Rational Modular Encoding in the DCR Setting: Non-Interactive Range Proofs and Paillier-Based Naor-Yung in the Standard Model

Julien Devevey[1] Benoît Libert[2,1] Thomas Peters[3]

ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, Inria, UCBL), France

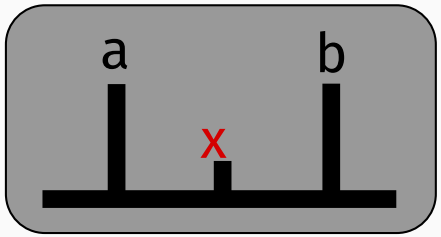
CNRS, Laboratoire LIP, France

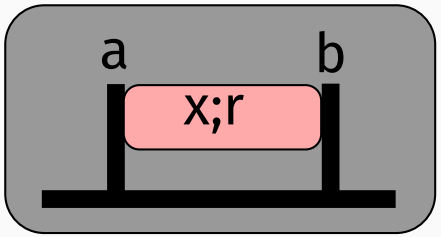
FNRS and Université catholique de Louvain, Belgium

Table of contents

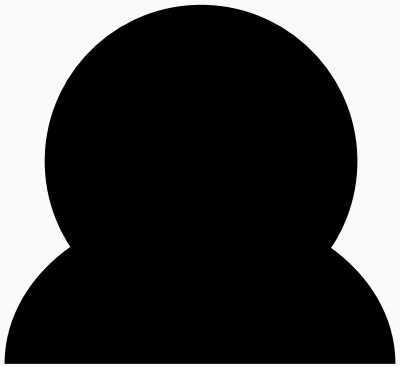
Introduction

Range Proofs

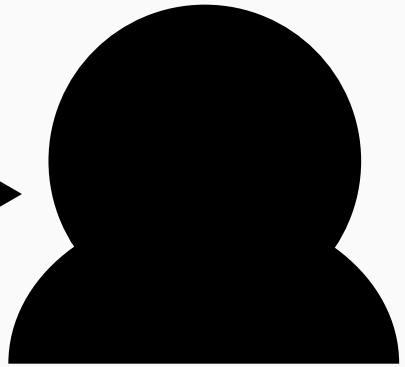




“My commitment belongs to [a,b]”



Prover



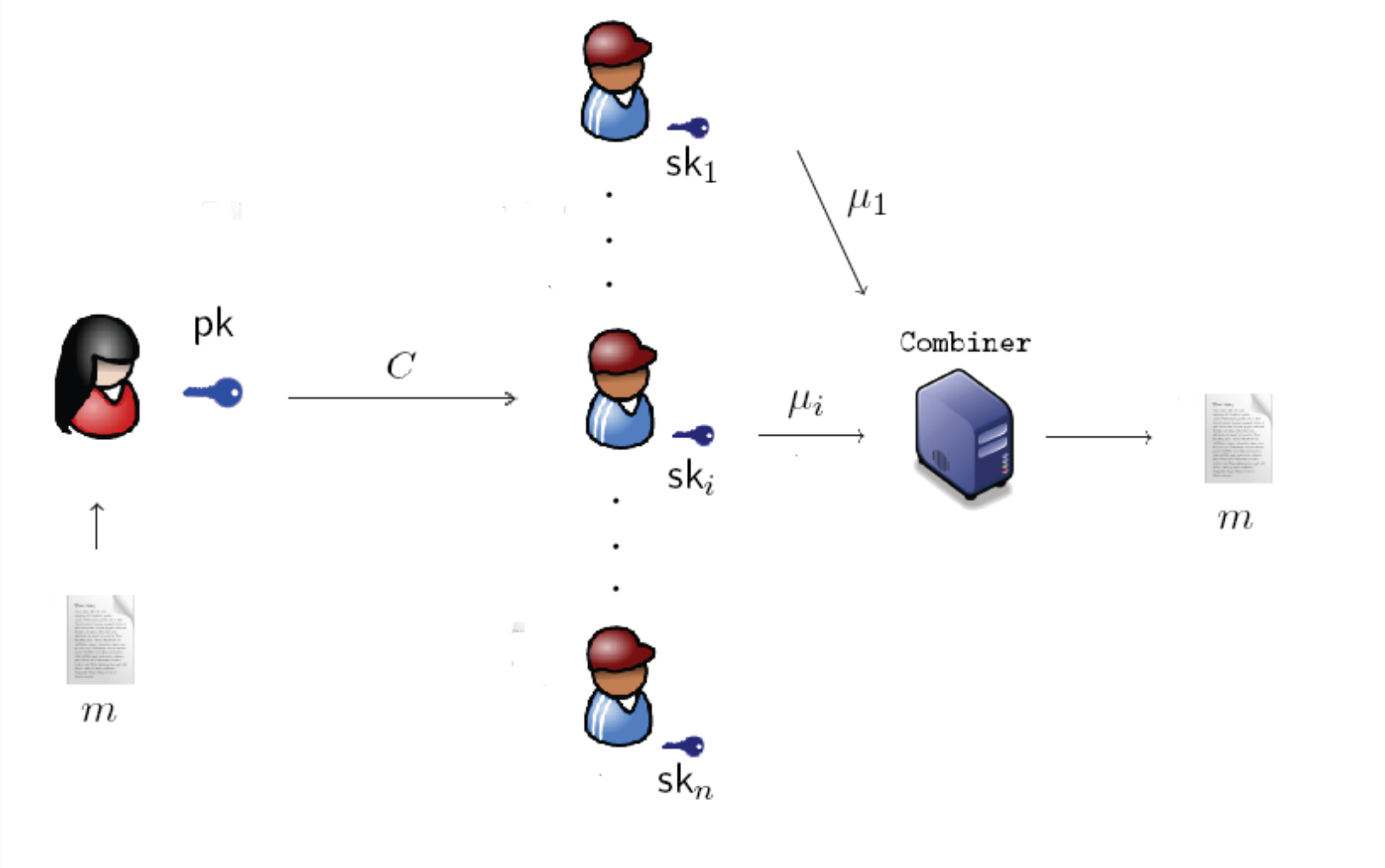
Verifier

Previous works and our results

	Setting	Unbounded	Constant rate
[*GS*08]	Pairings	✓	✗
[*CKLR*21]	DLog, Lattice, Class Group	✗	✓
Our work	DCR	✓	✓

- Unbounded means a, b are not a priori bounded by the parameters,
- The rate is the ratio of the length of commitment+proof over the length of the witness.

Threshold Cryptography



Previous works and our results

- Flawed instantiation of Naor-Yung under the DCR assumption in the Random Oracle Model (Fouque et al.; Asiacrypt'01).
- Recent construction satisfying IND-CCA2 security against adaptive adversaries in the standard model under the DCR assumption, with superlinear-size secret key shares (D. et al.; PKC'21).

Our result: A new sigma protocol letting us instantiate Naor-Yung in the standard model, leading to IND-CCA2 security against static adversaries under the DCR assumption with constant-size public key and key shares.

Previous works and our results

- Flawed instantiation of Naor-Yung under the DCR assumption in the Random Oracle Model (Fouque et al.; Asiacrypt'01).
- Recent construction satisfying IND-CCA2 security against adaptive adversaries in the standard model under the DCR assumption, with superlinear-size secret key shares (D. et al.; PKC'21).

Our result: A new sigma protocol letting us instantiate Naor-Yung in the standard model, leading to IND-CCA2 security against static adversaries under the DCR assumption with constant-size public key and key shares.

Definitions

Hardness assumptions

ζ-Decision Composite Residuosity assumption [Pai99, DJ01]

Given $N = pq$ and $\zeta > 1$ for primes p, q. The distributions $\{x = w^{N^\zeta} \bmod N^{\zeta+1} \mid w \leftarrow U(\mathbb{Z}_N^\star)\}$ and $\{x \mid x \leftarrow U(\mathbb{Z}_{N^{\zeta+1}}^\star)\}$ are computationally indistinguishable.

Lemma (Adapted from `(Damgård-Jurik; PKC'01)`)

Let $\zeta = \mathsf{poly}(\lambda)$. The $\zeta-$DCR assumption is equivalent to the 1-DCR assumption.

Trapdoor Sigma-Protocol

A trapdoor Sigma-protocol for a language $\mathcal{L} = (\mathcal{L}_{\mathsf{zk}}, \mathcal{L}_{\mathsf{sound}})$ and two NP relations $\mathcal{R}_{\mathsf{zk}}, \mathcal{R}_{\mathsf{sound}}$ is a 5-uple $\mathsf{Gen}, \mathsf{P}, \mathsf{V}, \mathsf{TrapGen}, \mathsf{BadChallenge}$ of algorithms that interact the following way. Let $\mathsf{crs} = \mathsf{Gen}(1^\lambda)$.

$\mathsf{P}(x, w)$		$\mathsf{V}(x)$
$(a, st) \leftarrow \mathsf{P}(\mathsf{crs}, x, w)$	$\xrightarrow{a}$	
	$\xleftarrow{\mathsf{Chall}}$	$\mathsf{Chall} \hookleftarrow \mathcal{C}$
$z \leftarrow \mathsf{P}(\mathsf{crs}, x, w, a, \mathsf{Chall}, st)$	$\xrightarrow{z}$	
		Accept or Reject.

Properties

- Completeness: if everything is done honestly, V always accepts.
- Special Zero-Knowledge: there exists a PPT simulator *ZKSim* that on input $\mathsf{crs}, x, \mathsf{Chall}$ returns a, z such that (a, Chall, z) is indistinguishable from a real transcript.
- Special Soundness: if $x \notin \mathcal{L}_{\mathsf{sound}}$, then for any first message a, there exists at most one challenge for which an accepting answer exists. It is computed by BadChallenge.
- CRS indistinguishability: $\mathsf{crs} \leftarrow \mathsf{Gen}(1^\lambda)$ is indistinguishable from crs produced by $(\mathsf{crs}, \tau) \leftarrow \mathsf{TrapGen}(1^\lambda)$, where τ is necessary to call *BadChallenge*.

Rational Encoding

Let $(r, s) \in [-R, R] \times [1, S]$, and define $\mathcal{E} : t = r/s \mapsto r \cdot s^{-1} \bmod N^\zeta$ with $2RS < N^\zeta$.

How do we recover t from $\mathcal{E}(t)$?

Define the following lattice:

$$\Lambda := \{(x, y) \in \mathbb{Z}^2 : s \cdot x = y \cdot r \bmod N^\zeta\} = \begin{pmatrix} N^\zeta & 0 \\ \mathcal{E}(t) & 1 \end{pmatrix} \cdot \mathbb{Z}^2.$$

As $(r, s) \in \Lambda$, Gauss' algorithm uniquely recovers r and s (Fouque et. al; FC'02).

Rational Encoding

Let $(r, s) \in [-R, R] \times [1, S]$, and define $\mathcal{E} : t = r/s \mapsto r \cdot s^{-1} \bmod N^\zeta$ with $2RS < N^\zeta$.

How do we recover t from $\mathcal{E}(t)$?

Define the following lattice:

$$\Lambda := \{(x, y) \in \mathbb{Z}^2 : s \cdot x = y \cdot r \bmod N^\zeta\} = \begin{pmatrix} N^\zeta & 0 \\ \mathcal{E}(t) & 1 \end{pmatrix} \cdot \mathbb{Z}^2.$$

As $(r, s) \in \Lambda$, Gauss' algorithm uniquely recovers r and s `(Fouque et. al; FC'02)`.

Encrypting using Rationals

- $\mathsf{KeyGen}(1^\lambda)$: $\mathsf{pk} = N = pq$ and $\mathsf{sk} = p, q$, where $p, q \geq 2^\lambda$ are two primes.
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{Msg} \in \mathbb{N}; r)$: let ℓ_M, ζ be the smallest integers such that $\mathsf{Msg} \leq M = 2^{\ell_M} - 1$ and $N^\zeta \geq 2^{2\lambda+1}M$. Using the randomness $r \in \mathbb{Z}_N^*$, return

$$(\mathsf{ct}, \ell_m) = \left((1+N)^{\mathsf{Msg}} \cdot r^{N^\zeta} \bmod N^{\zeta+1}, \ell_M\right).$$

- $\mathsf{Dec}(\mathsf{sk}, (\mathsf{ct}, \ell_m))$: Get Msg' by applying the Damgård-Jurik decryption algorithm. Use Gauss' algorithm to write $\mathsf{Msg}' = m \cdot c^{-1} \bmod N^\zeta$, return $\lfloor m/c \rceil \in \mathbb{Z}$.

Constant Rate Unbounded Non-Interactive Range Proofs

Which language?

Commitments to an integer $x \in [0, B]$ are encryptions of x. If we also commit to $B - x, x_1, x_2, x_3$ where $1 + 4(B - x)x = x_1^2 + x_2^2 + x_3^3$ and prove membership of

$$\begin{aligned}\mathcal{L}_{\mathrm{zk}}^{B} = \Big\{ & (\mathsf{ct}, \{C_i\}_{i=1}^{3}) \in (\mathbb{Z}_{N^{\zeta+1}}^{*})^4 | \exists x_0, x_1, x_2, x_3 \in [0, B], \\ & \exists s_0, s_1, s_2, s_3 \in \mathbb{Z}_N^* : 1 + 4(B - x_0)x_0 = x_1^2 + x_2^2 + x_3^2 \\ & \wedge \mathsf{ct} = (1+N)^{B-x_0} \cdot s_0^{N^\zeta} \bmod N^{\zeta+1} \\ & \wedge C_i = (1+N)^{x_i} \cdot s_i^{N^\zeta} \bmod N^{\zeta+1} \forall i \in [3] \Big\},\end{aligned}$$

we prove that $x \in [0, B]$. The soundness language is similar, up to some rational multiplication: $\mathsf{Dec}(\mathsf{sk}, C_i) = \lfloor x_i / c \rceil$ and $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \lfloor x / c \rceil$.

Construction

The crs is $\lambda, N = pq$. Let a statement $\mathsf{ct} = (1+N)^x \cdot w^{n^\zeta} \mod N^{\zeta+1}$.

- 1. P generates $(\mathsf{ct}, \{C_i = \mathsf{Enc}(N, x_i; s_i)\}_{i=0}^3)$ with witnesses $\{x_i, s_i\}_{i=0}^3$, where $x_0 = B - x$, $s_0 = w^{-1}$ and $1 + 4(B-x)x = \sum_{i=1}^3 {x_i}^2$.
  2. It samples $\sigma \hookleftarrow U(\mathbb{Z}_N^*), r_i \hookleftarrow U([0, B^*]), \alpha_i \hookleftarrow U(\mathbb{Z}_N^*), i \in [0,3]$.
  3. It sets $R = \mathsf{Enc}(N, 4r_0x_0 - \sum_{i=1}^3 r_ix_i; \sigma(s_1s_2s_3)^{-1}w^{4r_0})$ and $R_i = \mathsf{Enc}(N, r_i; \alpha_i)$ for all $i \in [0,3]$.
  4. It sends $R, \{R_i\}_{i=0}^3, \{C_i\}_{i=1}^3$.

Construction(2)

- On input $\mathsf{Chall} \hookleftarrow U([0, 2^{\lambda} - 1])$, P computes
  1. $\tau = \sigma \cdot (w^{-4x_0} \cdot \prod_{i=1}^{3} s_i^{x_i})^{\mathsf{Chall}}$,
  2. $z_i = r_i + \mathsf{Chall} \cdot x_i$,
  3. $t_i = \alpha_i \cdot s_i^{\mathsf{Chall}} \bmod N$.

  It sends $z = (\tau, \{z_i, t_i\}_{i=0}^{3})$.

- V accepts if
  1. $z_i \in [0, B^*]$,
  2. $R_i = \mathsf{Enc}(N, z_i; t_i) \cdot C_i^{-\mathsf{Chall}} \bmod N^{\zeta+1}, \forall i \in [0, 3]$,
  3. $R = \prod_{i=1}^{3} C_i^{-z_i} \cdot \mathsf{ct}^{4z_0} \cdot \tau^{N^{\zeta}} (1+N)^{\mathsf{Chall}} \bmod N^{\zeta+1}$.

Construction(2)

- On input $\mathsf{Chall} \hookleftarrow U([0, 2^{\lambda} - 1])$, P computes
  1. $\tau = \sigma \cdot (w^{-4x_0} \cdot \prod_{i=1}^{3} s_i^{x_i})^{\mathsf{Chall}}$,
  2. $z_i = r_i + \mathsf{Chall} \cdot x_i$,
  3. $t_i = \alpha_i \cdot s_i^{\mathsf{Chall}} \bmod N$.

  It sends $z = (\tau, \{z_i, t_i\}_{i=0}^{3})$.

- V accepts if
  1. $z_i \in [0, B^*]$,
  2. $R_i = \mathsf{Enc}(N, z_i; t_i) \cdot C_i^{-\mathsf{Chall}} \bmod N^{\zeta+1}, \forall i \in [0, 3]$,
  3. $R = \prod_{i=1}^{3} C_i^{-z_i} \cdot \mathsf{ct}^{4z_0} \cdot \tau^{N^{\zeta}} (1 + N)^{\mathsf{Chall}} \bmod N^{\zeta+1}$.

Properties

Theorem

This sigma-protocol satisfies

- Completeness,
- Special Zero-Knowledge,
- Special Soundness and CRS Indistinguishability, for a BadChallenge function that uses linear programming and Lenstra's algorithm,
- Unboundedness: when crs is fixed, it does not constrain B,
- Constant-rate: ratio size of commitment+transcript over size of witness is upper bounded by a constant.

Moreover, it can be compiled into a multi-theorem NIZK without losing the unboundedness property.

Instantiating Naor-Yung under the DCR Assumption

Threshold Public-Key Encryption (TPKE)

A compact TPKE is a 5-uple (KeyGen, Enc, PartDec, PartVerify, Combine) of algorithms that interact the following way:

Server i	Alice	Bob
	$(\mathsf{pk}, \{\mathsf{sk}_i\}) \leftarrow \mathsf{KeyGen}(1^\lambda, t)$	
	$\mathsf{sk}_i \longleftarrow$	$\longrightarrow \mathsf{pk}$
		$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
		$\longleftarrow \mathsf{ct}$
	$\mathsf{ct} \longleftarrow$	
$m_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$		
	$\longrightarrow m_i$	
	$m' \leftarrow \mathsf{Combine}(\mathsf{pk}, \{m_j\}_{j \in \mathcal{S}}, \mathsf{ct})$	

Under the condition that $|\mathsf{pk}|, |\mathsf{ct}| = \mathsf{poly}(\lambda)$.

It is correct if $\forall |\mathcal{S}| \geq t, m = m'$ with proba $\geq 1 - \mathsf{negl}(\lambda)$.

Threshold Public-Key Encryption (TPKE)

A compact TPKE is a 5-uple (KeyGen, Enc, PartDec, PartVerify, Combine) of algorithms that interact the following way:

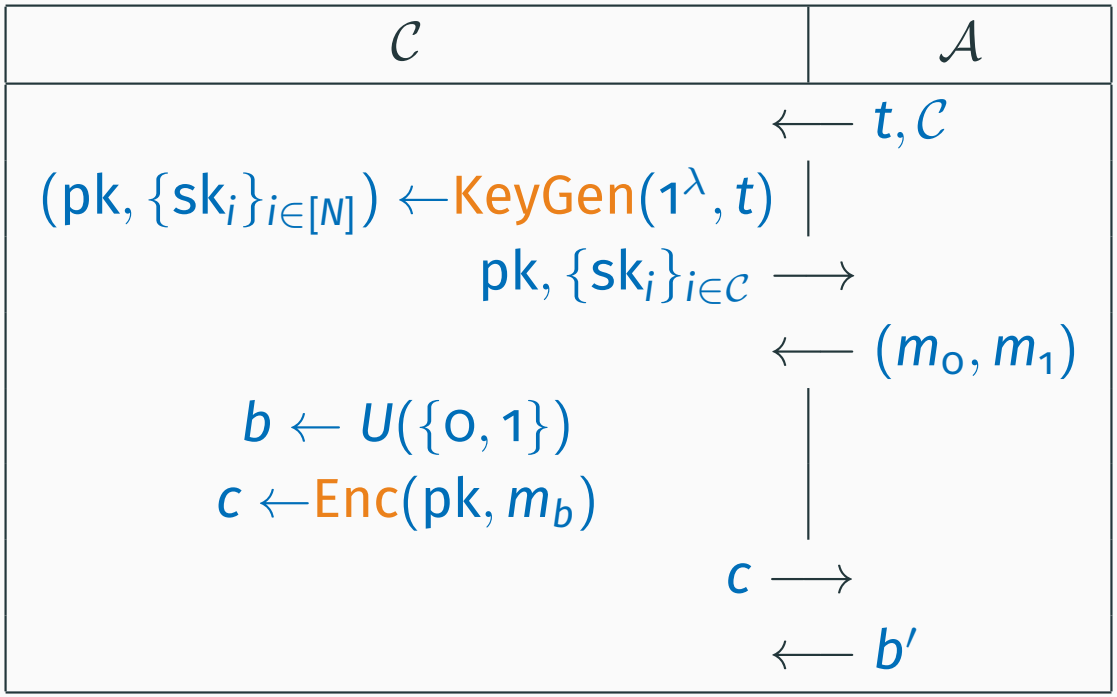
Server i	Alice	Bob
	$(\mathsf{pk}, \{\mathsf{sk}_i\}) \leftarrow \mathsf{KeyGen}(1^\lambda, t)$	
	$\mathsf{sk}_i \longleftarrow$	$\longrightarrow \mathsf{pk}$
		$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
		$\longleftarrow \mathsf{ct}$
	$\mathsf{ct} \longleftarrow$	
$m_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$		
	$\longrightarrow m_i$	
	$m' \leftarrow \mathsf{Combine}(\mathsf{pk}, \{m_j\}_{j \in \mathcal{S}}, \mathsf{ct})$	

Under the condition that $|\mathsf{pk}|, |\mathsf{ct}| = \mathsf{poly}(\lambda)$.

It is correct if $\forall |\mathcal{S}| \geq t, m = m'$ with proba $\geq 1 - \mathsf{negl}(\lambda)$.

Static IND-CCA2 security for TPKE

No PPT adversary $\mathcal{A}$ with a $\mathsf{PartDec}(\mathsf{sk}_i, \cdot)$ oracle for any $i \in [\ell]$ has non-negligible advantage:



- $\mathcal{C}$ is comprised of exactly $t-1$ elements,
- $\mathcal{A}$ can make partial decryption queries (i, c) for the challenge,

as long as it cannot trivially win. Its advantage is $|\Pr(b = b') - 1/2|$.

Proving equality of plaintexts

First step: build a trapdoor sigma-protocol for the language:

$$\mathcal{L}_{\mathsf{zk}} = \{(\mathsf{ct}_1, \mathsf{ct}_2, \ell_M) | \mathsf{ct}_1, \mathsf{ct}_2 \text{ are both encryptions of the same } m \in [0, M]\},$$

where $\mathsf{ct}_b \in \mathbb{Z}_{N_b^{\zeta+1}}$, and

$$\mathcal{L}_{\mathsf{sound}} = \{(\mathsf{ct}_1, \mathsf{ct}_2, \ell_M) | \mathsf{ct}_1, \mathsf{ct}_2 \text{ are both encryptions of the same } m/c \\ m \in [-R, R] \wedge c \in [0, C]\},$$

where $C = 2^\lambda - 1$ and ζ is the smallest integer such that $2RC < \min(N_1^\zeta, N_2^\zeta)$.

Proving equality of plaintexts (2)

Let $(\mathsf{ct}_1, \mathsf{ct}_2, \ell_M)$ be a commitment to m with witnesses w_1, w_2.

- P samples $a \hookleftarrow U([0, R]), r_b \hookleftarrow U(\mathbb{Z}_{N_b}^*), b \in \{1, 2\}$ and sends

$$\left(A_b = (1 + N_b)^a \cdot r_b{}^{N_b^\zeta} \bmod N_b^{\zeta+1}\right)_{b=1}^{2}.$$

- On input $\mathsf{Chall} \hookleftarrow U([0, 2^\lambda - 1])$, P sends

$$z = a + \mathsf{Chall} \cdot m, \quad \left(z_b = r_b \cdot w_b^{\mathsf{Chall}}\right)_{b=1}^{2}.$$

- V checks if $z \in [0, R]$ and if

$$A_b \cdot \mathsf{ct}_b{}^{-\mathsf{Chall}} = z_b^{N_b^\zeta} \cdot (1 + N_b)^z \bmod N_b^{\zeta+1}, b \in \{1, 2\}.$$

Proving equality of plaintexts (2)

Let $(\mathsf{ct}_1, \mathsf{ct}_2, \ell_M)$ be a commitment to m with witnesses w_1, w_2.

- P samples $a \hookleftarrow U([0, R]), r_b \hookleftarrow U(\mathbb{Z}_{N_b}^*), b \in \{1, 2\}$ and sends

$$\left(A_b = (1 + N_b)^a \cdot {r_b}^{N_b^\zeta} \bmod N_b^{\zeta+1}\right)_{b=1}^{2}.$$

- On input $\mathsf{Chall} \hookleftarrow U([0, 2^\lambda - 1])$, P sends

$$z = a + \mathsf{Chall} \cdot m, \quad \left(z_b = r_b \cdot w_b^{\mathsf{Chall}}\right)_{b=1}^{2}.$$

- V checks if $z \in [0, R]$ and if

$$A_b \cdot {\mathsf{ct}_b}^{-\mathsf{Chall}} = z_b^{N_b^\zeta} \cdot (1 + N_b)^z \bmod N_b^{\zeta+1}, b \in \{1, 2\}.$$

Proving equality of plaintexts (2)

Let $(\mathsf{ct}_1, \mathsf{ct}_2, \ell_M)$ be a commitment to m with witnesses w_1, w_2.

- P samples $a \hookleftarrow U([0, R]), r_b \hookleftarrow U(\mathbb{Z}_{N_b}^*), b \in \{1, 2\}$ and sends

$$\left(A_b = (1 + N_b)^a \cdot {r_b}^{N_b^\zeta} \bmod N_b^{\zeta+1}\right)_{b=1}^{2}.$$

- On input $\mathsf{Chall} \hookleftarrow U([0, 2^\lambda - 1])$, P sends

$$z = a + \mathsf{Chall} \cdot m, \quad \left(z_b = r_b \cdot w_b^{\mathsf{Chall}}\right)_{b=1}^{2}.$$

- V checks if $z \in [0, R]$ and if

$$A_b \cdot {\mathsf{ct}_b}^{-\mathsf{Chall}} = z_b^{N_b^\zeta} \cdot (1 + N_b)^z \bmod N_b^{\zeta+1}, b \in \{1, 2\}.$$

Properties

Theorem

This sigma-protocol satisfies

- Completeness,
- Special Zero-Knowledge,
- Special Soundness and CRS Indistinguishability, for a BadChallenge function that uses linear programming and Lenstra's algorithm.

Moreover, it can be compiled into a one-time simulation sound NIZK using a new compiler, without imposing a bound on the plaintext space.

Construction of the TPKE (intuition)

- Take two instantiations of the encryption scheme. Share the secret key of the first with Shamir's secret sharing.
- Ciphertexts are encryptions under both encryption schemes and a proof of plaintext equality.
- Partial decryption is done using the partial secret key.
- Recombining is done by recombining the secret key in the exponent.

Theorem (Security)

This construction is IND-CCA2 secure under static corruption queries.

Construction of the TPKE (intuition)

- Take two instantiations of the encryption scheme. Share the secret key of the first with Shamir's secret sharing.
- Ciphertexts are encryptions under both encryption schemes and a proof of plaintext equality.
- Partial decryption is done using the partial secret key.
- Recombining is done by recombining the secret key in the exponent.

Theorem (Security)

This construction is IND-CCA2 secure under static corruption queries.

Thank you for your attention!