Vector Commitments over Rings and Compressed Σ-Protocols

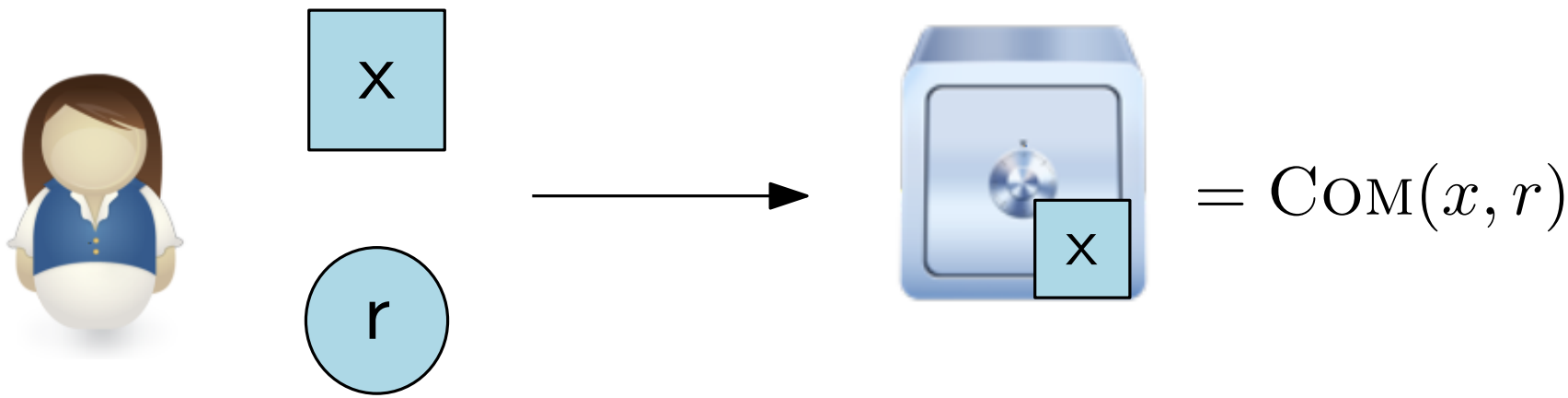
Thomas Attema	CWI Amsterdam, Leiden University, TNO
Ignacio Cascudo	IMDEA Software Institute
Ronald Cramer	CWI Amsterdam, Leiden University
Ivan Damgård	Aarhus University
Daniel Escudero	JP Morgan AI Research

TCC 22

Chicago, November 7, 2022

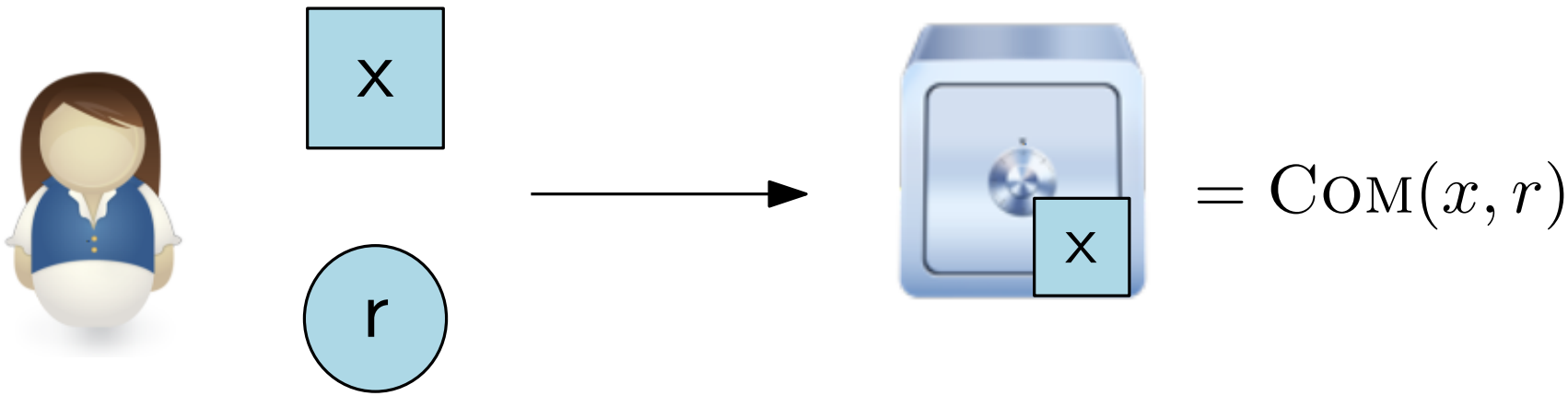
Commitments

Commit:

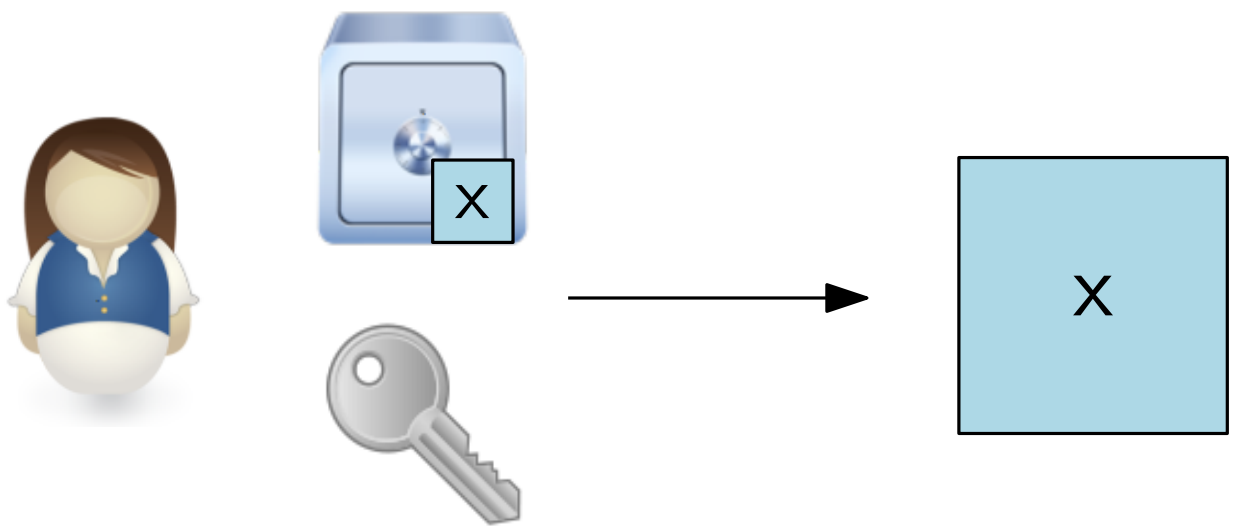


Commitments

Commit:

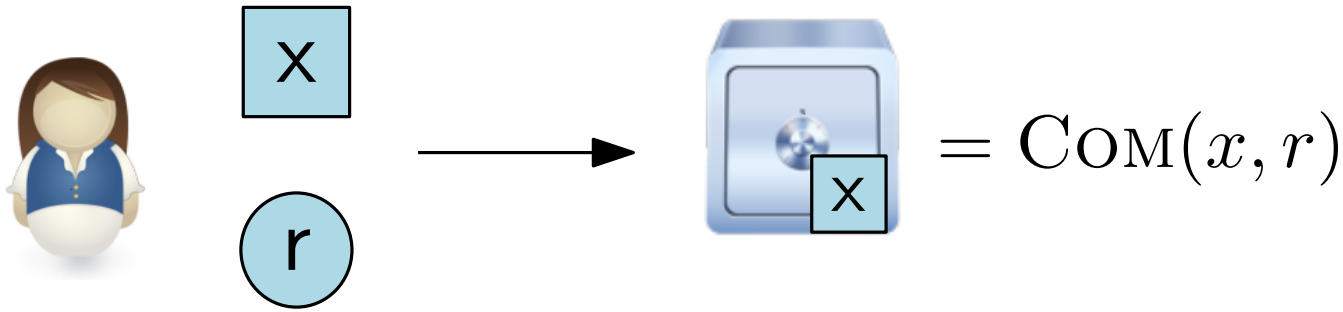


Open:



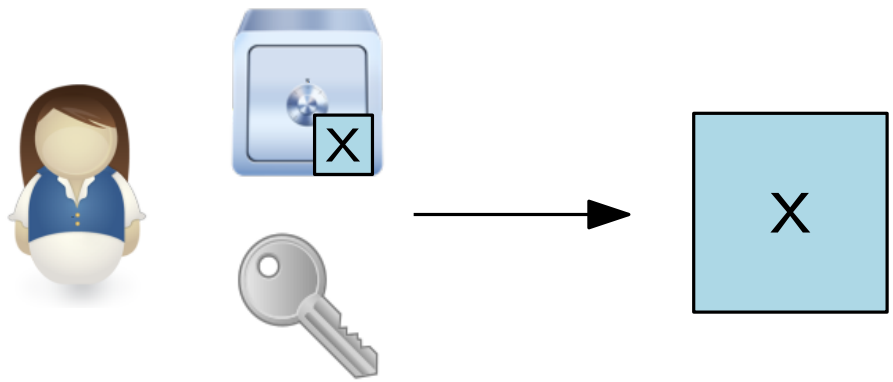
Commitments

Commit:



- Binding: Commitment cannot be opened to different x, x'
- Hiding: Commitment does not give info on x before being opened

Open:



Homomorphism

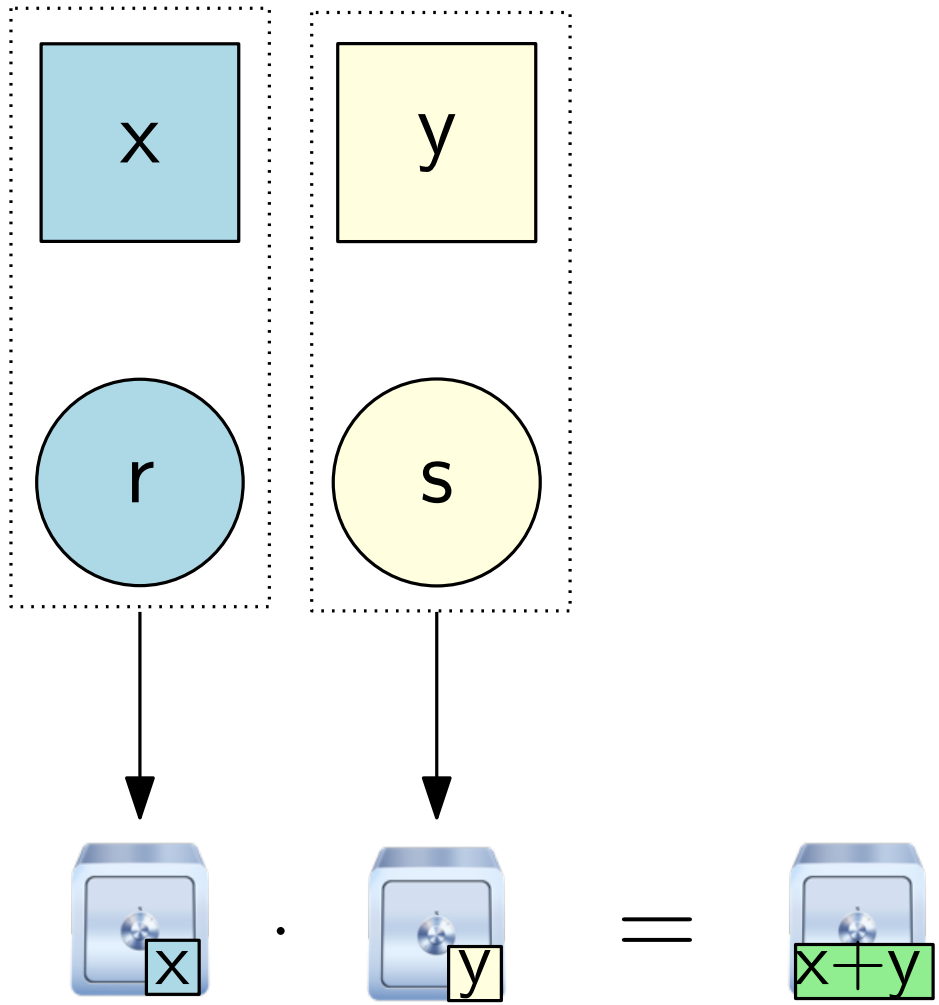
We set $\textsc{Com} : \mathbb{G} \times \mathcal{R} \to \mathbb{H}$ with $(\mathbb{G}, +)(\mathbb{H}, \cdot)$ groups:

There exists
$R : \mathbb{G}^2 \times \mathcal{R}^2 \to \mathcal{R}$
with:
$\textsc{Com}(x + y, R(x, y, r, s)) =$
$\quad \textsc{Com}(x, r) \cdot \textsc{Com}(y, s)$

Homomorphism

We set $\textsc{Com} : \mathbb{G} \times \mathcal{R} \to \mathbb{H}$ with $(\mathbb{G}, +)(\mathbb{H}, \cdot)$ groups:

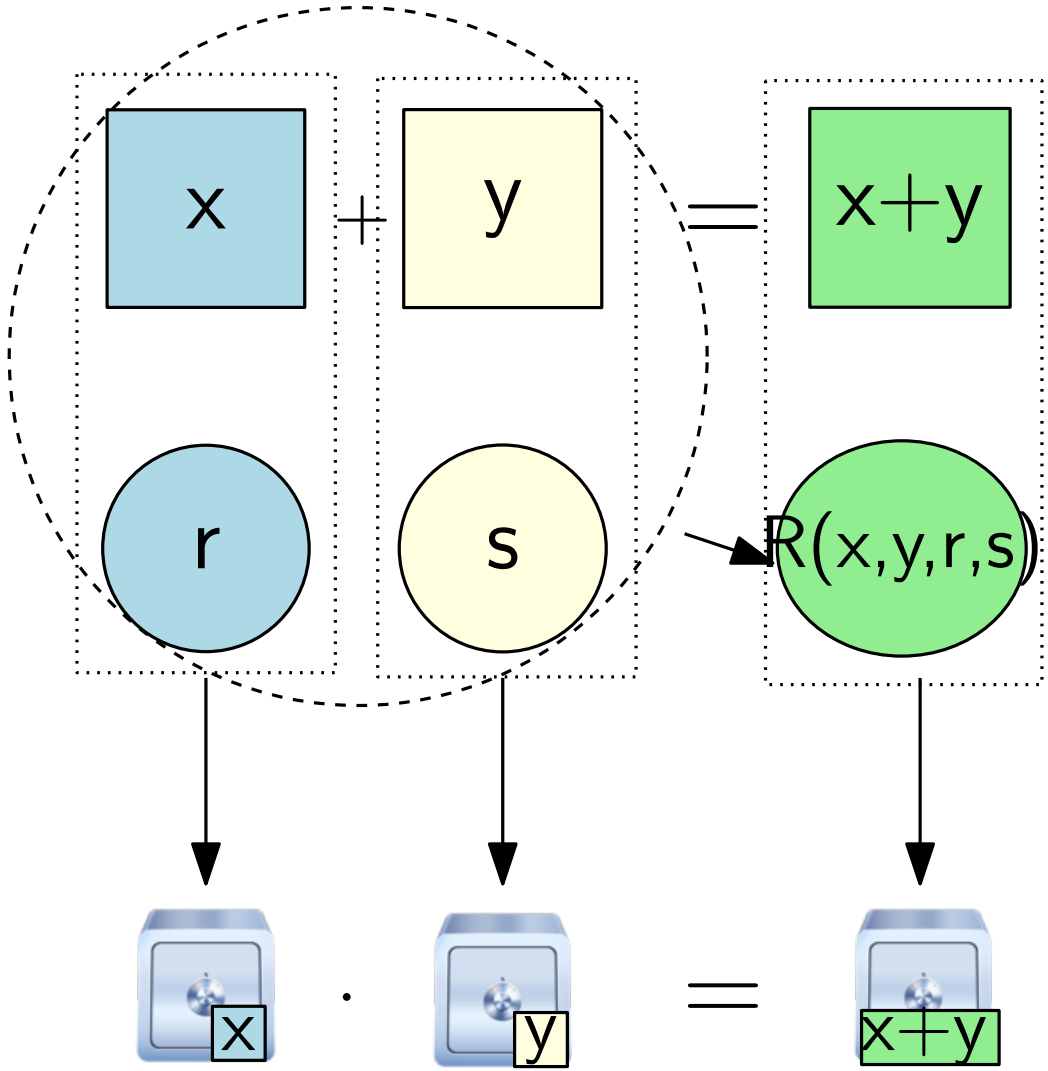
There exists
$R : \mathbb{G}^2 \times \mathcal{R}^2 \to \mathcal{R}$
with:
$\textsc{Com}(x + y, R(x, y, r, s)) =$
$\textsc{Com}(x, r) \cdot \textsc{Com}(y, s)$



Homomorphism

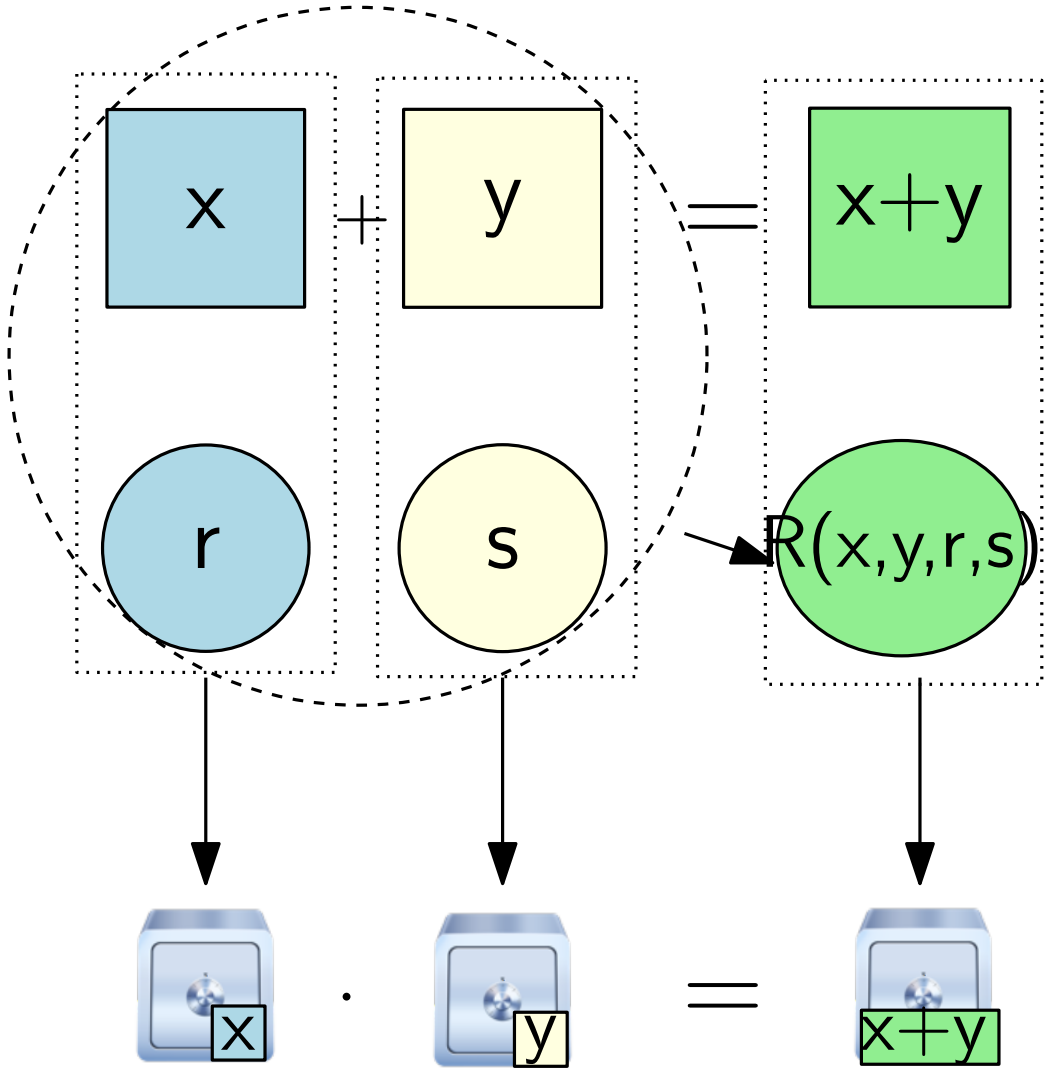
We set $\textsc{Com} : \mathbb{G} \times \mathcal{R} \to \mathbb{H}$ with $(\mathbb{G}, +)(\mathbb{H}, \cdot)$ groups:

There exists
$R : \mathbb{G}^2 \times \mathcal{R}^2 \to \mathcal{R}$
with:
$\textsc{Com}(x + y, R(x, y, r, s)) =$
$\textsc{Com}(x, r) \cdot \textsc{Com}(y, s)$



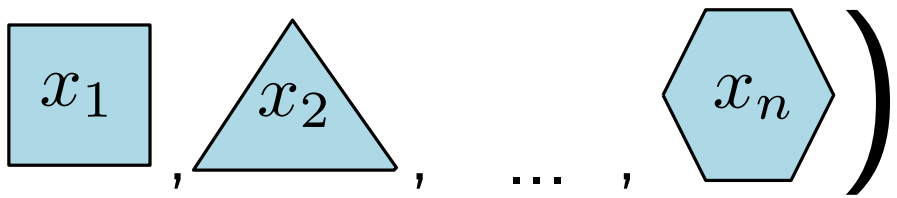
Homomorphic commitments and hiding

Opening $\textsc{Com}(x+y, R(x,y,r,s))$ must not reveal information on x, y beyond the opened value $x+y$



Vector commitments

Commitment on group $\mathbb{G} = (\mathbb{G}')^n$

x= 

- Succinct commitment
- Succinct position opening (opening a coordinate x_i)

Succinct: $O(\text{polylog } n)$

Homomorphic properties as above
(group operation in $\mathbb{G}$ is componentwise)

Linear opening

Suppose $\mathbb{G} = \mathbb{Z}_m$.
Position opening is special case of NIZK for the relation
$\mathcal{X}_L = \{(P, y; x, \gamma) : \textsc{Com}(x, \gamma) = P,\ L(x) = y\}$
where $L : \mathbb{Z}_m^n \to \mathbb{Z}_m$ is linear.

Linear opening

Suppose $\mathbb{G} = \mathbb{Z}_m$.
Position opening is special case of NIZK for the relation
$\mathcal{X}_L = \{(P, y; x, \gamma) : \textsc{Com}(x, \gamma) = P,\ L(x) = y\}$
where $L : \mathbb{Z}_m^n \to \mathbb{Z}_m$ is linear.

Indeed, for opening i-th position to y, prove $L_i(x) = y$
where $L_i : x \mapsto x_i$

Results

We construct **vector commitments** for $\mathbb{Z}_m^n$ for *every* m (*not necessarily prime*).

- Our commitments are homomorphic with respect to $(\mathbb{Z}_m, +)$
- They have $O(1)$ size

Results

We construct **vector commitments** for $\mathbb{Z}_m^n$ for *every* m (*not necessarily prime*).

- Our commitments are homomorphic with respect to $(\mathbb{Z}_m, +)$
- They have $O(1)$ size

We generalize **compressed Σ-protocols** and construct ZK-NIZK for $\mathcal{X}_L = \{(P, y; x, \gamma) : \textsc{Com}(x, \gamma) = P,\ L(x) = y\}$.

- Our proofs have $O(\log n \log\log n)$ size
- In particular, our commitments have $O(\log n \log\log n)$-size position opening
- Can be amortized to prove $d = O(\log\log n)$ statements in $\mathcal{X}_L$ with same complexity.

Homomorphic vector commitments over $\mathbb{Z}_m$

Goal: To construct homomorphic vector commitments with message space $\mathbb{G}' = \mathbb{Z}_m^n$, for **non-necessarily prime** m.

Known constructions do not work, e.g.:

- Pedersen commitment does not work in general, e.g. if $m = 2^k$, DL easy in group of order m.
- Damgård-Fujisaki (**integer** homomorphic vector commitment) reveals information on summands when a sum modulo m is opened.

Our construction:

Our construction has two steps:

- Concrete constructions of single-value homomorphic commitment.
- Generic construction of vector commitment from single-value commitment.

Single-value commitment to Vector commitment

Suppose $\textsc{Com}' : \mathbb{Z}_m \times \mathcal{R} \to \mathbb{H}$ single-value homomorphic commitment.

We construct $\textsc{Com} : \mathbb{Z}_m^n \times \mathcal{R} \to \mathbb{H}$:

Setup:
Setup of $\textsc{Com}' +$
Randomly sample $a_i \in \mathbb{Z}_m$ and $r_i \in \mathcal{R}, i = 1, \ldots, n$
Set $g_i = \textsc{Com}'(a_i, r_i) \in \mathbb{H}$

Commit:
$\textsc{Com}(x, r) = g_1^{x_1} \cdot \ldots g_n^{x_n} \cdot \textsc{Com}'(0, r)$

Note: a_i and r_i in setup should not be known by any party.
Done either obliviously or by trusted party

Single-value commitments over $\mathbb{Z}_m$, m odd

Consider for now $\mathcal{R} = \mathbb{H} = \mathbb{Z}_N^*$, where N RSA-modulus, $\gcd(m, \varphi(N)) = 1$

Setup:

a is selected at random in $\mathbb{H}$.

Output $g = a^m \in \mathbb{H}$

Commit:

$\textsc{Com}(x, r) = g^x \cdot r^m$

Construction for $\mathbb{Z}_m$, m even

Obstacle for RSA-based construction before:
$\gcd(m, \varphi(N)) \neq 1$

We take $N = p \cdot q$, with $p \equiv q \equiv 3 \bmod 4$.
We use $\mathbb{H} = J^+ = \{x \in \mathbb{Z}_N^*$ with Jacobi symbol $+1\}$ and
$\mathcal{R} = \mathbb{Z}_N^* \times \{0, 1\}$

Setup:
Random $g \in J^+$

Commit:
$\textsc{Com}(x, (r, b)) = g^x \cdot r^m \cdot (-1)^b$

Commit and Proof for linear forms

Given $L : \mathbb{Z}_m^n \to \mathbb{Z}_m$ linear.

We want a proof for language

$\{(P, y; x, \gamma) : \mathrm{COM}_{pk}(x, \gamma) = P,\ L(x) = y\}$

We may assume $m = p^k$ (otherwise we use CRT).

Commit and Proof for linear forms

Given $L : \mathbb{Z}_m^n \to \mathbb{Z}_m$ linear.
We want a proof for language
$\{(P, y; x, \gamma) : \text{COM}_{pk}(x, \gamma) = P,\ L(x) = y\}$
If m prime, a standard Σ-protocol with soundness $1/m$ is:

$$(P, y; \vec{x}, \gamma),\ P = \text{COM}(\vec{x}, \gamma),\ y = L(\vec{x})$$

Prover		Verifier
$\vec{r} \leftarrow_R \mathbb{Z}_m^n,\quad \rho \leftarrow_R \mathcal{R}^d$		
$A = \text{COM}(\vec{r}, \rho),\quad t = L(\vec{r})$	$\xrightarrow{A,t}$	
		$c \leftarrow_R \mathbb{Z}_m$
	$\xleftarrow{c}$	
$\vec{z} = \vec{r} + c\vec{x}$		
$\psi = R(\vec{r}, c\vec{x}, \rho, R(\vec{x}, c, \gamma))$	$\xrightarrow{\vec{z},\psi}$	$\text{COM}'(\vec{z}, \psi) \stackrel{?}{=} A \cdot P^c$
		$L(\vec{z}) \stackrel{?}{=} t + cy$

Using compressed Σ-protocols (Attema-Cramer Crypto20):
Soundness of compression step: $2/m$
Recursion $\log n - 2$ times $\rightsquigarrow$ comm. complexity $O(\log n)$ and soundness $(2 \log n - 3)/m$

Commit and Proof for linear forms

Given $L : \mathbb{Z}_m^n \to \mathbb{Z}_m$ linear.

We want a proof for language

$\{(P, y; x, \gamma) : \textsc{Com}_{pk}(x, \gamma) = P,\ L(x) = y\}$

But in general (if $m = p^k$), we need challenge set $\mathcal{C}$ to be *exceptional*, i.e. $c, c' \in \mathcal{C}$, $c \neq c'$ must satisfy $c - c'$ invertible.

Soundness: $1/|\mathcal{C}|$

Soundness of compressing steps: $2/|\mathcal{C}|$

$(P, y; \vec{x}, \gamma)$,
$P = \textsc{Com}(\vec{x}, \gamma)$
$y = L(\vec{x})$

Prover		Verifier
$\vec{r} \leftarrow_R \mathbb{Z}_m^n, \quad \rho \leftarrow_R \mathcal{R}^d$ $A = \textsc{Com}(\vec{r}, \rho), \quad t = L(\vec{r})$	$\xrightarrow{A,t}$	
		$c \leftarrow_R \mathcal{C} \subseteq \mathbb{Z}_m$
	$\xleftarrow{c}$	
$\vec{z} = \vec{r} + c\vec{x}$ $\psi = R'\left(\vec{r}, c\vec{x}, \rho, R'(\vec{x}, c, \gamma)\right)$	$\xrightarrow{\vec{z},\psi}$	$\textsc{Com}'(\vec{z}, \psi) \stackrel{?}{=} A \cdot P^c$ $L(\vec{z}) \stackrel{?}{=} t + cy$

Galois Rings

$\mathbb{Z}_{p^k}$ may not have large exceptional sets, e.g. if $p^k = 2^k$, exceptional sets have size 2 at most $\rightsquigarrow$ Soundness $1/2$

Compressing is even worse: Soundness $2/|\mathcal{C}| = 1$, hence not even repeting is good!.

Galois Rings

$\mathbb{Z}_{p^k}$ may not have large exceptional sets, e.g. if $p^k = 2^k$, exceptional sets have size 2 at most $\rightsquigarrow$ Soundness $1/2$

Compressing is even worse: Soundness $2/|\mathcal{C}| = 1$, hence not even repeting is good!.

Solution: Using Galois rings.
Galois rings are extensions of $\mathbb{Z}_{p^k}$

$\mathcal{S} = \mathbb{Z}_{p^k}[X]/(f)$
where $f \in \mathbb{Z}_{p^k}[X]$ of degree d, s.t. f mod p irreducible in $\mathbb{Z}_p[X]$ of degree d

Galois Rings

$\mathbb{Z}_{p^k}$ may not have large exceptional sets, e.g. if $p^k = 2^k$, exceptional sets have size 2 at most $\rightsquigarrow$ Soundness $1/2$

Compressing is even worse: Soundness $2/|\mathcal{C}| = 1$, hence not even repeting is good!.

Solution: Using Galois rings.
Galois rings are extensions of $\mathbb{Z}_{p^k}$

$\mathcal{S} = \mathbb{Z}_{p^k}[X]/(f)$
where $f \in \mathbb{Z}_{p^k}[X]$ of degree d, s.t. f mod p irreducible in $\mathbb{Z}_p[X]$ of degree d

$\mathcal{S}$ has exceptional sets of size p^d.

Com. to a vector in $\mathcal{S}^n = d$ com. to vectors in $\mathbb{Z}_m^n$

Final result, compressed Sigma Protocol

$L : \mathbb{Z}_{p^k}^n \to \mathbb{Z}_{p^k}$ linear.

Let $\mathcal{X} = \{(P, y; x, \gamma) : \textsc{Com}(x, \gamma) = P,\ L(x) = y\}$

We have a protocol for $\mathcal{X}^d$ with:

- $d = \mathcal{O}(\lambda + \log\log n)$
- Communication complexity $\mathcal{O}(\lambda \log n + \log n \log\log n)$
- Soundness error $2^{-\lambda}$

Final result, compressed Sigma Protocol

$L : \mathbb{Z}_{p^k}^n \to \mathbb{Z}_{p^k}$ linear.
Let $\mathcal{X} = \{(P, y; x, \gamma) : \textsc{Com}(x, \gamma) = P,\ L(x) = y\}$
We have a protocol for $\mathcal{X}^d$ with:

- $d = \mathcal{O}(\lambda + \log\log n)$
- Communication complexity $\mathcal{O}(\lambda \log n + \log n \log\log n)$
- Soundness error $2^{-\lambda}$

In particular, given $P = Com(x, r)$:
Position opening $x_i = y$ has communication complexity
$O_\lambda(\log n \log\log n)$

Other results in paper

Commitments:

- Single value commitments from "commitment friendly groups".
- Constructions on class groups to remove or relax trusted setup

Compressed Sigma-protocols:

- More details
- Comparison with other approaches

Application:

- Verifiable computation on encrypted data (Bois et al. PKC 21)

Thanks!