PrivaSapien assignment

Soumyadip Guria

July 2024

1 Protocol for part 2

PJ Morgan		**Wells Neargo**
$x_1, x_2, ..., x_{100}$		$y_1, y_2, ..., y_{200}$
$a_1, a_2, ..., a_{10}$		$b_1, b_2, ..., b_{15}$
$p \xleftarrow{\$} \mathbb{Z}_n$		$q \xleftarrow{\$} \mathbb{Z}_n$
Calculates$H(x_1)^p, ..., H(x_{100})^p$	$\xrightarrow{\text{Sends to Wells Neargo}}$	
Calculates$H(a_1)^p, ..., H(a_{10})^p$	$\xrightarrow{\text{Sends to Wells Neargo}}$	
	$\xleftarrow{\text{Sends to PJ Morgan}}$	Calculates$H(y_1)^q, ..., H(x_{200})^q$
	$\xleftarrow{\text{Sends to PJ Morgan}}$	Calculates$H(b_1)^q, ..., H(b_{15})^q$
$A = \{H(b_1)^{pq}, ..., H(b_{15})^{pq}\}$		
$B = \{H(y_1)^{pq}, ..., H(y_{200})^{pq}\}$	$\xrightarrow{\text{Shuffles \& sends}}$	
		$C = \{H(a_1)^{pq}, ..., H(a_{10})^{pq}\}$
	$\xleftarrow{\text{Shuffles \& sends}}$	$D = \{H(x_1)^{pq}, ..., H(x_{100})^{pq}\}$
Finds intersection of A & D		Finds intersection of B & C

The cardinality of each intersection will be the number of new customers that are already verified by other banks.

Since at the last step shuffling is done no bank can get to know about the details of the customers and only know the number of customers.

Here we are calculating power of hashes, as a result this protocol is not that much scalable.