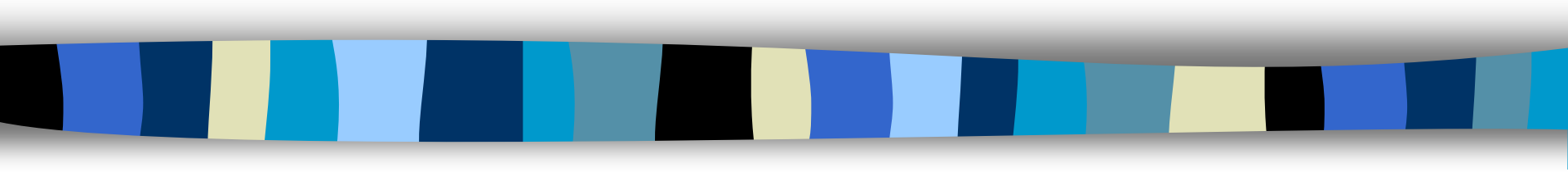
Data Security and Privacy



Commutative and Homomorphic Encryption Schemes

Commutative Encryption

Definition: an encryption scheme is commutative if
$E_{K1}[E_{K2}[M]] = E_{K2}[E_{K1}[M]]$

- Given an encryption scheme that is commutative, then $D_{K1}[D_{K2}[E_{K1}[E_{K2}[M]] = M$
- That is, if message is encrypted twice, the order does not matter.
- Most symmetric encryption scheme (such as DES and AES) are not commutative

Examples of Commutative Encryption Schemes

- Private key: Pohlig-Hellman Exponentiation Cipher with the same modulus p
  - encryption key is e, decryption key is d, where $ed \equiv 1 \pmod{(p-1)}$
  - $E_{e1}[M] = M^{e1} \bmod p$ and $D_{d1}[C] = C^{d1} \bmod p$
  - $E_{e1}[E_{e2}[M]] = M^{e1e2} = E_{e1}[E_{e2}[M]] \pmod p$

The SRA Mental Poker Protocol

- How do two parties play poker without a trusted third party?
  - Need to deal each one a hand of card, and after placing bet, be able to show hand.
  - Setup: Alice and Bob agree on using M_1, M_2, …, M_{52} to denote the 52 cards.
- Any ideas?

The SRA Mental Poker Protocol

- Alice encrypts M_1, M_2, …, M_{52} using her key, then randomly permute them and send the ciphertexts to Bob
- Bob picks 5 ciphertexts as Alice's hand and sends them to Alice
- Alice decrypts them to get his hand
- Bob picks 5 other ciphertexts as his hand, encrypts them using his key, and sends them to Alice
- Alice decrypts the 5 ciphertexts and sends to Bob
- Bob decrypts what Alice sends and gets his hand
- Both Alice and Bob reveals their key pairs to the other party and verify that the other party was not cheating. (Why need this step?)

Homomorphic Encryption

- Encryptions that allow computations on the ciphertexts
  - $E_k[m_1] \bullet E_k[m_2] = E_k[m_1 \circ m_2]$
- Applications
  - E-voting: everyone encrypts votes as 1 or 0, aggregate all ciphertexts before decrypting; no individual vote is revealed.
    - Requires additive homomorphic encryption: $\circ$ is +
  - Secure cloud computing.
    - Requires full homomorphic encryption, i.e., homomorphic properties for both + and $\times$

Homomorphic Properties of Some Encryption Schemes

- Multiplicative homomorphic encryption
  - Unpadded RSA: $m_1^e \times m_2^e = (m_1 \times m_2)^e$
  - El Gamal: Given public key $(g, h=g^a)$, ciphertexts $(g^{r1}, h^{r1}m_1)$ and $(g^{r2}, h^{r2}m_2)$, multiple both components $(g^{r1+r2}, h^{r1+r2}m_1m_2)$
- Additive homomorphic encryption schemes
  - Paillier cryptosystem (will explore in HW problem)
- Fully homomorphic encryption also exist
  - Significantly slower than other PK encryption