Zero-knowledge proof of a shuffle for CL ciphertexts

Agathe BEAUGRAND

IMB/LIRMM

October 19th, 2023

Outline

Private Set Intersection-sum

Party A

Set $\mathcal{A} = \{a_1, \dots, a_r\}$
with associated values
$V = \{v_1, \dots, v_r\} \in \mathbb{Z}^r$

Party B

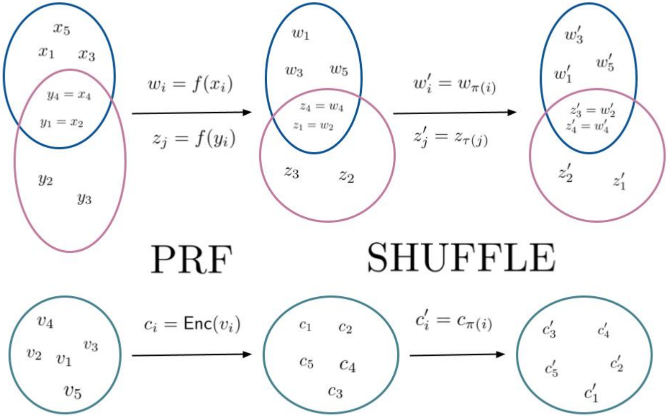
Set $\mathcal{B} = \{b_1, \dots, b_s\}$

A and B want to compute

$$S = \sum_{\substack{i \in [\![1,r]\!] \\ x_i \in X \cap Y}} v_i \in \mathbb{Z},$$

without revealing anything to the other more than S (and the cardinality of the intersection).

The protocol [MPRSY20]



$$e = \mathsf{Enc}(S) = c'_2 \cdot c'_4$$

Choice of the encryption scheme

- We want to compute a sum directly in the ciphertexts : need for a linearly homomorphic scheme : Elgamal in the exponent, Paillier ?
- Shuffles for Paillier are less efficient than for Elgamal
- CL is a scheme with a bigger space of messages with respect to Elgamal in the exponent ;

The CL encryption scheme [CL15]

We assume we have

- a cyclic group $G = \langle g \rangle$ of unknown order,
- a subgroup $F = \langle f \rangle$ of prime order q,
- an q-th power $h \in G^q$ such that $G \simeq \langle h \rangle \times F$
- the discrete logarithm is efficiently computable in F,
- the HSM assumption holds : it is hard to distinguish between a q-th power and a general element of G

(In practice, constructed from class groups)

The CL encryption scheme

Algorithm 1: KeyGen

1: $x \hookleftarrow \mathcal{D}_q$,

2: $sk \leftarrow x$ and $pk \leftarrow h^x$

3: **return** (sk, pk)

Algorithm 2: Encrypt(pk, m)

1: $r \hookleftarrow \mathcal{D}_q$

2: $c_1 \leftarrow h^r$

3: $c_2 \leftarrow f^m pk^r$

4: **return** (c_1, c_2)

Algorithm 3: Decrypt$((c_1, c_2), sk)$

1: $d \leftarrow c_2 c_1^{-sk}$

2: $m \leftarrow \mathrm{Solve}_{\mathrm{DL}}(d)$

3: **return** m

Theorem

Under the HSM assumption, this encryption scheme is secure against chosen-plaintext attack.

Principle of a shuffle

For a linearly homomorphic encryption scheme, and a set of ciphertexts $c_1, \ldots, c_n$, we set

$$c'_i = \mathsf{Enc}(0, \rho_i) \cdot c_{\pi(i)}$$

with $\pi \in \mathcal{S}_n$ random permutation.

With an IND-CPA encryption scheme, we achieve **unlinkability**.
We add a zero-knowledge proof that the shuffle was performed correctly (which makes the shuffle **verifiable**).

Idea of the ZK-proof [BG12]

1. The Prover commits to the permutation π in C_π.
2. Prover and Verifier run a product argument to check that C_π is a commitment to a permutation.
3. Prover and Verifier run a multiexponentiation argument to check that the ciphertexts were indeed mixed with respect to the permutation committed.
4. The proof of shuffle is accepted if both sub-arguments are accepted

An efficient proof of multiexponentiation

A proof of a multiexponentiation for CL ciphertexts is a proof of $(\mathbf{x}, \rho) \in \mathbb{Z}^n \times \mathbb{Z}$ such that

$$c = \mathrm{Enc}_{\mathrm{CL}}(0; \rho) \prod_{i=1}^{n} c_i^{x_i} = (h^{\rho}, pk^{\rho}) \cdot \prod_{i=1}^{n} (h^{x_i r_i}, pk^{r_i x_i} f^{m_i x_i})$$

and

$$\mathbf{C} = \mathrm{Com}(\mathbf{x})$$

An efficient proof of multiexponentiation

We separate the n ciphertexts in ℓ batchs of m ciphertexts $(n = m \times \ell)$ $\mathbf{c}_1, \ldots, \mathbf{c}_\ell$, and same for the x_i's : $\mathbf{x}_1 = (x_1, \ldots, x_m), \mathbf{x}_2 = (x_{m+1}, \ldots, x_{2m}), \ldots$.
The aim is to prove that the product of elements on the main diagonal of

$$\begin{pmatrix} \mathbf{c}_1^{\mathbf{x}_1} & \mathbf{c}_1^{\mathbf{x}_2} & \ldots & \mathbf{c}_1^{\mathbf{x}_\ell} \\ \mathbf{c}_2^{\mathbf{x}_1} & \mathbf{c}_2^{\mathbf{x}_2} & \ldots & \mathbf{c}_2^{\mathbf{x}_\ell} \\ . & . & . & . \\ . & . & . & . \\ \mathbf{c}_\ell^{\mathbf{x}_1} & \mathbf{c}_\ell^{\mathbf{x}_2} & \ldots & \mathbf{c}_\ell^{\mathbf{x}_\ell} \end{pmatrix}$$

is equal to c.
(Each element of the matrix is a multiexponentiation of size m).
We call E_k the product of the element on the k-th off-diagonal of this matrix.

An efficient proof of multiexponentiation

$\mathcal{P} \to \mathcal{V}$: computes and sends $(E_k)_{k \in [\![1,2\ell]\!] \setminus \{\ell\}}$.
$\mathcal{V} \to \mathcal{P}$: chooses a challenge z

$\mathcal{P} \to \mathcal{V}$: computes and sends $\widehat{\mathbf{x}} = \sum_{i=1}^{\ell} z^j \mathbf{x}_j$.

The Verifier checks if

$$c^{z^\ell} \cdot \prod_{\substack{k=1 \\ k \neq \ell}}^{2\ell} E_k^{z^k} = \prod_{i=1}^{\ell} \mathbf{c}_i^{z^{\ell-i}\widehat{\mathbf{x}}}$$

Looking at the elements to the power z^ℓ, we conclude that

$$c^{z^\ell} = \left(\prod_{i=1}^{\ell} \mathbf{c}_i^{\mathbf{x}_i} \right)^{z^\ell} = \left(\prod_{i=1}^{n} c_i^{x_i} \right)^{z^m}$$

Towards the real proof

We add masks to obtain zero-knowledge, and get a proof for multiexponentiation of size n, with communication in $O(\ell)$.

Choosing $m \sim \ell + m \sim \sqrt{n}$: proof is sublinear in communication.

Problems with CL ciphertexts

- To guarantee soundness, we have to use a specific assumption (*C-rough assumption*, [BDO23])
- Special soundness still not achieved... BUT we can still extract the " $\bmod q$" part from the commitments $\Rightarrow$ we define a new notion of "partial extractability"
- This new notion suits most cases in proofs about CL ciphertexts
  $\Rightarrow$ in particular concludes in the shuffle proof

To be published soon :

- A logarithmic proof of a shuffle
- Implementation of the PSI-sum protocol

Thanks for your attention !

- S. Bayer and J. Groth.
  Efficient zero-knowledge argument for correctness of a shuffle.
  In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 263–280. Springer, Heidelberg, Apr. 2012.
- L. Braun, I. Damgård, and C. Orlandi.
  Secure multiparty computation from threshold encryption based on class groups.
  In H. Handschuh and A. Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023*, pages 613–645, Cham, 2023. Springer Nature Switzerland.
- G. Castagnos and F. Laguillaumie.
  Linearly homomorphic encryption from DDH.
  In K. Nyberg, editor, *Topics in Cryptology – CT-RSA 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 487–505. Springer, Heidelberg, Apr. 2015.
- P. Miao, S. Patel, M. Raykova, K. Seth, and M. Yung.
  Two-sided malicious security for private intersection-sum with cardinality.
  In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 3–33. Springer, Heidelberg, Aug. 2020.