Verifiable Homomorphic Oblivious Transfer

and

Private Equality Test

Helger Lipmaa
Helsinki University of Technology
http://www.tcs.hut.fi/~helger

Overview of This Talk

- What are Oblivious Transfer and Private Equality Test?
- Building Block: Affine Cryptosystems
- New (Verifiable) Homomorphic Oblivious Transfer protocols
- New (Verifiable) Homomorphic Private Equality Tests
- Application: Proxy Verifiable HPET and Auctions

Overview of This Talk

- What are Oblivious Transfer and Private Equality Test?
- Building Block: Affine Cryptosystems
- New (Verifiable) Homomorphic Oblivious Transfer protocols
- New (Verifiable) Homomorphic Private Equality Tests
- Application: Proxy Verifiable HPET and Auctions

$\binom{n}{1}$-Oblivious Transfer

- Sender has private input, database $\mu = (\mu_1, \ldots, \mu_n)$
- Chooser has private input, index $\sigma \in [1, n]$
- Chooser and Sender participate in the two-party protocol
- Chooser has private output μ_σ
- Nothing more will be leaked. If $\sigma \notin [1, n]$, chooser gets garbage
- Numerous applications in cryptography

Verifiable $\binom{n}{1}$-Oblivious Transfer

- Sender has private input, database $\mu = (\mu_1, \ldots, \mu_n)$
- Chooser has private input, index $\sigma \in [1, n]$
- Chooser and Sender participate in the two-party protocol
- Chooser has private output μ_σ and commitments to μ_i for $i \in [1, n]$
- Nothing more will be leaked
- Numerous applications in cryptography

Verifiable $\binom{n}{1}$-Oblivious Transfer

- Sender has private input, database $\mu = (\mu_1, \ldots, \mu_n)$
- Chooser has private input, index $\sigma \in [1, n]$
- Chooser and Sender participate in the two-party protocol
- Chooser has private output μ_σ and commitments to μ_i for $i \in [1, n]$
- Nothing more will be leaked. *If $\sigma \notin [1, n]$, chooser gets garbage*
- Numerous applications in cryptography

Private Equality Test

- Sender has private input, W_{Sen}
- Chooser has private input, W_{Cho}
- Chooser and Sender participate in the two-party protocol
- Chooser has private output $[W_{Sen} = W_{Cho}]$ (one bit)
- Nothing more will be leaked.

Verifiable Private Equality Test

- Sender has private input, W_{Sen}
- Chooser has private input, W_{Cho}
- Chooser and Sender participate in the two-party protocol
- Chooser has private output $[W_{Sen} = W_{Cho}]$ (one bit) and a commitment to W_{Sen}
- Nothing more will be leaked

Overview of This Talk

- What are Oblivious Transfer and Private Equality Test?
- Building Block: Affine Cryptosystems
- New (Verifiable) Homomorphic Oblivious Transfer protocols
- New (Verifiable) Homomorphic Private Equality Tests
- Application: Proxy Verifiable HPET and Auctions

Affine Cryptosystems, 1/4

- A public-key cryptosystem is a triple $\Pi = (G_\Pi, E, D)$ of key generation, encryption and decryption algorithms
- Denote the plaintext space by $\mathcal{M}_\Pi(x)$, where x is the private key
- $\mathcal{R}_\Pi(x)$ is the randomness space and $\mathcal{C}_\Pi(x)$ is the ciphertext space
- Π is homomorphic:

$$E_K(m_1; r_1)E_K(m_2; r_2) = E_K(m_1 + m_2; r_1 \circ r_2)$$

Affine Cryptosystems, 2/4

- For two random variables (distributions) X and Y over discrete support U, define their *statistical difference* as

$$\Delta(X||Y) := \max_{S \subseteq U} |\Pr[X \in S] - \Pr[Y \in S]| \ .$$

- Π is ε-*affine* if there exist two PPT algorithms (S, T), s.t. for any pair of private and public keys (x, K),

$$\max_{a,b \in \mathcal{M}_\Pi(x), a \neq 0} \Delta\left(S(1^k, K)a + b || T(1^k, K)\right) \leq \varepsilon_k \ .$$

Affine Cryptosystems, 3/4

- Π is perfectly affine if it is 0-affine and statistically affine if it is $(1/2 - \varepsilon)$-affine.

- Π is computationally affine if it is affine w.r.t. any a, b that can be efficiently generated

Affine Cryptosystems, 4/4

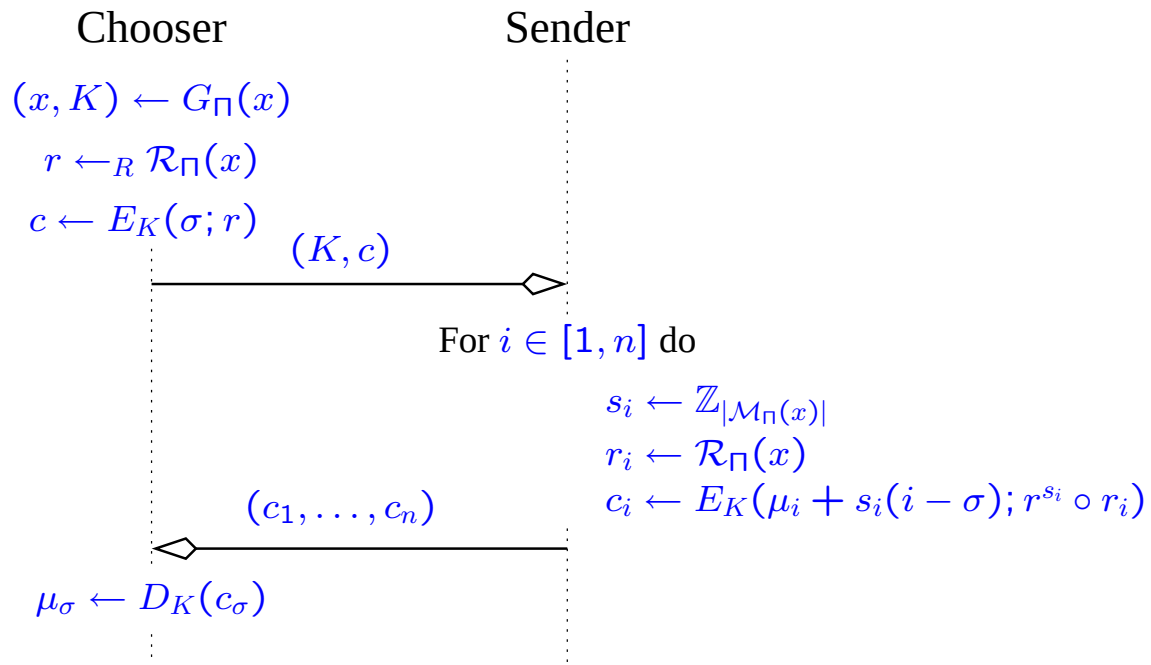
- Π is perfectly affine if $\mathcal{M}_\Pi(x)$ is a cyclic group of known order
- Π is computationally affine if $\mathcal{M}_\Pi(x)$ is a cyclic group, where it is hard for the decrypter to factor $|\mathcal{M}_\Pi(x)|$
- If decrypter can factor $\mathcal{M}_\Pi(x)$ then Π is not affine!
- Perfectly affine: ElGamal
- Computationally affine:
  - ⋆ Damgård-Jurik [DJ03], Bresson-Catalano-Pointcheval

Overview of This Talk

- What are Oblivious Transfer and Private Equality Test?
- Building Block: Affine Cryptosystems
- New (Verifiable) Homomorphic Oblivious Transfer protocols
- New (Verifiable) Homomorphic Private Equality Tests
- Application: Proxy Verifiable HPET and Auctions

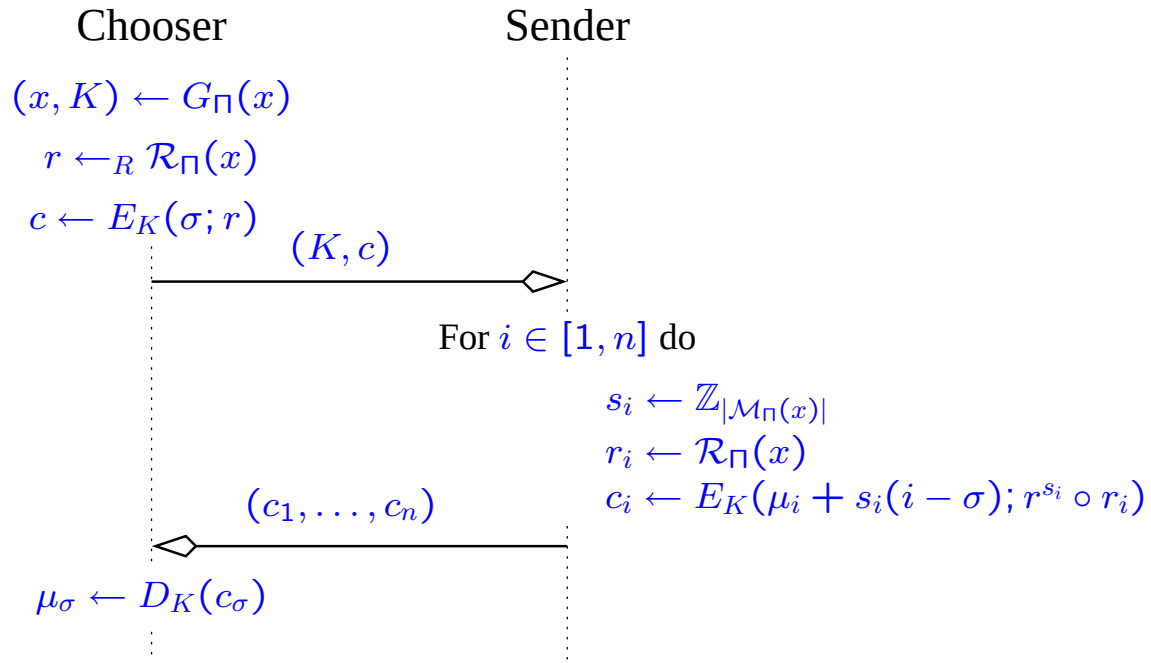
Aiello-Ishai-Reingold OT Protocol *AIR*

Assume that $\Pi = (G_\Pi, E, D; S, T)$ is a perfectly affine homomorphic cryptosystem



The New Homomorphic OT Protocol *HOT*

Assume that $\Pi = (G_\Pi, E, D; S, T)$ is an affine homomorphic cryptosystem



Comparison

- When Π is perfectly affine, HOT=AIR: perfect sender-privacy
- When Π is computationally affine: computational sender-privacy
  - ⋆ AIR was not defined for composite $|\mathcal{M}_{\Pi}(x)|$
- If Π is not affine, sender-privacy can be trivially broken

Weak sender-privacy

- There are many homomorphic cryptosystems that are not affine
- It would be nice to extend HOT to such PKCs
- Idea: weaken the security requirement

$\binom{n}{1}$-Oblivious Transfer: Weak Security

- Sender has private input, database $\mu = (\mu_1, \ldots, \mu_n)$. Chooser has private input, index $\sigma \in [1, n]$
- Chooser has private output μ_σ
- Nothing more will be leaked
- If $\sigma \notin [1, n]$, chooser gets some information about *one* element μ_i, $i \in [1, n]$
- Sufficient in many applications (i.e., pay per view)

Weak Sender-Privacy of HOT

Theorem. HOT is weakly sender-private if the smallest prime divisor of $|\mathcal{M}_{\Pi}(x)|$ is $\geq n$.

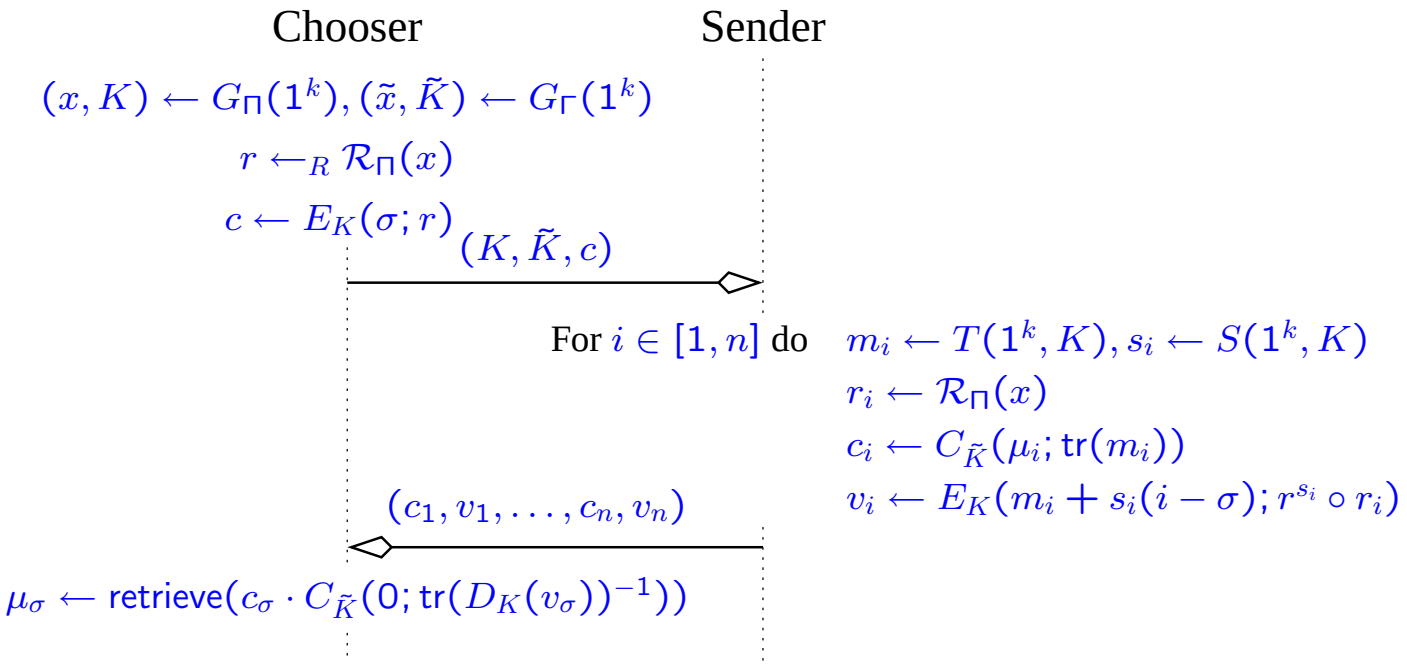
Weak Sender-Privacy of HOT

Theorem. HOT is weakly sender-private if the smallest prime divisor of $|\mathcal{M}_{\Pi}(x)|$ is $\geq n$.

Π	Security	Weak security
ElGamal	Perfect	Perfect
DJ03	Computational	Perfect
DJ01	—	Perfect
Paillier	—	Perfect
Naccache-Stern	—	Perfect (possibly)
Okamoto-Uchiyama	—	Perfect (possibly)

Verifiable Homomorphic OT Protocol *VHOT*

Assume that $\Pi = (G_\Pi, E, D; S, T)$ is an affine homomorphic cryptosystem, $\Gamma = (G_\Gamma, C)$ is a homomorphic commitment scheme, $\mathsf{tr} : \mathcal{M}_\Pi(x) \to \mathcal{R}_\Gamma(\tilde{x})$ and $\mathsf{retrieve} : C_{\tilde{K}}(m; 1) \mapsto m$



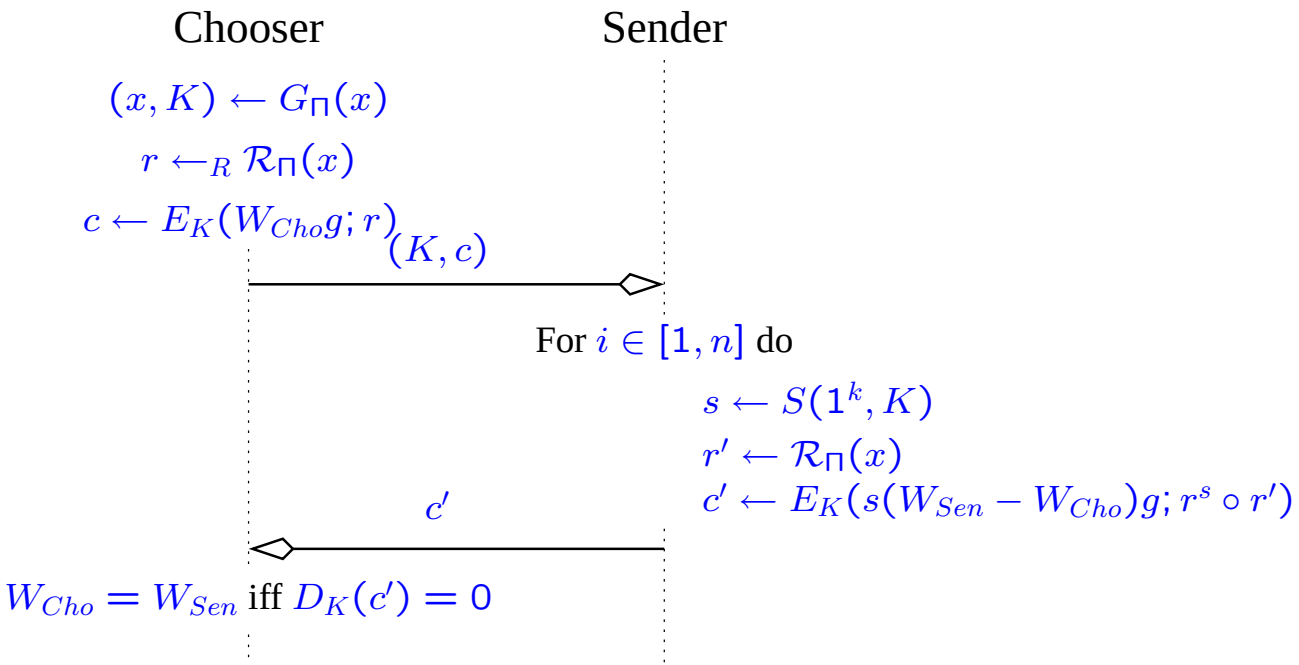
Security of the VHOT protocol

- Perfectly sender-private when Γ is perfectly hiding, tr is injection, $|\mathcal{M}_\Pi| = |\mathcal{R}_\Gamma|$ is a prime
- Statistically sender-private when Γ is statistically hiding, $|\mathcal{M}_\Pi| \approx |\mathcal{R}_\Gamma|$, ...
- Perfect privacy: Π is ElGamal and Γ is Pedersen (with the same plaintext group)
  Drawback: $\mathsf{retrieve} : g^m \longrightarrow m$ involves computation of discrete logarithm (ok if m is known to be small)
- Statistical privacy: Π is ElGamal and Γ is CGHN [CGHN01], then $\mathsf{retrieve}$ is an efficient function

VHOT: Comparison with Previous Work

- The only previous two-round verifiable $\binom{n}{1}$-OT was by Ambainis, Jakobsson and Lipmaa [AJL04]
- AJL was statistically private and retrieve was inefficient
- VHOT with suitable Π and Γ is either perfectly private *or* has efficient retrieve

Homomorphic PET



Homomorphic PET: Discussion

- Sender/chooser-private under the same settings as the HOT protocol
- Can be made verifiable

Proxy verifiable HPET and Application

- Proxy setting: P acts as an intermediate proxy between the chooser and several senders. Importantly, P will not get to know whether $W_{Cho} = W_{Sen_i}$ without the help of Cho

- Application in the auctions [LAN02] where the bidders had to prove in ZK that their bid was/wasn't equal to the highest bid: with proxy verifiable HPET, they can do it before they or the auctioneer gets to know the highest bid

- Therefore, a bidder or the auctioneer cannot discontinue the payment enforcement procedure when the results are not to his or her likings

Conclusions

- HOT: extension of the AIR OT protocol to a wider variety of settings
- Definition of affine cryptosystems
- Weak security fot OT protocols: sufficient in many applications
- New efficient verifiable OT protocol
- 2-round PET protocol, and its verifiable variant
- Proxy verifiable PET protocol, and an application

Questions?

?