Removing the Strong RSA Assumption from Arguments over the Integers

Geoffroy Couteau, Thomas Peters, and David Pointcheval

École Normale Supérieure, CNRS, INRIA, PSL

June 14, 2017

Zero-Knowledge Argument

- Interactive protocol between a prover P and a verifier V;
- P knows a proof π of a statement;
- Example: I know a proof of Riemann hypothesis, but I do not want you to steal my million.

Correctness: if the proof is true, V will output "ok".

Soundness: No malicious prover P' can make V output "ok" on a wrong statement.

Zero-Knowledge: V learns nothing from the protocol, except that the statement is true.

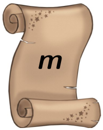
Zero-Knowledge Argument over the Integers

- Zero-knowledge proofs of relations between committed values play a fundamental role in cryptography
- We have efficient ZKA to prove algebraic relations between (finite) group elements
- Some important types of statements are not captured well by such relations (e.g.: proving that $a \geq b$)

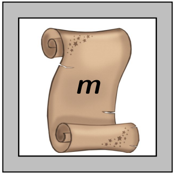
Observation: These statements are well capture by algebraic relations over *integers* (aka Diophantine relations)

Example: $x \geq 0 \Leftrightarrow \exists (x_0, x_1, x_2, x_3) \in \mathbb{Z}^4, x = \sum_i x_i^2$

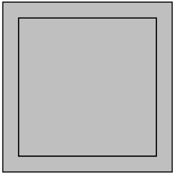
Commitment Schemes over Groups of Unknown Order



Commitment Schemes over Groups of Unknown Order

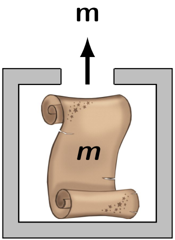


Commitment Schemes over Groups of Unknown Order



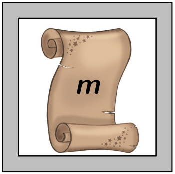
Hiding

Commitment Schemes over Groups of Unknown Order



Binding

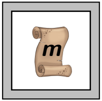
Commitment Schemes over Groups of Unknown Order



Fujisaki-Okamoto (1997):

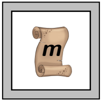
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown

Commitment Schemes over Groups of Unknown Order



Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

Commitment Schemes over Groups of Unknown Order

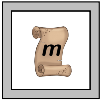


Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

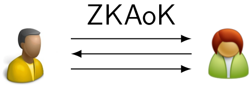
Anonymous Credentials | MPC | E-Cash | E-Voting

Group Sig. | Range Proofs | Auctions | PPSS

Commitment Schemes over Groups of Unknown Order



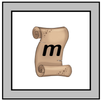
Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization



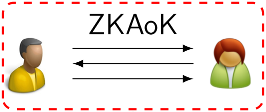
Anonymous Credentials | MPC | E-Cash | E-Voting

Group Sig. | Range Proofs | Auctions | PPSS

Commitment Schemes over Groups of Unknown Order



Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

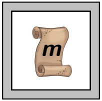


Strong-RSA

Anonymous Credentials | MPC | E-Cash | E-Voting

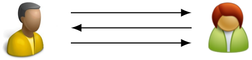
Group Sig. | Range Proofs | Auctions | PPSS

Commitment Schemes over Groups of Unknown Order



Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

ZKAoK

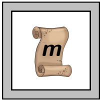


Strong-RSA

Anonymous Credentials | MPC | E-Cash | E-Voting

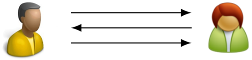
Group Sig. | Range Proofs | Auctions | PPSS

Commitment Schemes over Groups of Unknown Order



Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

ZKAoK



This work: RSA

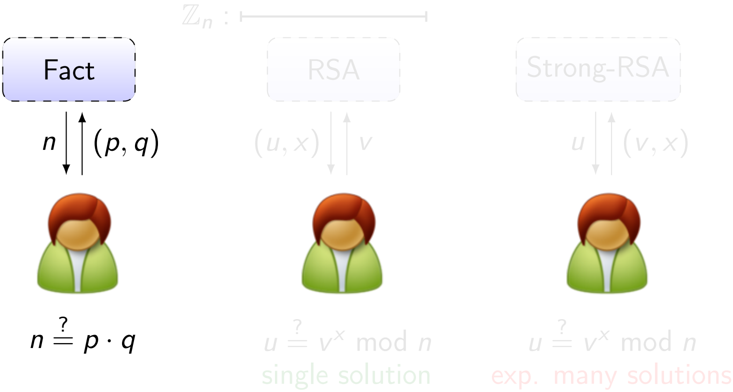
Anonymous Credentials | MPC | E-Cash | E-Voting

Group Sig. | Range Proofs | Auctions | PPSS

Preliminaries on RSA Groups

$\mathbb{Z}_n$, with $n = pq$, $p = 2p' + 1$, and $q = 2q' + 1$.

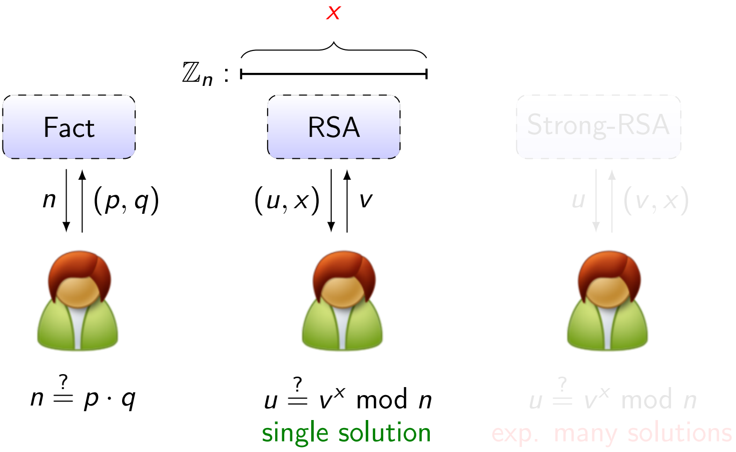
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

$\mathbb{Z}_n$, with $n = pq$, $p = 2p' + 1$, and $q = 2q' + 1$.

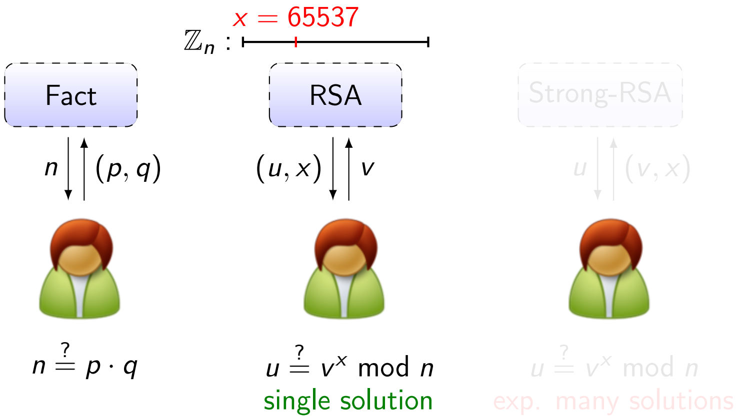
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

$\mathbb{Z}_n$, with $n = pq$, $p = 2p' + 1$, and $q = 2q' + 1$.

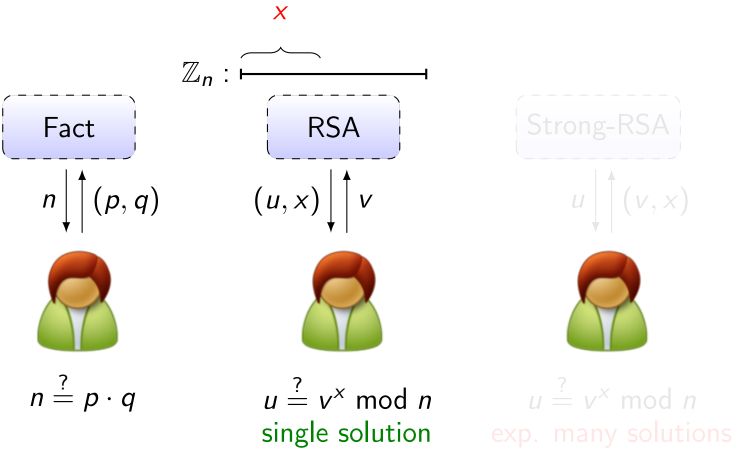
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

$\mathbb{Z}_n$, with $n = pq$, $p = 2p' + 1$, and $q = 2q' + 1$.

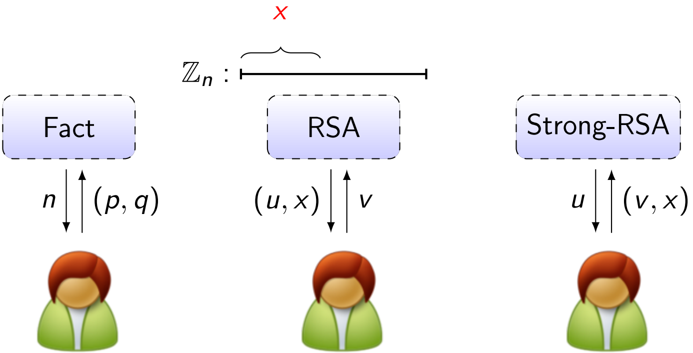
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

$\mathbb{Z}_n$, with $n = pq$, $p = 2p' + 1$, and $q = 2q' + 1$.

$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



$n \stackrel{?}{=} p \cdot q$

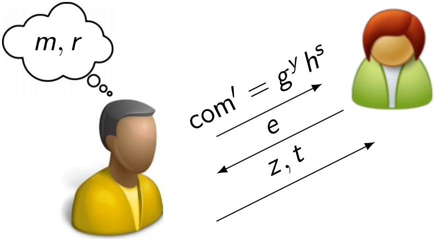
$u \stackrel{?}{=} v^x \bmod n$
single solution

$u \stackrel{?}{=} v^x \bmod n$
exp. many solutions

Zero-Knowledge Argument of Knowledge of an Opening

$n = p \cdot q$, $\langle g \rangle = \mathrm{QR}[n]$, $h^\alpha = g$

$$\mathrm{com} = g^m h^r$$



$z \leftarrow em + y$

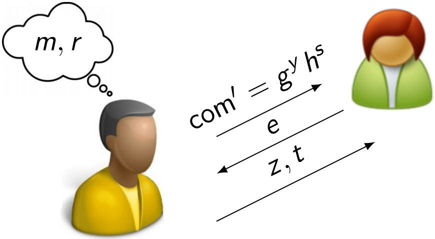
$t \leftarrow er + s$

V checks whether $\mathrm{com}^e \mathrm{com}' = g^z h^t$.

Zero-Knowledge Argument of Knowledge of an Opening

$n = p \cdot q$, $\langle g \rangle = \mathrm{QR}[n]$, $h^\alpha = g$

$$\boxed{\mathrm{com} = g^m h^r}$$



$$z \leftarrow em + y$$
$$t \leftarrow er + s$$

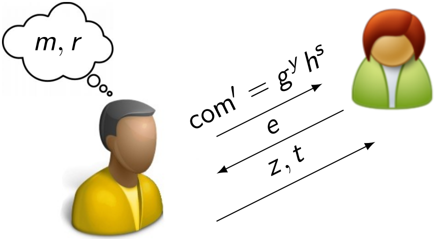
V checks whether $\mathrm{com}^e \mathrm{com}' = g^z h^t$.

Soundness. With rewinding, extract $(m, r) = \left(\frac{z_0 - z_1}{e_0 - e_1}, \frac{t_0 - t_1}{e_0 - e_1}\right)$

Zero-Knowledge Argument of Knowledge of an Opening

$n = p \cdot q$, $\langle g \rangle = \mathrm{QR}[n]$, $h^{\alpha} = g$

$$\boxed{\mathrm{com} = g^m h^r}$$



$z \leftarrow em + y$
$t \leftarrow er + s$

V checks whether $\mathrm{com}^e \mathrm{com}' = g^z h^t$.

Soundness. With rewinding, extract $(m, r) = \left(\frac{z_0 - z_1}{e_0 - e_1}, \frac{t_0 - t_1}{e_0 - e_1}\right)$

Requires inversions over the exponents of $\mathbb{G}$!

Our Solution in a Nutshell

The analysis considers a simulator that solves a strong-RSA challenge by interacting with a malicious prover who produces an accepting proof with probability ε.

- The simulator gets a random small RSA challenge x before the proof, and perfectly hides it in his interaction with the prover;
- We study the constraints on the exponent chosen by the adversary;
- We show information-theoretically that if the exponent is larger than $O(1/\varepsilon)$, some non-trivial relation is satisfied;
- This relation allows to factor the modulus, hence the exponent must remain smaller than $O(1/\varepsilon)$;
- Therefore, the exponent chosen by the prover is equal to x with non-negligible probability $O(\varepsilon)$, contradicting RSA.

Applications, Other Contributions

Applications.

- Relations between committed values (e.g. [CM99])
- Range proofs ([Lip03])

Other Contributions.

- Can convert an FO commitment (integers) into a Gennaro commitment (modulo a small prime)
- Allows integer ZK proofs with efficient verification

Thank you for your attention

Questions?