Range Proofs

Efficient Range Proofs with Transparent Setup from Bounded Integer Commitments

authors:

* Geoffroy Couteau (IRIF – CNRS)
* Michael Klooß (KIT)
* Huang Lin (Mercury's Wing – Suterusu)
* Michael Reichle (ENS – CNRS – PSL University – Inria)

on: June 10, 2021

» Application

Privacy-Preserving Technologies

» Application

Privacy-Preserving Technologies

» Application

» Application

Privacy-Preserving Technologies

» Application

Privacy-Preserving Technologies

» Application

» Commitments

$$c = \boxed{x\ ;r} \xrightarrow[open]{x,r} \text{Verify}(c, x, r) = 1$$

» Commitments

$$c = \boxed{x\,;r} \xrightarrow[\textit{open}]{x,r} \mathsf{Verify}(c, x, r) = 1$$

Properties

- **Hiding**: The commitment does not reveal x.
- **Binding**: The commitment *can* not be opened to something else than x.

» Commitments

$$c = \boxed{x\,;r} \xrightarrow[\textit{open}]{x,r} \mathrm{Verify}(c, x, r) = 1$$

Properties

* **Hiding**: The commitment does not reveal x.
* **Binding**: The commitment *can* not be opened to something else than x.
* **Msg Space**: $x \in \mathbb{Z}_q$

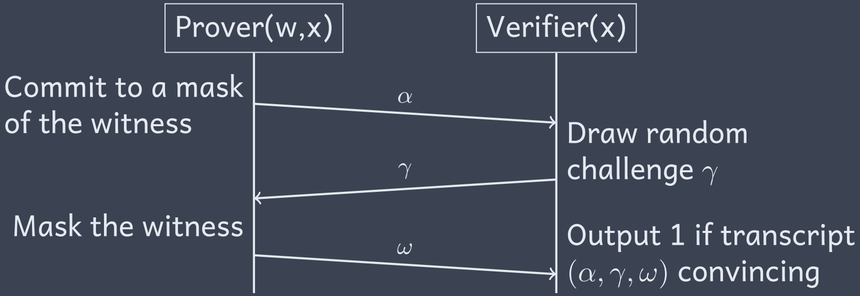
» Commitments

$$c = \boxed{x\,;r} \xrightarrow[\text{open}]{x,r} \mathsf{Verify}(c, x, r) = 1$$

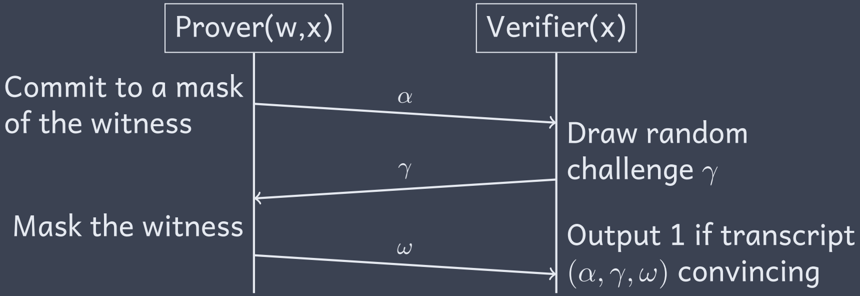
Properties

- **Hiding**: The commitment does not reveal x.
- **Binding**: The commitment can not be opened to something else than x.
- **Msg Space**: $x \in \mathbb{Z}_q$
- **Homomorphy**:
  - Additive: $\boxed{x_0\,;r_0} + \boxed{x_1\,;r_1} = \boxed{x_0 + x_1\,;r_0 + r_1}$
  - Scalar: $n \cdot \boxed{x\,;r} = \boxed{n \cdot x\,;n \cdot r}$

» Σ-Protocols


Prover(w,x)
Verifier(x)
Commit to a mask of the witness
α
Draw random challenge γ
γ
Mask the witness
ω
Output 1 if transcript (α, γ, ω) convincing

» Σ-Protocols



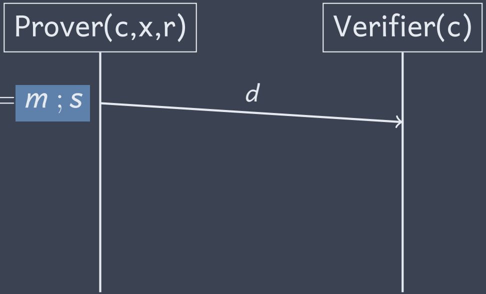
Properties

- **Zero-Knowledge:** Transcripts can be simulated without w.
- **Soundness:** A witness w can be extracted from accepted transcripts.

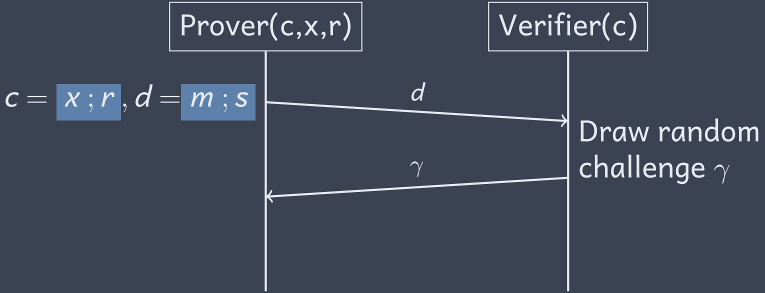
» Proof of Opening

Protocol

$c = x \,;\, r,\ d = m \,;\, s$



» Proof of Opening



» Proof of Opening

Prover(c,x,r)		Verifier(c)
$c = \boxed{x\,;r}, d = \boxed{m\,;s}$	$\xrightarrow{d}$	
	$\xleftarrow{\gamma}$	Draw random challenge γ
$z = m + \gamma x,$ $t = s + \gamma r$	$\xrightarrow{z,\, t}$	

» Proof of Opening

Protocol

Prover(c,x,r)		Verifier(c)
$c = \boxed{x\,;r}, d = \boxed{m\,;s}$	$\xrightarrow{d}$	
	$\xleftarrow{\gamma}$	Draw random challenge γ
$z = m + \gamma x,$ $t = s + \gamma r$	$\xrightarrow{z,\,t}$	$\boxed{m\,;s} + \gamma \boxed{x\,;r} = \boxed{z\,;t}$?

» Proof of Opening

Reminder

- Statement: $c = \boxed{x\,;r}$
- Honest transcript: $d = \boxed{m\,;s}, \gamma, z = m + \gamma x, t = s + \gamma r$

» Proof of Opening

Extraction

Reminder

* Statement: $c = \boxed{x\,;r}$
* Honest transcript: $d = \boxed{m\,;s}, \gamma, z = m + \gamma x, t = s + \gamma r$

Assume $\mathcal{A}$ can output accepting transcripts

$$tr_0 = [d, \gamma_0, z_0, t_0] \text{ and } tr_1 = [d, \gamma_1, z_1, t_1]$$

» Proof of Opening

Reminder

* Statement: $c = \boxed{x\ ;r}$
* Honest transcript: $d = \boxed{m\ ;s}, \gamma, z = m + \gamma x, t = s + \gamma r$

Assume $\mathcal{A}$ can output accepting transcripts

$$tr_0 = [d, \gamma_0, z_0, t_0] \text{ and } tr_1 = [d, \gamma_1, z_1, t_1]$$

Then

$$d + \gamma_0 c = \boxed{z_0\ ;t_0} \wedge d + \gamma_1 c = \boxed{z_1\ ;t_1}$$

» Proof of Opening

Reminder

* Statement: $c = \boxed{x\ ;r}$
* Honest transcript: $d = \boxed{m\ ;s}, \gamma, z = m + \gamma x, t = s + \gamma r$

Assume $\mathcal{A}$ can output accepting transcripts

$$tr_0 = [d, \gamma_0, z_0, t_0] \text{ and } tr_1 = [d, \gamma_1, z_1, t_1]$$

Then

$$d + \gamma_0 c = \boxed{z_0\ ;t_0} \wedge d + \gamma_1 c = \boxed{z_1\ ;t_1}$$
$$\Rightarrow (\gamma_0 - \gamma_1)c = \boxed{z_0 - z_1\ ;t_0 - t_1}$$

» Proof of Opening

Extraction

Reminder

- Statement: $c = \boxed{x\,;r}$
- Honest transcript: $d = \boxed{m\,;s}, \gamma, z = m + \gamma x, t = s + \gamma r$

Assume $\mathcal{A}$ can output accepting transcripts

$$tr_0 = [d, \gamma_0, z_0, t_0] \text{ and } tr_1 = [d, \gamma_1, z_1, t_1]$$

Then

$$d + \gamma_0 c = \boxed{z_0\ ;t_0} \wedge d + \gamma_1 c = \boxed{z_1\ ;t_1}$$
$$\Rightarrow (\gamma_0 - \gamma_1)c = \boxed{z_0 - z_1\ ;t_0 - t_1}$$
$$\Rightarrow c = \boxed{(z_0 - z_1)/(\gamma_0 - \gamma_1)\ ;(t_0 - t_1)/(\gamma_0 - \gamma_1)}$$

» Proof of Opening

Extraction

Reminder

* Statement: $c = \boxed{x \,;\, r}$
* Honest transcript: $d = \boxed{m \,;\, s}, \gamma, z = m + \gamma x, t = s + \gamma r$

Assume $\mathcal{A}$ can output accepting transcripts

$$tr_0 = [d, \gamma_0, z_0, t_0] \text{ and } tr_1 = [d, \gamma_1, z_1, t_1]$$

Then

$$d + \gamma_0 c = \boxed{z_0 \,;\, t_0} \wedge d + \gamma_1 c = \boxed{z_1 \,;\, t_1}$$
$$\Rightarrow (\gamma_0 - \gamma_1)c = \boxed{z_0 - z_1 \,;\, t_0 - t_1}$$
$$\Rightarrow c = \boxed{(z_0 - z_1)/(\gamma_0 - \gamma_1) \,;\, (t_0 - t_1)/(\gamma_0 - \gamma_1)}$$

In total: $x = (z_0 - z_1)/(\gamma_0 - \gamma_1)$ in $\mathbb{Z}_q$

» Range Proofs

Definition

Zero-knowledge proof for $\mathsf{R} = \{((x, r), (\boxed{x\,;r}, a, b)) \mid x \in [a, b]\}$

» Range Proofs

Approach

Zero-knowledge proof for $\mathrm{R} = \{((x, r), (\boxed{x\,; r}, a, b)) \mid x \in [a, b]\}$

$$x \in [0, 2^\ell) \iff x = \sum_{i=0..\ell-1} x_i 2^i \text{ and } x_i \in \{0, 1\}$$

Approaches

- **Binary Decomposition:**
  - commit to the decomposition
  - prove that $x_i \in \{0, 1\}$
  - most common approach (Lattice, DLOG, ..)

» Range Proofs

Approach

Zero-knowledge proof for $\mathrm{R} = \{((x, r), (x\,;r, a, b)) \mid x \in [a, b]\}$

$$x \in [a, b] \iff x - a, b - x \geq 0$$

Approaches

* **Integer Commitments:**
  * prove that $(b - x)(x - a) = \sum_{i=1..4} x_i^2$
  * $x \in \mathbb{Z}$
  * require trusted setup, large parameters

» Range Proofs

Decomposition

Simplification for $B = b - a$

$$x \in [a, b] \iff x - a \in [0, b - a] \iff x(B - x) = \sum_{i=1..4} x_i^2$$

» Range Proofs

Simplification for $B = b - a$

$$x \in [a, b] \iff x - a \in [0, b - a] \iff x(B - x) = \sum_{i=1..4} x_i^2$$

Optimization [Gro05]

$$x \in [0, B] \iff 1 + 4x(B\text{-}x) = \sum_{i=1..3} x_i^2$$

» Setting

Range Proof

* (generic) commitment: $c_0 = \boxed{x_0 \mod \boldsymbol{q} \,;\, r_0}$
* avoid trusted setup
* optimize efficiency

» Approach I

Idea

Use 3 square decomposition in $\mathbb{Z}_q$:

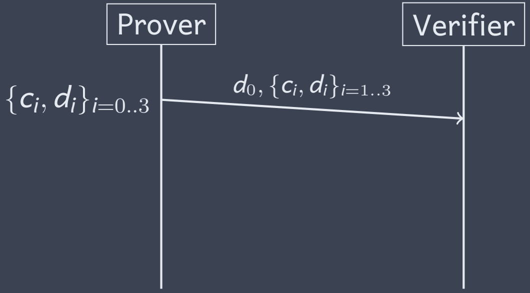
$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

Approach I

Idea

Use 3 square decomposition in $\mathbb{Z}_q$:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

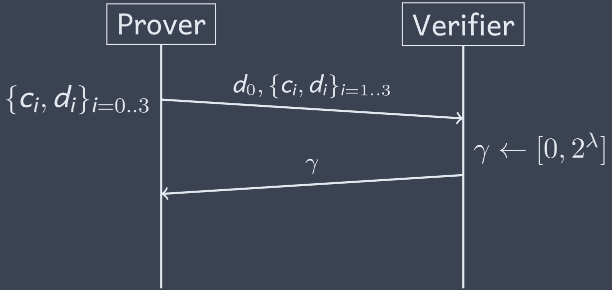


» Approach I

Idea

Use 3 square decomposition in $\mathbb{Z}_q$:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

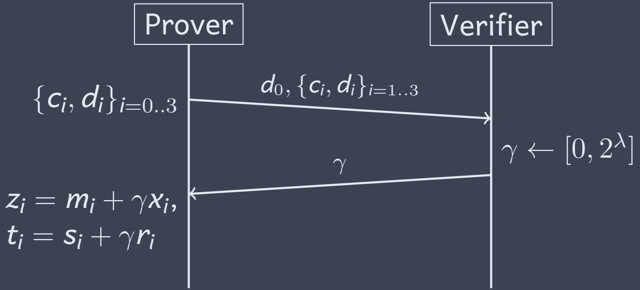


» Approach I

Idea

Use 3 square decomposition in $\mathbb{Z}_q$:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$



» Approach I

Idea

Use 3 square decomposition in $\mathbb{Z}_q$:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

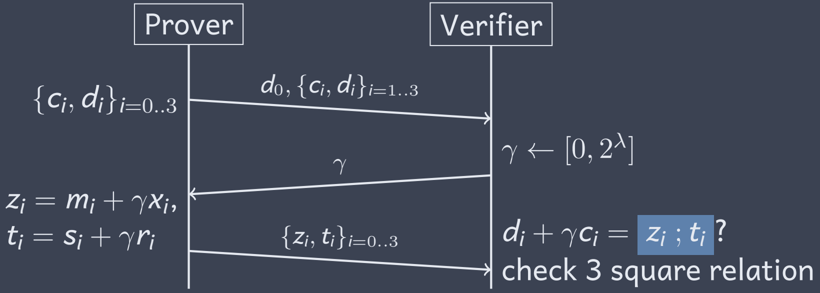
Prover		Verifier
$\{c_i, d_i\}_{i=0..3}$	$\xrightarrow{d_0, \{c_i, d_i\}_{i=1..3}}$	
	$\xleftarrow{\gamma}$	$\gamma \leftarrow [0, 2^\lambda]$
$z_i = m_i + \gamma x_i$, $t_i = s_i + \gamma r_i$	$\xrightarrow{\{z_i, t_i\}_{i=0..3}}$	

» Approach I

Idea

Use 3 square decomposition in $\mathbb{Z}_q$:

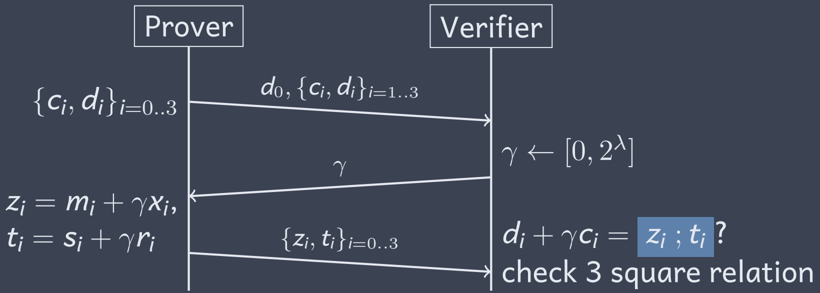
$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$



» Approach I

Problem

3 square decomposition in $\mathbb{Z}_q$ does not imply positivity



» Approach II

Idea

Avoid overflows by ensuring short witnesses

Prover		Verifier
$\{c_i, d_i\}_{i=0..3}$	$\xrightarrow{d_0, \{c_i, d_i\}_{i=1..3}}$	
	$\xleftarrow{\gamma}$	$\gamma \leftarrow [0, 2^\lambda]$
$z_i = m_i + \gamma x_i$, $t_i = s_i + \gamma r_i$	$\xrightarrow{\{z_i, t_i\}_{i=0..3}}$	$d_i + \gamma c_i = z_i \,;\, t_i$?
		check 3 square relation
		check z_i short

» Approach II

Problem

Extracted $x_0 = \frac{z_0 - z_0'}{\gamma - \gamma'} \mod q$ not short

Prover | **Verifier**

Prover: $\{c_i, d_i\}_{i=0..3}$

Prover → Verifier: $d_0, \{c_i, d_i\}_{i=1..3}$

Verifier: $\gamma \leftarrow [0, 2^\lambda]$

Verifier → Prover: γ

Prover: $z_i = m_i + \gamma x_i$, $t_i = s_i + \gamma r_i$

Prover → Verifier: $\{z_i, t_i\}_{i=0..3}$

Verifier:
$d_i + \gamma c_i = \boxed{z_i \,;\, t_i}$?
check 3 square relation
check z_i short

» Approach II

Example

Problem

$$\frac{1}{2} = 3057 \mod 6113 \text{ is large}$$

» Approach II

Example

Problem

$$\frac{1}{2} = 3057 \mod 6113 \text{ is large}$$

Idea

Map fractions in $\mathbb{Z}_q$ to integers via division in $\mathbb{Q}$

» Approach II

Example

Problem

$$\frac{1}{2} = 3057 \mod 6113 \text{ is large}$$

Idea

Map fractions in $\mathbb{Z}_q$ to integers via division in $\mathbb{Q}$

Encoding

$$\left\lfloor \frac{1}{2} \right\rceil = 1 \text{ is small}$$

» Approach III

Relax commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

» Approach III

Relax commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Properties

- binding if z, γ short

» Approach III

Relax commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Properties

* binding if z, γ short
* retains (restricted) homomorphic properties

» Approach III

Relax commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Properties

- binding if z, γ short
- retains (restricted) homomorphic properties
- retains shortness

» Approach III

Relax commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Properties

- binding if z, γ short
- retains (restricted) homomorphic properties
- retains shortness
- honest commitment unchanged

» Approach III

Relax commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Properties

* binding if z, γ short
* retains (restricted) homomorphic properties
* retains shortness
* honest commitment unchanged

$\rightarrow$ Bounded integer commitment scheme

» Binding Property

Relaxed commitment scheme:

$$z \cdot \gamma^{-1} \mod q \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Binding Proof

Receive $z_0 \cdot \gamma_0^{-1} \mod q$ and $z_1 \cdot \gamma_1^{-1} \mod q$

» Binding Property

Relaxed commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Binding Proof

Receive $\boxed{z_0 \cdot \gamma_0^{-1} \mod q}$ and $\boxed{z_1 \cdot \gamma_1^{-1} \mod q}$

* Binding $\Rightarrow z_0 \cdot \gamma_0^{-1} = z_1 \cdot \gamma_1^{-1} \mod q$

» Binding Property

Relaxed commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Binding Proof

Receive $\boxed{z_0 \cdot \gamma_0^{-1} \mod q}$ and $\boxed{z_1 \cdot \gamma_1^{-1} \mod q}$

* Binding $\Rightarrow z_0 \cdot \gamma_0^{-1} = z_1 \cdot \gamma_1^{-1} \mod q$
  $\Rightarrow z_0 \cdot \gamma_1 = z_1 \cdot \gamma_0 \mod q$

» Binding Property

Relaxed commitment scheme:

$$z \cdot \gamma^{-1} \mod q \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Binding Proof

Receive $z_0 \cdot \gamma_0^{-1} \mod q$ and $z_1 \cdot \gamma_1^{-1} \mod q$

* Binding $\Rightarrow z_0 \cdot \gamma_0^{-1} = z_1 \cdot \gamma_1^{-1} \mod q$
  $\Rightarrow z_0 \cdot \gamma_1 = z_1 \cdot \gamma_0 \mod q$
* Shortness $\Rightarrow z_0\gamma_1 = z_1\gamma_0$ over $\mathbb{Q}$

» Binding Property

Relaxed commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Binding Proof

Receive $\boxed{z_0 \cdot \gamma_0^{-1} \mod q}$ and $\boxed{z_1 \cdot \gamma_1^{-1} \mod q}$

* Binding $\Rightarrow z_0 \cdot \gamma_0^{-1} = z_1 \cdot \gamma_1^{-1} \mod q$
  $\Rightarrow z_0 \cdot \gamma_1 = z_1 \cdot \gamma_0 \mod q$
* Shortness $\Rightarrow z_0 \gamma_1 = z_1 \gamma_0$ over $\mathbb{Q}$
  $\Rightarrow \frac{z_0}{\gamma_0} = \frac{z_1}{\gamma_1}$ over $\mathbb{Q}$

» Binding Property

Relaxed commitment scheme:

$$\boxed{z \cdot \gamma^{-1} \mod q} \text{ commits to } x = \left\lfloor \frac{z}{\gamma} \right\rceil \in \mathbb{Z}$$

Binding Proof

Receive $\boxed{z_0 \cdot \gamma_0^{-1} \mod q}$ and $\boxed{z_1 \cdot \gamma_1^{-1} \mod q}$

* Binding $\Rightarrow z_0 \cdot \gamma_0^{-1} = z_1 \cdot \gamma_1^{-1} \mod q$
  $\Rightarrow z_0 \cdot \gamma_1 = z_1 \cdot \gamma_0 \mod q$
* Shortness $\Rightarrow z_0\gamma_1 = z_1\gamma_0$ over $\mathbb{Q}$
  $\Rightarrow \frac{z_0}{\gamma_0} = \frac{z_1}{\gamma_1}$ over $\mathbb{Q}$
  $\Rightarrow \left\lfloor \frac{z_0}{\gamma_0} \right\rceil = \left\lfloor \frac{z_1}{\gamma_1} \right\rceil$ over $\mathbb{Q}$

» Approach III

Obtain range proof for relaxed committed value

Prover | Verifier

$\{c_i, d_i\}_{i=0..3}$ $\xrightarrow{d_0, \{c_i, d_i\}_{i=1..3}}$

$\gamma \leftarrow [0, 2^\lambda]$

$\xleftarrow{\gamma}$

$z_i = m_i + \gamma x_i,$

$t_i = s_i + \gamma r_i$ $\xrightarrow{\{z_i, t_i\}_{i=0..3}}$

$d_i + \gamma c_i = \boxed{z_i \,;\, t_i}$?

check 3 square relation

check z_i short

Extraction

$$\frac{z - z'}{\gamma - \gamma'} \in \mathbb{Z}_q \mapsto \left\lfloor \frac{z - z'}{\gamma - \gamma'} \right\rceil \in \mathbb{Z} \text{ short}$$

» Showing the Decomposition

Requires sending additional group elements and integers.

* Commitments c_1, c_2, c_3 to decomposition x_1, x_2, x_3
* Proof of openings of c_1, c_2, c_3
* Additional mask (DLOG, Lattice, Class Groups)
* Additional commitments (Lattice)

» Limitations - Homomorphism

$\boxed{z \cdot \gamma^{-1} \; ; r}$ commits to $x = \lfloor z/\gamma \rceil \in \mathbb{Z}$

* **Honest:** $\boxed{x_0 \; ; r} + \boxed{x_1 \; ; s} = \boxed{x_0 + x_1 \; ; r + s}$

» Limitations - Homomorphism

$\boxed{z \cdot \gamma^{-1} ; r}$ commits to $x = \lfloor z/\gamma \rceil \in \mathbb{Z}$

* **Honest:** $\boxed{x_0 ; r} + \boxed{x_1 ; s} = \boxed{x_0 + x_1 ; r + s}$
* **Small Constants:**
    * $\boxed{z \cdot \gamma^{-1} ; r} + \boxed{a ; 0} = \boxed{(z + \gamma a) \cdot \gamma^{-1} ; r}$
    * commits to $x + a = \lfloor z/\gamma \rceil + a$

» Limitations - Homomorphism

$\boxed{z \cdot \gamma^{-1} \,;\, r}$ commits to $x = \lfloor z/\gamma \rceil \in \mathbb{Z}$

* **Honest:** $\boxed{x_0 \,;\, r} + \boxed{x_1 \,;\, s} = \boxed{x_0 + x_1 \,;\, r + s}$
* **Small Constants:**
  * $\boxed{z \cdot \gamma^{-1} \,;\, r} + \boxed{a \,;\, 0} = \boxed{(z + \gamma a) \cdot \gamma^{-1} \,;\, r}$
  * commits to $x + a = \lfloor z/\gamma \rceil + a$
* **Dishonest:**
  * $\boxed{z_0 \cdot \gamma^{-1} \,;\, r} + \boxed{z_1 \cdot \gamma^{-1} \,;\, s} = \boxed{(z_0 + z_1) \cdot \gamma^{-1} \,;\, r + s}$
  * commits to $\lfloor z_0/\gamma \rceil + \lfloor z_1/\gamma \rceil + \{0, 1\}$
  * worse for non-equal denominator

» Limitations - Homomorphism

$\boxed{z \cdot \gamma^{-1}\,;r}$ commits to $x = \lfloor z/\gamma \rceil \in \mathbb{Z}$

- Honest: $\boxed{x_0\,;r} + \boxed{x_1\,;s} = \boxed{x_0 + x_1\,;r+s}$
- Small Constants:
  - $\boxed{z \cdot \gamma^{-1}\,;r} + \boxed{a\,;0} = \boxed{(z+\gamma a) \cdot \gamma^{-1}\,;r}$
  - commits to $x + a = \lfloor z/\gamma \rceil + a$
- Dishonest:
  - $\boxed{z_0 \cdot \gamma^{-1}\,;r} + \boxed{z_1 \cdot \gamma^{-1}\,;s} = \boxed{(z_0 + z_1) \cdot \gamma^{-1}\,;r+s}$
  - commits to $\lfloor z_0/\gamma \rceil + \lfloor z_1/\gamma \rceil + \{0, 1\}$
  - worse for non-equal denominator

$\rightarrow$ ensure that committed integers are small enough

$\rightarrow$ be careful about guarantees

» Limitations - Group Size

Need to ensure no overflow in square decomposition:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

» Limitations - Group Size

Need to ensure no overflow in square decomposition:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

Can only check size of z_i:

$$1 + 4z_0(B - z_0) = \sum_{i=1..3} z_i^2$$

» Limitations - Group Size

Need to ensure no overflow in square decomposition:

$$1 + 4x_0(B - x_0) = \sum_{i=1..3} x_i^2$$

Can only check size of z_i:

$$1 + 4z_0(B - z_0) = \sum_{i=1..3} z_i^2$$

$\rightarrow$ ensure that both sides are smaller than the modulus q
$\rightarrow$ leads to large group size

» Optimizations

$$z_i = m_i + \gamma x_i$$

* **Rejection Sampling:** shorter masks $\rightarrow$ smaller modulus

» Optimizations

$$z_i = m_i + \gamma x_i$$

* **Rejection Sampling**: shorter masks $\rightarrow$ smaller modulus
* **Repetitions**: shorter challenge $\rightarrow$ smaller modulus

» Optimizations

$$z_i = m_i + \gamma x_i$$

* **Rejection Sampling**: shorter masks $\rightarrow$ smaller modulus
* **Repetitions**: shorter challenge $\rightarrow$ smaller modulus
* **Fiat-Shamir**: non-interactive range proof

» Settings

* **DLOG**: improves on Bulletproofs [BBB+18]
* **Lattice**: efficient for large batches
* **Class Groups**: first concretely efficient unbounded integer commitment scheme without trusted setup

» DLOG

Pedersen Commitments

- $\mathbb{G}$: group with prime order q
- $g, h \in \mathbb{G}$: generators
- $x \in Z_q, r \leftarrow [0, 2^{2\lambda}]$

$$\boxed{x\,;r} = g^x h^r$$

- based on DLSE assumption

» DLOG

Pedersen Commitments

* $\mathbb{G}$: group with prime order q
* $g, h \in \mathbb{G}$: generators
* $x \in Z_q, r \leftarrow [0, 2^{2\lambda}]$

$$\boxed{x\,;r} = g^x h^r$$

* based on DLSE assumption

* Decomposition: use (honest) homomorphic properties
* Efficient range proofs for single x

» DLOG

Security Parameter	80	128
Range	$B = 32$	
Proof size	88%	81%
Prover's work	12%	11%
Range	$B = 64$	
Proof size	89%	80%
Prover's work	6%	6%

Our work compared to Bulletproofs [BBB+18]. Prover's work compared in group multiplications.

» Lattices

[BDL+18] commitments

* $q \in \mathbb{N}$ prime
* matrix $A \in \mathbb{Z}_q^{(l1+n)\times(l1+n+l2)}$
* $\vec{x} \in \mathbb{Z}_q^n, \vec{r} \leftarrow D_\sigma^{l1+n+l2}$

$$\boxed{\vec{x}\,;\vec{r}} = A \cdot \vec{r} + (\vec{0} \,\|\, \vec{x})$$

* based on SIS and LWE assumption

* Decomposition with polynomial trick
* Perform range proof for each component
* Amortized proofs more efficient than the state of the art in standard lattice setting

» Class Groups

Pedersen Commitments

* Groups $\mathbb{G}$ with hidden order
* based on ORD and SI assumption
* extraction differs:

$$x = \frac{z}{2^\ell}$$

» Class Groups

Pedersen Commitments

* Groups $\mathbb{G}$ with hidden order
* based on ORD and SI assumption
* extraction differs:

$$x = \frac{z}{2^\ell}$$

* Same structure as DLOG version
* Larger group elements
* No bounds on the committed values

» References

B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell.
Bulletproofs: Short proofs for confidential transactions and more.
In *2018 IEEE Symposium on Security and Privacy*, pages 315–334, San Francisco, CA, USA, May 21–23, 2018. IEEE Computer Society Press.

C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, and C. Peikert.
More efficient commitments from structured lattice assumptions.
In *SCN 18: 11th International Conference on Security in Communication Networks*, *Lecture Notes in Computer Science* 11035, pages 368–385, Amalfi, Italy, September 5–7, 2018. Springer, Heidelberg, Germany.

J. Groth.
Non-interactive zero-knowledge arguments for voting.
In *ACNS 05: 3rd International Conference on Applied Cryptography and Network Security*, *Lecture Notes in Computer Science* 3531, pages 467–482, New York, NY, USA, June 7–10, 2005. Springer, Heidelberg, Germany.