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)
MULTI-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

ENCRIPTION
AN ABSTRACT

HOMOMORPHISM

\[ \begin{array}{c}
\mathbb{G} \\
\begin{array}{c}
a \otimes b \\
\end{array} \\
\end{array} \rightarrow \begin{array}{c}
\mathbb{H} \\
\begin{array}{c}
x \oplus y \\
\end{array} \\
\end{array} \\
\begin{array}{c}
f \\
\end{array} \\
\begin{array}{c}
g \\
\end{array} \]
AN ABSTRACT

HOMOMORPHISM

\[ a \otimes b = g(f(a) \oplus f(b)) \]
AN ABSTRACT HOMOMORPHISM

\[ x \oplus y = f(g(x) \otimes f(y)) \]

\[ a \otimes b \xrightarrow{f} x \oplus y \]

\[ \text{G} \xrightarrow{f} \text{H} \]

\[ g \]

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

ENCRYPTION

\[ c = \text{Enc}_{pk}(m) \]
\[ m = \text{Dec}_{sk}(c) \]
RANDOMIZED PUBLIC KEY ENCRYPTION

\[ c_1 = Enc_{pk}(m, r_1) \]
\[ c_2 = Enc_{pk}(m, r_2) \]
RANDOMIZED PUBLIC KEY ENCRYPTION

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

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

If \( r_1 \neq r_2 \) then \( c_1 \neq c_2 \), but

\( \text{Dec}_{sk}(c_1) = \text{Dec}_{sk}(c_2) = m \)
RANDOMIZED PUBLIC KEY ENCRYPTION

NOTATION DENOTING AN ENCRYPTED PLAINTEXT

\[
[a] = Enc_{pk}(a, r) \\
[b] = Enc_{pk}(b, r')
\]
ADDITIVELY HOMOMORPHIC ENCRYPTION
ADDITIVELY HOMOMORPHIC ENCRYPTION

\[ [a] \cdot [b] = [a + b] \]
ADDITIVELY HOMOMORPHIC
ENCRIPTION

\[ a^b = [ab] \]
SECURE COMPARISON

PROTOCOL

\[ f(x, y) = \begin{cases} 
0, & x = y \\
\text{random\#}, & \text{otherwise}
\end{cases} \]
2-PARTY SECURE COMPARISON PROTOCOL

\[ a \xrightarrow{[a]} b \]

\[ \text{Dec}_{sk}(c) = r \cdot (a - b) \]

\[ ([a] \cdot [-b])^r = [r \cdot (a - b)] = c \]
ADDITIVELY
HOMOMORPHIC SCHEMES

PAILLIER (1999)

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

EXPONENTIAL ELGAMAL (1984, 1997)

\[ [g^a] \cdot [g^b] = [g^{a+b}] \]
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
Offline Retailer → Comparison → Data Vault

User ID → Public Key

www.ehealthinformation.ca

Website → Encryption → Data Vault

User ID → Public Key

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
RESULTS OF MATCHES CAN BE USED TO DE-DUPLICATE, LINK, OR RETURN A LOOKUP OUTCOME
CONTACT

kelemam@ehealthinformation.ca

@kelemam