Optimal Linear Multiparty Conditional Disclosure of Secrets Protocols

Amos Beimel and Naty Peter

Ben-Gurion University

Asiacrypt 2018

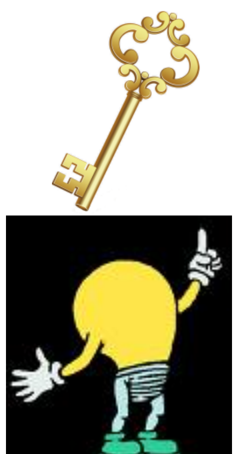
December 6, 2018

Conditional Disclosure of Secrets (CDS)

x_1 x_2 x_3 x_4



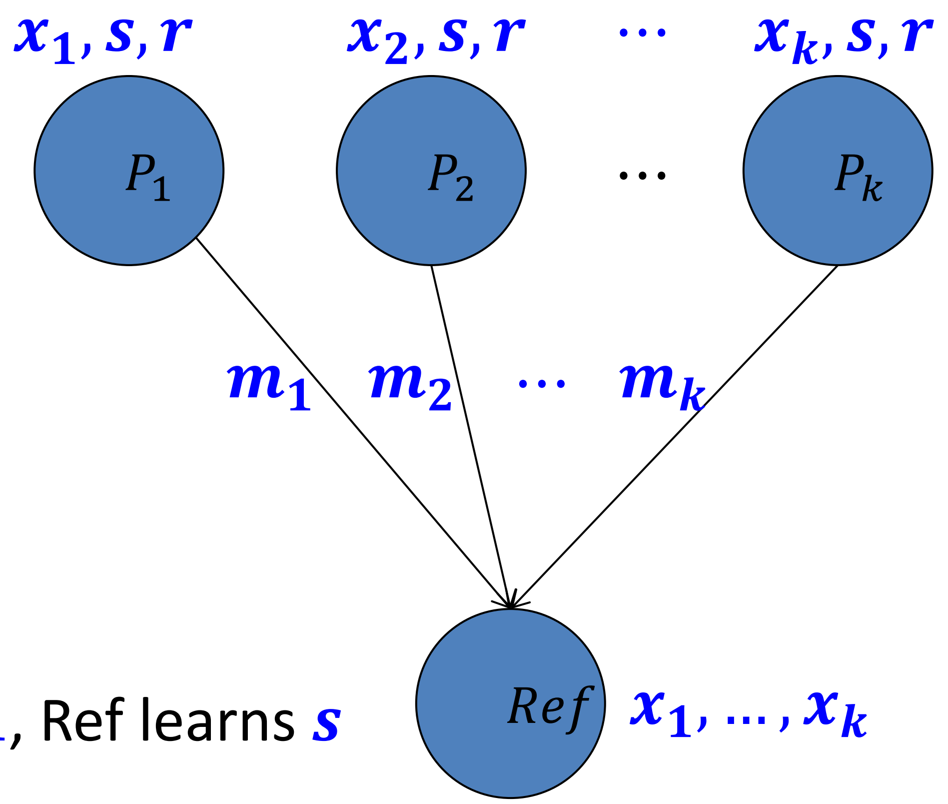

m_1 m_2 m_3 m_4



Conditional Disclosure of Secrets (CDS)

[GertnerIshaiKushilevitzMalkin98]

- A function: $\boldsymbol{f}: [N]^k \to \{0,1\}$
- Each party has a private input
- The parties know a secret $\boldsymbol{s}$
- Common randomness $\boldsymbol{r}$
- Referee knows $\boldsymbol{x_1, \dots, x_k}$
- Each party sends one message
- <u>Correctness</u>: If $\boldsymbol{f(x_1, \dots, x_k) = 1}$, Ref learns $\boldsymbol{s}$
- <u>Privacy</u>: If $\boldsymbol{f(x_1, \dots, x_k) = 0}$, Ref learns nothing



Learns $\boldsymbol{s}$ if and only if $\boldsymbol{f(x_1, \dots, x_k) = 1}$

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 $\boldsymbol{O}(\mathbf{2}^{\mathbf{0.999}\boldsymbol{n}})$ [LiuVaikuntanathan18]
- We construct optimal CDS protocols for general functions
- We construct efficient CDS protocols for sparse and dense functions
  - Sparse $=$ the number of $\mathbf{1}$-inputs of $\boldsymbol{f}$ is at most $\boldsymbol{N}^{\boldsymbol{\gamma}}$
  - Dense $=$ the number of $\mathbf{0}$-inputs of $\boldsymbol{f}$ is at most $\boldsymbol{N}^{\boldsymbol{\gamma}}$
- 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 $\boldsymbol{s} \in \mathbb{F}$
- Common randomness: Field elements $\boldsymbol{r_1, \dots, r_\ell} \in \mathbb{F}$
- The message of $\boldsymbol{P_i}$:
  - A vector over $\mathbb{F}$
  - Each coordinate is a linear combination of $\boldsymbol{s}$ and $\boldsymbol{r_1, \dots, r_\ell}$
  - The combination can depend on $\boldsymbol{x_i}$

- 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. $f(x_1, \dots, x_k) = x_1 \wedge \cdots \wedge x_k$
- Common randomness $r_1, \dots, r_{k-1} \in \mathbb{F}_2$

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 $\boldsymbol{f}: [\boldsymbol{N}]^{\boldsymbol{k}} \rightarrow \{\mathbf{0}, \mathbf{1}\}$ be a function
- There is a *linear* CDS protocol for every function with message size $\boldsymbol{O}\left(\boldsymbol{N}^{\boldsymbol{k}}\right)$ [GertnerIshaiKushilevitzMalkin98]
- For $\boldsymbol{k} = \mathbf{2}$, there is a *linear* CDS protocol for every function with message size $\boldsymbol{O}\left(\boldsymbol{N}^{\mathbf{1/2}}\right)$ [GayKerenidisWee15]
- There is a *non-linear* CDS protocol for every function with message size $\mathbf{2}^{\widetilde{\boldsymbol{O}}\left(\sqrt{\boldsymbol{k} \log \boldsymbol{N}}\right)}$ [LiuVaikuntanathanWee18]
- For $\boldsymbol{k} = \mathbf{2}$, the message size is $\mathbf{2}^{\widetilde{\boldsymbol{O}}\left(\sqrt{\log \boldsymbol{N}}\right)} \ll \boldsymbol{O}(\boldsymbol{N})$

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 $\boldsymbol{f}$?

Main Result: Linear CDS Protocols

- Thm 1: Let $\boldsymbol{f}: [\boldsymbol{N}]^{\boldsymbol{k}} \rightarrow \{\mathbf{0}, \mathbf{1}\}$ be a function. Then, there is a linear CDS protocol for $\boldsymbol{f}$ with message size $\boldsymbol{O}\left(\boldsymbol{N}^{(\boldsymbol{k}-\mathbf{1})/\mathbf{2}}\right)$
  - Same result was independently and in parallel proven by [LiuVaikuntanathanWee18]
- Example: If $\boldsymbol{k} = \mathbf{5}$ then the message size is $\boldsymbol{O}\left(\boldsymbol{N}^{\mathbf{2}}\right)$

- Thm 2: Let $\boldsymbol{f}: [\boldsymbol{N}]^{\boldsymbol{k}} \rightarrow \{\mathbf{0}, \mathbf{1}\}$ be a function *s.t. the number of* $\mathbf{1}$*-inputs of* $\boldsymbol{f}$ *is at most* $\boldsymbol{N}^{\boldsymbol{\gamma}}$. Then, there is a linear CDS protocol for $\boldsymbol{f}$ with message size $\widetilde{\boldsymbol{O}}\left(\boldsymbol{N}^{\boldsymbol{\gamma}(\boldsymbol{k}-\mathbf{1})/(\boldsymbol{k}+\mathbf{1})}\right)$
  - Same result for a function $\boldsymbol{f}$ *s.t. the number of* $\mathbf{0}$*-inputs of* $\boldsymbol{f}$ is at most $\boldsymbol{N}^{\boldsymbol{\gamma}}$
- Example: If $\boldsymbol{k} = \mathbf{5}, \boldsymbol{\gamma} = \mathbf{2}$ then the message size is $\widetilde{\boldsymbol{O}}\left(\boldsymbol{N}^{\mathbf{4/3}}\right)$

Construction Technique

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

1. We start with a linear $\mathbf{2}$-party CDS protocol
2. We use the $\mathbf{2}$-party protocol to construct a linear $\mathbf{3}$-party CDS protocol
3. We simulate the $\mathbf{3}$-party protocol to get a linear k-party CDS protocol

Warm-up: Linear $\mathbf{2}$-party CDS

implicit in [GayKerenidisWee15]

- A secret $s \in \{0,1\}$ and a function $f: [N]\times[N] \to \{0,1\}$
- Common randomness $r_1, \dots, r_N \in \{0,1\}$
- 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

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

- If $f(a,b) = 1$ then r_b does not appear in m_1

  ➔ The referee can unmask s

- Message size N

Example: Linear $\mathbf{2}$-party CDS

- A secret $s \in \{0,1\}$ and a function $f: [3] \times [3] \to \{0,1\}$
- $f(a,b) = 1$ 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 $\mathbf{3}$-party CDS

- A secret $\boldsymbol{s} \in \{\mathbf{0}, \mathbf{1}\}$ and a function $\boldsymbol{f}: [\boldsymbol{N}]\times[\boldsymbol{N}]\times[\boldsymbol{N}] \to \{\mathbf{0}, \mathbf{1}\}$
- Common randomness $\boldsymbol{r}_{\mathbf{1}}, \dots, \boldsymbol{r}_{\boldsymbol{N}}, \boldsymbol{q}_{\mathbf{1}}, \dots, \boldsymbol{q}_{\boldsymbol{N}} \in \{\mathbf{0}, \mathbf{1}\}$
- For every $\boldsymbol{z} \in [\boldsymbol{N}]$, let

$$\boldsymbol{s}_{\boldsymbol{z}} = \boldsymbol{s} \oplus \boldsymbol{q}_{\boldsymbol{z}} \oplus \bigoplus_{\boldsymbol{y}, \boldsymbol{f}(\boldsymbol{a}, \boldsymbol{y}, \boldsymbol{z}) = \mathbf{0}} \boldsymbol{r}_{\boldsymbol{y}}$$

- Denote the $\mathbf{3}$ parties by Alice, Bob, and Charlie

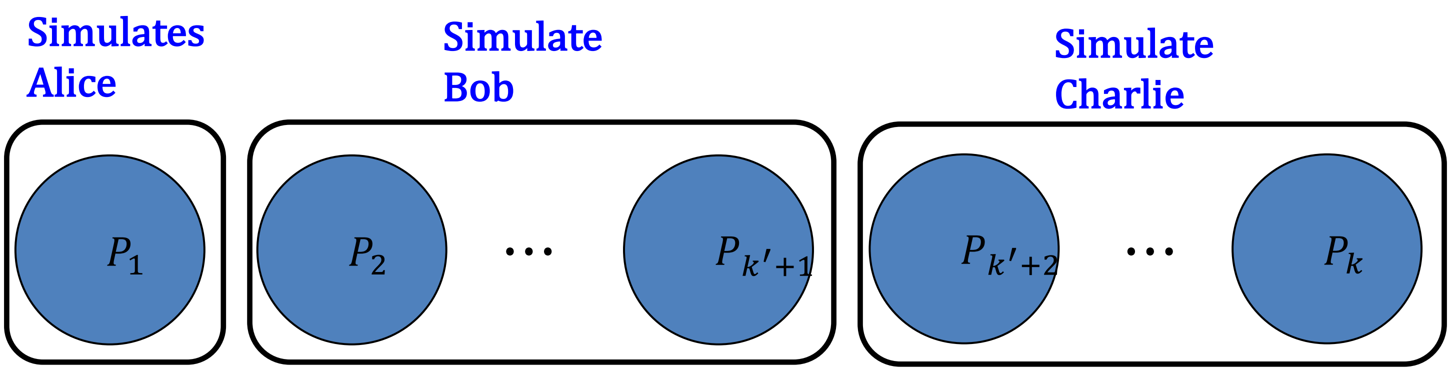
1. Message of Alice on input $\boldsymbol{a}$ is $\boldsymbol{m}_{\mathbf{1}} = \boldsymbol{s}_{\mathbf{1}}, \dots, \boldsymbol{s}_{\boldsymbol{N}}$
2. Message of Bob on input $\boldsymbol{b}$ is $\boldsymbol{m}_{\mathbf{2}} = \boldsymbol{r}_{\mathbf{1}}, \dots, \boldsymbol{r}_{\boldsymbol{b}-\mathbf{1}}, \boldsymbol{r}_{\boldsymbol{b}+\mathbf{1}}, \dots, \boldsymbol{r}_{\boldsymbol{N}}$
3. Message of Charlie on input $\boldsymbol{c}$ is $\boldsymbol{m}_{\mathbf{3}} = \boldsymbol{q}_{\boldsymbol{c}}$

- Message size $\mathbf{2}\boldsymbol{N}$

General Protocol: Linear $\boldsymbol{k}$-party CDS

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

- We simulate the $\boldsymbol{3}$-party protocol:



- The message size of this protocol is $\boldsymbol{O}\left(\boldsymbol{N}^{\boldsymbol{k}'}\right) = \boldsymbol{O}\left(\boldsymbol{N}^{(\boldsymbol{k}-\boldsymbol{1})/\boldsymbol{2}}\right)$

Main Result: Lower Bounds for CDS

Using the results of [BeimelFarrasMintzPeter17] we get:

- Thm 3: There exists a function $\boldsymbol{f}$ such that in any linear CDS protocol for $\boldsymbol{f}$ with a one-bit secret, the size of at least one message is $\boldsymbol{\Omega(k^{-1} \cdot N^{(k-1)/2})}$
- Conclusion 1: Our linear CDS protocol is optimal
- Conclusion 2: Gap between linear and non-linear CDS protocols

- Thm 4: There exists a function $\boldsymbol{f}$ *s.t. the number of* $\mathbf{1}$*-inputs of* $\boldsymbol{f}$ *is at most* $\boldsymbol{N^{\gamma}}$ s.t. in any linear CDS protocol for $\boldsymbol{f}$ with a one-bit secret, the size of at least one message is $\boldsymbol{\Omega(k^{-1} \cdot N^{\gamma(k-1)/2k})}$
  - Same result for a function $\boldsymbol{f}$ *in which the number of* $\mathbf{0}$*-inputs of* $\boldsymbol{f}$ *is at most* $\boldsymbol{N^{\gamma}}$
- Example: If $\boldsymbol{k=5, \gamma=2}$ then the message size is $\boldsymbol{\Omega\left(N^{4/5}\right)}$, compared to the message size of $\boldsymbol{\tilde{O}\left(N^{4/3}\right)}$ in our protocol

Conclusions

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

<u>Our Results</u>:

- 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.

<u>Open problems</u>:

- Show optimal (linear) CDS protocols for sparse and dense functions
- Close the gap for the message size of non-linear CDS protocols

Thanks!