# CSC3631 Cryptography - Anonymous Credentials

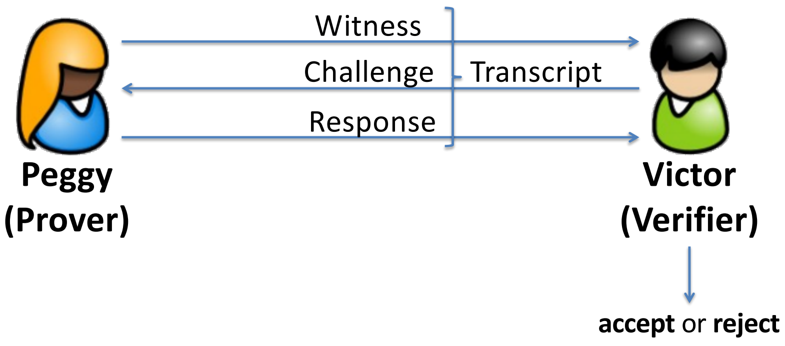
Thomas Gross





## Interactive Proof Systems

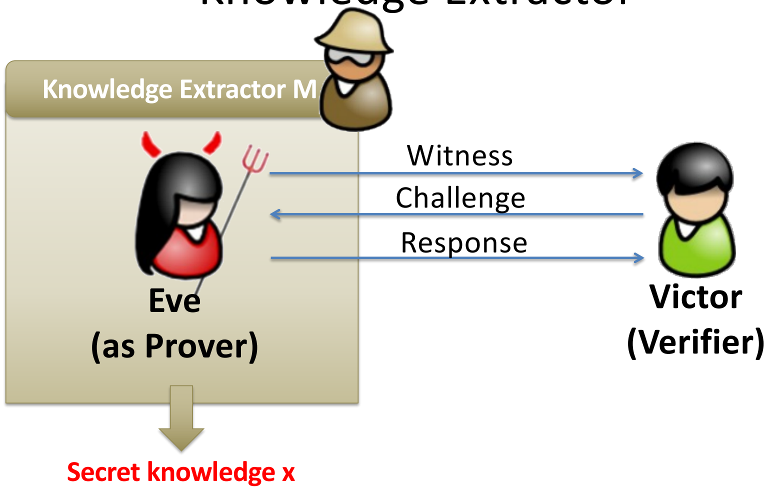
**Focusing on 3-round "Sigma" protocols**







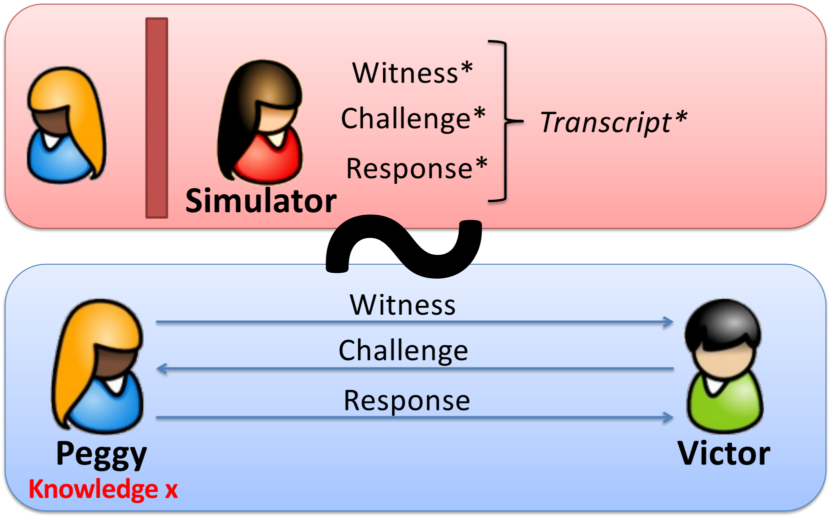

## Knowledge Extractor





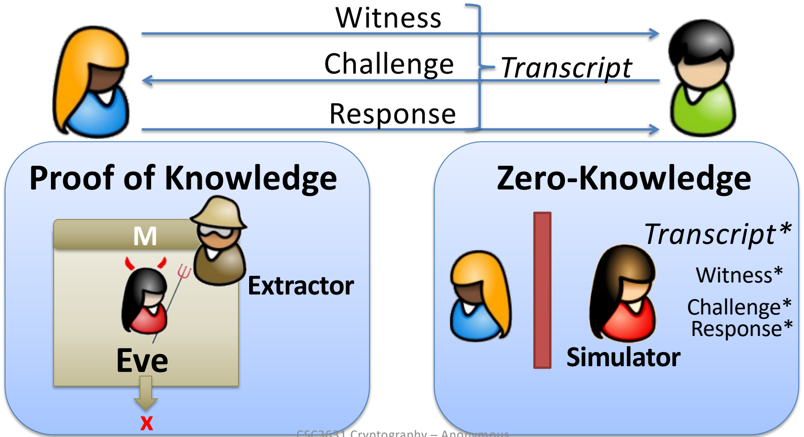



## Simulator



# Summary

**Interactive Proofs (3-round):**






6

# Zero-Knowledge Proof Notation

We can prove knowledge of **linear equations in the exponent**.

To **prove knowledge** of a secret x and a relation to a public y, we write:

**PK** $\{(x)$:

$y = g^x \pmod{p}$

$\}$



7

# Translates to a Schnorr Proof…

sk=(G, q, g, x) *pk*=(G, q, g, y)

*Witness:* $t = g^r$ (**mod** p)

*Challenge:* **random** c in $\{0,1\}^t < q$

*Response:* $s = r + cx$ (**mod** q)

**Peggy (Prover)** **Victor (Verifier)**

**PK** $\{(x)$:

$y = g^x \pmod{p}$

$\}$

**accept only if** $g^s \stackrel{?}{=} t y^c$



8

# … and a Signature Scheme

**(Fiat-Shamir)**

sk=(G, q, g, x) *pk*=(G, q, g, y)

*Witness:* $t = g^r$ (**mod** p)

*Challenge:* **“random”** c in $\{0,1\}^t < q$ c = **H**(m||t)

*Response:* $s = r - cx$ (**mod** q)

**Peggy (Signer)** **Victor (Verifier)**

**SPK** $\{(x)$:

$y = g^x \pmod{p}$

$\}$

**accept only if**

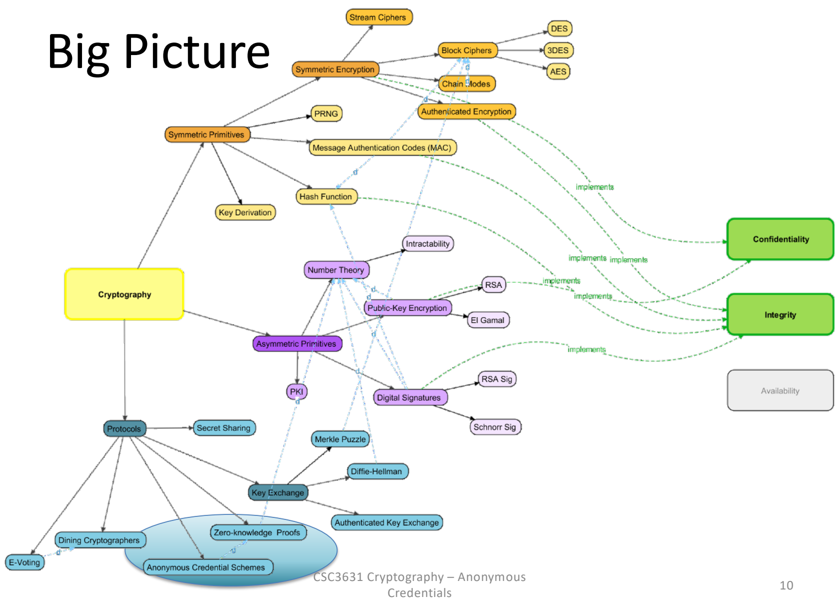
$t \stackrel{?}{=} g^s y^c$

$c \stackrel{?}{=} \mathbf{H}(m||t)$



9

# Big Picture








# Roadmap

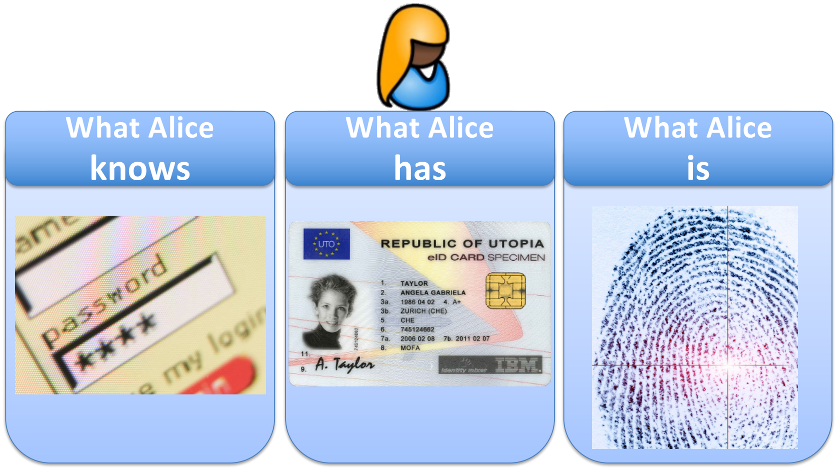
- **Privacy-preserving Authentication**
- Commitment Schemes
- Anonymous Credentials

**Goal for today:**
- **How do Anonymous Credentials work on a high level?**





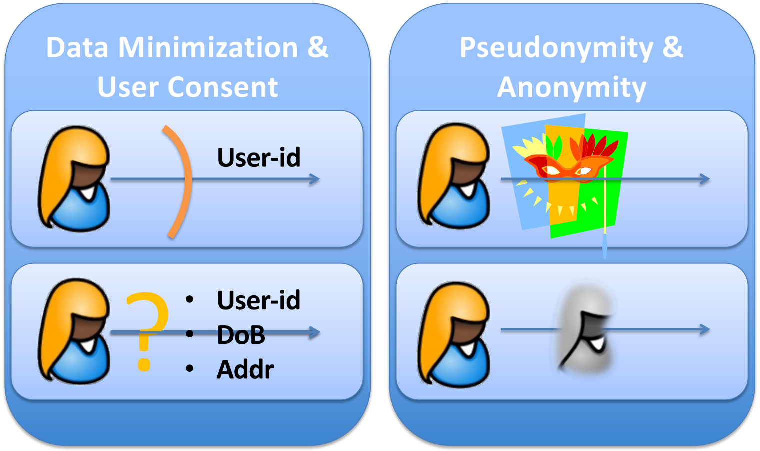
# Authentication
**(Usually wrt. unique identifier)**








# Privacy



## How well do Authentication and Privacy Interact?



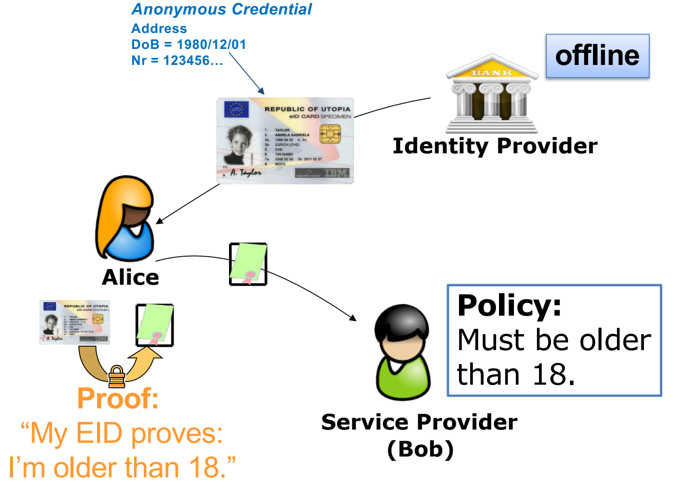


## Standard EID Authentication






## Attribute-based Credentials










## Roadmap

- Privacy-preserving Authentication
- **Commitment Schemes**
- Anonymous Credentials

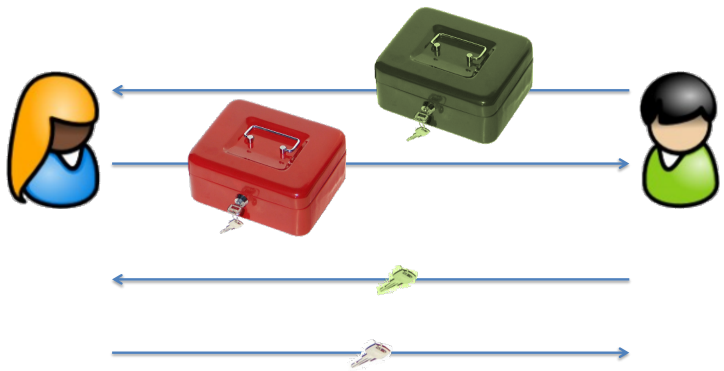
**Goal for today:**

- **How do Anonymous Credentials work on a high level?**

# How to play Scissor-Stone-Paper by e-mail?



# How to play Scissor-Stone-Paper by mail?





# Commitment Schemes

**Committing to a value while keeping it hidden.**

($C$, $r$) ← **Commit**($x$):

**Input:** Secret $x$

**Output:** Commitment $C$ and randomness $r$

**Accept** or **Reject** ← **Verify**($C$, $r$, $x$)

**Input:** Secret $x$, $r$, commitment $C$

**Output:** **Accept** only if the secret is indeed the one committed to



# Properties (Informal)

**Binding:**

The committer cannot change the committed value after the commitment.

**Hiding:**

The committed value is hidden from the verifier.

## Key Generation

**How to create a strong setting for prime-order groups?**

**GenGroup**($1^n$)

**Input:** key length $n$

**Create a cyclic group** $G$, sub-group of $(\mathbf{Z}_p)^*$
with generator $g$ with prime-order $q$.

**Choose random** $y$ in $\mathbf{Z}_q$

Compute **second generator** $h = g^y$ (**mod** $p$)

**Output:** $(G, q, g, h, p)$



## Pedersen Commitment

$(G, g, h, q, p) \leftarrow$ **GenGroup**($1^n$)


**Commit**($x$):

**Choose random** $r$ in $\mathbf{Z}_q$

Compute $C = g^x h^r$ (**mod** $p$)

**Verify**($C, r, x$):

Check $C \stackrel{?}{=} g^x h^r$ (**mod** $p$) is fulfilled



## Integer Commitment

$(N, R, S) \leftarrow$ **GenSRSAGroup**($1^n$)


**Commit**($x$):

**Choose random** $r$ in $\{0,1\}^l$

Compute $C = R^x S^r$ (**mod** $N$)

**Verify**($C, r, x$):

Check $C \stackrel{?}{=} R^x S^r$ (**mod** $N$) is fulfilled



## Security Properties

The Pedersen and the Integer Commitment schemes are **computationally binding** and **information-theoretically hiding**.

# Summary

Commitment schemes allow to commit to a message while hiding it.

**Key properties:**

**Binding** **and** **Hiding***

***)** Only one of the two can be information-theoretically strong.



# Roadmap

- Privacy-preserving Authentication
- Commitment Schemes
- **Anonymous Credentials**

**Goal for today:**

- **How do Anonymous Credentials work on a high level?**



# Foundations Anonymous Credentials

**Hardness:** Strong RSA (informal)

Given a public random element $\boldsymbol{Z}$, it is hard to compute a pair $(\boldsymbol{A}, \boldsymbol{e})$ such that

$$Z = A^e \pmod{N}$$

**Camenisch-Lysyanskaya Signature:**

$$Z = R^x S^v A^e \pmod{N}$$

**Signature:** $(A, e, v)$



# Quadratic Residues

- An integer $a$ is called a **quadratic residue** modulo $N$ if

  **gcd**$(a, N) = 1$ and $a = b^2 \pmod{N}$

  for some integer $b$.
- In this case, we say $b$ is a **square root** of $a$ modulo $N$.
- We call the group of quadratic residues modulo $N$: $\mathbf{QR}_N$.

## Camenisch-Lysyanskaya Key Generation

**GenSRSAGroup**($1^n$) and **GenCL**($1^n$)
**Input:** key length $n$

**Create special RSA modulus** $N=pq$; $p$, $q$ safe primes
$p = 2p'+1$, $q = 2p'+1$; $p'$ and $q'$ also prime.
Create generator $S$ (of Quadratic Residues $\mathbf{QR}_N$)
With group order $(p-1)(q-1)/4$
**Create group setup:** Choose at random $Z$, $R$ (in $\mathbf{QR}_N$)

**Output:** $pk=(N, S, Z, R)$, $sk=(p, q)$



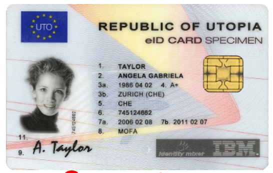


## Signing a hidden message

$C_x := R^x S^{v'} \pmod N$

$\sigma' := (A, e, v'')$

$v := v' + v''$




Random large prime $e$
Random $v''$ in $\{0, 1\}^{l_N+l_m+l}$
Compute $A$ such that
$Z = C_x S^{v''} A^e \pmod N$

Secret x $\sigma = (A, e, v)$

$A := (Z / C_x S^{v''})^{1/e} \pmod N$





## Security of Camenisch-Lysyanskaya

The Camnisch-Lysyanskaya (CL) signature scheme is **existentially unforgeable** for blocks of messages under the Strong RSA assumption.





## Re-Blinding

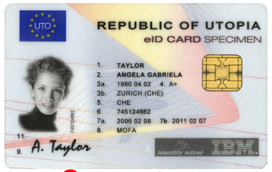
- **Choose random** $r$
- **Compute** $A' := AS^{-r} \pmod N$
- **Compute corresponding** $v' := v+er$
- $(A', e, v')$ is a valid signature as well.

- If $r$ is chosen uniformly random, then $A'$ is distributed randomly over $(\mathbf{Z}_N)^*$ (Blinding by exponentiation)

# Proving knowledge of a signed secret

Prove knowledge of $x$

$A'$, **SPK**$\{(x, e, v'):\ Z = R^x S^{v'} A'^e \pmod{N}\}$




Random $r$
$(A', v') :=$ **Reblind**$(A, r)$

Secret x $\quad \sigma = (A, e, v)$



# Summary

Modern authentication systems and EID cards will use zero-knowledge proofs of knowledge.

**Prove knowledge of attributes**

Fulfilling **policy statements**,

While keeping the attributes themselves **confidential**.