Removing the Strong RSA Assumption from Arguments over the Integers

Geoffroy Couteau, Thomas Peters, and David Pointcheval

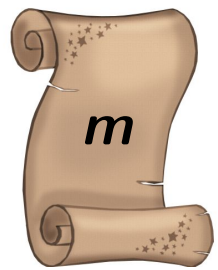
École Normale Supérieure, CNRS, INRIA, PSL

European Research Council

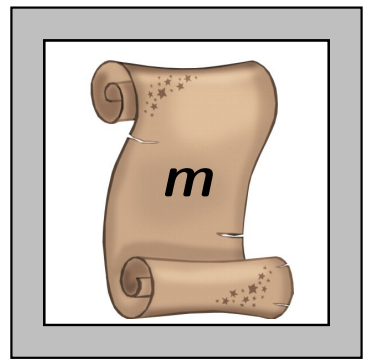
Established by the European Commission

May 2, 2017

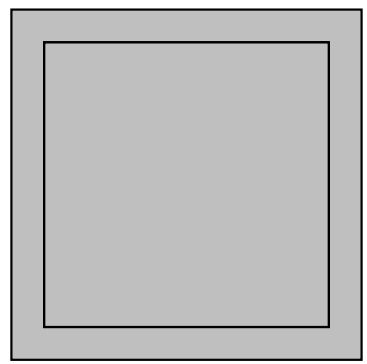
Commitment Schemes over Groups of Unknown Order



Commitment Schemes over Groups of Unknown Order

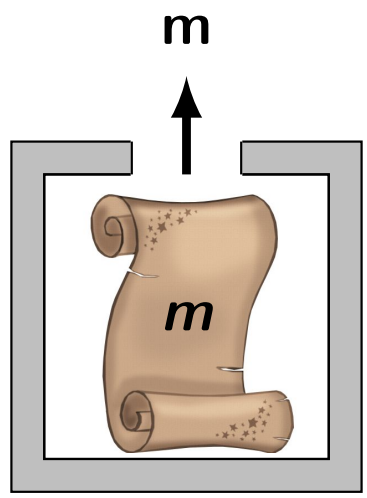


Commitment Schemes over Groups of Unknown Order



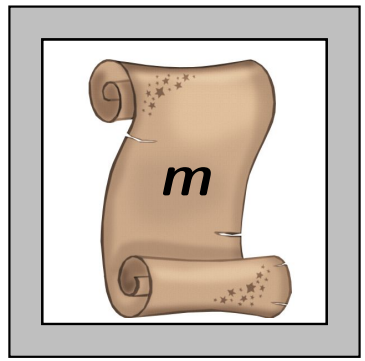
Hiding

Commitment Schemes over Groups of Unknown Order



Binding

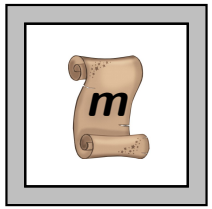
Commitment Schemes over Groups of Unknown Order



Fujisaki-Okamoto (1997):

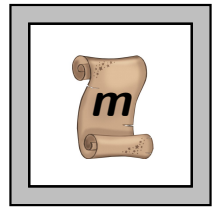
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown

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

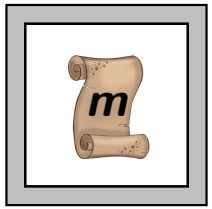


Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

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

Group Sig. | Range Proofs | Auctions | PPSS

Commitment Schemes over Groups of Unknown Order

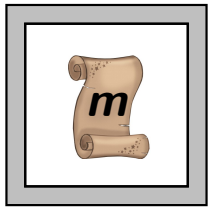


Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization

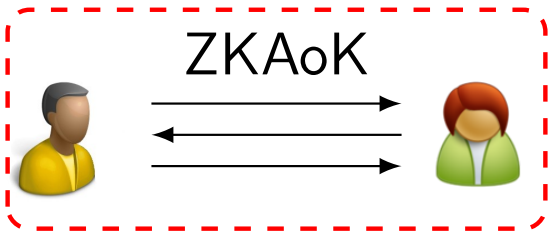
Anonymous Credentials | MPC | E-Cash | E-Voting

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

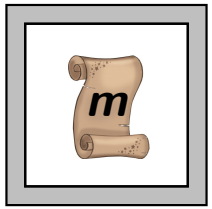


Strong-RSA

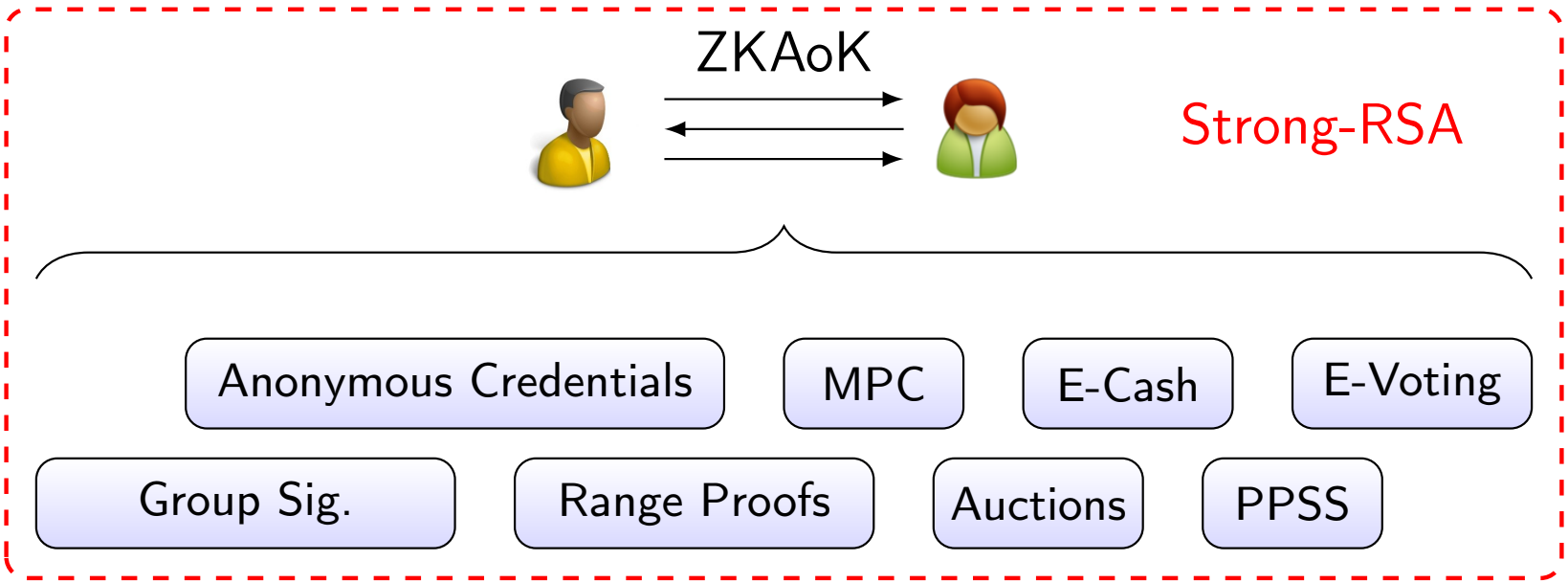
Anonymous Credentials | MPC | E-Cash | E-Voting

Group Sig. | Range Proofs | Auctions | PPSS

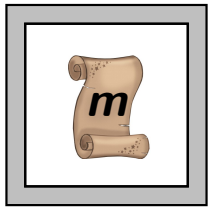
Commitment Schemes over Groups of Unknown Order



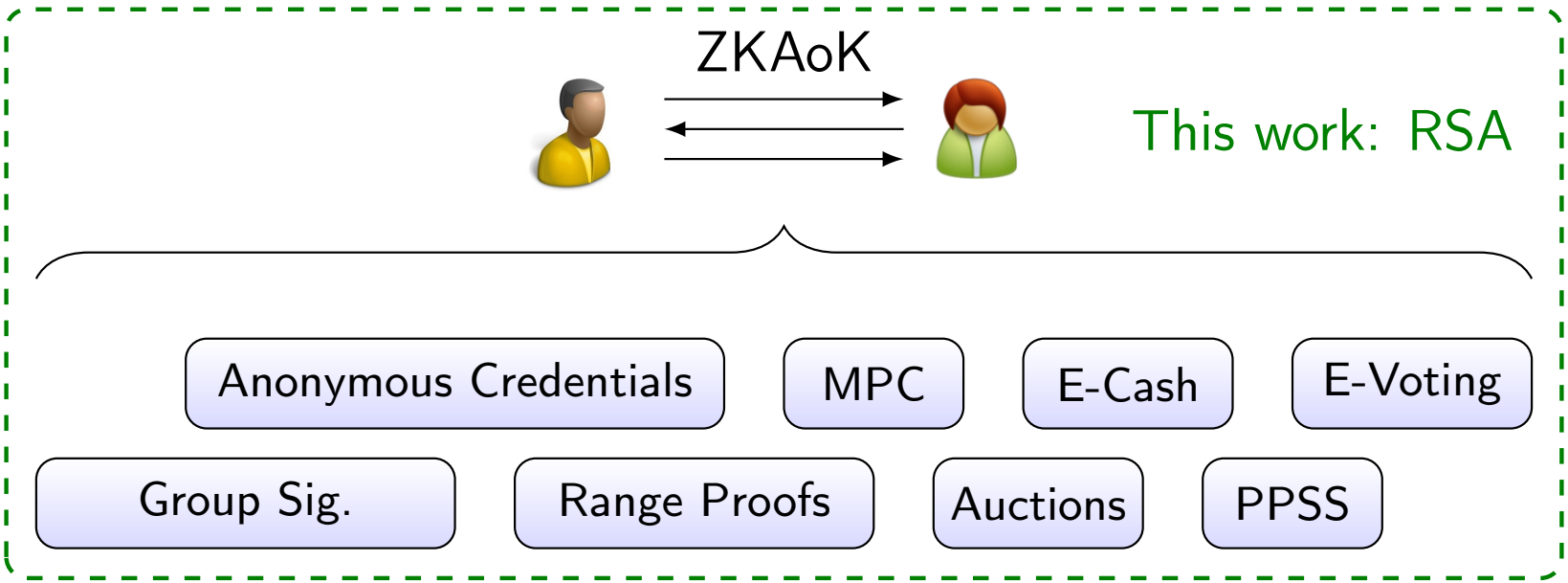
Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization



Commitment Schemes over Groups of Unknown Order



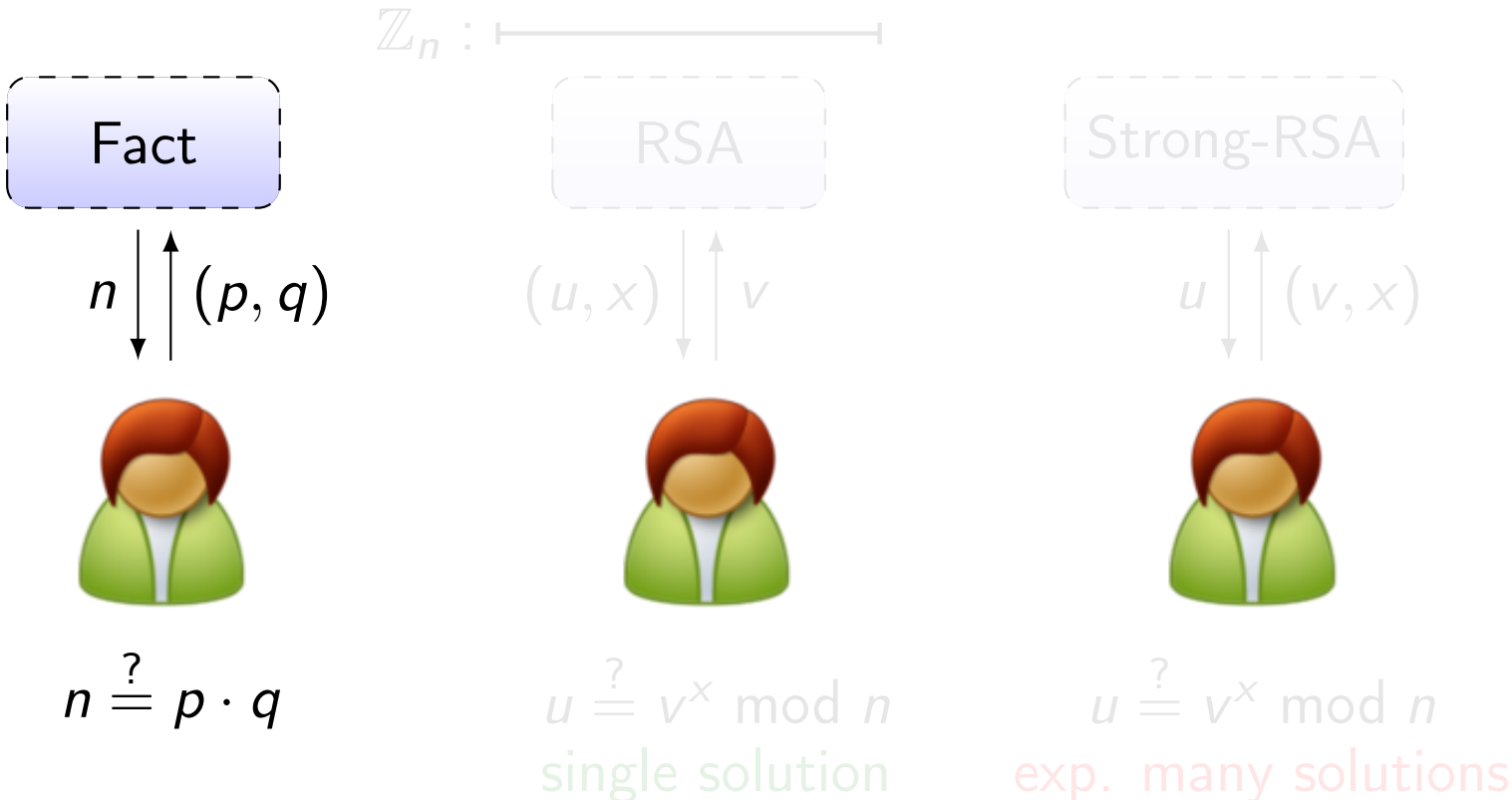
Fujisaki-Okamoto (1997):
$m \in \mathbb{G}$, $|\mathbb{G}|$ unknown
Perfectly hiding, binding under Factorization



Preliminaries on RSA Groups

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

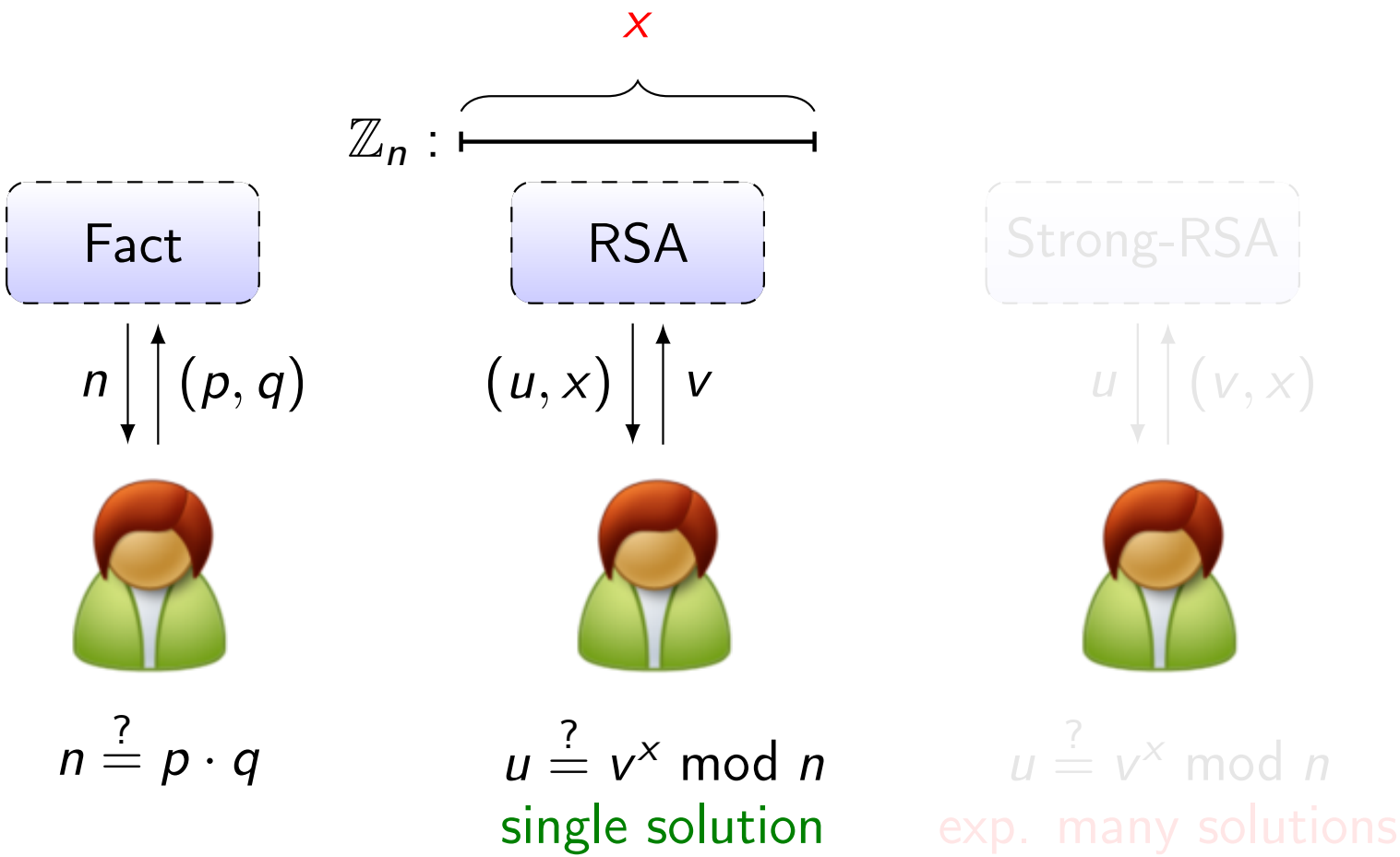
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

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

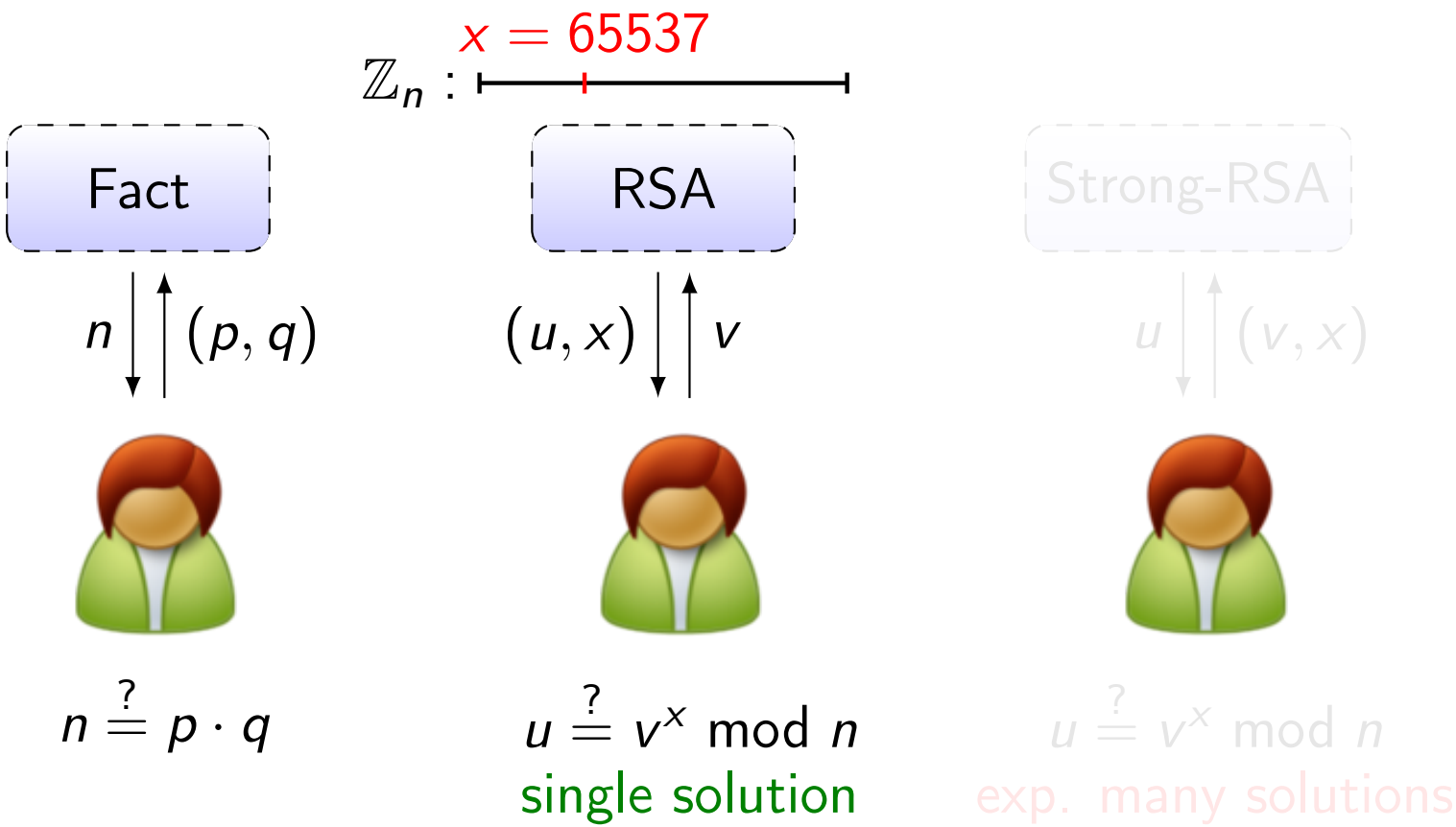
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

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

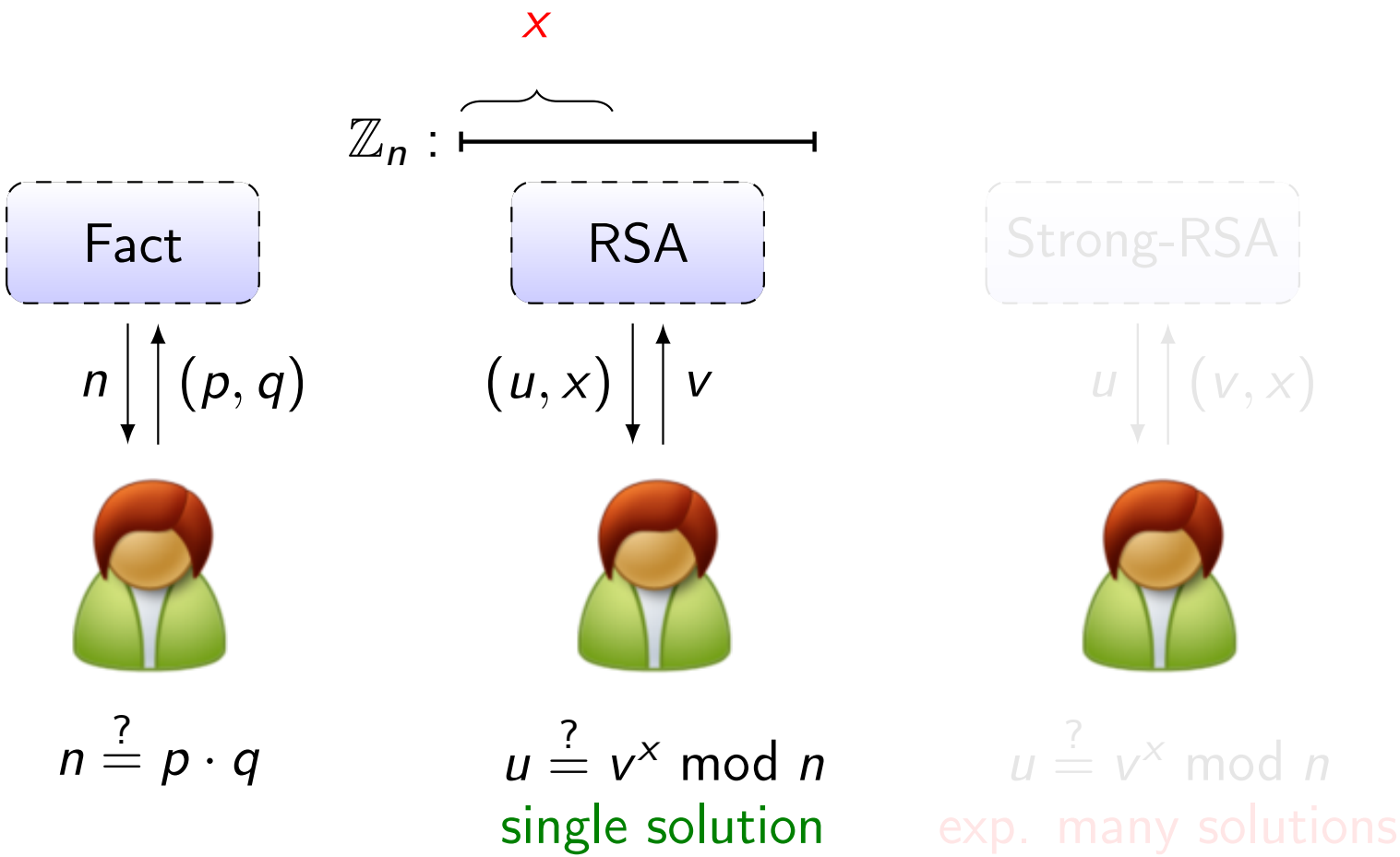
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

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

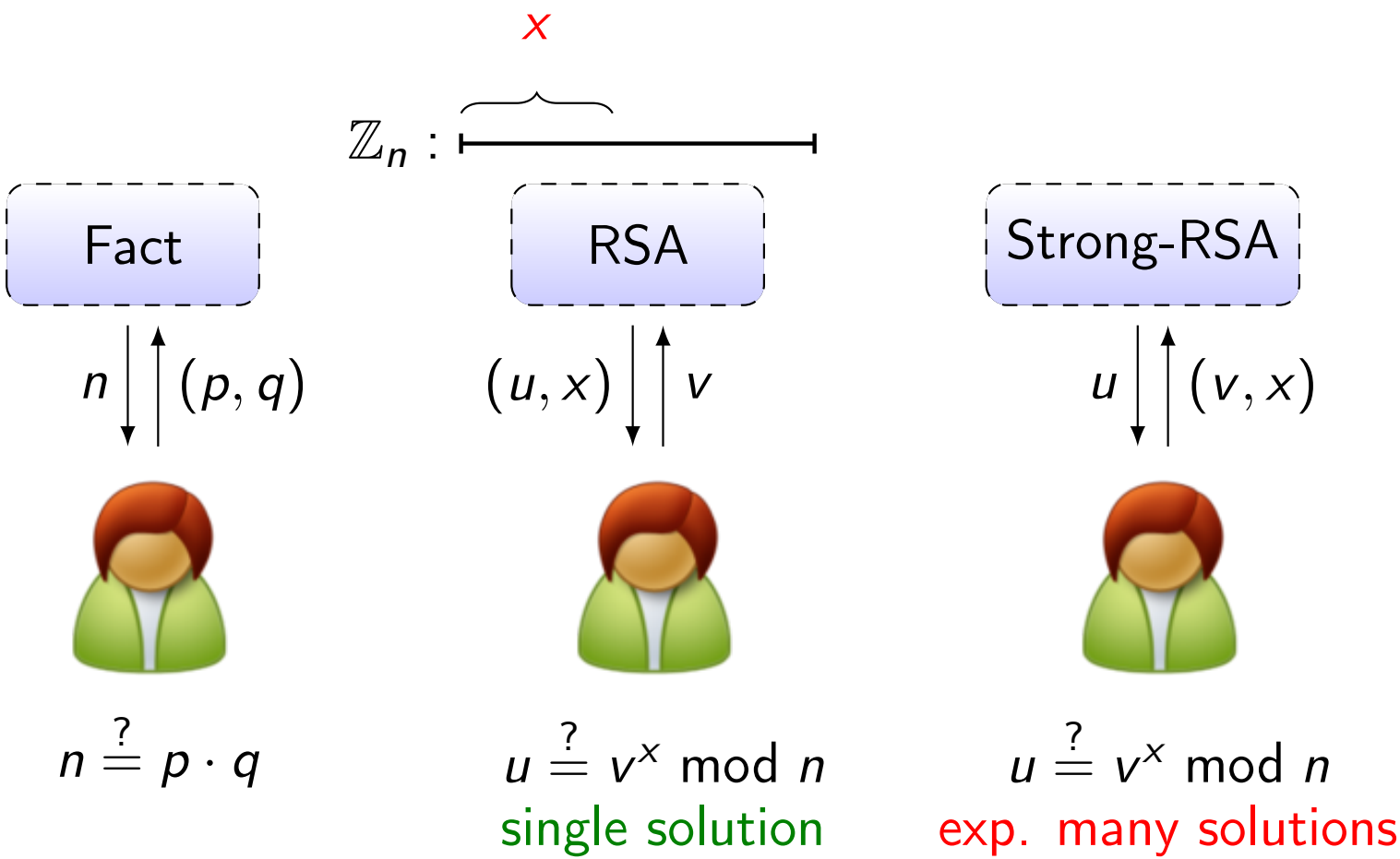
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Preliminaries on RSA Groups

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

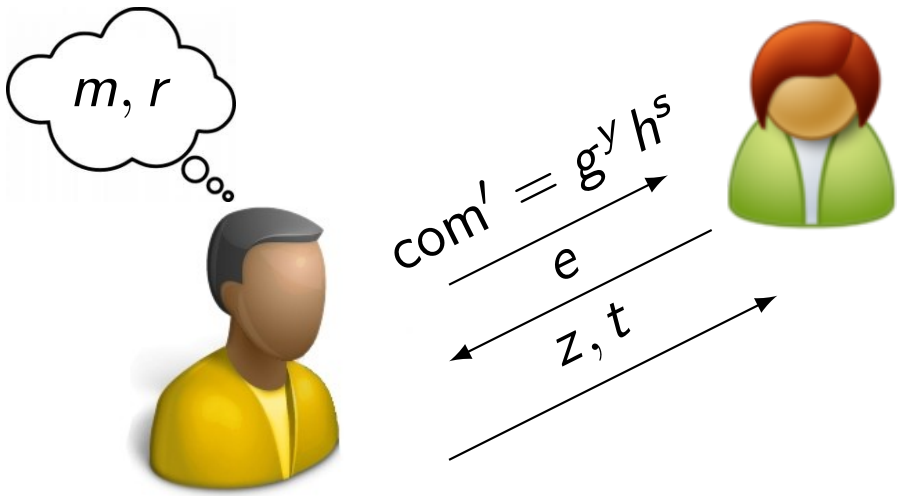
$$|\mathrm{QR}[n]| = \frac{(p-1)(q-1)}{4} = p'q'$$



Zero-Knowledge Argument of Knowledge of an Opening

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

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



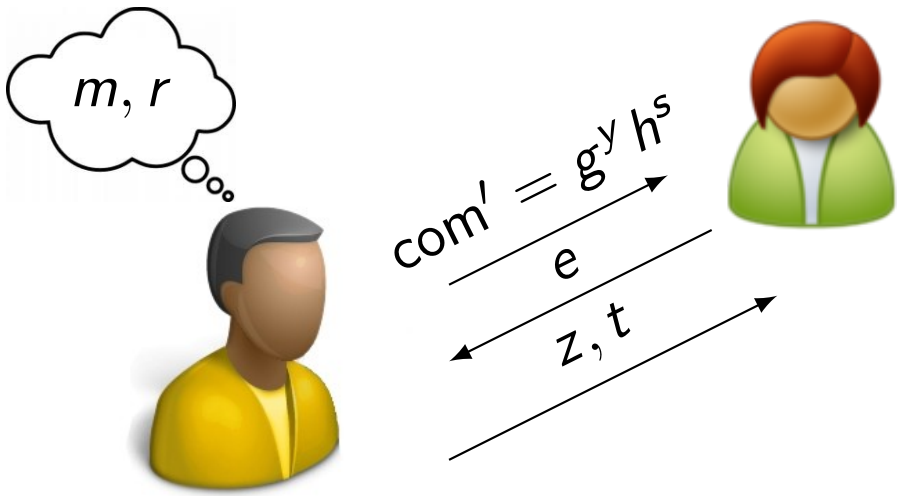
$z \leftarrow em + y$
$t \leftarrow er + s$

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

Zero-Knowledge Argument of Knowledge of an Opening

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

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



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

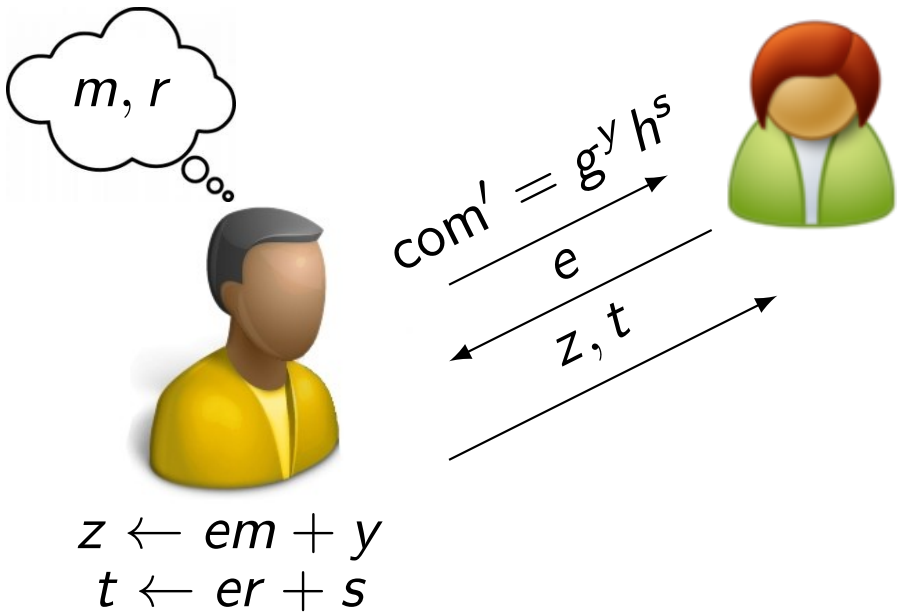
V checks whether $\mathrm{com}^e \mathrm{com}' = g^z h^t$.

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

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

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



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

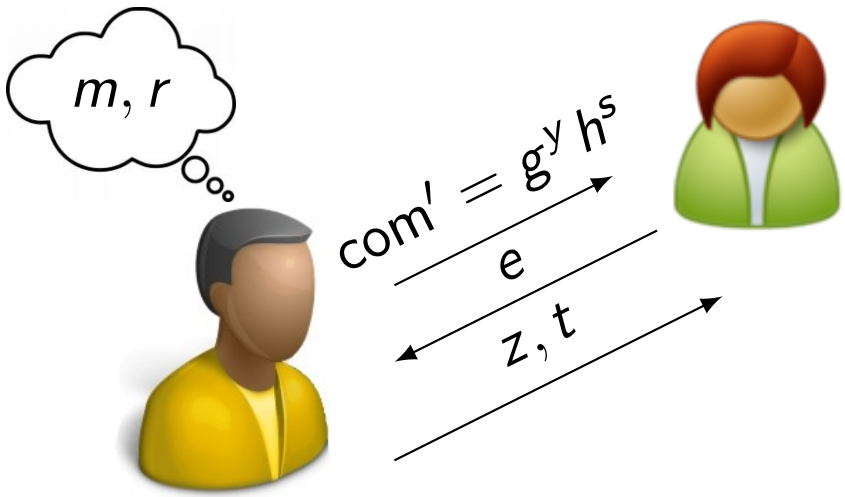
V checks whether $\mathrm{com}^e \mathrm{com}' = g^z h^t$.

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

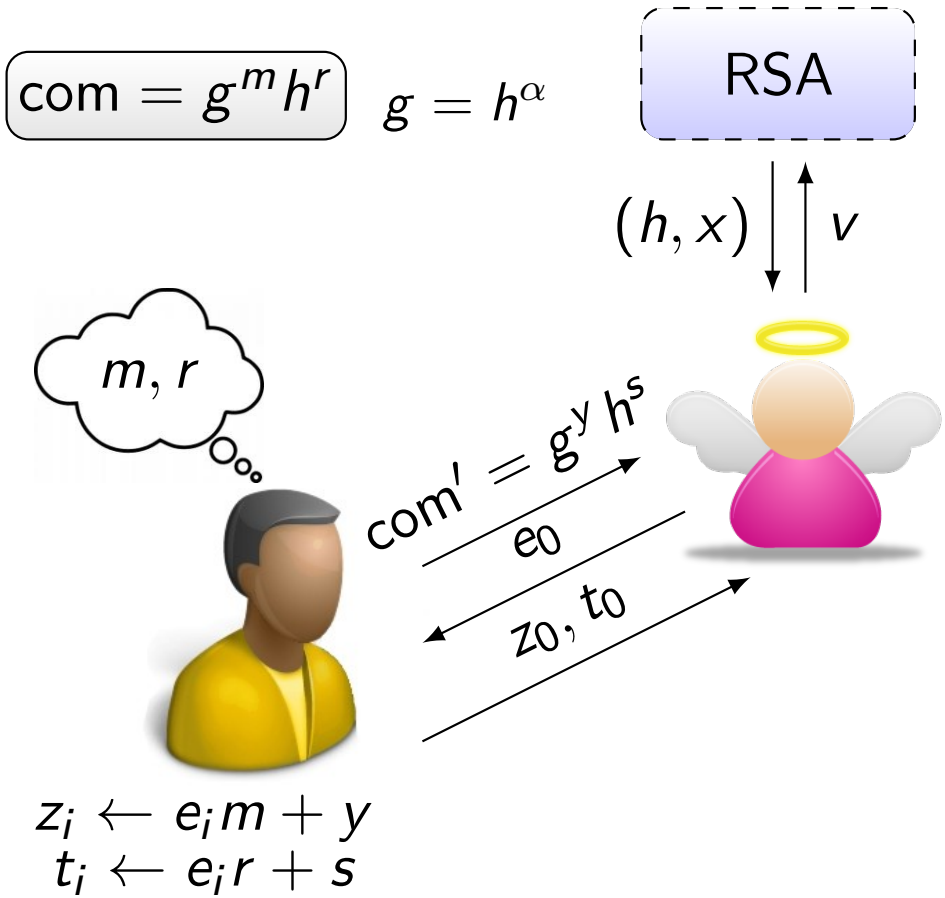
Requires inversions over the exponents of $\mathbb{G}$!

Soundness Argument

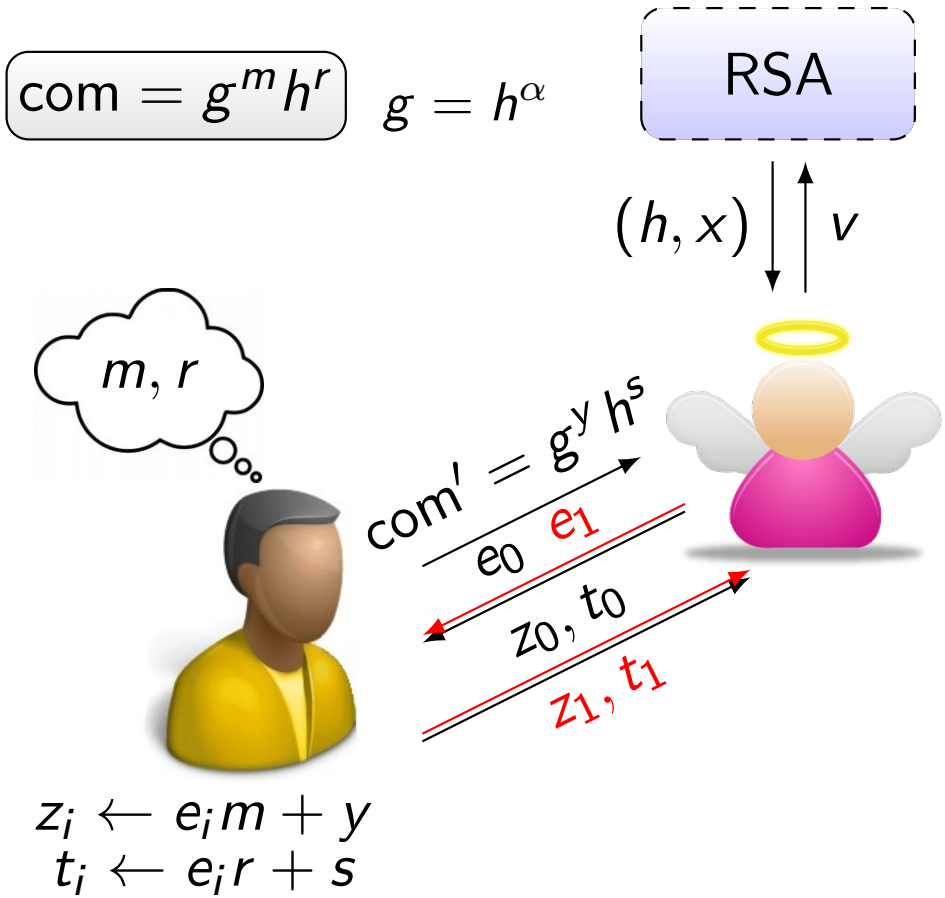
$\boxed{\text{com} = g^m h^r}$ $g = h^\alpha$



Soundness Argument

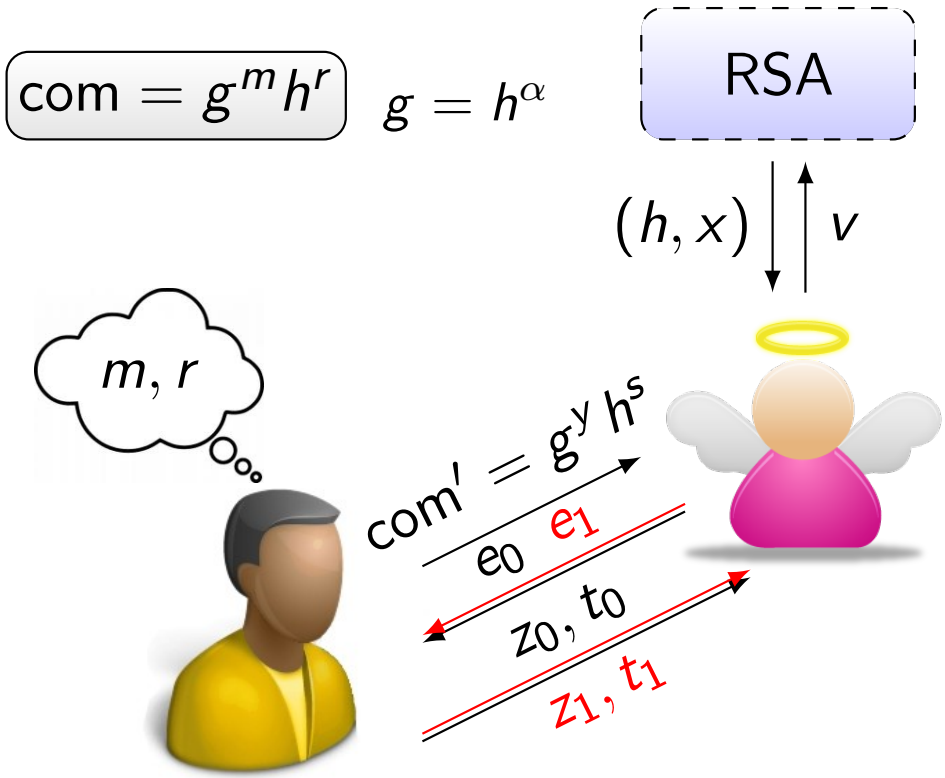


Soundness Argument



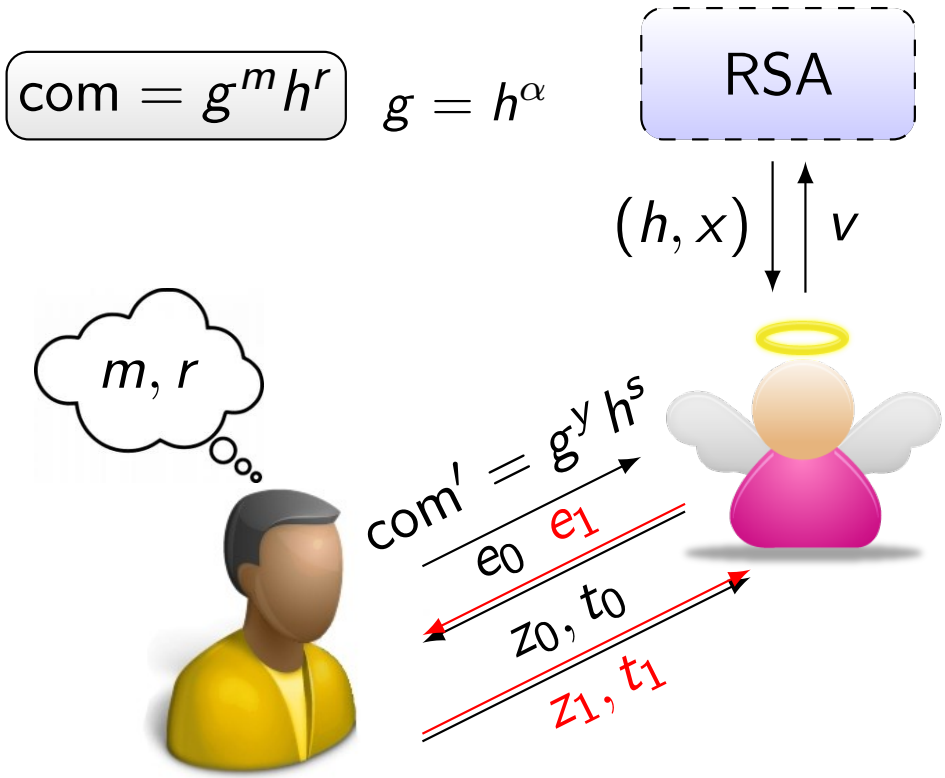
Rewind P w/ (e_0, e_1);
with pr. ε^2,
$\mathrm{com}^{e_0 - e_1} = g^{z_0 - z_1} h^{t_0 - t_1}$

Soundness Argument



Rewind P w/ (e_0, e_1); with pr. ε^2, $\text{com}^e = g^z h^t$, but we cannot divide by e!

Soundness Argument

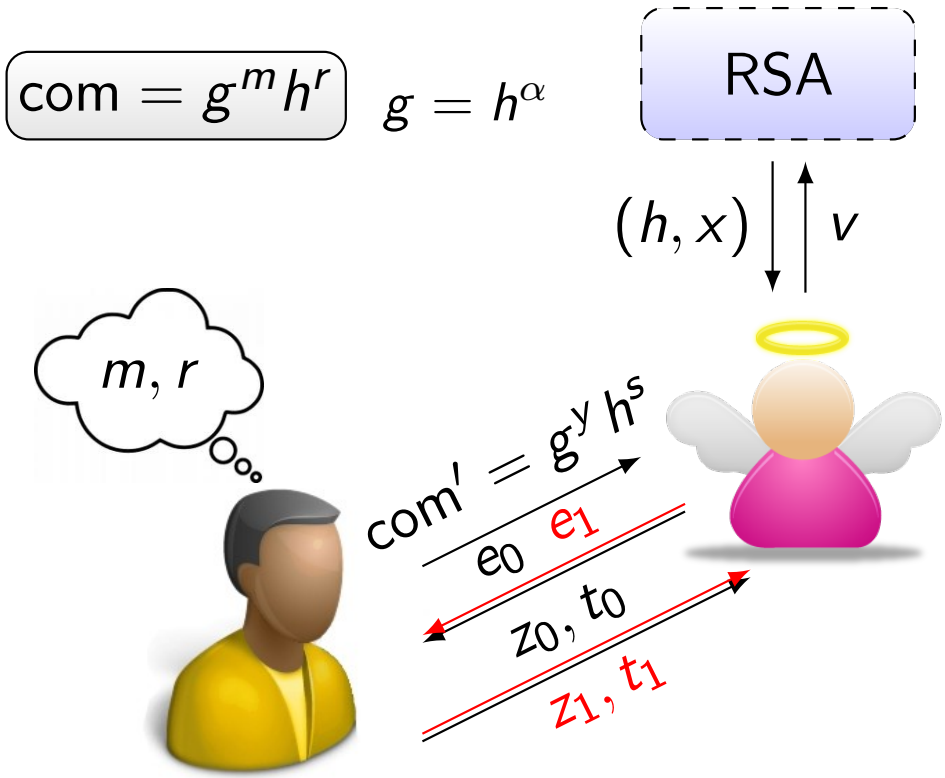


Rewind P w/ (e_0, e_1); with pr. ε^2, $\text{com}^e = g^z h^t$, but we cannot divide by e!

Case 1.

$e \mid z$ and $e \mid t$

Soundness Argument



Rewind P w/ (e_0, e_1); with pr. ε^2, $\text{com}^e = g^z h^t$, but we cannot divide by e!

Case 1.

$e \mid z$ and $e \mid t$

$$\text{com} = \pm g^{z/e} h^{t/e}$$

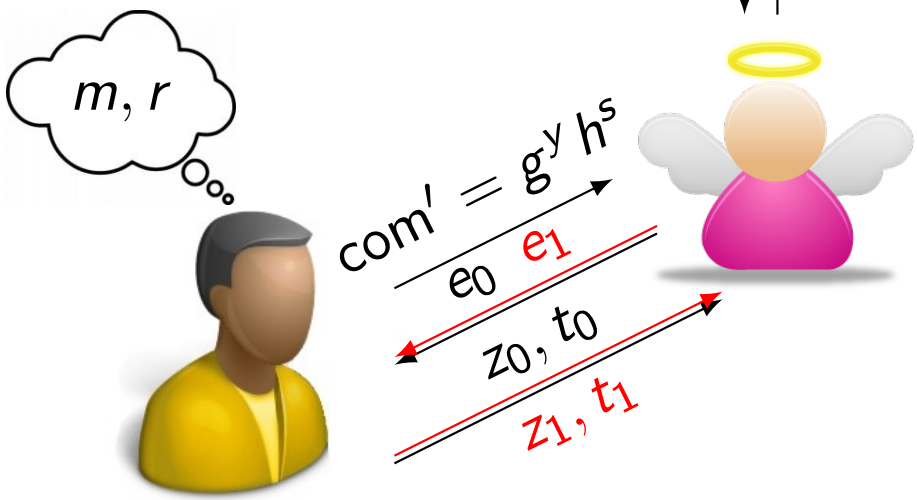
Soundness Argument

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

RSA

(h, x) v

Rewind P w/ (e_0, e_1);
with pr. ε^2,
$\text{com}^e = g^z h^t = h^{\alpha z + t}$



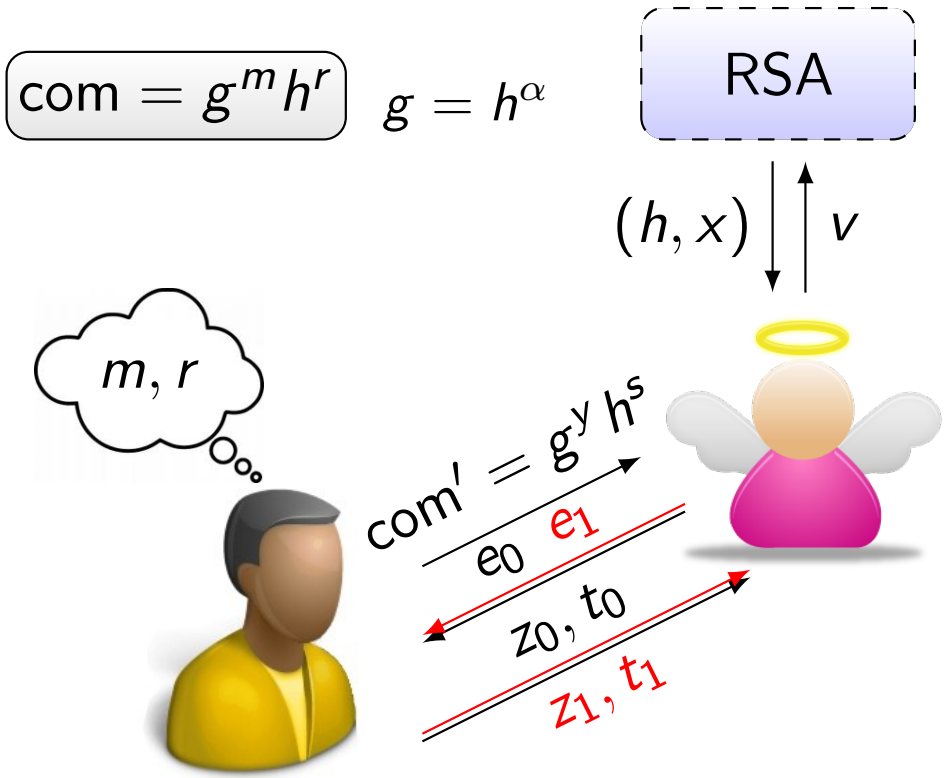
$z_i \leftarrow e_i m + y$
$t_i \leftarrow e_i r + s$

$z = z_0 - z_1, e = e_0 - e_1,$
$t = t_0 - t_1$

Case 2.

$e \nmid z$ or $e \nmid t$

Soundness Argument



Rewind P w/ (e_0, e_1); with pr. ε^2,
$\text{com}^e = g^z h^t = h^{\alpha z + t}$

Case 2.

$e \nmid z$ or $e \nmid t$

[DF02]: With probability $1/2$, $e \nmid \alpha z + t$.

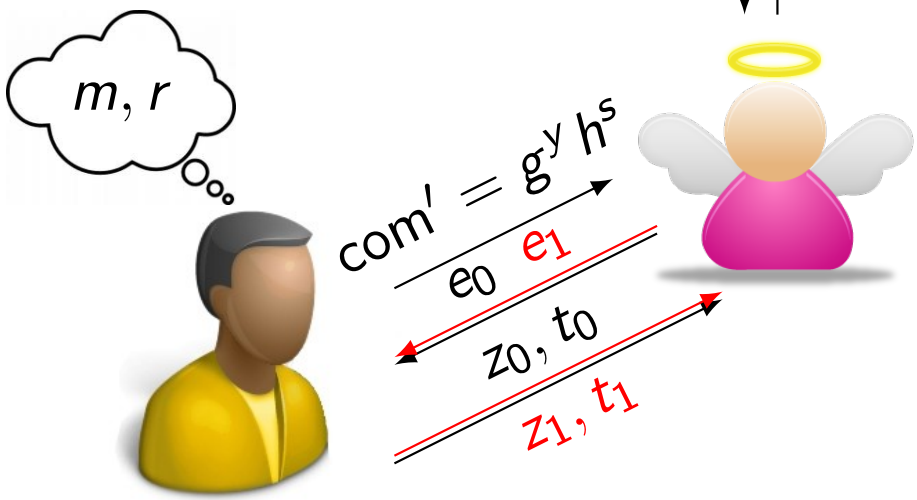
Soundness Argument

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

RSA

(h, x) v

Rewind P w/ (e_0, e_1);
with pr. ε^2,
$\text{com}^e = g^z h^t = h^{\alpha z + t}$



$z_i \leftarrow e_i m + y$
$t_i \leftarrow e_i r + s$

$z = z_0 - z_1, e = e_0 - e_1,$
$t = t_0 - t_1$

Case 2.

Shamir's gcd trick:
$e / \gcd(e, \alpha z + t) = \pi$
can find v such that
$v^\pi = \pm h$

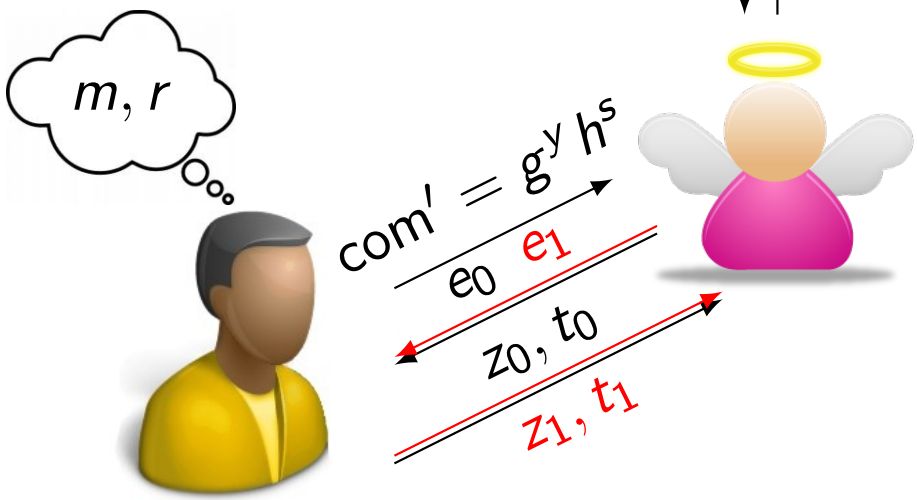
Soundness Argument

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

RSA

(h, x) v

Rewind P w/ (e_0, e_1);
with pr. ε^2,
$\text{com}^e = g^z h^t = h^{\alpha z + t}$



$z_i \leftarrow e_i m + y$
$t_i \leftarrow e_i r + s$

$z = z_0 - z_1, e = e_0 - e_1,$
$t = t_0 - t_1$

Case 2.

Solves a Strong RSA challenge w/ π

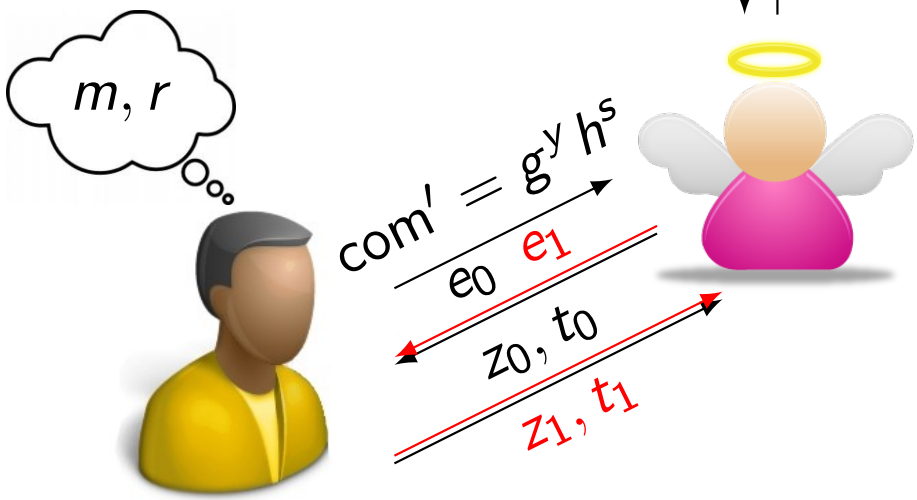
Soundness Argument

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

RSA

(h, x) v

Rewind P w/ (e_0, e_1);
with pr. ε^2,
$\text{com}^e = g^z h^t = h^{\alpha z + t}$



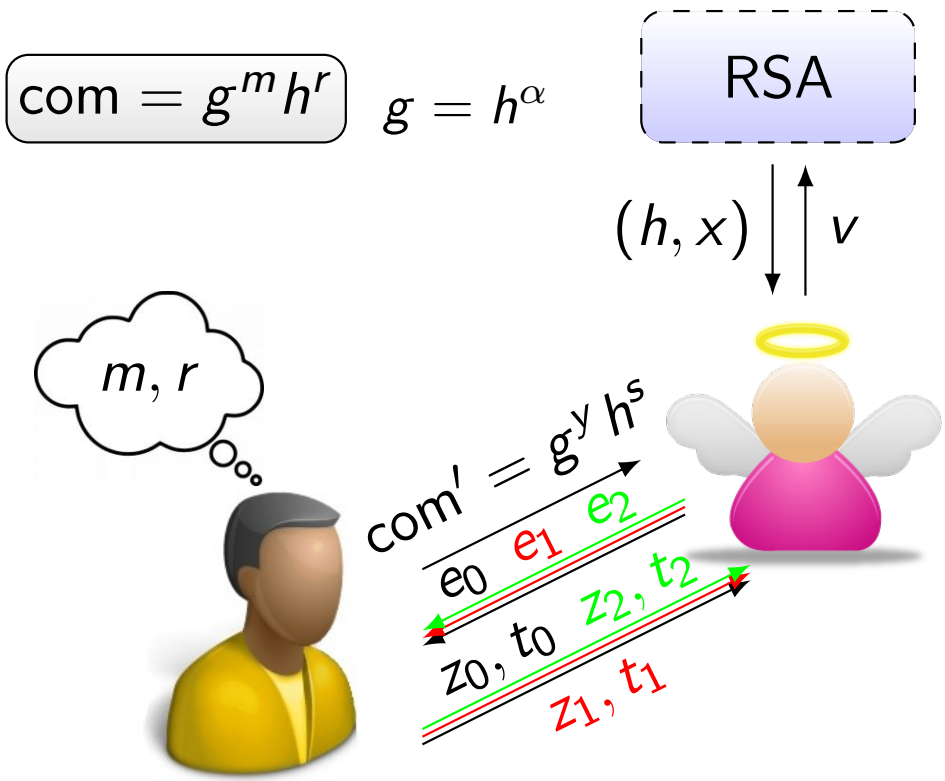
$z_i \leftarrow e_i m + y$
$t_i \leftarrow e_i r + s$

$z = z_0 - z_1, e = e_0 - e_1,$
$t = t_0 - t_1$

Case 2.

Core observation:
π can't be too large.

Soundness Argument

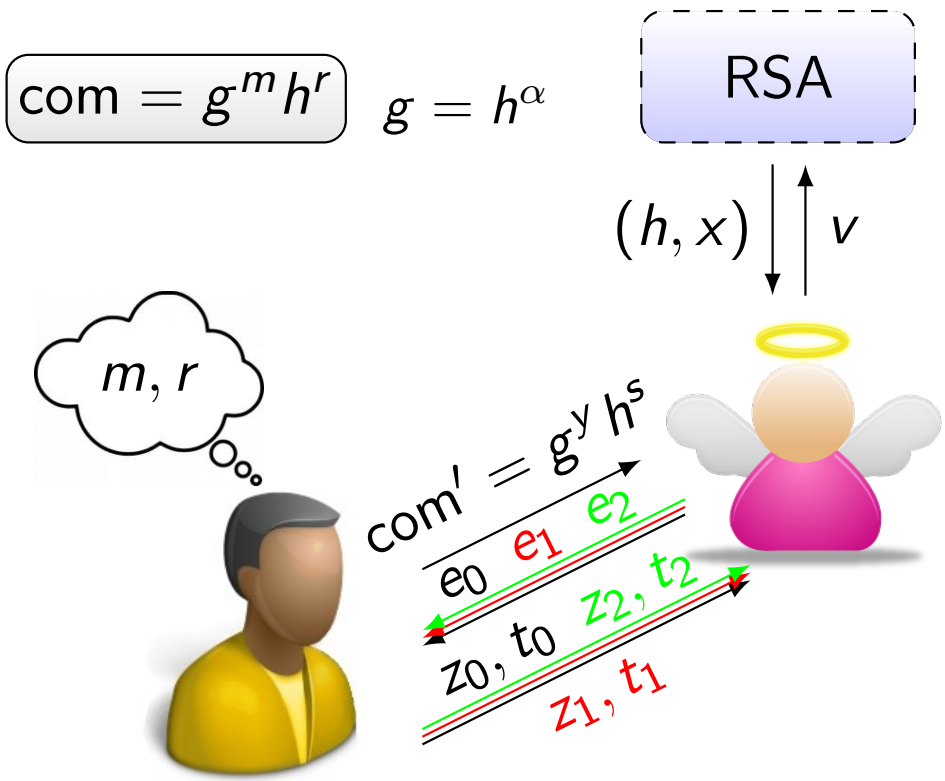


Rewind P w/ (e_0, e_1, e_2);
with pr. ε^3,
$\text{com}^e = g^z h^t$,
$\text{com}^{e'} = g^{z'} h^{t'}$
$\rightarrow g^a = h^b$

Case 2.

Suppose $\pi > 8/\varepsilon$

Soundness Argument



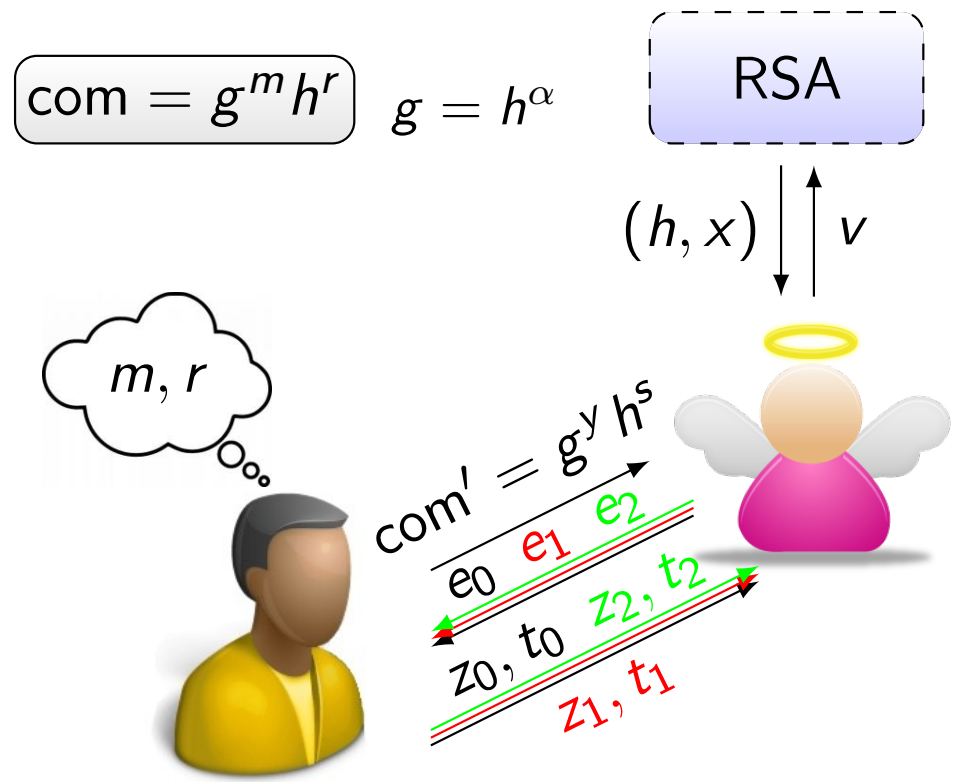
$z = z_0 - z_1, e = e_0 - e_1,$
$t = t_0 - t_1$

Rewind P w/ (e_0, e_1, e_2);
with pr. ε^3,
$\text{com}^e = g^z h^t$,
$\text{com}^{e'} = g^{z'} h^{t'}$
$\rightarrow g^a = h^b$

Case 2.

Suppose $\pi > 8/\varepsilon$
$g^a = h^b$ factors n unless
$a = b = 0$

Soundness Argument



$z_i \leftarrow e_i m + y$
$t_i \leftarrow e_i r + s$

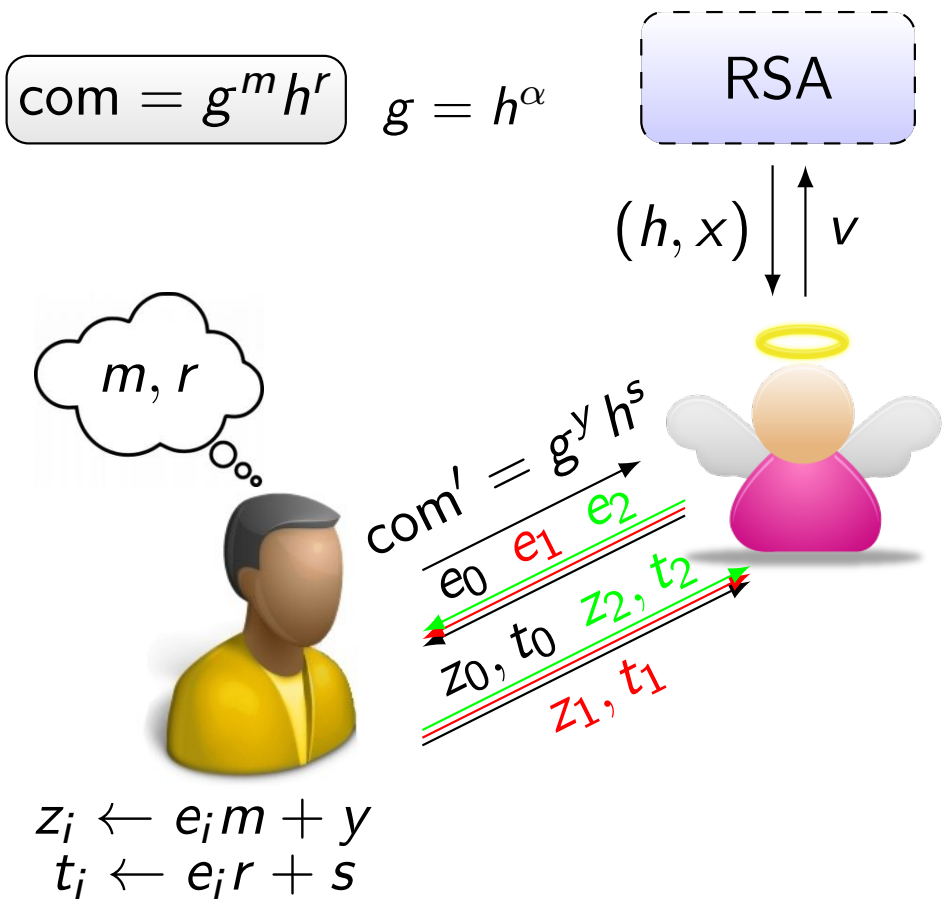
π' divides e', e' is random
$\Pr[\pi = \pi'] \leq \Pr[\pi \text{ divides } e'] = O(\varepsilon)$

Rewind P w/ (e_0, e_1, e_2);
with pr. ε^3,
$com^e = g^z h^t$,
$com^{e'} = g^{z'} h^{t'}$
$\rightarrow g^a = h^b$

Case 2.

Suppose $\pi > 8/\varepsilon$
$g^a = h^b$ factors n unless
$a = b = 0 \Rightarrow \pi = \pi'$

Soundness Argument



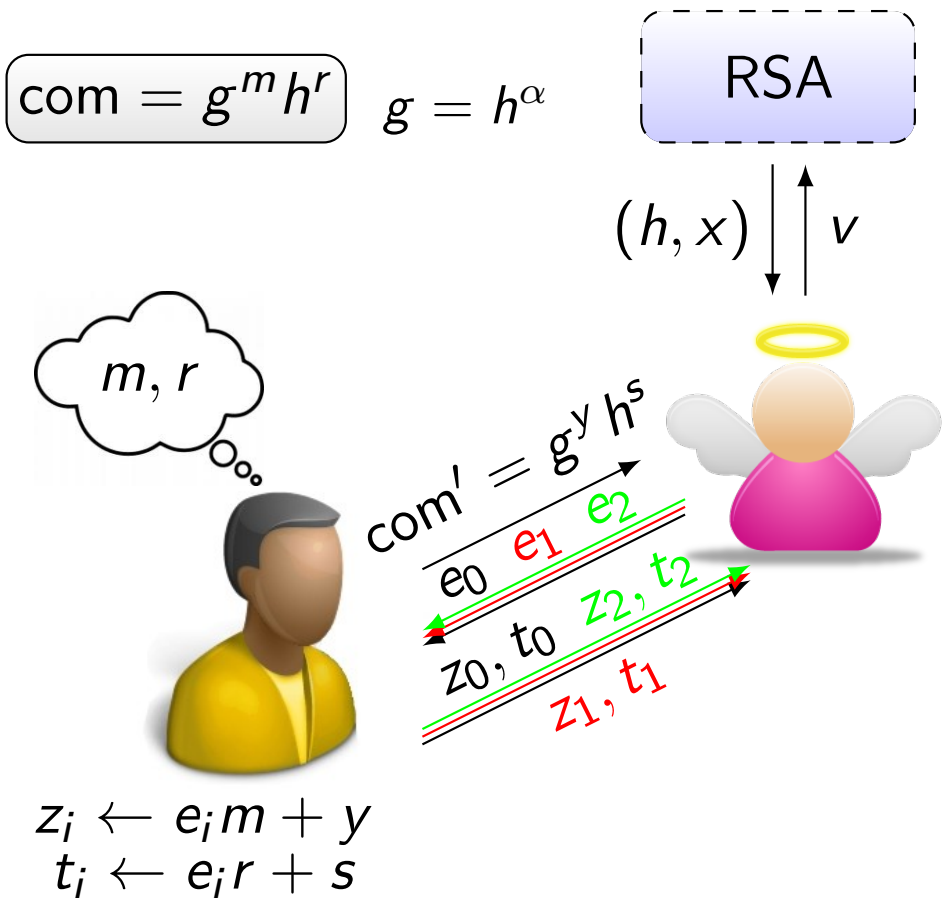
Factors n with $\frac{1}{\text{poly}}$ probability

Rewind P w/ (e_0, e_1, e_2);
with pr. ε^3,
$\text{com}^e = g^z h^t$,
$\text{com}^{e'} = g^{z'} h^{t'}$
$\rightarrow g^a = h^b$

Case 2.

Suppose $\pi > 8/\varepsilon$
$g^a = h^b$ factors n unless
$a = b = 0 \Rightarrow \pi = \pi'$

Soundness Argument

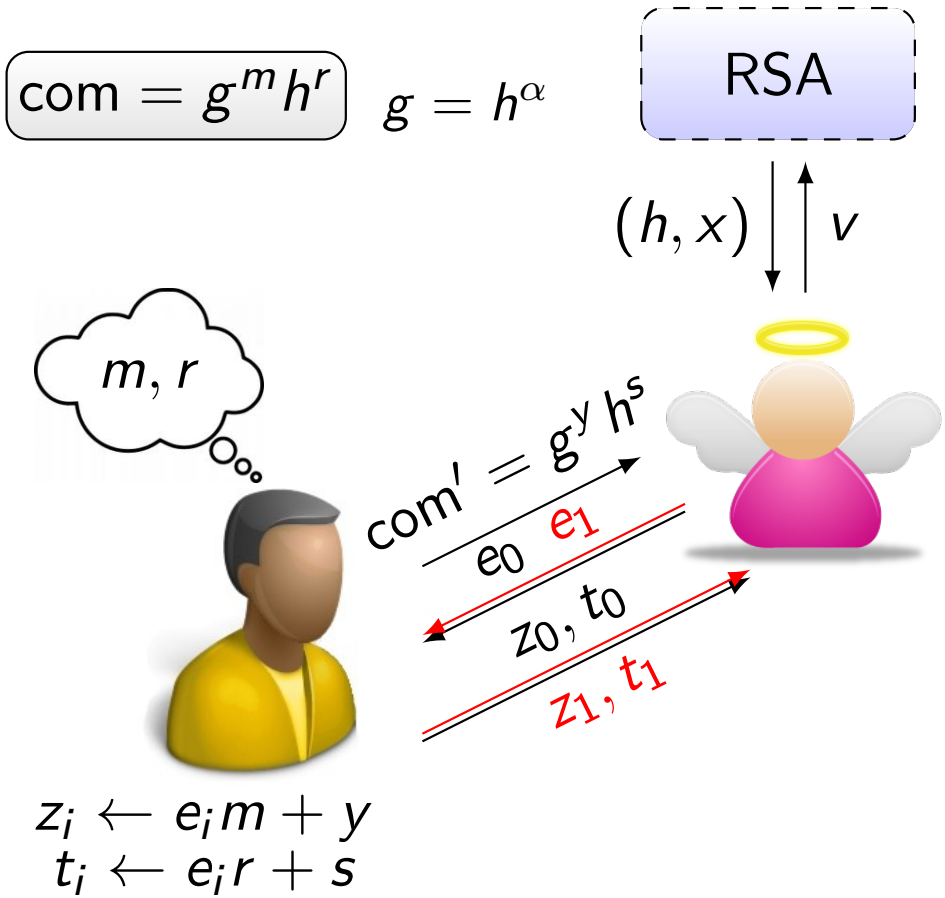


Rewind P w/ (e_0, e_1, e_2);
with pr. ε^3,
$\text{com}^e = g^z h^t$,
$\text{com}^{e'} = g^{z'} h^{t'}$
$\rightarrow g^a = h^b$

Case 2.

Suppose $\pi > 8/\varepsilon$
$g^a = h^b$ factors n

Soundness Argument

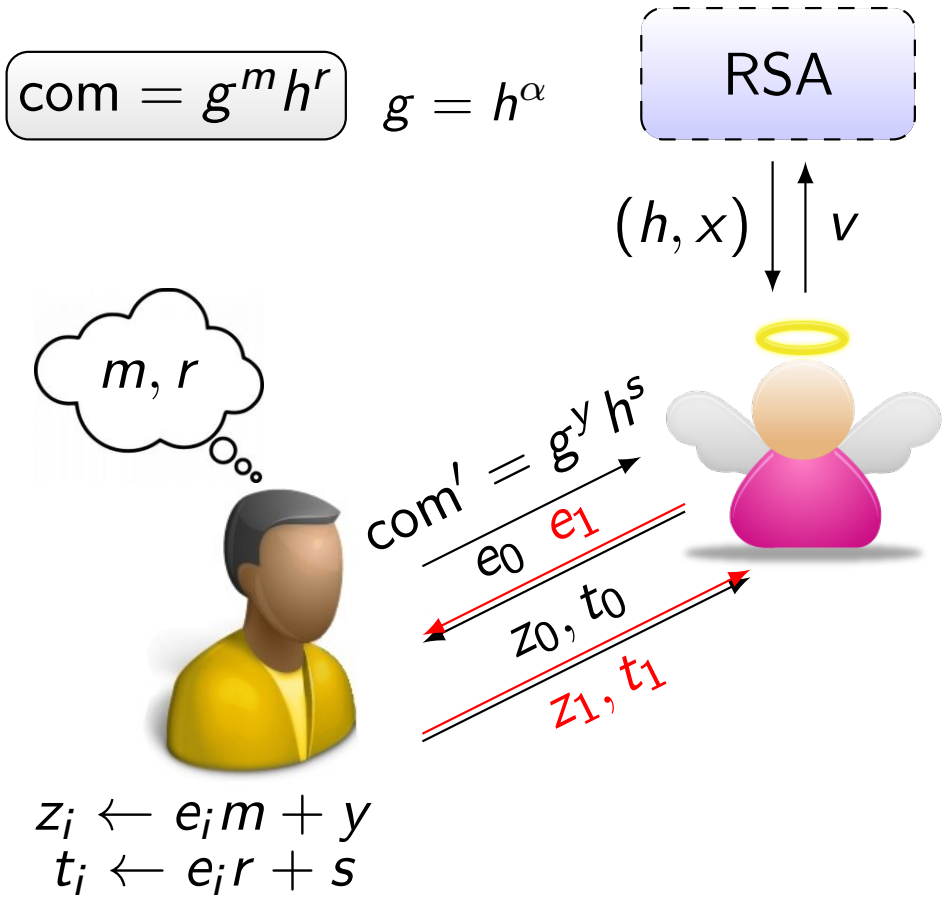


Rewind P w/ (e_0, e_1); with pr. ε^2, $com^e = g^z h^t$, but we cannot divide by e!

Case 2.

$\pi \leq 8/\varepsilon$

Soundness Argument



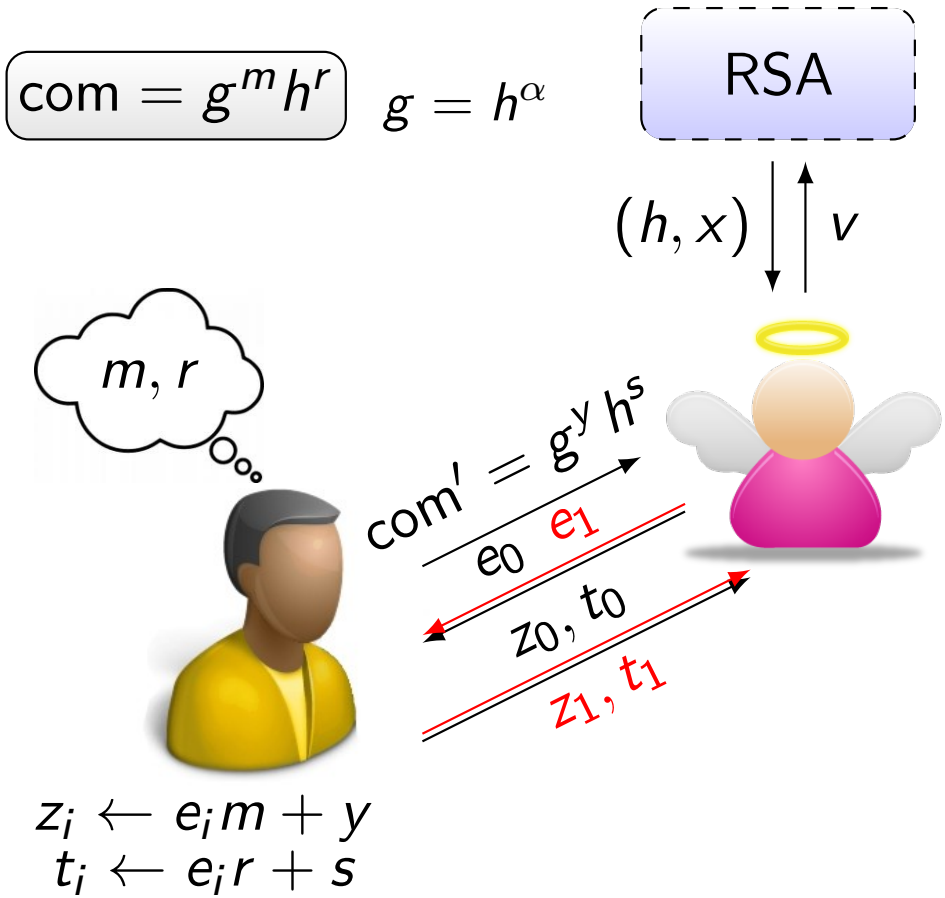
Rewind P w/ (e_0, e_1); with pr. ε^2, $com^e = g^z h^t$, but we cannot divide by e!

Case 2.

$\pi \leq 8/\varepsilon$

A random small RSA challenge is equal to π with $O(\varepsilon)$ probability

Soundness Argument



Sim gets (m, r) or solves RSA with $O(\varepsilon^3)$ proba

Rewind P w/ (e_0, e_1); with pr. ε^2, $\text{com}^e = g^z h^t$, but we cannot divide by e!

Case 2.

$\pi \leq 8/\varepsilon$

A random small RSA challenge is equal to π with $O(\varepsilon)$ probability

Applications, Other Contributions, and Open Problems

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

Open Problems.

- Can we build short algebraic RSA-based signatures?

Thank you for your attention

Questions?