SECURE

MULTI-PARTY COMPUTATION

UNDERSTANDING AD EFFECTIVENESS

DR. KHALED EL EMAM
ELECTRONIC HEALTH INFORMATION LABORATORY

POTENTIAL PROBLEMS WITH

HASHING SCHEMES

MUST BE SALTED

REQUIRES SHARING OF SECRETS (SALT)
→ TRUST OTHER PARTY NOT TO LOSE KEY
→ CANNOT PROTECT USER ID IN BROWSER

OPEN TO FREQUENCY ATTACKS IF USER ID DOES NOT HAVE A UNIFORM DISTRIBUTION (EG, NAMES)

MUTLI-PARTY COMPUTATION

TRUST MODELS

TRUSTED 3RD PARTY

PASSIVE ADVERSARY (HONEST-BUT-CURIOUS)

FULLY MALICIOUS

SECURE MULTI-PARTY

COMPUTATION

CONS:

SPEED, COMPLEX, BESPOKE

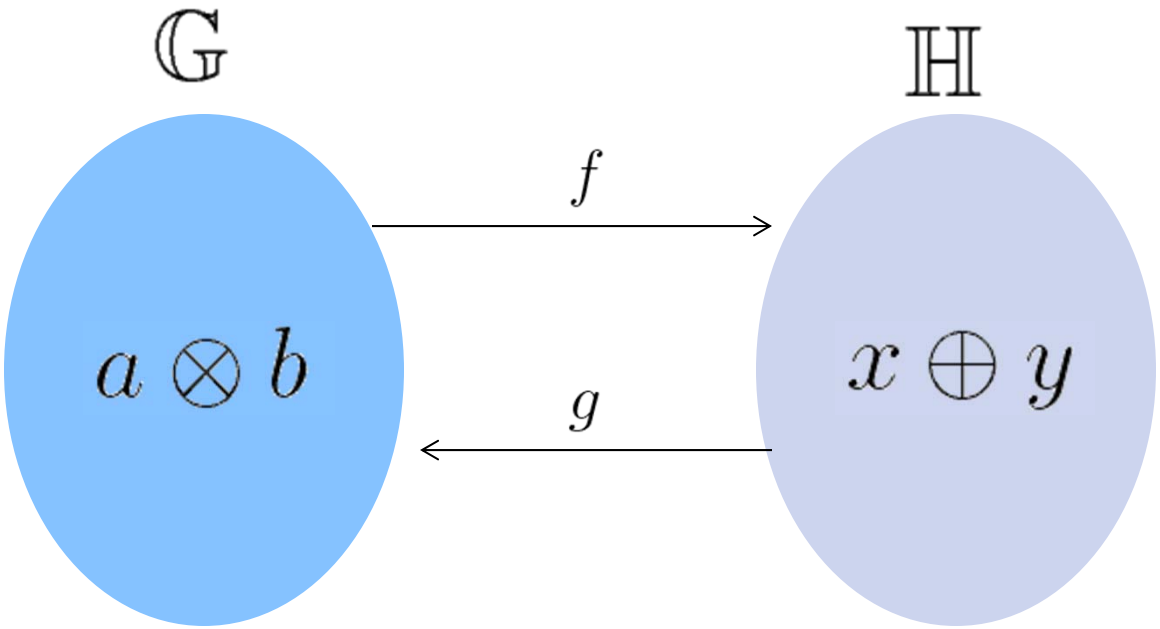
PROS:

SECURITY GUARANTEES

HOMOMORPHIC ENCRYPTION

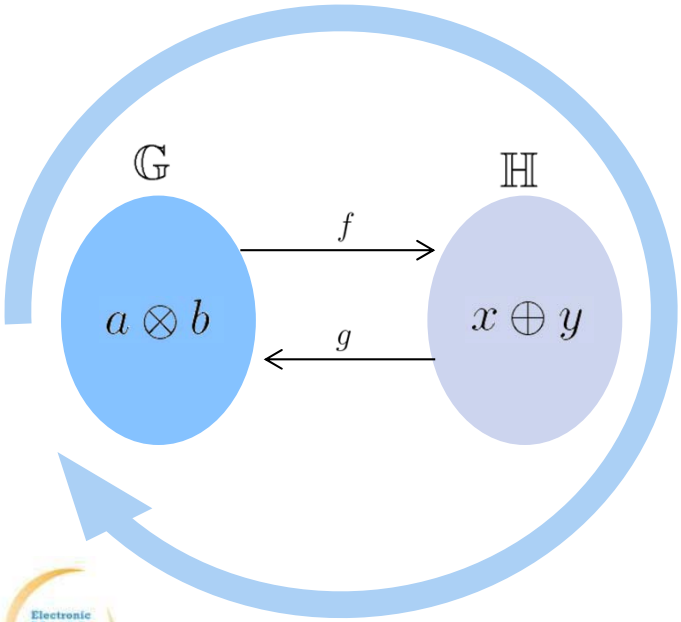
AN ABSTRACT

HOMOMORPHISM



AN ABSTRACT

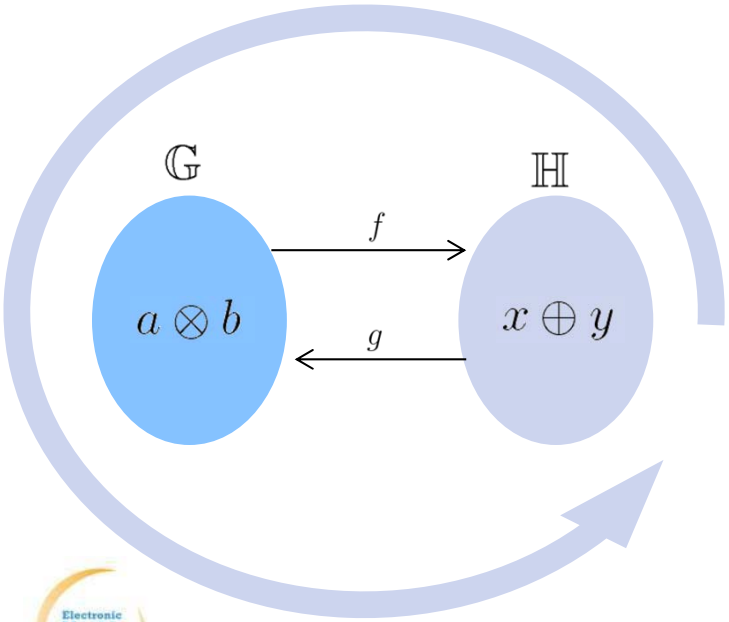
HOMOMORPHISM



$$a \otimes b = g\big(f(a) \oplus f(b)\big)$$

AN ABSTRACT

HOMOMORPHISM



$$x \oplus y = f\big(g(x) \otimes f(y)\big)$$

PUBLIC KEY
ENCRYPTION

PUBLIC KEY

ENCRYPTION

$$c = \mathsf{Enc}_{pk}(m)$$

$$m = \mathsf{Dec}_{sk}(c)$$

RANDOMIZED PUBLIC KEY

ENCRYPTION

$$c_1 = \mathsf{Enc}_{pk}(m, r_1)$$

$$c_2 = \mathsf{Enc}_{pk}(m, r_2)$$

RANDOMIZED PUBLIC KEY

ENCRYPTION

$$c_1 = \mathsf{Enc}_{pk}(m, r_1)$$

$$c_2 = \mathsf{Enc}_{pk}(m, r_2)$$

$$\textit{If } r_1 \neq r_2 \textit{ then } c_1 \neq c_2, \textit{ but}$$

$$Dec_{sk}(c_1) = Dec_{sk}(c_2) = m$$

RANDOMIZED PUBLIC KEY

ENCRYPTION

NOTATION DENOTING AN ENCRYPTED PLAINTEXT

$$[a] = \mathsf{Enc}_{pk}(a, r)$$

$$[b] = \mathsf{Enc}_{pk}(b, r')$$

ADDITIVELY HOMOMORPHIC ENCRYPTION

ADDITIVELY HOMOMORPHIC

ENCRYPTION

$$[a] \cdot [b] = [a + b]$$

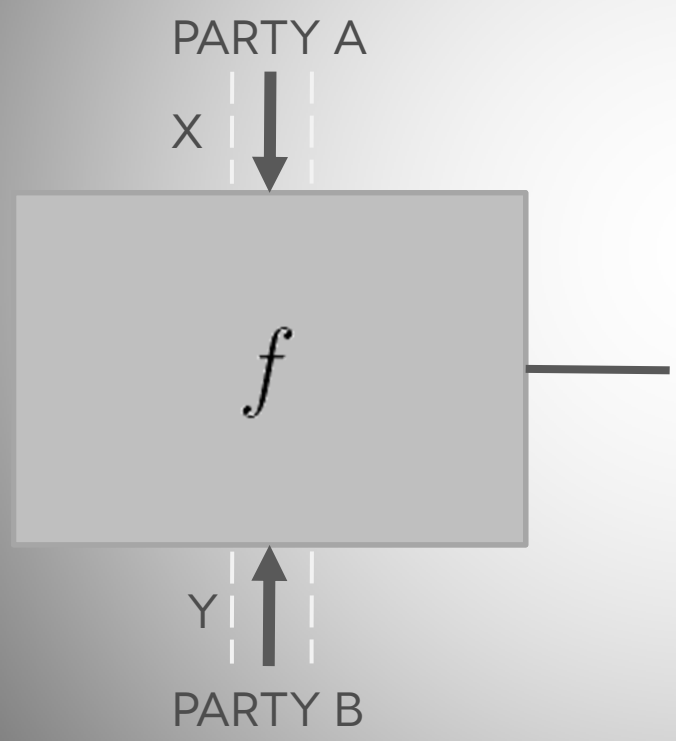
ADDITIVELY HOMOMORPHIC

ENCRYPTION

$$[a]^b = [ab]$$

SECURE COMPARISON

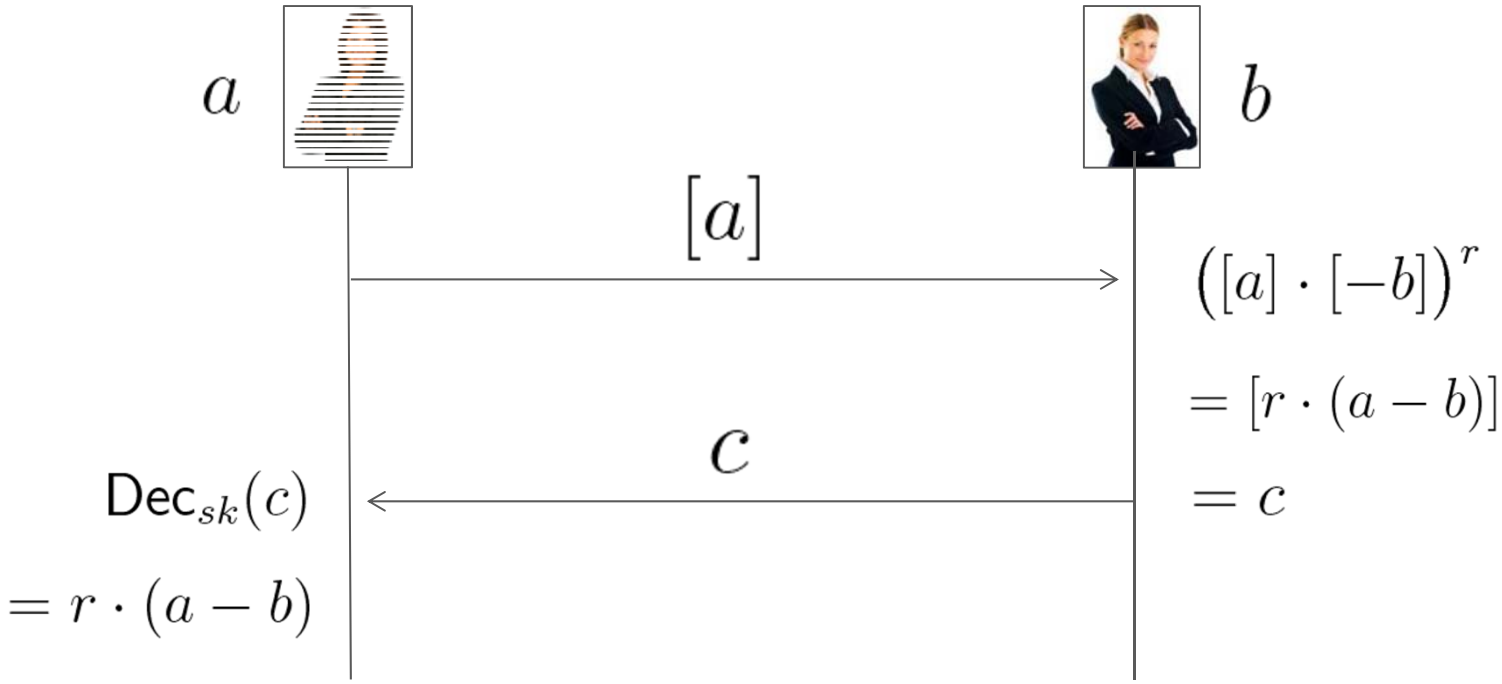
PROTOCOL



OUTPUT

$$f(x,y) = \begin{cases} 0, & x == y \\ random\#, & otherwise \end{cases}$$

2-PARTY SECURE COMPARISON PROTOCOL



ADDITIVELY

HOMOMORPHIC SCHEMES

PAILLIER (1999)

$$[a] \cdot [b] = [a + b]$$

EXPONENTIAL ELGAMAL (1984,1997)

$$[g^a] \cdot [g^b] = [g^{a+b}]$$

Electronic Health Information Laboratory, CHEO Research Institute, 401 Smyth Road, Ottawa K1H 8L1, Ontario; www.ehealthinformation.ca

FULLY

HOMOMORPHIC SCHEMES

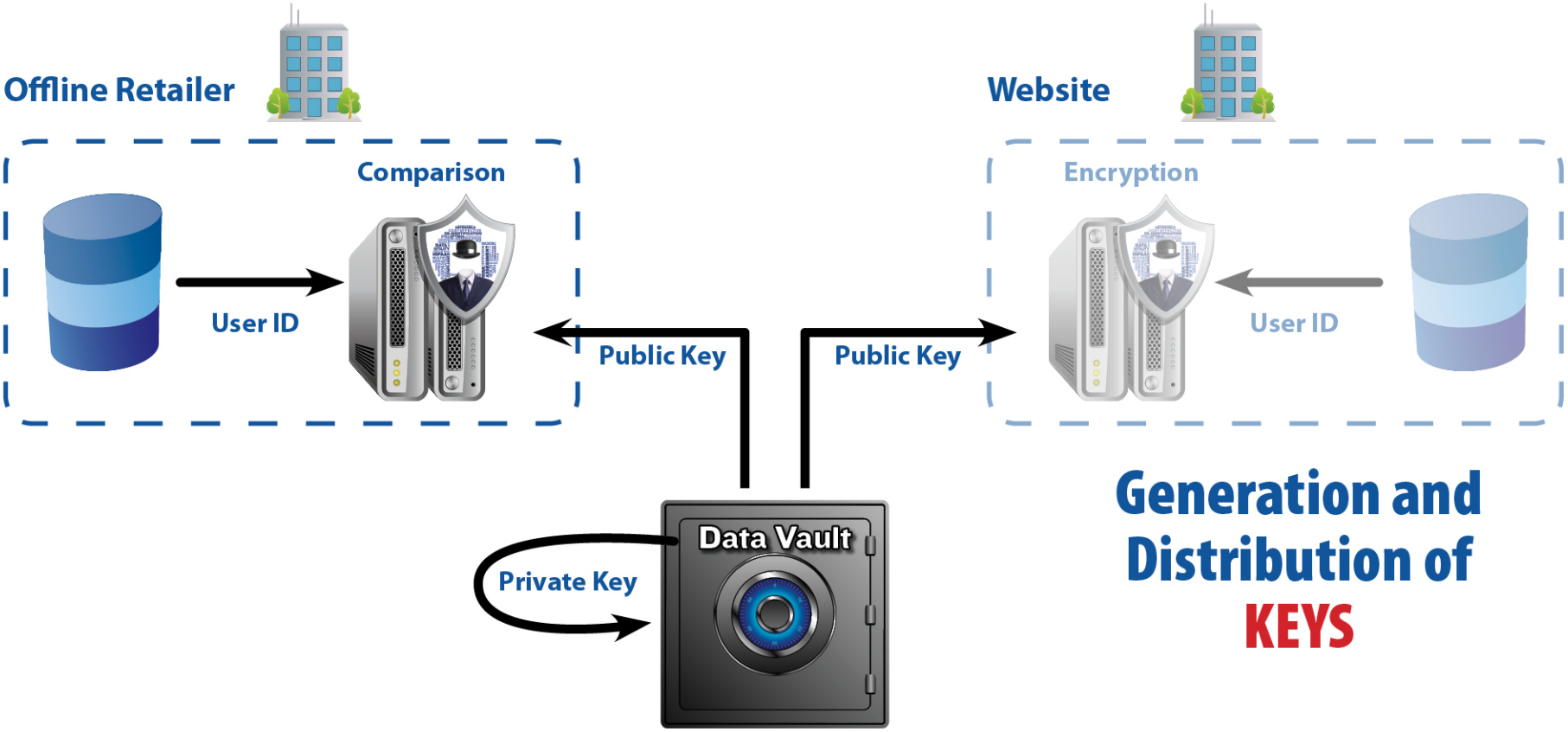
GENTRY (2009)

$$[a] \otimes [b] = [ab]$$

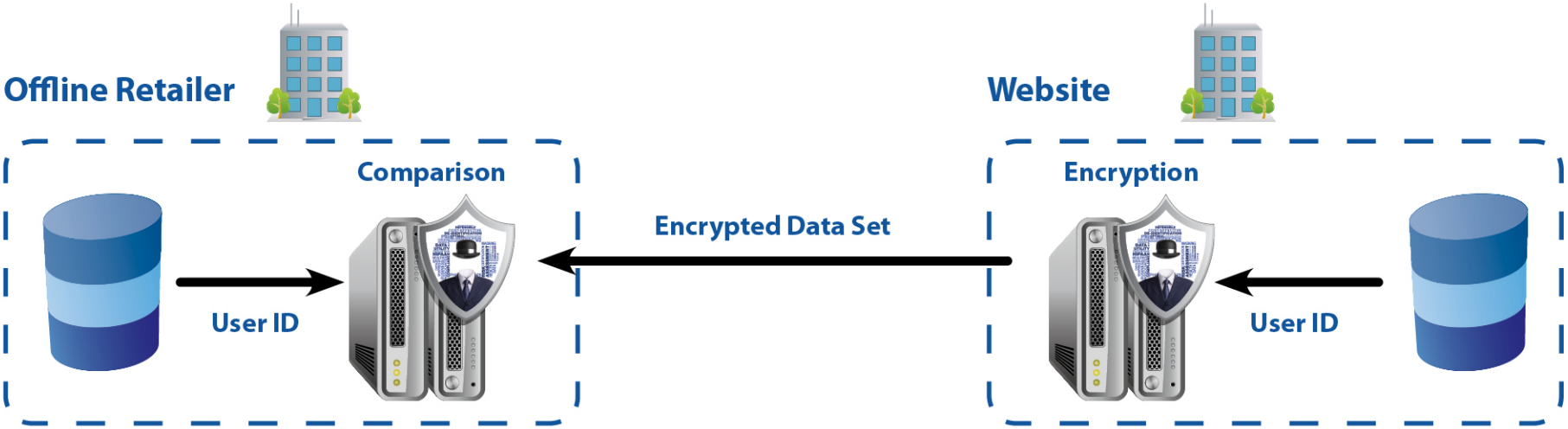
$$[a] \oplus [b] = [a + b]$$

ANONYMOUS LINKING

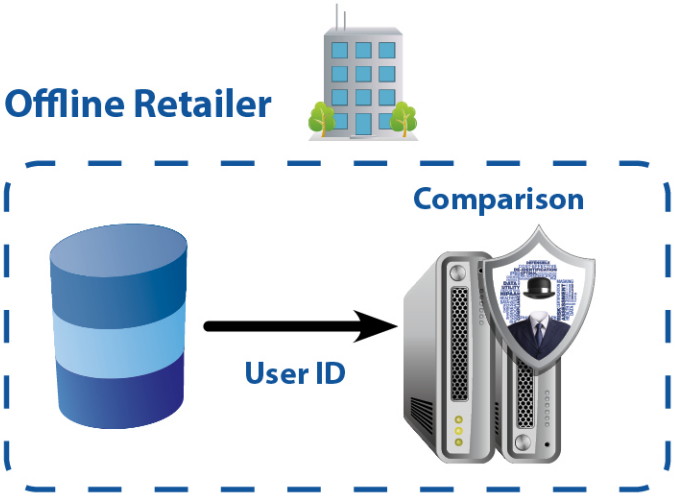
- TYPICAL USE CASES:
  - The best fields to link databases on are unique identifiers: username, email address, SSN, Credit Card number, account number
  - Organizations do not have the authority to exchange data, but need to match records, track individuals, de-duplicate databases or do lookups
- Anonymous linking allows the linking of records in distributed databases without sharing any sensitive or personal information

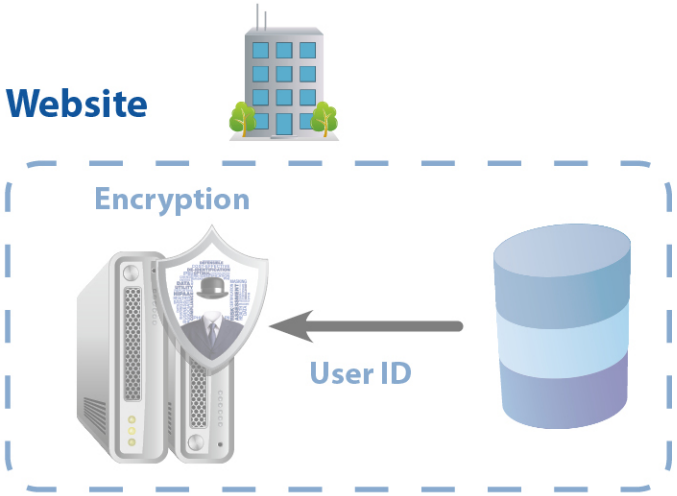


Generation and Distribution of KEYS

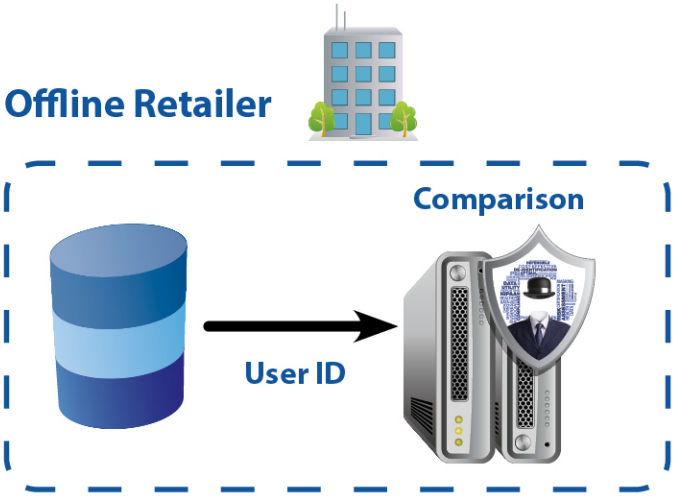


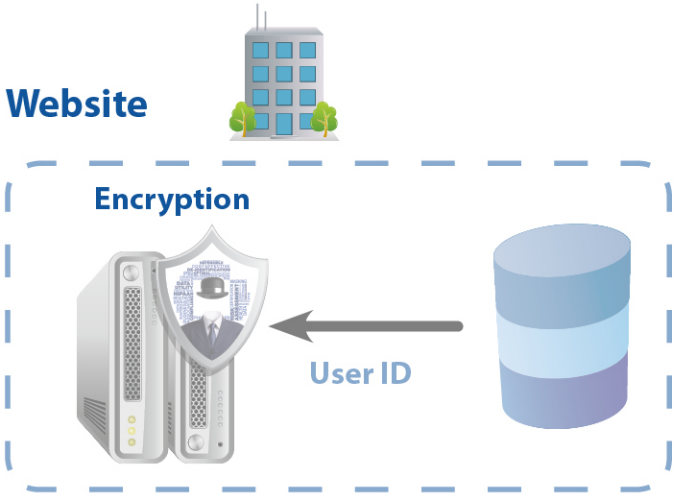
Encryption of User ID Using a PUBLIC KEY



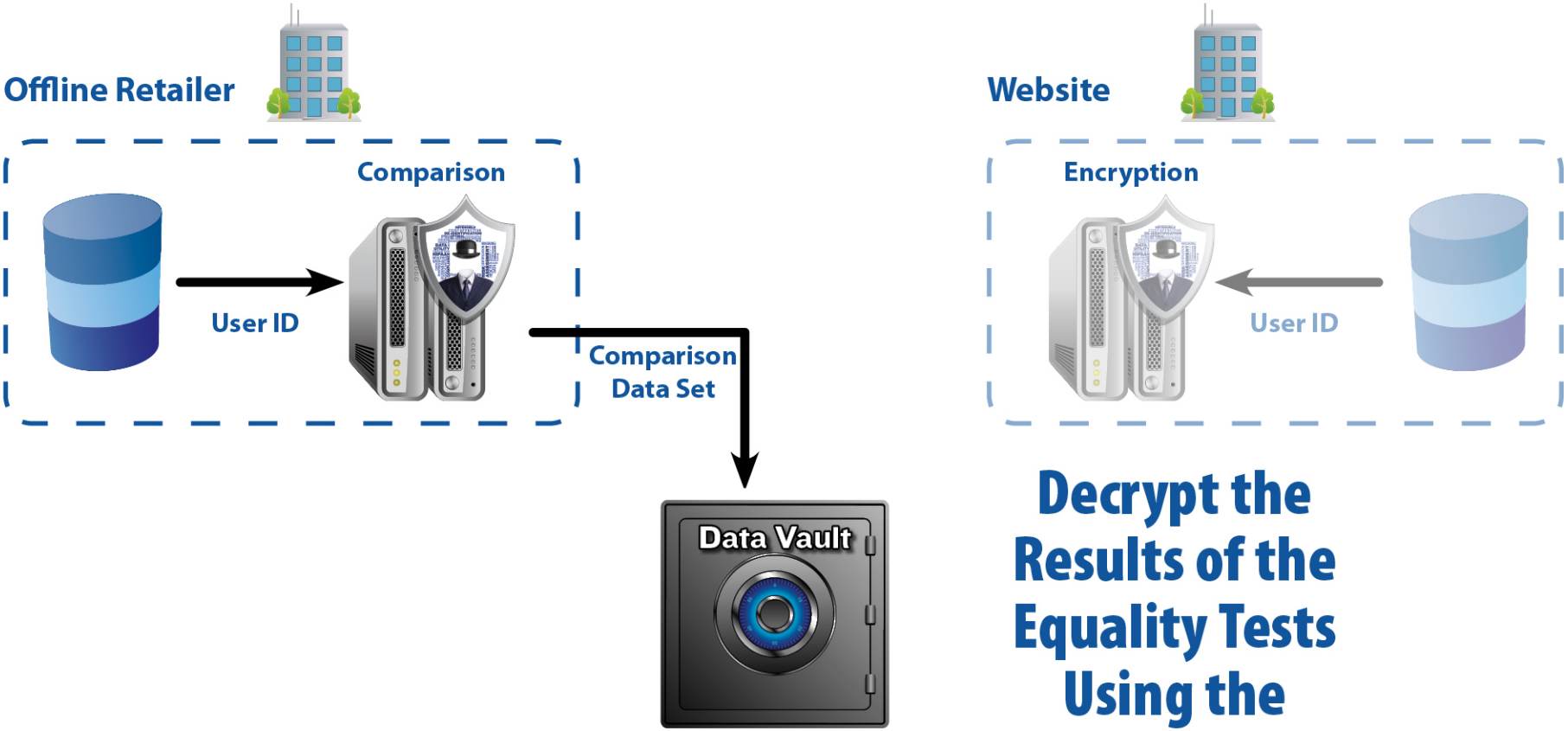


Encryption of User ID Using the Same PUBLIC KEY

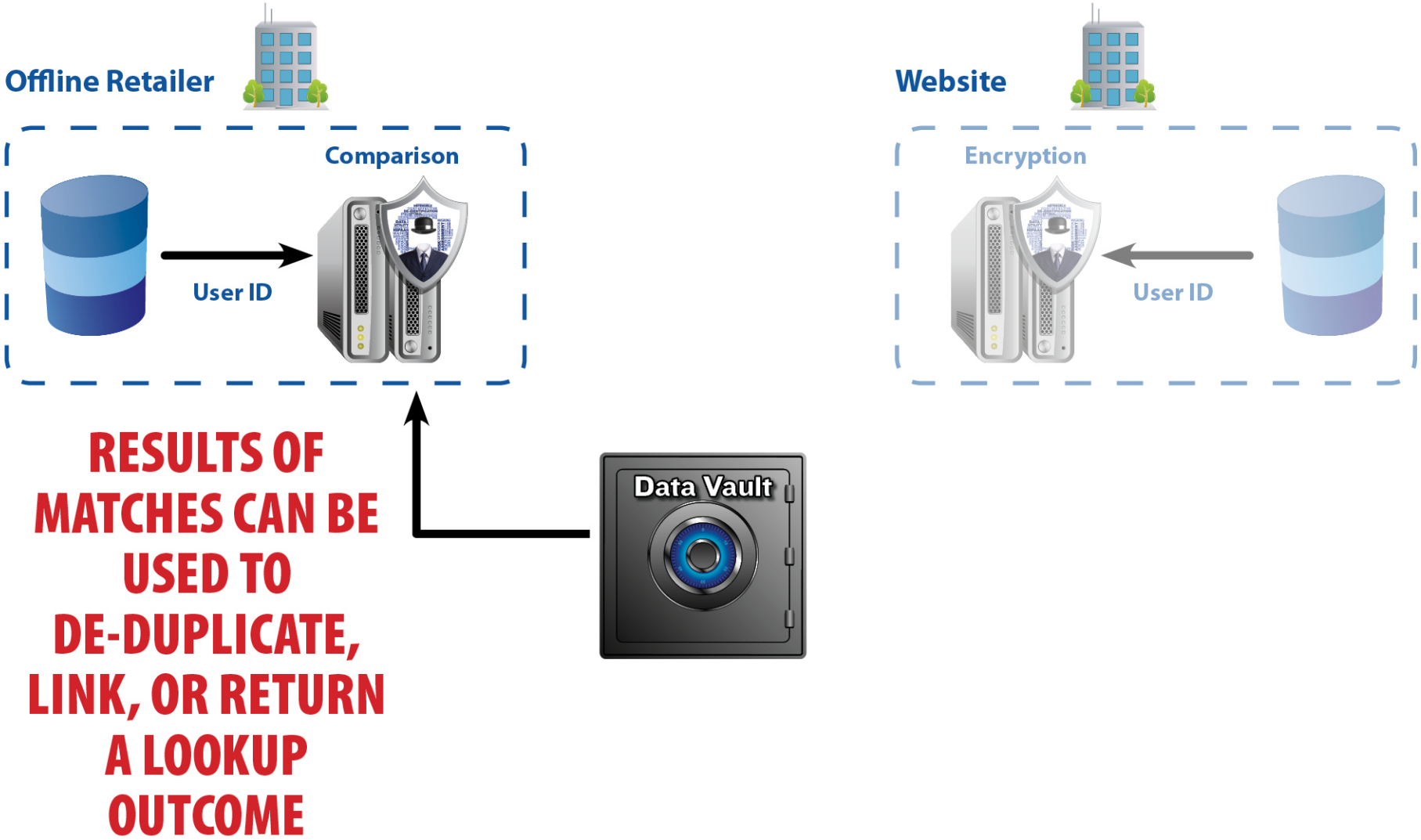




Perform Homomorphic EQUALITY TEST On the Two Encrypted Values



Decrypt the Results of the Equality Tests Using the PRIVATE KEY


Offline Retailer
Comparison
User ID
Website
Encryption
User ID
Data Vault
RESULTS OF MATCHES CAN BE USED TO DE-DUPLICATE, LINK, OR RETURN A LOOKUP OUTCOME

CONTACT

kelemam@ehealthinformation.ca

@kelemam