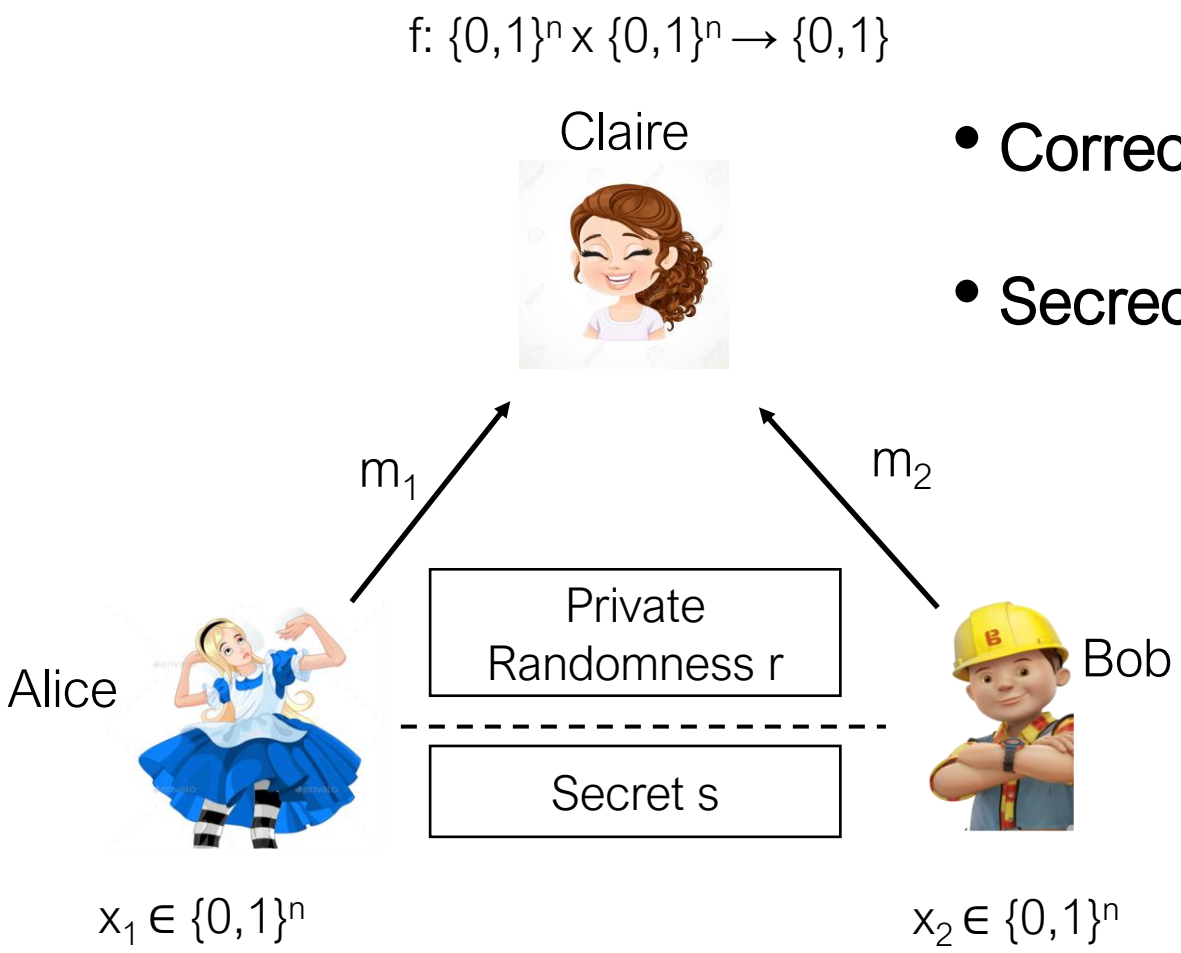
Multi-Clients Verifiable Computation via Conditional Disclosure of Secrets

Rishabh Bhadauria
Carmit Hazay
Bar-Ilan University

BIU Center for Research in Applied Cryptography and Cyber Security

Conditional Disclosure of Secrets (CDS) [GIKM00]



- **Correctness**: s is recovered if $f(x_1,x_2) = 1$
- **Secrecy**: $Sim(x_1,x_2) \approx (m_1,m_2)$ if $f(x_1,x_2) = 0$

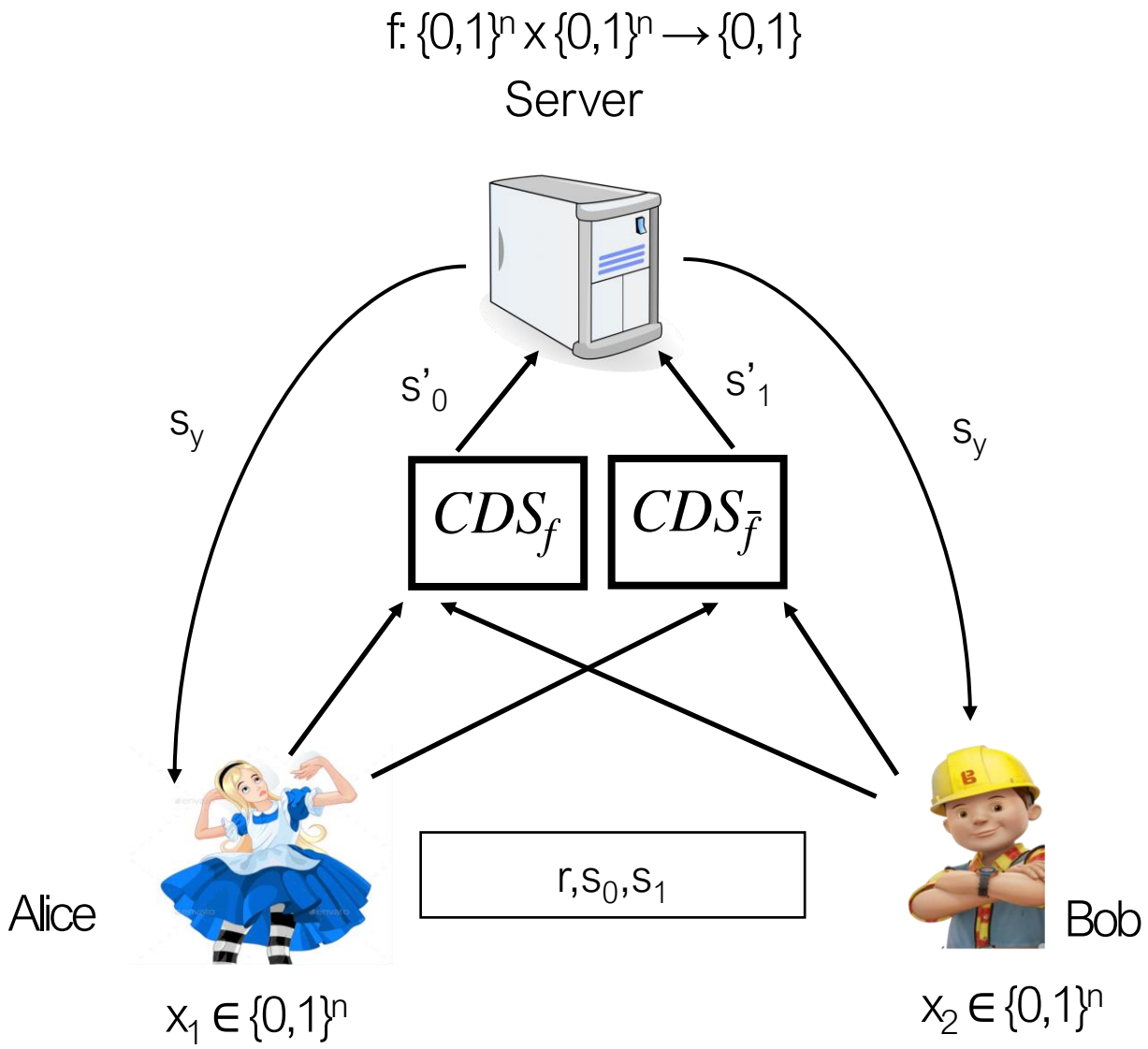
Motivation for CDS

Private Information Retrieval [GIKM00]

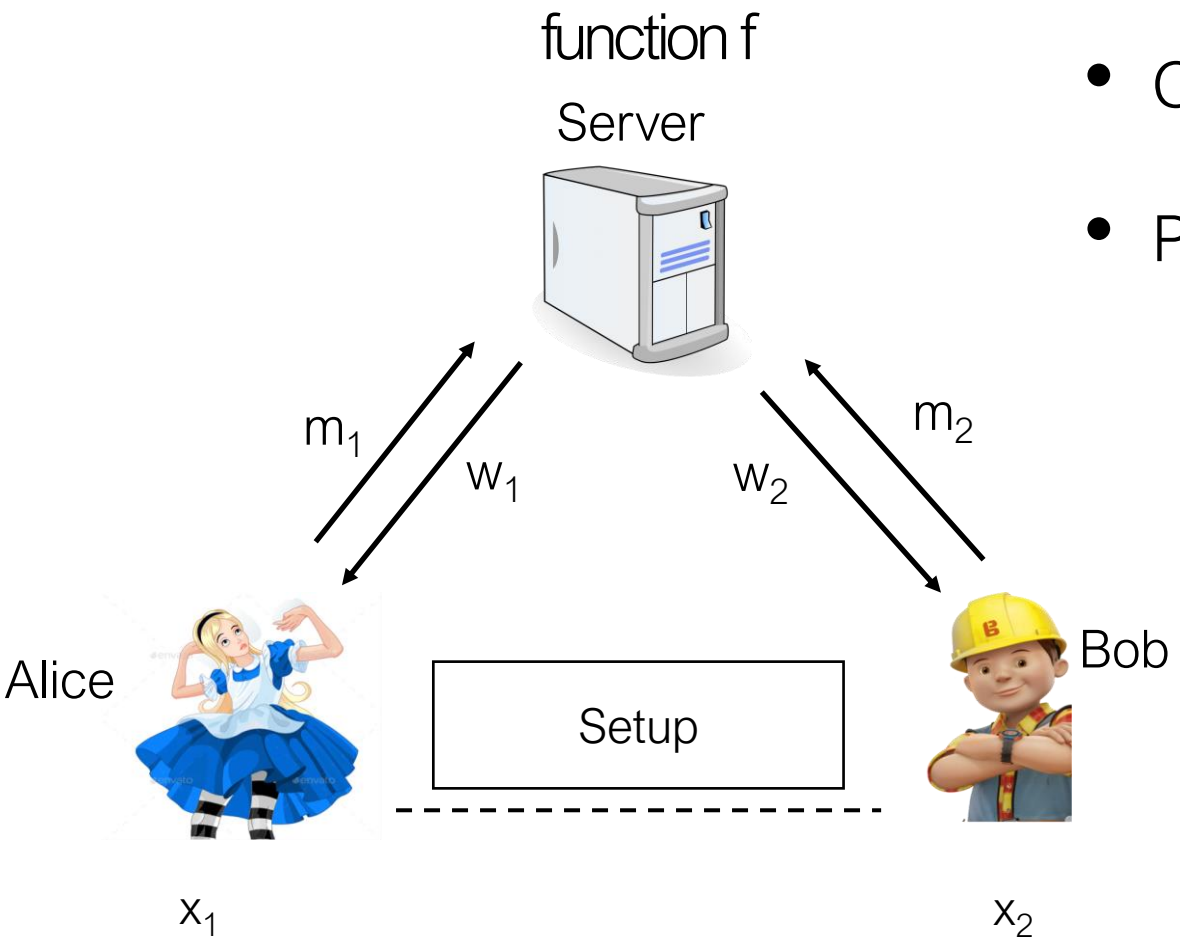
Secret-Sharing [BIKK14, LV18, BP18, ABFNP19, ABNP20]

Attributed-based Encryption [Attrapadung14, Wee14, GKW15]

Verifiable Computation from CDS [PRV12]



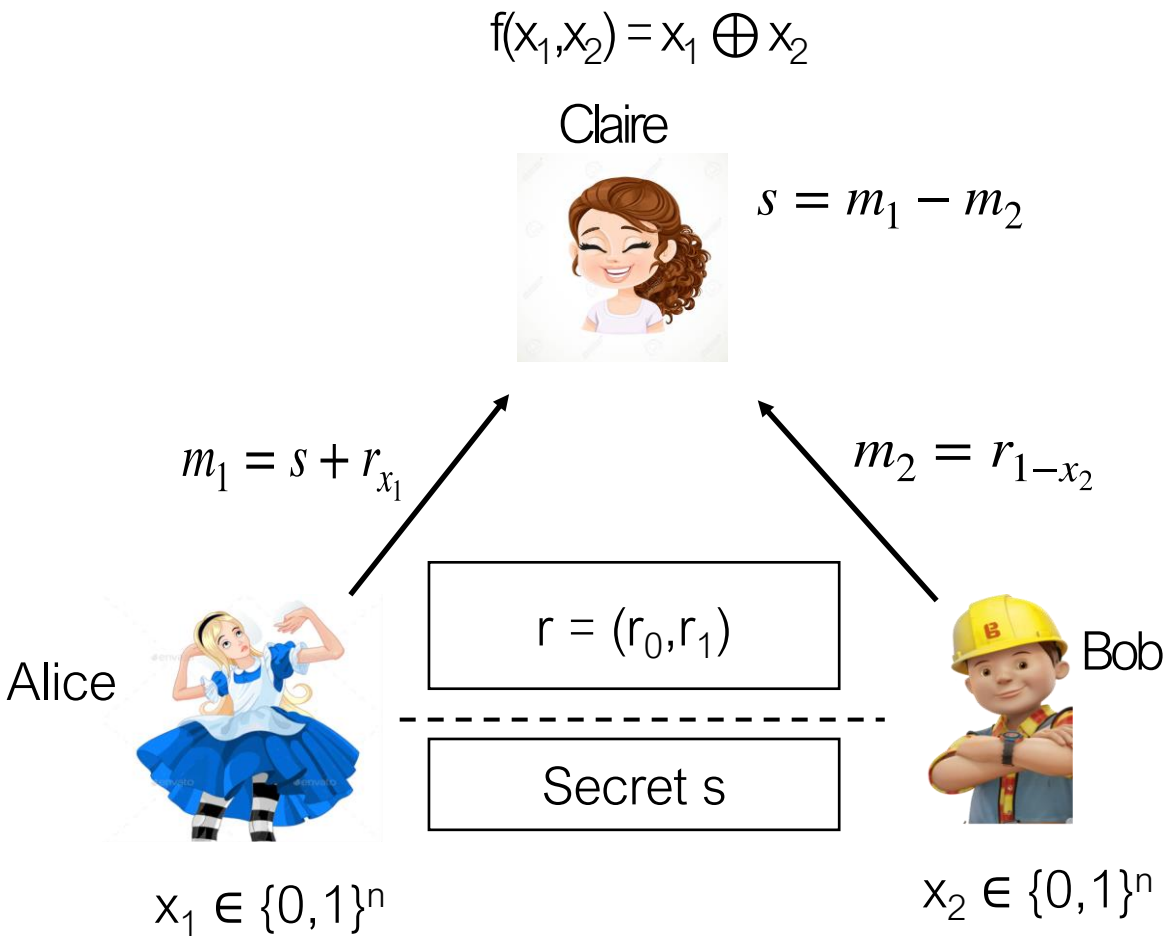
Multi-Clients Verifiable Computation (MVC) [CCKC13]



Learns $y=f(x_1,x_2)$ from w_1 and w_2 respectively

- Correctness: y is computed correctly by server
- Privacy (opt.): Nothing about inputs other than y is revealed

Example of CDS



Our Results

Explore connection between MVC and CDS

Extend definition of CDS : Private CDS & Oblivious CDS

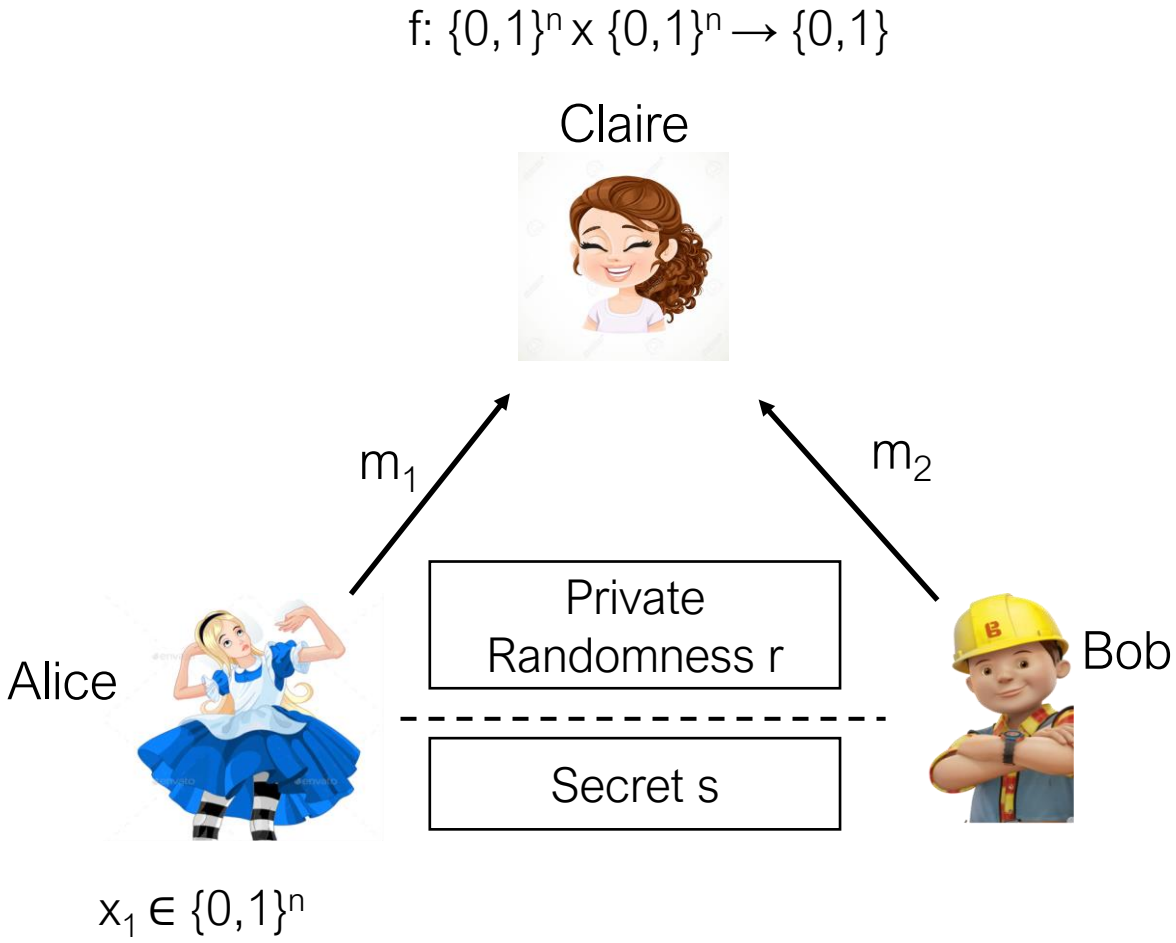
Construct new classes of private CDS for equality, inequality, private set-intersection (PSI) cardinality and more

Advantages of using CDS

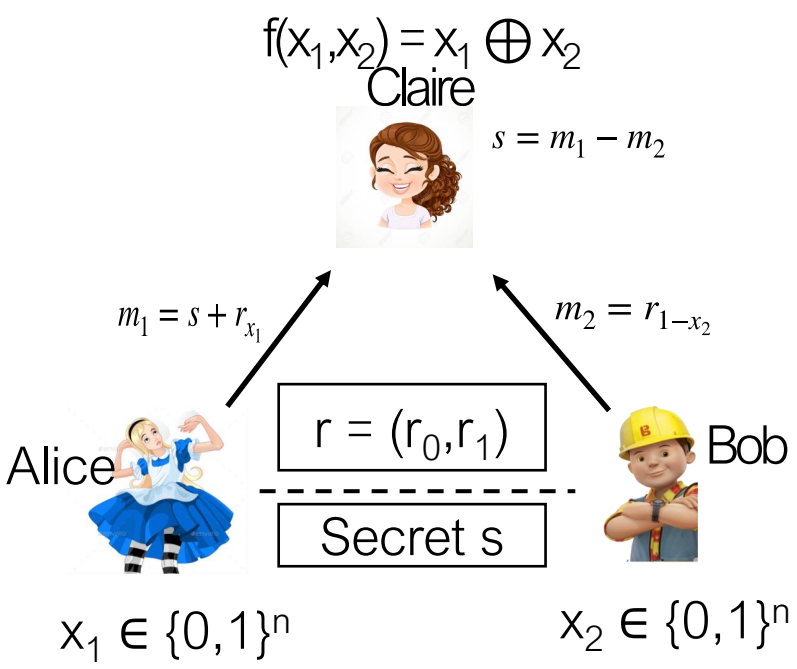
Non-interactive solutions

Batching

Transparent setup



Variants of CDS



Private CDS (Input privacy)

Correctness: The secret s is recovered if $f(x_1, x_2) = 1$

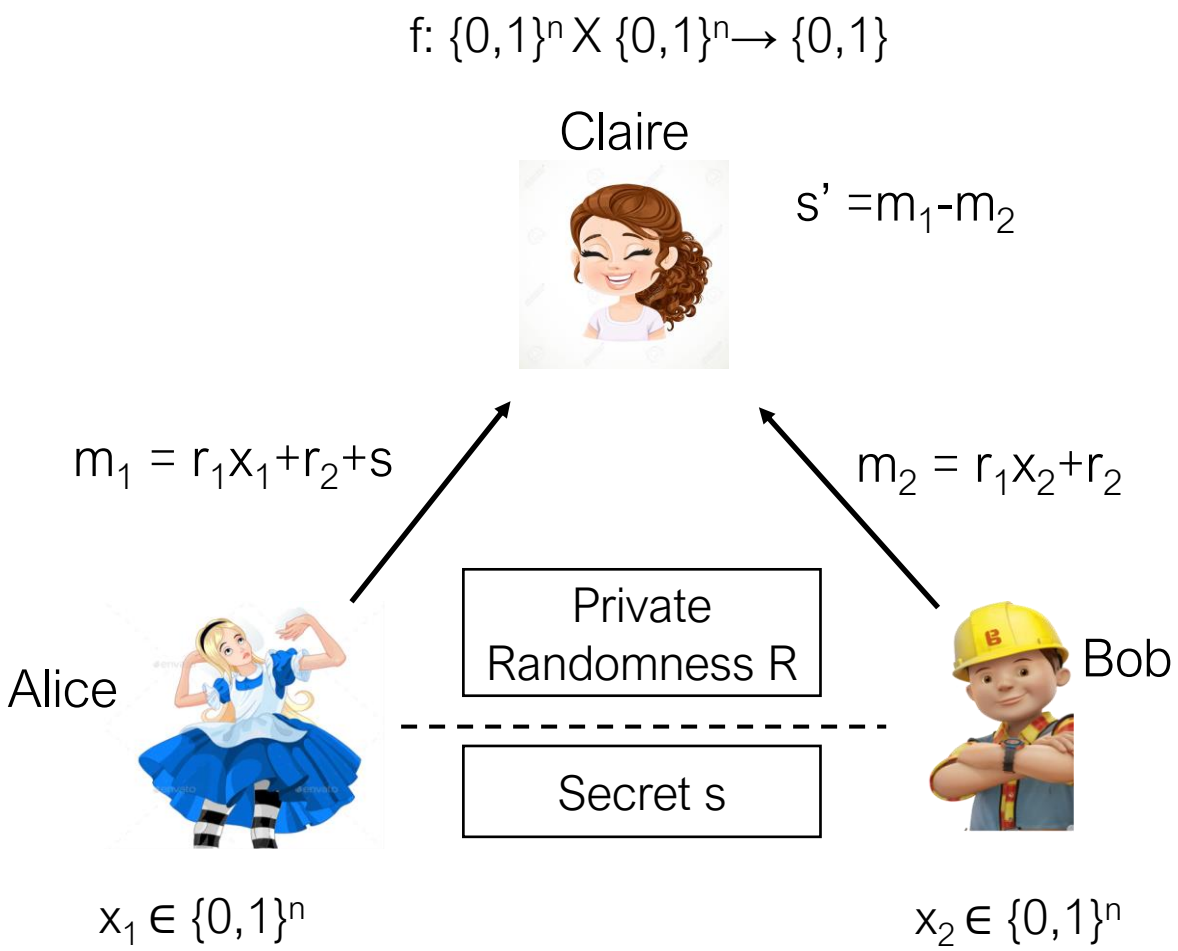
Privacy: Claire learns nothing about x_1 and x_2 other than what is revealed by $f(x_1, x_2)$

Oblivious CDS (input & output privacy)

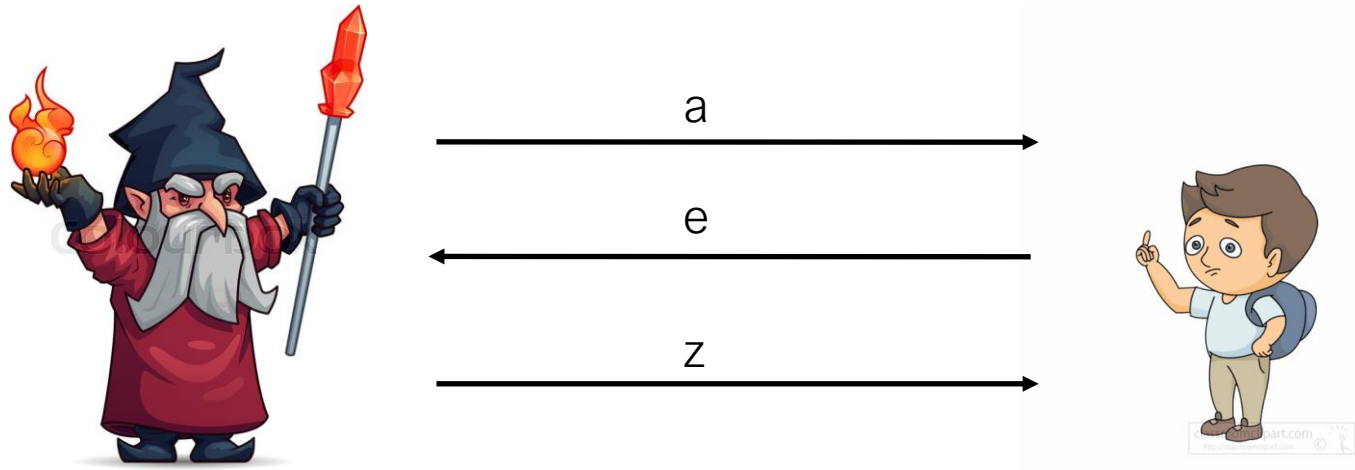
Correctness: The secret s is recovered if $f(x_1, x_2) = 1$

Obliviousness: Claire learns nothing about x_1, x_2 or $f(x_1, x_2)$

Oblivious CDS for Equality



Sigma Protocol



3-round public coin zkPOK (Zero-Knowledge Proof of Knowledge)

Prover proves that it knows a witness w s.t. (x,w) ∈ R

Verifier's randomness is public

Schnorr's Protocol

$x = g^w$

$a = g^r$

e

$z = r + ew \bmod q$

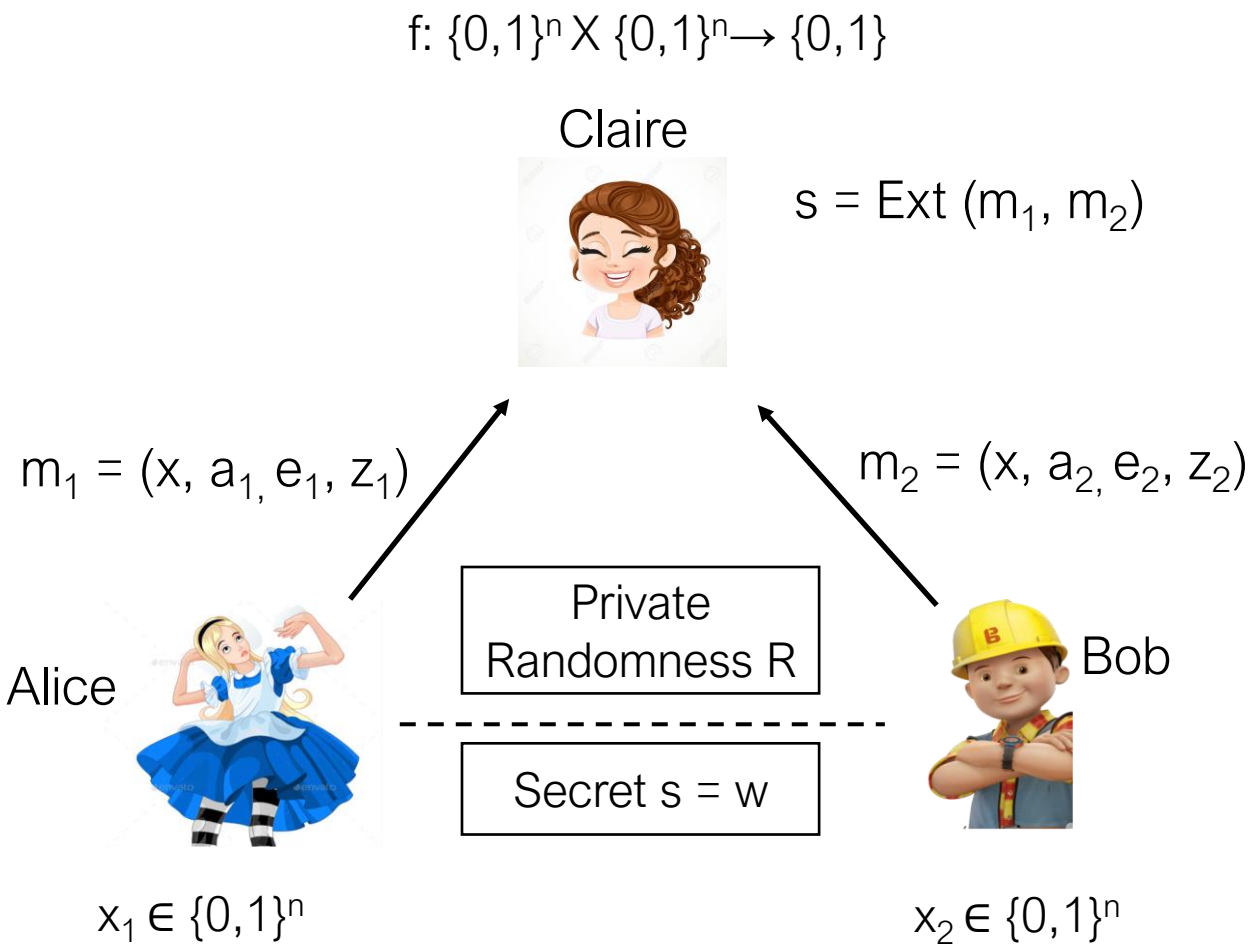
V checks:

$g^z = ax^e$

Private CDS for Equality

Parties embed their inputs into the transcript of Sigma protocol

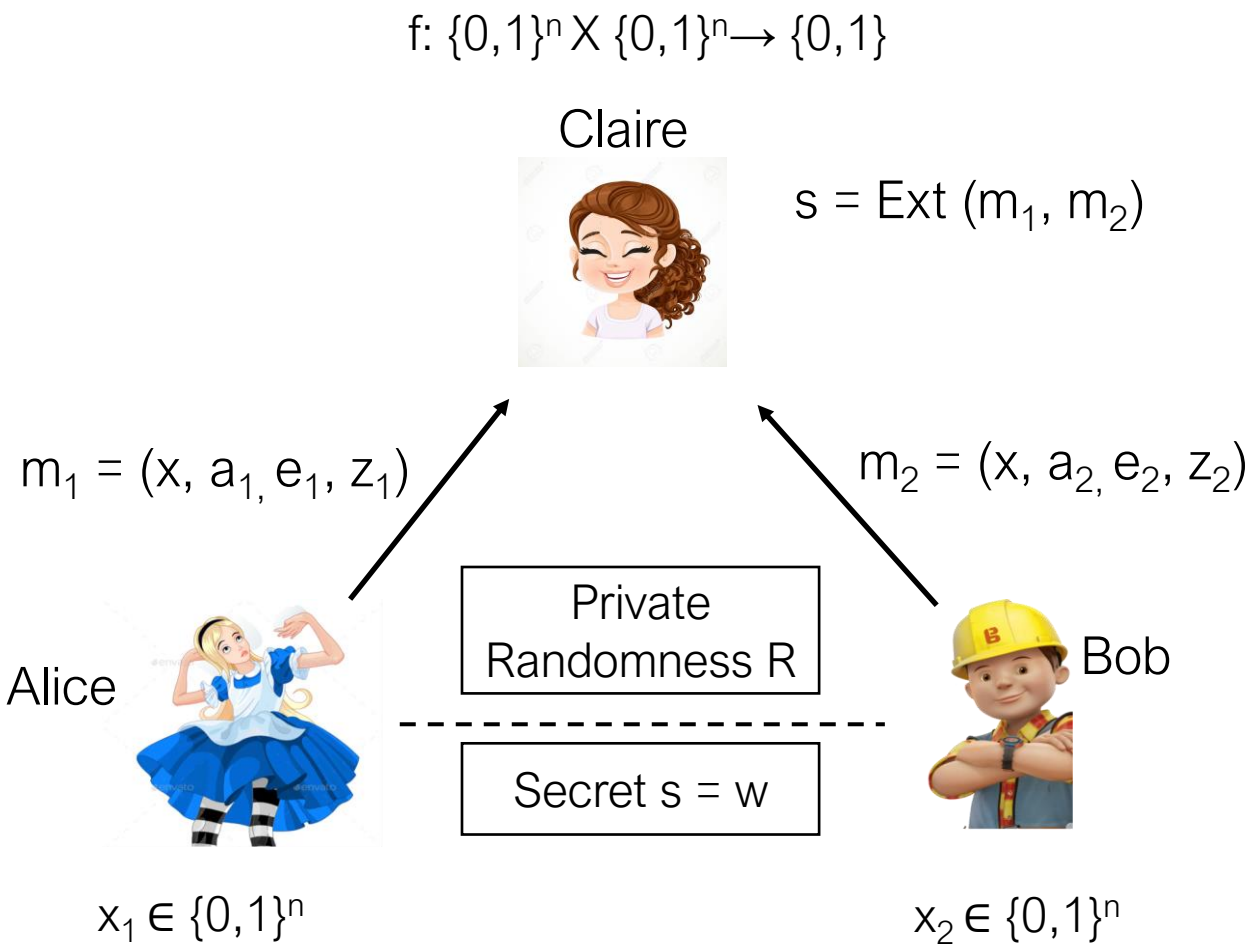
Security argument utilizes the special soundness property to extract the secret



Private CDS for Inequality

Parties embed their inputs into the transcript of Sigma protocol

Security argument utilizes the special soundness property to extract the secret



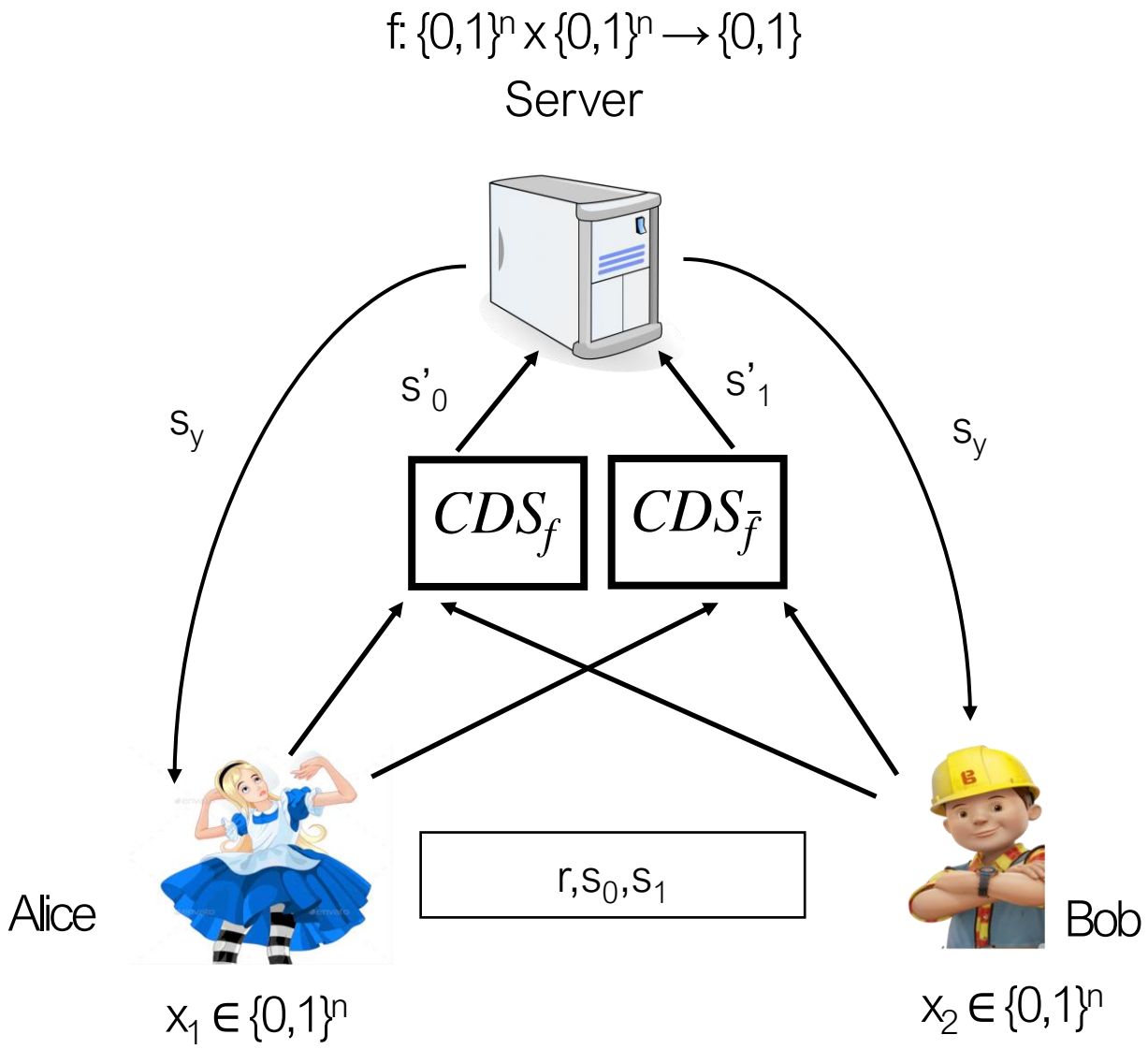
Additional CDS Constructions

CDS for PSI cardinality based on protocols from [LRG19]

Techniques can be extended to set-union cardinality, set-membership and small domain range predicates

Prior work [PTT11, CPPT14] relies on stronger assumptions but achieves additional properties

Verifiable Computation from CDS [PRV12]



New VC based on our CDS

Malicious security

2-Client Verifiable Computation for Equality

Construction	Setup	Round Complexity	Online Comm.	Offline Comm.	Hardness Assump.	Security
[Cou18]	Correlated*	≥ 3	$\mathcal{O}(\lambda\ell)$	$3\ell + o(\ell)$	OWF +OT	Passive
[MR18]	Correlated	3	$\mathcal{O}(\lambda\ell)$	$\mathcal{O}(\lambda\ell)$	OWF+OT	Active
[BGI19]	Correlated**	2	ℓ	$\lambda\ell$	OWF	Passive
Our Work	Uniform	2	3ℓ	6ℓ	OWF	Passive
Our Work	Uniform	2	10ℓ	7ℓ	OWF+Σ-protocol***	Active

Table 1: A comparison of our equality protocol with prior work where λ is the security parameter, the inputs are of size ℓ bits and OT is oblivious transfer.

* This work uses two types of correlated randomness that are generated using OT for XOR and AND shares.

** This correlation requires keys for computing distributed point functions.

*** We concretely rely here on the hardness of discrete logarithm in groups.

Thank You