Optimal Linear Multiparty Conditional Disclosure of Secrets Protocols

Amos Beimel and Naty Peter

Ben-Gurion University

Asiacrypt 2018

December 6, 2018
Conditional Disclosure of Secrets (CDS)
Conditional Disclosure of Secrets (CDS)

[GertnerIshaiKushilevitzMalkin98]

• A function: $f: [N]^k \rightarrow \{0, 1\}$
• Each party has a private input
• The parties know a secret $s$
• Common randomness $r$
• Referee knows $x_1, \ldots, x_k$
• Each party sends one message

Correctness: If $f(x_1, \ldots, x_k) = 1$, Ref learns $s$
Privacy: If $f(x_1, \ldots, x_k) = 0$, Ref learns nothing

Learns $s$ if and only if $f(x_1, \ldots, x_k) = 1$
Motivation for Multiparty CDS Protocols

- A simple and interesting primitive

- Used to construct:
  - Secret-sharing for *uniform* access structures
  - Secret-sharing for *general* access structures
  - Attribute-based encryption (ABE)
  - Symmetric private information retrieval (SPIR)
  - And more
Our Results

• We study linear multiparty CDS protocols
  – Many applications require linear protocols
  – Used to construct linear secret sharing with share size $O(2^{0.999n})$ [LiuVaikuntanathan18]

• We construct optimal CDS protocols for general functions

• We construct efficient CDS protocols for sparse and dense functions
  – Sparse = the number of 1-inputs of $f$ is at most $N^\gamma$
  – Dense = the number of 0-inputs of $f$ is at most $N^\gamma$

• We show a transformation from CDS protocols to secret sharing for uniform access structures

• We present lower bounds for linear CDS protocols and for linear secret sharing schemes for uniform access structures
  – Our protocols for general functions are optimal
Linear CDS Protocols: Definition

- A CDS protocol is linear if every message sent to the referee is a linear combination of the secret and the randomness

- **Input**: A secret $s \in \mathbb{F}$
- **Common randomness**: Field elements $r_1, \ldots, r_\ell \in \mathbb{F}$
- **The message of $P_i$**:
  - A vector over $\mathbb{F}$
  - Each coordinate is a linear combination of $s$ and $r_1, \ldots, r_\ell$
  - The combination can depend on $x_i$

- Equivalently, a CDS protocol is linear if the reconstruction function of the secret is a linear combination of the elements in the messages it gets
Example: A Simple Linear CDS Protocol

- A secret $s \in \mathbb{F}_2$
- A function $f: \{0, 1\}^k \rightarrow \{0, 1\}$ s.t. $f(x_1, \ldots, x_k) = x_1 \land \cdots \land x_k$
- Common randomness $r_1, \ldots, r_{k-1} \in \mathbb{F}_2$

1. For $1 \leq i \leq k - 1$, the message of $P_i$ on input $x_i$ is $m_i = x_i \cdot r_i$
2. Message of $P_k$ on input $x_k$ is $m_k = x_k \cdot r_1 \oplus \cdots \oplus x_k \cdot r_{k-1} \oplus x_k \cdot s$

- If $x_1 = \cdots = x_k = 1$ then Ref computes

$$\bigoplus_{i=1}^{k} m_i = \bigoplus_{i=1}^{k-1} x_i \cdot r_i \oplus x_k \cdot r_1 \oplus \cdots \oplus x_k \cdot r_{k-1} \oplus x_k \cdot s = s$$

- Message size $k$
Known Upper Bounds for CDS Protocols

• Let \( f : [N]^k \to \{0, 1\} \) be a function

• There is a \textit{linear} CDS protocol for every function with message size \( O(N^k) \) [GertnerIshaiKushilevitzMalkin98]

• For \( k = 2 \), there is a \textit{linear} CDS protocol for every function with message size \( O(N^{1/2}) \) [GayKerenidisWee15]

• There is a \textit{non-linear} CDS protocol for every function with message size \( 2^{\tilde{O}(\sqrt{k \log N})} \) [LiuVaikuntanathanWee18]

• For \( k = 2 \), the message size is \( 2^{\tilde{O}(\sqrt{\log N})} \ll O(N) \)
Questions

• Can we construct more efficient linear CDS protocols for general functions?

• Can we construct efficient linear CDS protocols for a sparse or a dense function $f$?
Main Result: Linear CDS Protocols

• **Thm 1**: Let $f: [N]^k \rightarrow \{0, 1\}$ be a function. Then, there is a linear CDS protocol for $f$ with message size $O(N^{(k-1)/2})$
  
  – Same result was independently and in parallel proven by [LiuVaikuntanathanWee18]

• Example: If $k = 5$ then the message size is $O(N^2)$

• **Thm 2**: Let $f: [N]^k \rightarrow \{0, 1\}$ be a function s.t. the number of 1-inputs of $f$ is at most $N^\gamma$. Then, there is a linear CDS protocol for $f$ with message size $\tilde{O}(N^{\gamma(k-1)/(k+1)})$
  
  – Same result for a function $f$ s.t. the number of 0-inputs of $f$ is at most $N^\gamma$

• Example: If $k = 5, \gamma = 2$ then the message size is $\tilde{O}(N^{4/3})$
Construction Technique

• Our linear CDS protocol for any function \( f: [N]^k \rightarrow \{0, 1\} \) with message size \( \mathcal{O}(N^{(k-1)/2}) \) is constructed as follows:

1. We start with a linear 2-party CDS protocol

2. We use the 2-party protocol to construct a linear 3-party CDS protocol

3. We simulate the 3-party protocol to get a linear \( k \)-party CDS protocol
Warm-up: Linear 2-party CDS implicit in [GayKerenidisWee15]

- A secret $s \in \{0, 1\}$ and a function $f: [N] \times [N] \rightarrow \{0, 1\}$
- Common randomness $r_1, \ldots, r_N \in \{0, 1\}$
- Denote the 2 parties by Alice and Bob

1. Message of Alice on input $a$ is

   $$m_1 = s \oplus \bigoplus_{y, f(a,y)=0} r_y$$

2. Message of Bob on input $b$ is

   $$m_2 = r_1, \ldots, r_{b-1}, r_{b+1}, \ldots, r_N$$

   - If $f(a, b) = 1$ then $r_b$ does not appear in $m_1$
     ⇒ The referee can unmask $s$

- Message size $N$
Example: Linear 2-party CDS

- A secret $s \in \{0, 1\}$ and a function $f: [3] \times [3] \rightarrow \{0, 1\}$
- $f(a, b) = 1$ if and only if $a = b = 2$
- Common randomness $r_1, r_2, r_3 \in \{0, 1\}$

- Recall: Alice’s message is $m_1 = s \oplus \bigoplus_{y,f(a,y)=0} r_y$

- If $a = b = 2$ then $m_1 = s \oplus r_1 \oplus r_3$ and $m_2 = r_1, r_3$

- If $a = 2, b = 3$ then $m_1 = s \oplus r_1 \oplus r_3$ and $m_2 = r_1, r_2$
Our Basic Protocol: Linear 3-party CDS

- A secret $s \in \{0, 1\}$ and a function $f: [N] \times [N] \times [N] \rightarrow \{0, 1\}$
- Common randomness $r_1, \ldots, r_N, q_1, \ldots, q_N \in \{0, 1\}$
- For every $z \in [N]$, let
  $$s_z = s \oplus q_z \oplus \bigoplus_{y,f(a,y,z)=0} r_y$$
- Denote the 3 parties by Alice, Bob, and Charlie
  1. Message of Alice on input $a$ is $m_1 = s_1, \ldots, s_N$
  2. Message of Bob on input $b$ is $m_2 = r_1, \ldots, r_{b-1}, r_{b+1}, \ldots, r_N$
  3. Message of Charlie on input $c$ is $m_3 = q_c$
- Message size $2N$
General Protocol: Linear $k$-party CDS

- A function $f: [N]^k \rightarrow \{0, 1\}$
- Let $k' = (k - 1)/2$ (assume $k > 3$ is odd)

- We simulate the 3-party protocol:

  - The message size of this protocol is $O(N^{k'}) = O(N^{(k-1)/2})$
Main Result: Lower Bounds for CDS

Using the results of [BeimelFarrasMintzPeter17] we get:

• **Thm 3**: There exists a function $f$ such that in any linear CDS protocol for $f$ with a one-bit secret, the size of at least one message is $\Omega(k^{-1} \cdot N^{(k-1)/2})$

• Conclusion 1: Our linear CDS protocol is optimal

• Conclusion 2: Gap between linear and non-linear CDS protocols

• **Thm 4**: There exists a function $f$ s.t. the number of 1-inputs of $f$ is at most $N^\gamma$ s.t. in any linear CDS protocol for $f$ with a one-bit secret, the size of at least one message is $\Omega(k^{-1} \cdot N^{\gamma(k-1)/2k})$
  
  — Same result for a function $f$ in which the number of 0-inputs of $f$ is at most $N^\gamma$

• Example: If $k = 5, \gamma = 2$ then the message size is $\Omega(N^{4/5})$, compared to the message size of $O(N^{4/3})$ in our protocol
Conclusions

• CDS ⇒ ABE, SPIR, Secret sharing for uniform and general A.S.
• Linear CDS ⇒ Linear secret sharing with share size $O(2^{0.999n})$

Our Results:
• Optimal linear CDS protocols for general functions
• Linear CDS protocols for sparse and dense functions
• An Efficient transformation from CDS protocols to uniform A.S.
• Lower bounds on the message size in linear CDS protocols and on the total size of the shares in linear schemes for uniform A.S.

Open problems:
• Show optimal (linear) CDS protocols for sparse and dense functions
• Close the gap for the message size of non-linear CDS protocols
Thanks!