

Lower Bounds???

Cost of insecure solution is 1…

Lower-bounds via Communication Complexity Games

[GayKerWee15, A-ArkRayVas17, A-Hol-Mis-Sha18, A-Vas19]

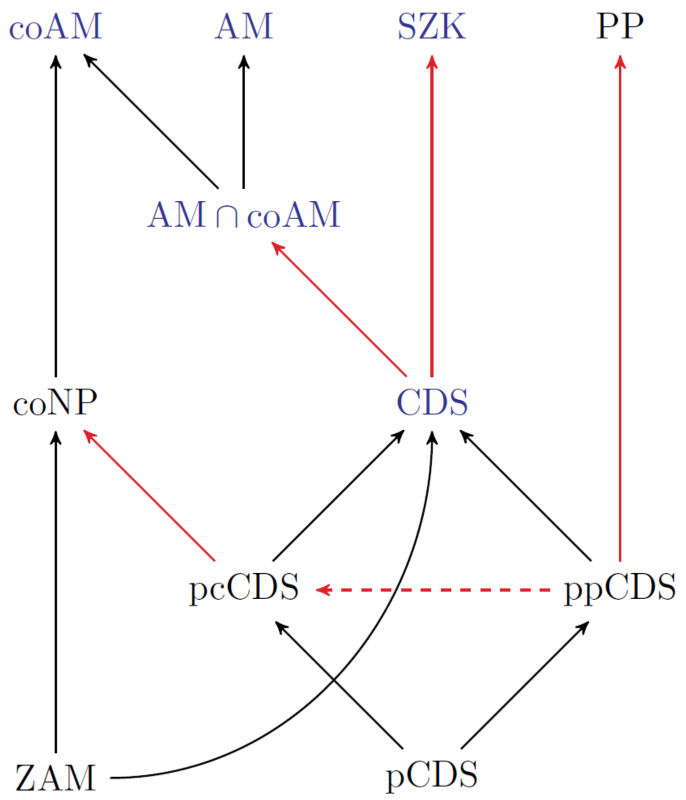
Rich connections (inclusions and separations):

Best known lower Bounds:

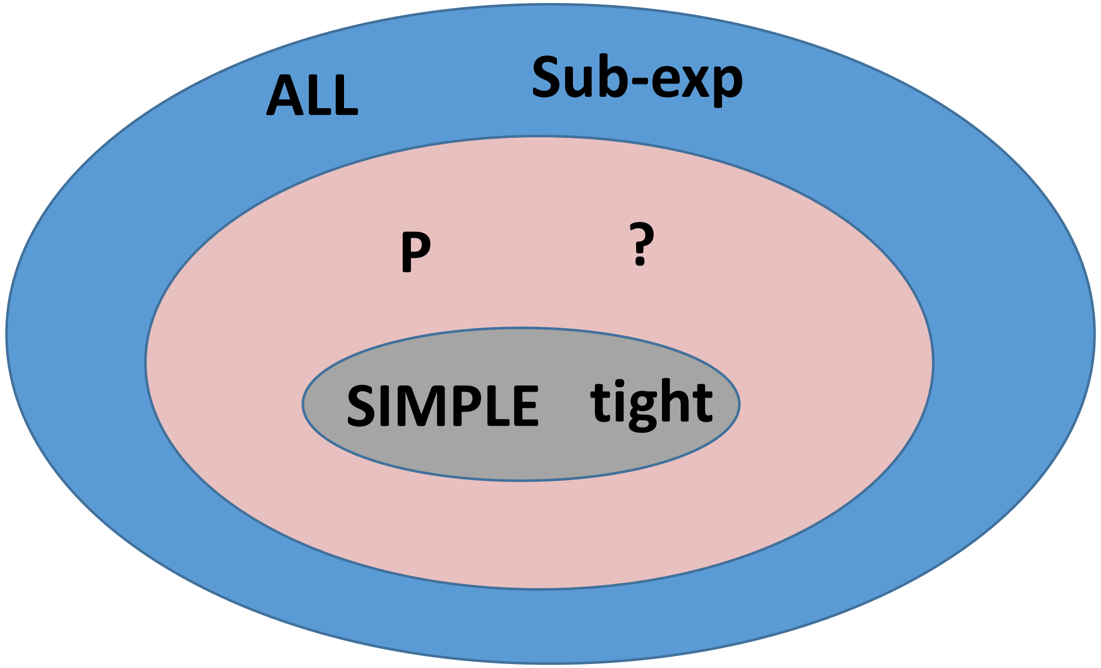
- For many (explicit functions) perfect-CDS(f) > $n - o(n)$
- For imperfect-CDS non-explicit CDS(f) > $n - o(n)$
- Trade-offs between Alice and Bob

Q: CDS(DISJOINTNESS**)?**

$$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$



Solid arrow: inclusion,
Dashed arrow: separation
Blue classes: explicit bounds are unknown.



Thank You !