C/C++ implementation of a cryptographic protocol using Paillier's homomorphic cryptographic primitive.

Mentee: Joshua Robinson         Mentor: Vincent Bindschaedler

Alice

1. Creates public key (pub_key) and private key (prv_key) as well as calculating ciphertext for Alice's wealth $E(-A)$.

ACTIONS :

\[
\text{prv_key, pub_key} = \text{paillier_key_gen}
\]

\[
E(-A) = \text{enc}(\text{pub_key}, \text{Alice}\_wealth)
\]

Alice and Bob are both wealthy people and they want to ascertain who is wealthier without disclosing the amount of wealth they have. We are assuming both parties are semi-honest: they provide true information, but will not hesitate to snoop information that is not for them to know.

Send pub_key and $E(A)$

2. Uses pub_key to calculate ciphertext for Bob's wealth $E(B)$.

Uses pub_key to calculate the homomorphic multiplication of $E(-A)$ and $E(B)$, which is just $E(A - B)$.

Uses pub_key to multiply $E(A - B)$ by a random integer, $X$, to get $E(X(A-B))$.

ACTIONS :

\[
E(B) = \text{enc}(\text{pub_key}, \text{Bob}\_wealth)
\]

\[
E(A-B) = \text{mul}(\text{pub_key}, E(B), E(-A))
\]

\[
E(X(A-B)) = \text{pow}(\text{pub_key}, E(A-B), X); \text{ where } X \text{ is random integer.}
\]

Send $E(X(A-B))$

3. Uses the public key and private key previously calculated to get $X(A-B)$.

Use the sign of $X(A-B)$ to determine who is richer.

ACTIONS :

\[
\text{result} = \text{sign}(\text{dec}(\text{pub_key}, \text{prv_key}, E(X(A-B))))
\]

If positive, Alice is poorer.

If negative, Alice is richer.

If zero, they are equally wealthy.

Send Result

Alice and Bob now know who is wealthier, but can never determine the other's wealth. Save for the case where they have the same exact wealth.

4. Receive the result and determine Bob's relative wealth.

Bob

The Protocol

The Paillier's Cryptosystem

• Asymmetric cryptographic system created by Paillier in 1999
• Additive homomorphic property
• Add two plaintexts with public key and their respective ciphertexts

Objective

• Implement a protocol using a modern cryptographic primitive
• It is useful in electronic banking and voicing
• C to implement the Paillier Cryptography
• C++ to implement an the protocol using NSPR