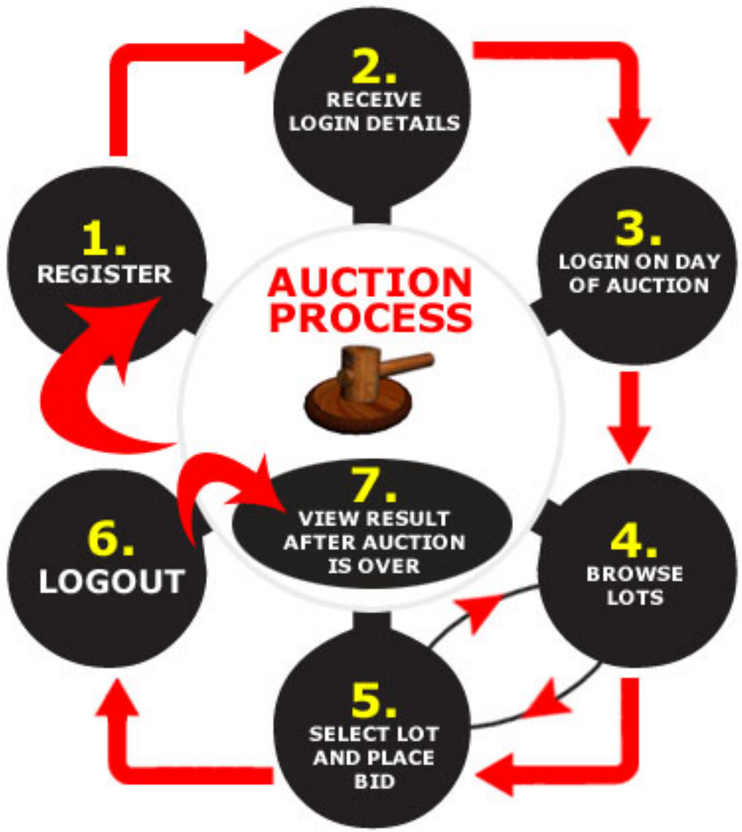
VI. Commitment schemes & oblivious transfer



What if you don't trust the auctioneer to keep bids to himself?

- You should not disclose your bid to the auctioneer or any other person until all bids are in. (hiding)
- Nobody should be able to modify their bids after placing them. (binding)

⇒ want a sealed electronic envelope!

Commitment schemes

Definition 6.1 Let $l : \mathbb{N} \to \mathbb{R}$ be a polynomial. A commitment scheme $\mathbb{K}$ for messages of length l(k) is a triple of ppts $(\text{Gen}, \text{Comm}, \text{Open})$, where

1. $\text{Gen}(1^k)$ outputs public parameters pp with $|pp| \geq k$.
2. Comm takes as input 1^k, public parameters $pp \in \text{Gen}(1^k)$, and a message $m \in \{0,1\}^{l(k)}$. It outputs a pair (c,d) of commitment c and open value d.
3. Open takes as input 1^k, public parameters $pp \in \text{Gen}(1^k)$, a commitment c, and an open value d. It ouputs $m \in \{0,1\}^{l(k)}$, or the failure symbol $\perp$.

For every k, every $pp \in \text{Gen}(1^k)$, and every message $m \in \{0,1\}^{l(k)}$: $\text{Open}_{pp}\left(1^k, \text{Comm}_{pp}(1^k, m)\right) = m$.

Commitment schemes

For realizations message space often $\mathbb{Z}_q$ rather then $\{0,1\}^{l(k)}$.
Can easily modifiy this.

$\mathbb{K}$ commitment scheme for messages of length l(k),
$pp \in Gen(1^k)$, and $m \in \{0,1\}^{l(k)}$. Define random variable R_m as follows:

R_m :

1. $(c,d) \leftarrow Comm_{pp}(1^k, m)$
2. return c

Commitment schemes - Hiding

$\mathbb{K}$ commitment scheme for messages of length g(k), $pp \in Gen(1^k)$, and $m \in \{0,1\}^{l(k)}$. Define random variable R_m as follows:

R_m :

1. $(c,d) \leftarrow Comm_{pp}(1^k, m)$
2. return c

Definition 6.2 Let $\mathbb{K}$ be a commitment scheme for messages of length l(k). $\mathbb{K}$ is called (perfectly) hiding, if for all $k \in \mathbb{N}$, all $pp \in Gen(1^k)$, and all $m, m' \in \{0,1\}^{l(k)}$ the random variables R_m and $R_{m'}$ are distributed identically.

The forging game

$\mathbb{K}$ commitment scheme, A ppt

Commitment forging game $\text{Comm-forge}_{A,\mathbb{K}}(k)$

1. $pp \leftarrow \text{Gen}(1^k)$.
2. $(c, d, \tilde{d}) \leftarrow A(1^k, pp)$
3. Output of experiment is 1, if and only if
   (a) $\text{Open}_{pp}(1^k, c, d) \neq \perp \wedge \text{Open}_{pp}(1^k, c, \tilde{d}) \neq \perp$
   (b) $\text{Open}_{pp}(1^k, c, d) \neq \text{Open}_{pp}(1^k, c, \tilde{d})$

Definition 6.3 Commitment scheme $\mathbb{K}$ is called (computationally) binding, if for every ppt adversary A there is a negligible function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ such that

$$\Pr\left[\text{Comm-forge}_{A,\mathbb{K}}(k) = 1\right] \leq \mu(k).$$

Pedersen commitment scheme

Gen on input 1^k chooses primes p,q such that $q \mid p-1$ and $q > 2^k$, chooses generator z of $\mathbb{Z}_p^*$ and sets $g := z^{p-1/q}$, chooses $e \leftarrow \mathbb{Z}_q^*$, sets $h := g^e$ and pp:=(p,q,g,h)

Comm on input $1^k, pp \in Gen(1^k)$, and message $m \in \mathbb{Z}_q$:

1. $d' \leftarrow \mathbb{Z}_q, d := (m, d')$
2. $c := g^m h^{d'} \bmod p$
3. output $(c,d) \in \mathbb{Z}_p^* \times (\mathbb{Z}_q \times \mathbb{Z}_q)$

Open on input $1^k, pp \in Gen(1^k)$, and $(c,d) \in \mathbb{Z}_p^* \times (\mathbb{Z}_q \times \mathbb{Z}_q)$, $d = (m, d')$, output m if $c = g^m h^{d'} \bmod p$, otherwise output $\perp$.

The subgroup discrete logarithm problem

Let Gen be a ppt that on input 1^k

- choose primes p,q such that $q \mid p-1$ and $q \geq 2^k$
- chooses a generator z for $\mathbb{Z}_p^*$ and sets $g := z^{(p-1)/q}$.

Let A be a ppt.

Subgroup DL game $\mathrm{SDL}_{A,Gen}(k)$

1. Run Gen(1^k) to obtain (p,q,g).
2. $e \leftarrow \mathbb{Z}_q, h := g^e \bmod p$.
3. A is given (p,q,g) and h. A outputs $e' \in \mathbb{Z}_q$.
4. Output of experiment is 1, if and only if $g^{e'} = h \bmod p$.

Write $\mathrm{SDL}_{A,Gen}(k) = 1$, if output is 1.

The subgroup discrete logarithm problem

Subgroup DL game $SDL_{A,Gen}(k)$

1. Run $Gen(1^k)$ to obtain (p,q,g).
2. $e \leftarrow \mathbb{Z}_q, h := g^e \bmod p$.
3. A is given (p,q,g) and h. A outputs $e' \in \mathbb{Z}_q$.
4. Output of experiment is 1, if and only if $g^{e'} = h \bmod p$.

Write $SDL_{A,Gen}(k) = 1$, if output is 1.

Definition 5.4 (restated) The SDL problem is hard relative to the generation algorithm Gen if for every ppt adversary A there is a negligible function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ such that

$$\Pr\left[SDL_{A,Gen}(k) = 1\right] \leq \mu(n).$$

Pedersen commitment scheme

Theorem 6.4

1. The Pedersen commitment scheme is (perfectly) hiding.
2. If the SDL problem is hard relative to the generation algorithm Gen (ignoring the last element), then the Pedersen commitment scheme is (computationally) binding.

Commitment schemes and Σ-protocols

Fact Using trapdoor commitment schemes every Σ-protocol can be transformed into a three round interactive protocol that has (computational) perfect zero-knowledge.

Oblivious transfer – 1-out-of-2 (1/2-OT)

2 participants:

- sender
- receiver

sender's input: $(x_0, x_1) \in \{0,1\}^* \times \{0,1\}^*$

receiver's input: $\sigma \in \{0,1\}$

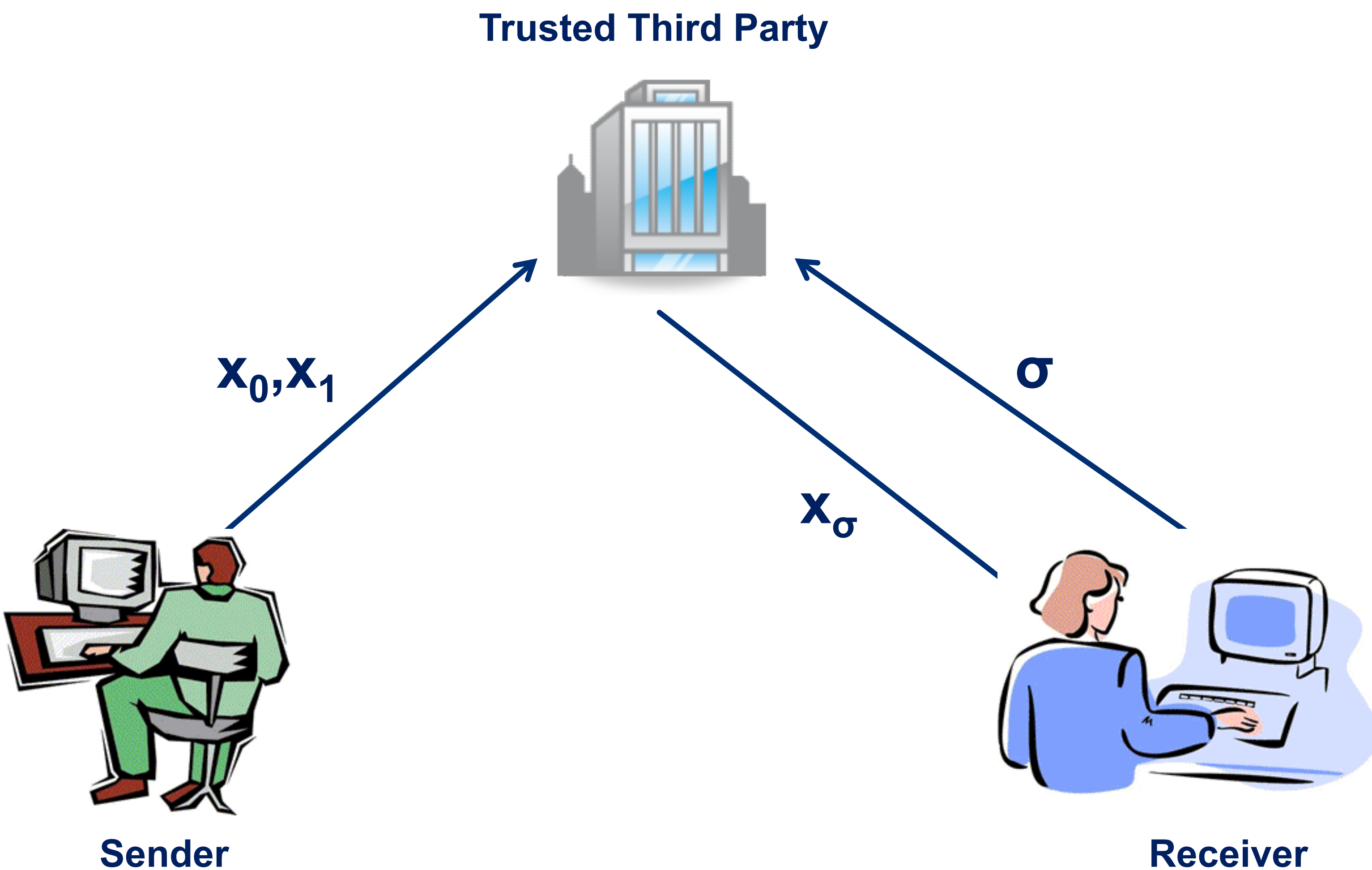
receiver obtains x_σ

sender obtains nothing ($= \varepsilon$)

Goals:

1. receiver learns nothing about $x_{1-\sigma}$
2. sender learns nothing about σ

1/2-OT in an ideal world and security



- Want to achieve the same functionality without TTP!
- Possible under many assumptions!

Summary

- authenticity, non-repudiation, and digital signatures
- unforgeable signatures
- RSA signatures, insecurity, hash-then-sign
- one-time signatures and Lamport signatures
- stateful signatures, tree-based signatures
- random oracles and RSA full-domain hash
- identification protocols, cheating provers and verifiers
- Fiat-Shamir, square roots modulo N, factoring, and cheating provers
- interactive protocols, zero-knowledge, perfect zero-knowledge

Summary

- zero-knowledge protocols and cheating verifiers
- Fiat-Shamir protocol and zero-knowledge
- proofs of knowledge and Σ-protocols
- Schnorr identification protocol
- discrete logarithm and cheating provers
- Schnorr protocol and zero-knowledge
- Okamoto protocol and zero-knowledge
- witness indistinguishability and witness hiding
- commitment schemes