New Communication-Efficient Oblivious Transfer Protocols Based on Pairings

Helger Lipmaa

Cybernetica AS, Estonia

September 18, 2008

Outline

Motivation: Functionality

- Alice wants to obtain a song from Bob's database
- Alice does *not* want Bob to know that she listens to C-pop
- Bob actually wants to get payed for providing the service
- Oblivious transfer: cryptographic protocol that provides exactly that
  - OT without Bob's privacy: CPIR
- Database has n elements, all elements are ℓ bits long

Motivation: Efficiency

- Protocol rounds — as few as possible
  - Communicating takes time
- Communication — as little as possible
- Computation — as little as possible
- Resources are both important for large databases ($n = 2^{20}$) and for small databases ($n = 2$)

Our Contribution

- A clear paradigm to construct 2-message $(n, 1)$-OT protocols
  - Bob (server) cryptocomputes and adds two polynomials
  - One polynomial takes care of correctness
  - Another polynomial takes care of privacy
- Concrete protocols, OTS and OTX
  - Efficient for different values of ℓ, n
- OTS/OTX can be used to guarantee Bob's privacy in any CPIR
  - Efficient CPIR-to-OT transformation

Basic Idea

- Assume Alice wants to retrieve D_σ, where $D = (D_0, \ldots, D_{n-1})$ is Bob's database
- We assume the existence of t-homomorphic cryptosystem
  - Given $\mathcal{E}nc(m_i), \ldots, \mathcal{E}nc(m_k)$, it's possible to cryptocompute $\mathcal{E}nc(f(m_1, \ldots, m_k))$ for degree-t polynomials t
  - $t = 1$: additively homomorphic cryptosystems (Paillier, ...)
  - $t = 2$: Boneh-Goh-Nissim 2007 (based on bilinear pairings)
  - $t > 2$: no candidates (yet)
- Alice sends $\mathcal{E}nc(\sigma)$ to Bob
- Bob cryptocomputes $\mathcal{E}nc(\mathrm{Correct}(\sigma) + CDS(\sigma))$
  - Correct guarantees correctness
  - CDS = *Conditional Disclosure of Secrets* guarantees privacy
  - $\deg(\mathrm{Correct}), \deg(CDS) \leq t$

Basic Idea: OTS

- Wlog, assume $t \mid n$
- $\mathsf{Correct}_i^t(\sigma)$ — unique polynomial such that

$$\mathsf{Correct}_i^t(\sigma) = \begin{cases} D_\sigma \ , & \lceil \sigma/t \rceil = i \ , \\ 0 \ , & \text{otherwise} \ . \end{cases}$$

- $\mathsf{CDSS}_i^{t-1}(\sigma)$ — unique polynomial such that

$$\mathsf{CDSS}_i^t(\sigma) = \begin{cases} 0 \ , & \lceil \sigma/t \rceil = i \ , \\ \star \ , & \text{otherwise} \ . \end{cases}$$

- Thus $\mathsf{Correct}_i^{t-1}(\sigma) + \mathsf{CDSS}_i^t(\sigma)$ is D_σ if $\lceil \sigma/t \rceil = i$, and $\star$ otherwise
- $(n, 1)$-OTS is a parallel repetition of n/t copies of $(t, 1)$-OTS
  - At ith copy Alice receives $\mathcal{E}nc(\mathsf{Correct}_i^{t-1}(\sigma) + \mathsf{CDSS}_i^t(\sigma))$ — either D_σ or $\star$

Basic Idea: OTX

- Wlog, assume $(t+1) \mid n$
- $\mathsf{Correct}_i^t(\sigma)$ — unique polynomial such that

$$\mathsf{Correct}_i^t(\sigma) = \begin{cases} D_\sigma \ , & \lceil \sigma/(t+1) \rceil = i \ , \\ 0 \ , & \text{otherwise} \ . \end{cases}$$

- $\mathsf{CDSX}_i^t(\sigma)$ — unique polynomial such that

$$\mathsf{CDSX}_i^t(\sigma) = \begin{cases} 0 \ , & \lceil \sigma/(t+1) \rceil = i \ , \\ \star \ , & \text{otherwise} \ . \end{cases}$$

- Thus $\mathsf{Correct}_i^t(\sigma) + \mathsf{CDSX}_i^t(\sigma)$ is D_σ if $\lceil \sigma/(t+1) \rceil = i$, and $\star$ otherwise
- $(n, 1)$-OTX repeats $n/(t+1)$ copies of $(t+1, 1)$-OTS
  - At ith copy Alice receives $\mathcal{E}nc(\mathsf{Correct}_i^t(\sigma) + \mathsf{CDSX}_i^t(\sigma))$ — either D_σ or $\star$

"Minor Complication" with OTX

- $\mathsf{CDSX}_i^t(\sigma)$ — unique polynomial such that

$$\mathsf{CDSX}_i^t(\sigma) = \begin{cases} 0 \ , & \lceil \sigma/(t+1) \rceil = i \ , \\ \star \ , & \text{otherwise} \ . \end{cases}$$

- Problem: CDSX must have degree $t+1$ and we can only cryptocompute degree-t polynomials
- We let Alice send to Bob encryptions of $(\sigma_2, \sigma_1, \sigma_0)$, such that $\sigma = (t+1)\sigma_2 + t\sigma_1 + \sigma_0$, $\sigma_1 \in \{0,1\}$, $\sigma_0 \in \{0,\ldots,t-1\}$ and $\sigma_0 = 0 \vee \sigma_1 = 0$
- $\mathsf{CDSX}_i^t(\sigma_2,\sigma_1,\sigma_0) := \star(\sigma_2 - i) + \star(\sigma_1 - 1)\sigma_1 + \star \cdot \prod_{i=0}^{t-1}(\sigma_0 - i) + \star\sigma_1\sigma_0$
- Clearly CDSX_i^t is a degree-t polynomial such that $\mathsf{CDSX}_i^t(\sigma) = 0$ if $\lceil \sigma/(t+1) \rceil = i$, and $\star$ otherwise

Comparison: OTS vs OTX

- OTS: Alice sends 1 public key and 1 ciphertext to Bob, Bob returns $\lceil n/t \rceil$ ciphertexts
- OTX: Alice sends 1 public key and 3 ciphertexts to Bob, Bob returns $\lceil n/(t+1) \rceil$ ciphertexts
- $n = 2$, $t = 2$: OTS sends 2 ciphertexts only
  - In previous $(2,1)$-OT protocols, at least 3 ciphertexts were sent
- $n = 3$, $t = 2$: OTS sends 3 ciphertexts
- For large n, OTX is more efficient

CPIR-to-OT Transformation

- CPIR: like OT but does not guarantee Bob's privacy
- Alice sends the first message of OTX to Bob
- Bob computes $D' = (\mathcal{E}nc(\star), \ldots, \mathcal{E}nc(D_\sigma), \ldots, \mathcal{E}nc(\star))$ as in OTX
- However, Bob does not send this to Alice but stores D' as a new database
- Alice and Bob execute CPIR on D'
- Clearly Alice receives $\mathcal{E}nc(D_\sigma)$ which she can decrypt
- Can parallelize — the transformation only takes 2 messages
- Computation/communication overhead: minimum
  - As shown in paper, the transformed OT has often less communication than original CPIR!

Open Problems

- OTS/OTX are more efficient for larger t
- For $t = 1$, they are comparable to known OT protocols
- For $t = 2$, they are more efficient in the number of ciphertexts
  - The only suitable known cryptosystem BGN has long ciphertexts
- No known ≥ 2-homomorphic cryptosystems
- Need to study!

Questions?