(Un)linkable Pseudonyms for Governmental Databases

Jan Camenisch, Anja Lehmann

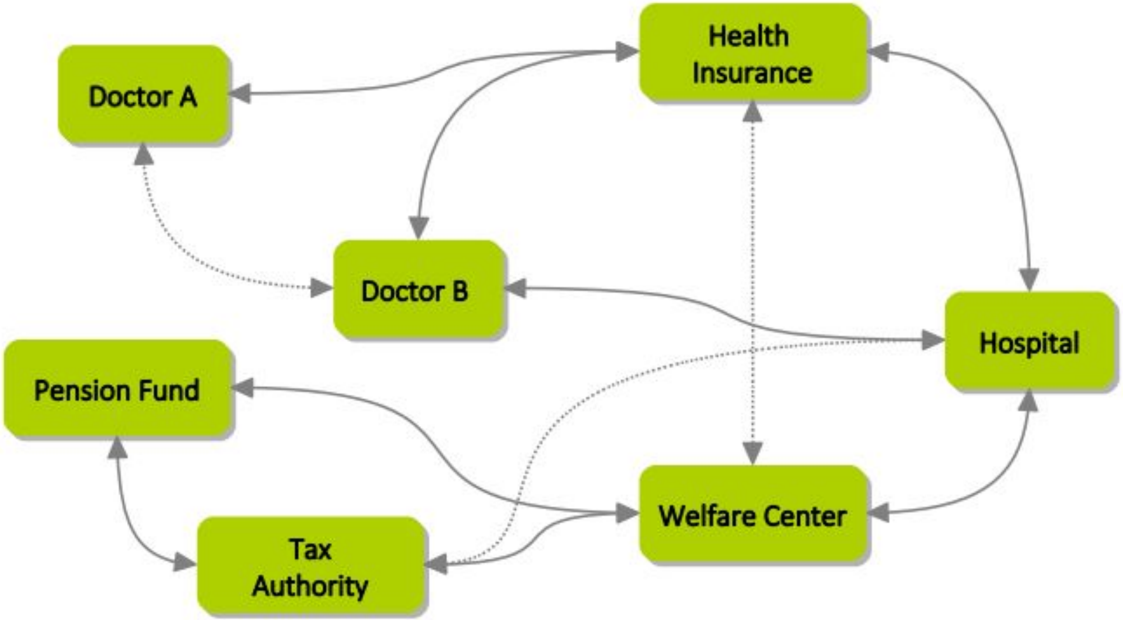
Guided By-
Dr. Maria Francis

Presented By:-
B.Subhasree-CS19B1005

Introduction

Decentralised system:

- Large data is distributed over several databases and organisations
- Eventually data needs to be exchanged or co-related



Global Identifier

Unique Identifier for each user

Advantages:

- Allows all entities to easily share and link data records

Disadvantages:

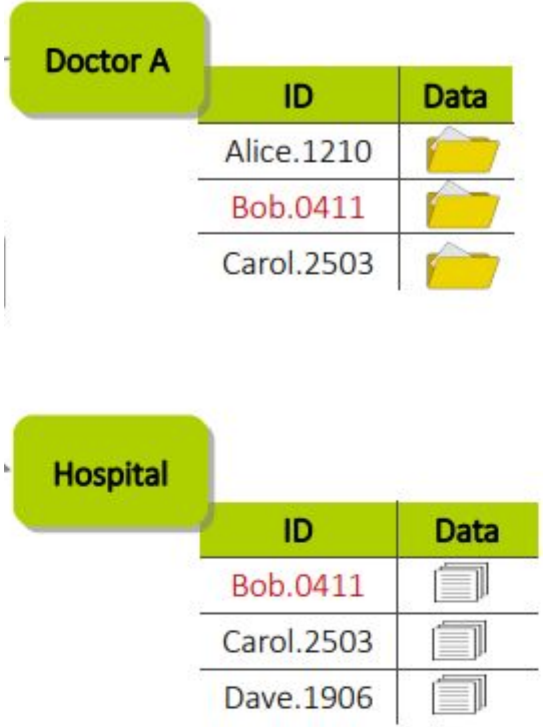
- Significant Privacy threat (In Data breach)
- Data can hardly be controlled & authorized

Solution:

- A certain control to limit dataflow(Central Authority)
- Data exchange need to authorized by central authority

Drawback:

- Central Authority knows requests
- Can reveal sensitive information



Doctor A

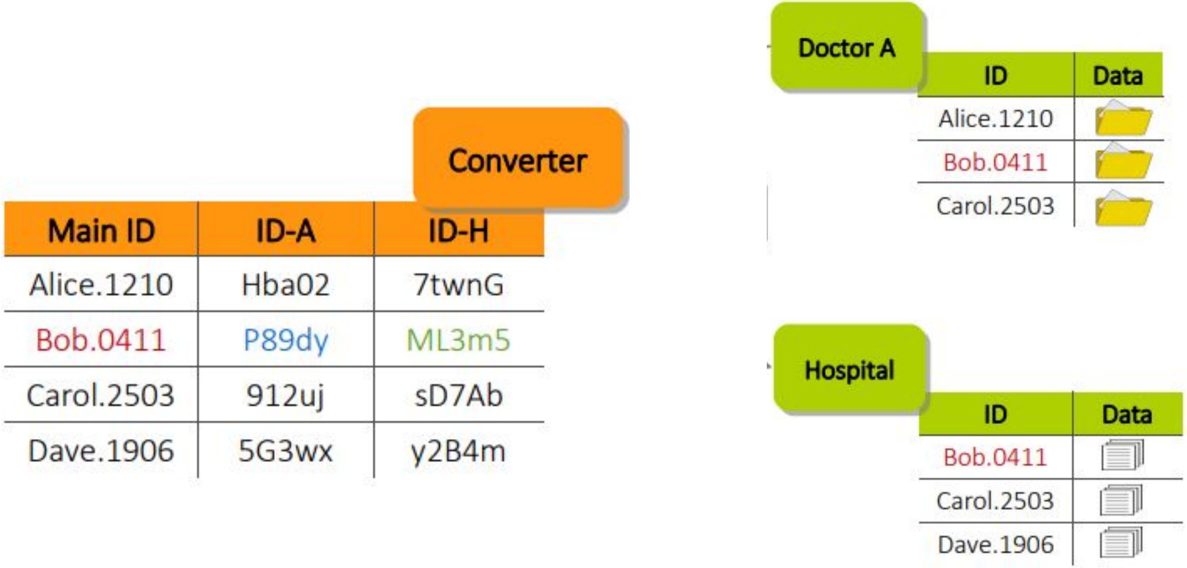
ID	Data
Alice.1210	📁
Bob.0411	📁
Carol.2503	📁

Hospital

ID	Data
Bob.0411	🗐
Carol.2503	🗐
Dave.1906	🗐

Pseudonym

- ❖ User data is associated with (unlinkable) server-local identifiers aka “pseudonyms”
- ❖ Only converter can link & convert pseudonyms ➔ central hub for data exchange



Converter

Main ID	ID-A	ID-H
Alice.1210	Hba02	7twnG
Bob.0411	P89dy	ML3m5
Carol.2503	912uj	sD7Ab
Dave.1906	5G3wx	y2B4m

Doctor A

ID	Data
Alice.1210	📁
Bob.0411	📁
Carol.2503	📁

Hospital

ID	Data
Bob.0411	🗐
Carol.2503	🗐
Dave.1906	🗐

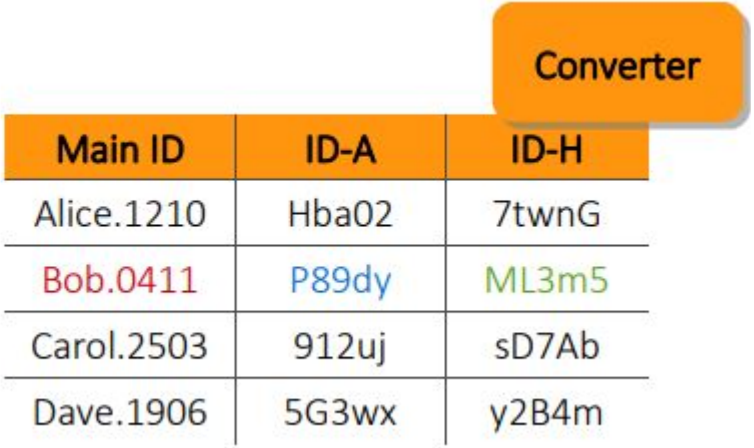
Drawback:

- ➔ Data sets maintained by the entities do not contain other unique identifying information which allows linkage without using the pseudonyms
- ➔ Converter still needs to be trusted(Learns from requests & knows all co-relations)

Existing Solutions

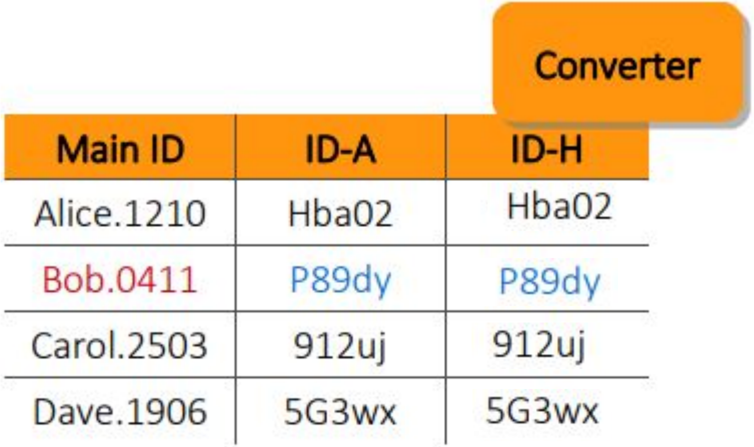
Use block cipher for encryption of unique identifier

$$P_A = Enc(K_A, uid_i) \quad K_A, K_B, K_C \text{ .... are server keys known only to converter}$$



Converter

Main ID	ID-A	ID-H
Alice.1210	Hba02	7twnG
Bob.0411	P89dy	ML3m5
Carol.2503	912uj	sD7Ab
Dave.1906	5G3wx	y2B4m



Converter

Main ID	ID-A	ID-H
Alice.1210	Hba02	Hba02
Bob.0411	P89dy	P89dy
Carol.2503	912uj	912uj
Dave.1906	5G3wx	5G3wx

- ❏ All keys are different
- ❏ Pseudonyms are unlinkable

Drawback:

- ➔ Converter still needs to be trusted
- ➔ Indirect identification by profession, age etc

- ❏ If all keys are same (K_A=K_B=K_C)
- ❏ Pseudonyms are linkable
- ❏ Protocol fails

Problem Statement

Main aim : Unlinkable pseudonyms but without trusted converter
Solution: Converter and server both contribute to the derivation of pseudonym

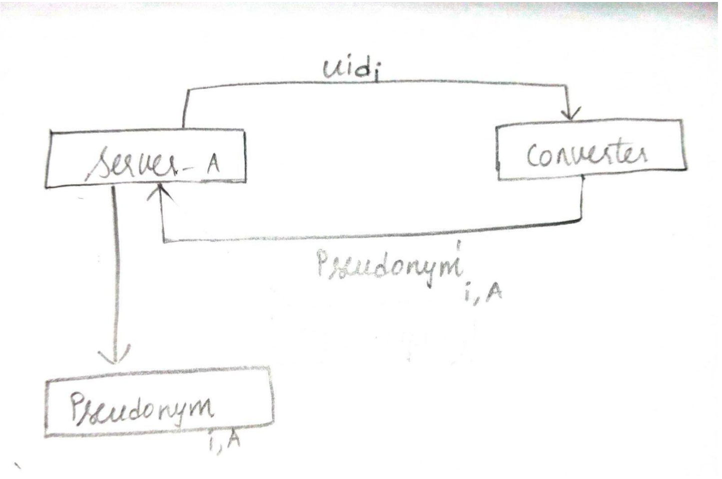
Advantages:

- Control about data exchange
- If records are lost, pieces cannot be linked together without the converter
- Converter cannot tell if requests are for the same pseudonym or not & Knows there's a data request from S_A to S_B

Protocol

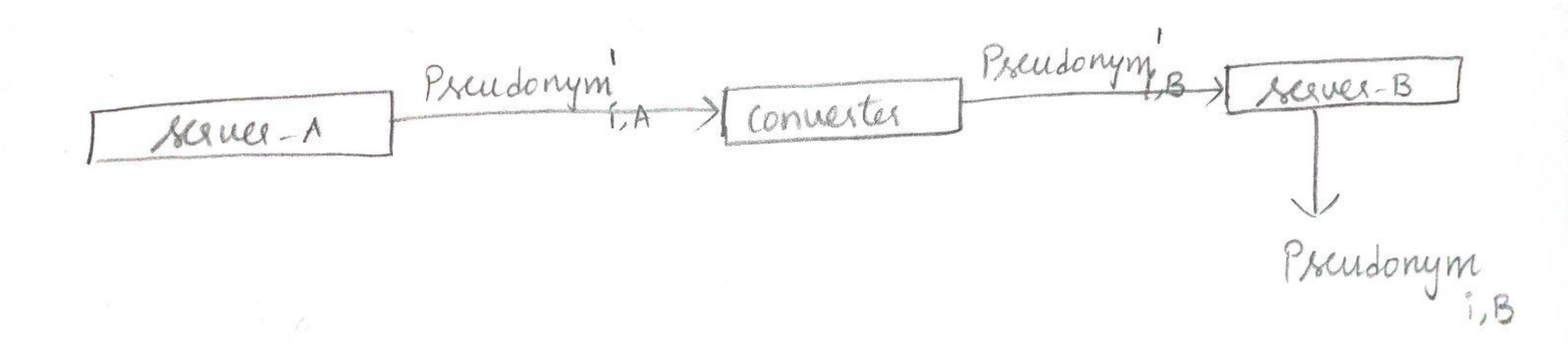
- Pseudonym Generation
- Conversion Request
- Conversion Response

Pseudonym Generation



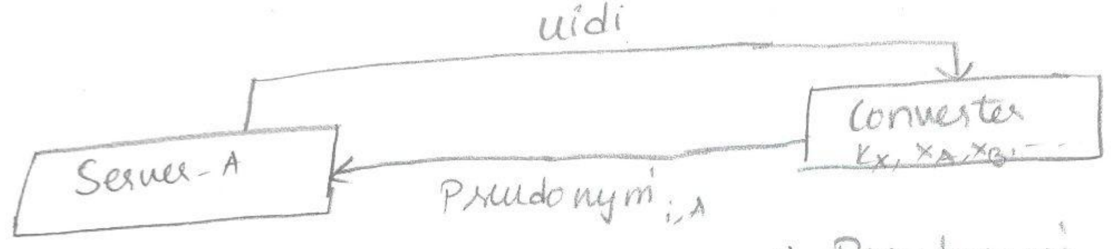
- Converter will use different keys to different servers corresponding to uid_i so that pseudonyms are unlinkable

Conversion Request & Response



- S_A wants some information from S_B
- We convert Pseudonym$_{i,A}$ to Pseudonym$_{i,B}$with the help of S_A,Converter & S_B

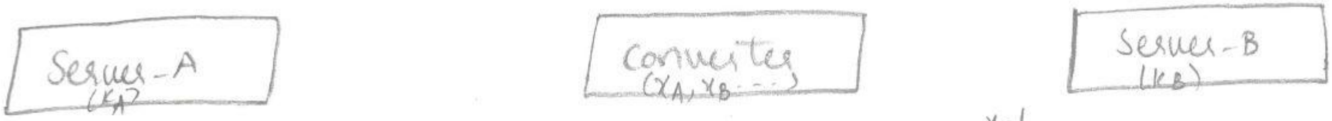
Pseudonym Generation



1) $Pseudonym'_{i,A} = PRF(K_X, uid_i)^{x_A}$

2) $Pseudonym_{i,A} = PRP(K_A, Pseudonym'_{i,A})$

Pseudonym Conversion



1) $Pseudonym'_{i,A} = PRP^{-1}[K_A, Pseudonym_{i,A}]$

2) $Pseudonym'_{i,B} = (Pseudonym'_{i,A})^{x_B/x_A}$

3) $Pseudonym_{i,B} = PRP(K_B, Pseudonym'_{i,B})$

Drawbacks

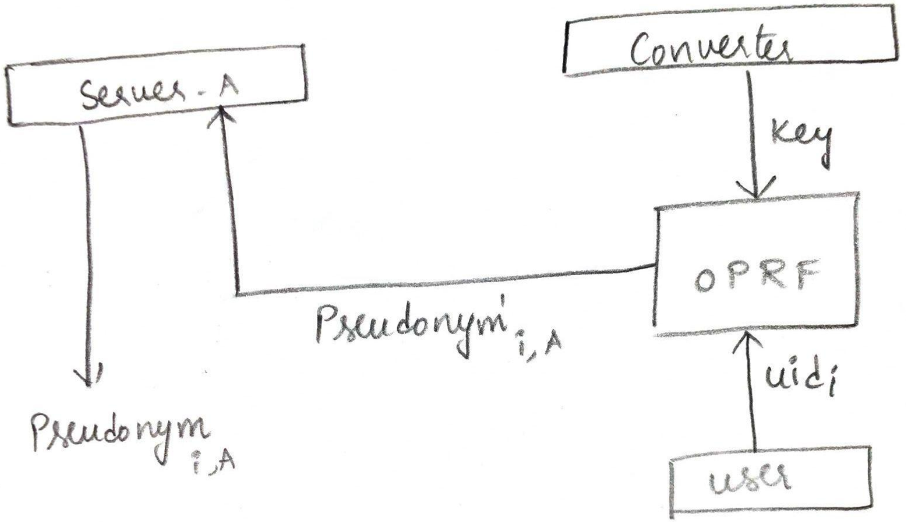
- Server knows uid_i at the generation process.
- A corrupted converter and a corrupted server can link pseudonyms

Solution:-

- To involve user in the process of conversion as well as generation of pseudonym
- To not fully involve converter in the process of conversion from $Pseudonym_A$ to $Pseudonym_B$

Proposed Solution-1

Pseudonym Generation:-

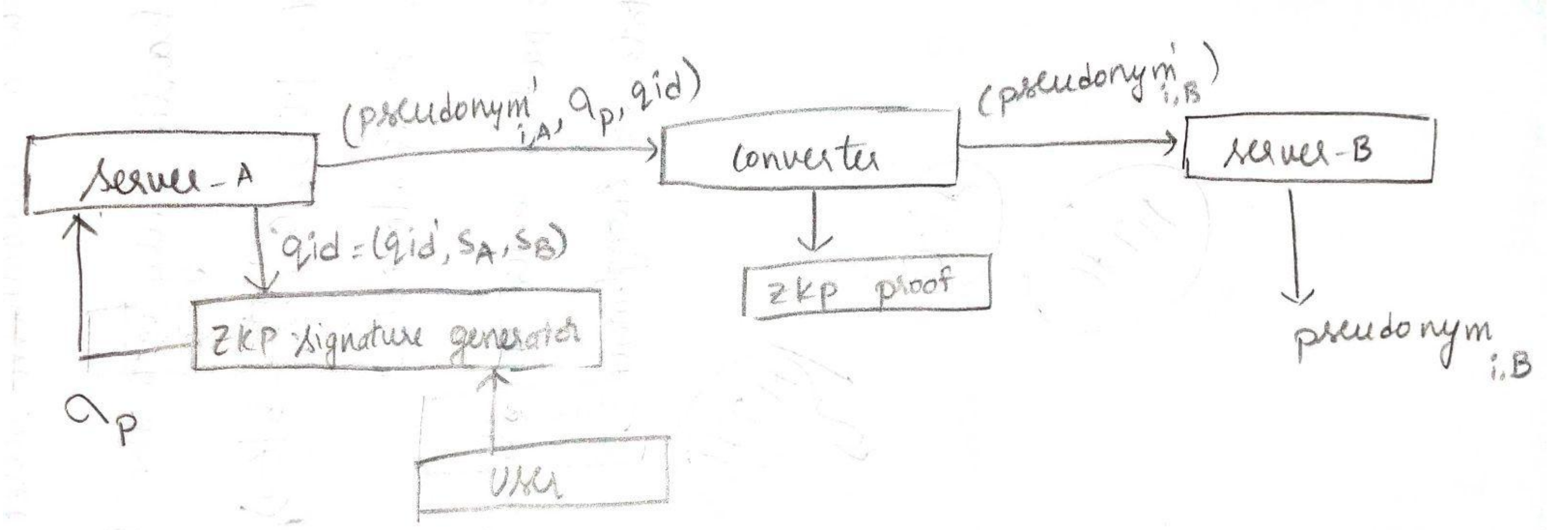


Oblivious Pseudorandom function(OPRF) generates output of PRF(m) without knowing message m to converter

Oblivious Pseudorandom functions

- PRF $f_k(m)=g^{1/(k+m)}$
- Encryption scheme additively homomorphic on message domain Z_n
- Converter blindly computes $z_i=PRF_G(k,uid_i)$
- User initiates pseudonym generation unlike previous where server triggers pseudonym generation

Conversion



- ZKP Signature generator will output user’s signature on query identifier(qid)
- Converter will give zkp that it indeed verified the qid and converted the pseudonym honestly

Drawback:-

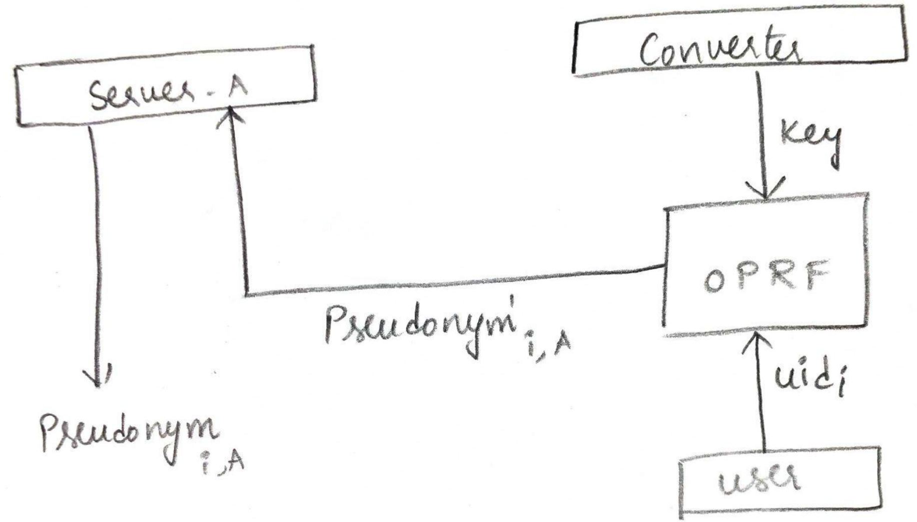
User Needs to involve in every conversion of pseudonym

Anonymous Credentials

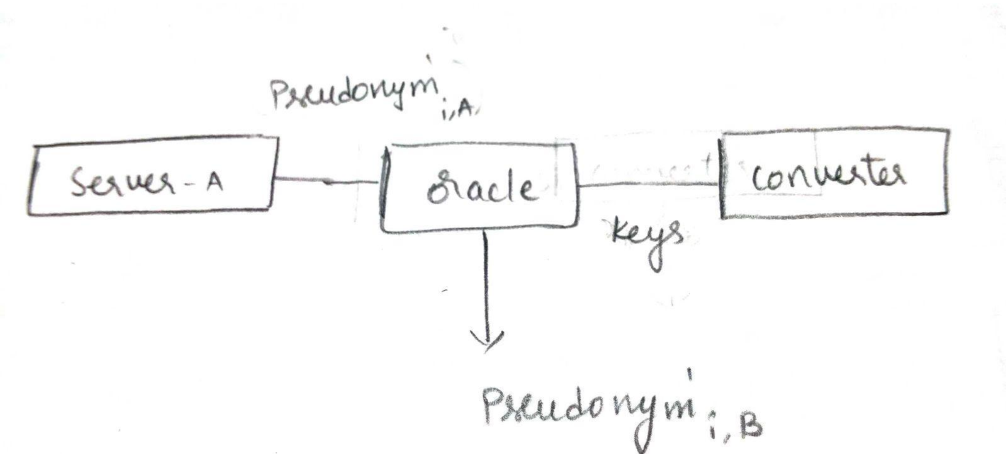
- Digital Credentials which one can obtain from issuers and can Verify without revealing any identifiable information.
- So even if the Verifiers collude, they cannot pinpoint the identity of the Credential presenter
- It allows a user to get a signature σ on a message m by sending a commitment of x to the signer
- User is basically using a zero-knowledge proof to convince the verifier of possessing a signature generated by the issuer

Proposed Solution-2

Pseudonym Generation:-

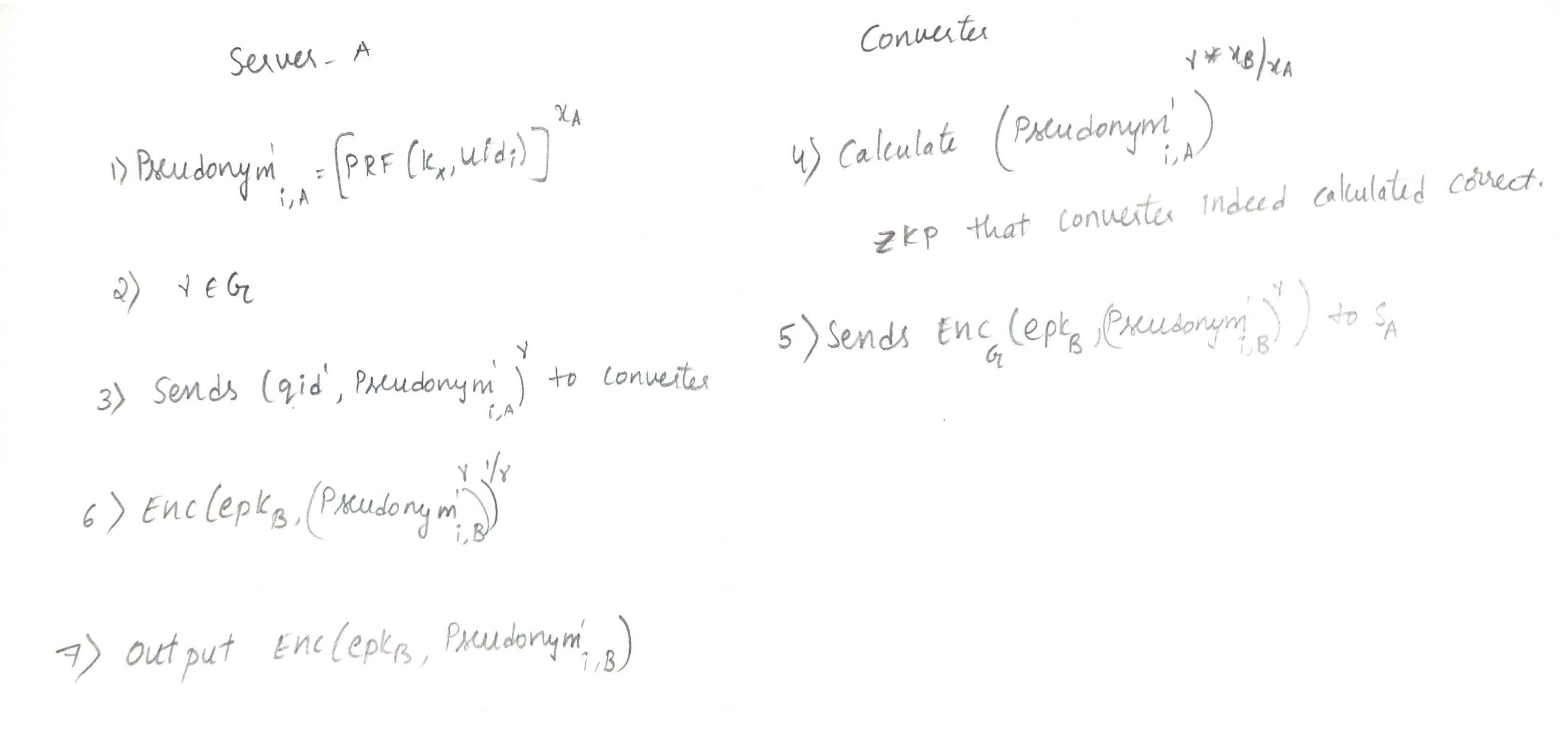


Conversion



- The oracle function blindly converts Pseudonym'$_{i,A}$ to Pseudonym'$_{i,B}$ without converter knowing Pseudonym'$_{i,A}$ & Pseudonym'$_{i,B}$

Oracle Function



Server - A

1) $\text{Pseudonym}'_{i,A} = [\text{PRF}(k_x, uid_i)]^{x_A}$

2) $\gamma \in G$

3) Sends $(qid', \text{Pseudonym}'_{i,A})^{\gamma}$ to converter

6) $\text{Enc}(epk_B, (\text{Pseudonym}'_{i,B})^{\gamma})^{1/\gamma}$

7) output $\text{Enc}(epk_B, \text{Pseudonym}'_{i,B})$

Converter

4) Calculate $(\text{Pseudonym}'_{i,A})^{\gamma * x_B / x_A}$

ZKP that converter indeed calculated correct.

5) Sends $\text{Enc}_G(epk_B, (\text{Pseudonym}'_{i,B})^{\gamma})$ to S_A

References

- H. Aamot, C. D. Kohl, D. Richter, and P. Knaup-Gregori. Pseudonymization of patient identifiers for translational research. BMC Medical Informatics and Decision Making 13:75, 2013
- R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. ePrint Archive, Report 2000/067.
- https://researcher.watson.ibm.com/researcher/files/zurich-ANJ/nym_CCS15.pdf
- Camenisch, Jan & Lehmann, Anja. (2017). Privacy-Preserving User-Auditable Pseudonym Systems. 269-284. 10.1109/EuroSP.2017.36.

THANK YOU!!