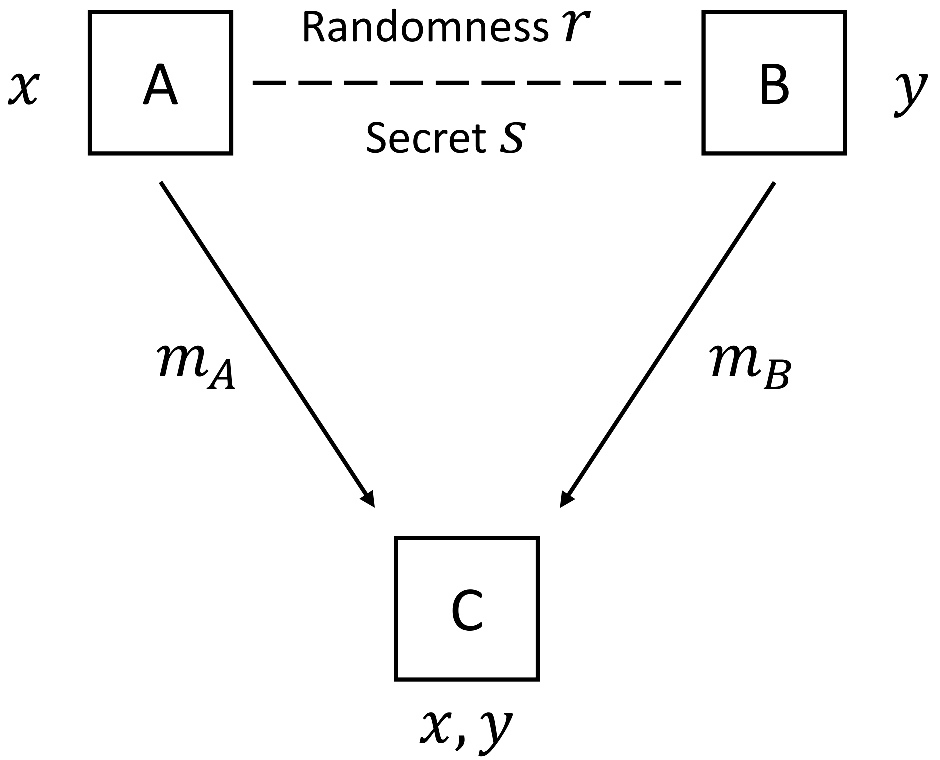
Conditional Disclosure of Secrets: Amplification, Closure, Amortization, Lower-bounds, and Separations

Benny Applebaum   Barak Arkis   Pavel Raykov   Prashant Nalini Vasudevan

Conditional Disclosure of Secrets [GIKM00]

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



<u>**δ-Correctness:**</u>

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

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

<u>**ϵ-Privacy:**</u>

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

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

<u>**Communication:**</u> $|m_A| + |m_B|$

<u>**Randomness:**</u> $|r|$

Connections and Applications

- Attribute-Based Encryption. [Att14,Wee14]
- Secret-sharing for certain graph-based access structures.
- Light-weight alternative to zero-knowledge proofs in some settings. [AIR01]
- Data privacy in information-theoretic PIR. [GIKM00]
- A minimal model of multi-party computation.

What Was Known Earlier

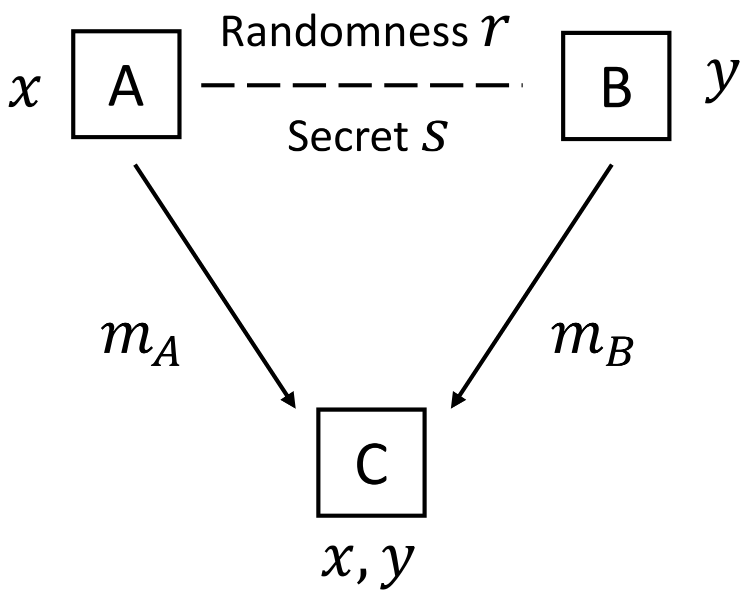
Upper bounds:

- Communication $2^{O(\sqrt{n \log n})}$ for any predicate on n-bit inputs. [LVW17]
- Communication $O(\sigma)$ for predicates with size-σ branching programs or span programs. [IW14,AR16]

Lower bounds:

- Explicit predicate that requires $\Omega(\log n)$ bits of communication. [GKW15]
- Same predicate requires $\Omega(\sqrt{n})$ bits for linear CDS. [GKW15]

CDS and Statistical Difference



Distribution of (m_A, m_B):

- input (x, y), $s = 0$: $(m_A, m_B)^0_{x,y}$
- input (x, y), $s = 1$: $(m_A, m_B)^1_{x,y}$

<u>δ-Correctness:</u>

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

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

$$\equiv \Delta\left((m_A, m_B)^0_{x,y}\,;(m_A, m_B)^1_{x,y}\right) > 1 - 2\delta$$

<u>ϵ-Privacy:</u>

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

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

$$\equiv \Delta\left((m_A, m_B)^0_{x,y}\,;(m_A, m_B)^1_{x,y}\right) < 2\epsilon$$

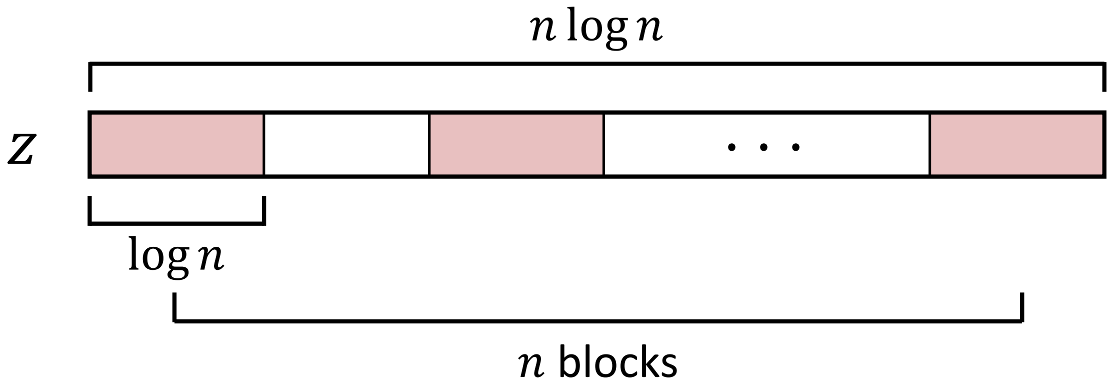
Separations

Explicit function $PCol: \{0,1\}^{4\text{n} \log n} \times \{0,1\}^{2\text{n} \log n} \rightarrow \{0,1\}$ that has:

- CDS complexity: $O(\log n)$
- Randomized communication complexity: $\Omega(n^{1/3})$
- Linear CDS complexity: $\Omega(n^{1/6})$

Inspired by oracle separations between SZK and other classes [Aar12], and the Pattern Matrix method [She11].

Collision Problems

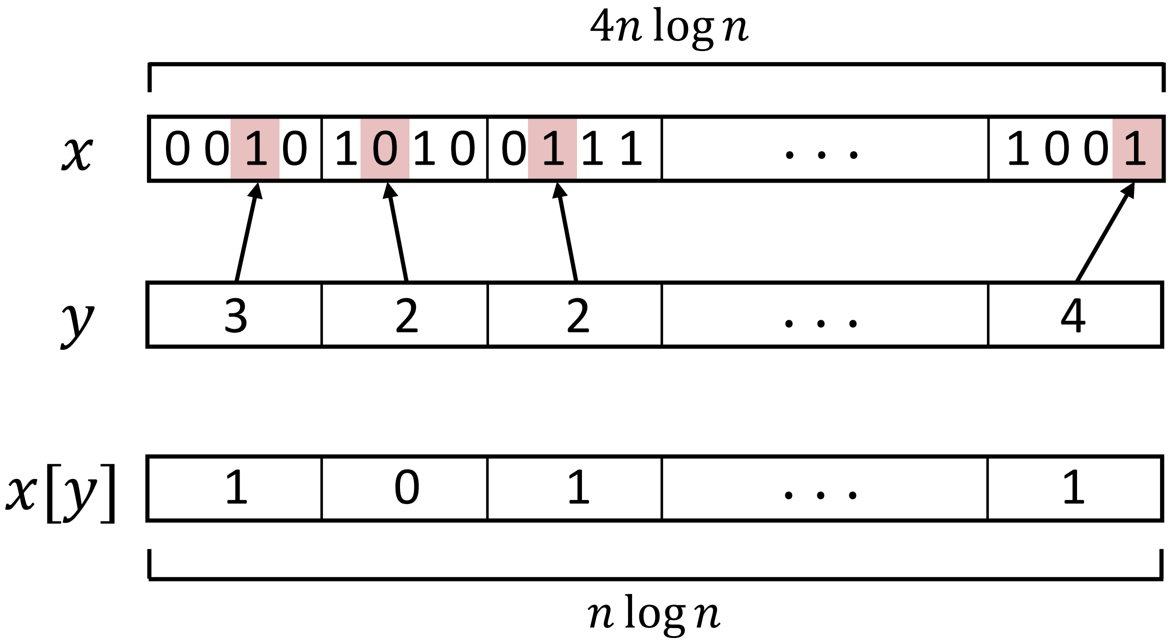


$$h_z : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$$

$$h_z(i) = i^{th} \text{ block in } z$$

$$Col(z) = \begin{cases} 0 \ \text{ if } \ h_z \text{ is 1–to–1} & \Rightarrow h_z(i) \text{ is uniformly distributed} \\ 1 \ \text{ if } \ h_z \text{ is 2–to–1} & \Rightarrow h_z(i) \text{ is far from uniform} \end{cases}$$

Collision Problems



$$PCol(x, y) = Col(x[y])$$

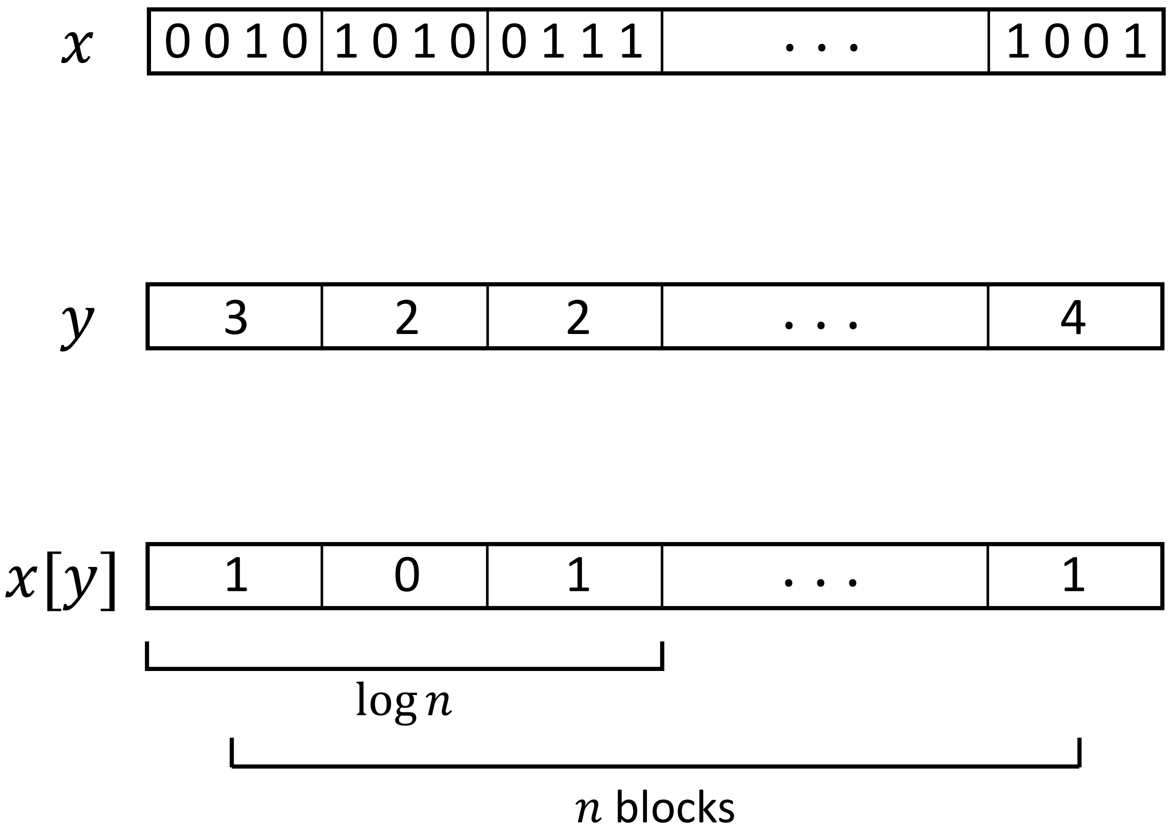
$$R(PCol) > \Omega(n^{1/3})$$

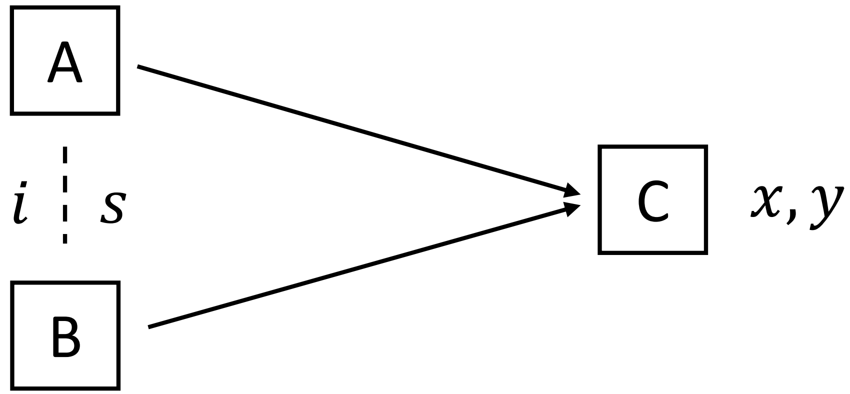
([Amb05,Kut05] + [She11])

$$\text{linCDS}(PCol) > \Omega(n^{1/6})$$

(left + [GKW15])

Collision Problems





Use PSM [FKN94] to send:

- $h_{x[y]}(i)$ if $s = 0$
- $r \leftarrow \{0,1\}^{\log n}$ if $s = 1$

If $PCol(x, y) = 0$, both are the same distribution, else they are far apart.

Closure

h - Boolean formula over $\{0,1\}^m$ of size σ

CDS for each of

$$f_1, \dots, f_m$$

Comm: $t_1, \dots, t_m$
Rand : $\rho_1, \dots, \rho_m$

CDS for

$$h(f_1, \dots, f_m)$$

Comm: $\sigma \cdot poly(t_i, \rho_i)$
Rand : $\sigma \cdot poly(t_i, \rho_i)$

Construction uses transformations for Statistical Difference [SV03,Oka96], and PSM protocols [FKN94].

Amplification

CDS for f

Single-bit secret
Corr: 0.1
Priv: 0.1
Comm: t

$\longrightarrow$

CDS for f

k-bit secret
Corr: $2^{-\Omega(k)}$
Priv: $2^{-\Omega(k)}$
Comm: $O(kt)$

Construction uses constant-rate ramp secret-sharing schemes [CCGdHV07].

Incomparable version follows from the Polarization Lemma [SV03].

Lower Bound

There exists a predicate $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ for which any perfect (single-bit) CDS requires communication at least $0.99n$.

Proven by reduction to the PSM lower bound of [FKN94].

Earlier bound was explicit, $\Omega(\log n)$ bits. [GKW15]

Amortization

For any predicate $f\colon\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and $m > 2^{2^{2n}}$, there is a perfect CDS protocol for f with m-bit secrets with communication complexity $O(mn)$.

Proven using techniques from the amortization of branching programs [Pot16].

m-fold repetition of best known general protocol [LVW17]: $m \cdot 2^{O(\sqrt{n \log n})}$

Summary

We prove the following properties of CDS:

- **Lower Bounds:** Non-explicit, $\Omega(n)$.
- **Separation:** From insecure communication and linear CDS.
- **Amortization:** $O(n)$ per bit of secret, if there are more than $2^{2^{2n}}$ bits.
- **Closure:** Under composition with formulas.
- **Amplification:** Of correctness and privacy from constant to $2^{-\Omega(k)}$ with $O(k)$ blowup.

To note:

- Connections with Statistical Difference and SZK.
- Barriers to PSM lower bounds.