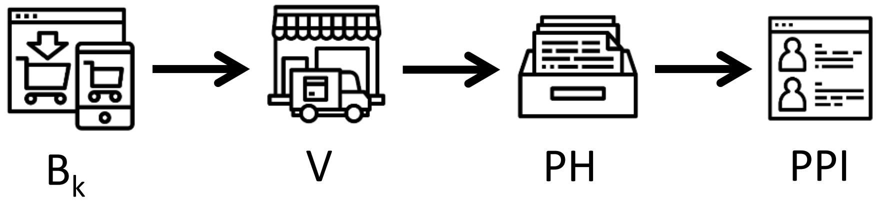
Unlinkable Updatable Hiding Databases and Privacy Preserving Loyalty Programs

Aditya Damodaran, Alfredo Rial, SnT, University of Luxembourg
{firstname.lastname}@uni.lu

Luxembourg National Research Fund

APSIA Research Group

1. Loyalty Programs



Loyalty programs (LP) allow vendors (V) to profile buyers (B_k) based on their purchase histories (PH) in exchange for loyalty points. This can reveal privacy sensitive information (PPI).

2. Shortcomings of Existing LP Schemes

Purchases are linkable

Though some schemes provide unlinkablity, no schemes in literature provide unlinkability for all purchases

Lack of Privacy

Profiling based on PH can reveal privacy sensitive information

No modular design

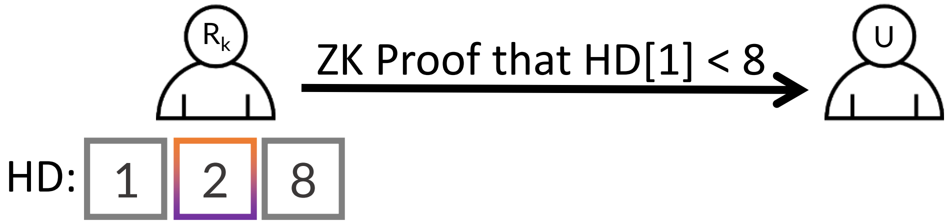
Existing schemes are not composed of modular building blocks

3. Our Contribution

We propose a protocol for a PPLP, based on a protocol for a concept we call a **Hiding Database.** This protocol ensures that *all purchases are unlinkable* and that *PH privacy is preserved* whilst still allowing for profiling. The protocol has also been *modularly designed* in the Universal Composability framework.

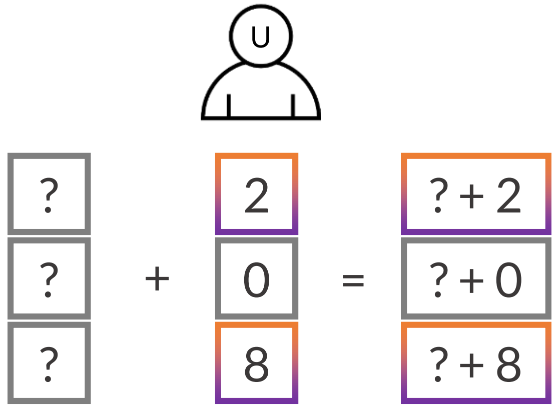
Hiding Database: A protocol between a Reader and an Updater, based on Vector Commitments, and consisting of two phases: *Read* and *Update*.

4. Hiding Database: Read Phase



A Reader (R_k) can prove facts about an entry in a hiding database (HD) to an Updater (U), without revealing the entry or its position. R_k uses a unique pseudonym during every read phase to hide its identity from U.

5. Hiding Database: Update Phase



An Updater (U) can update a Reader's (R_k) hiding database (HD) without learning the contents of this database. A unique pseudonym hides R_k's identity from U during an update phase.

6. Our Protocol for a Privacy Preserving LP

Loyalty point accrual and redemption: The Vendor updates a Buyer's HD (hidden from the vendor) with purchase history and loyalty point updates, using a HD update. Upon redemption, the buyer proves possession of the requisite number of points in Zero Knowledge, and the Vendor updates the Buyer's database again to deduct these points.

Profiling: The Buyer receives a profiling function as input, computes the result of said function on its purchase history stored in HD, and proves correctness of the result to the Vendor in Zero Knowledge using HD reads.

Supported by the Luxembourg National Research Fund (FNR) (C17/11650748)