**Anonymous Multi-Receiver Certificateless Hybrid Signcryption for Broadcast Communication**

* Alia Umrani, PhD student at College Cork, Ireland
* Lots of smart systems
* Security requirements in broadcast communication
  + Confidentiality, authentication: verification of where things are coming from, and anonymity: no device should be able to understand the other party
  + Encryption, digital signature, and pseudo-identity
* Current solution to solve all requirements are sign-then-encrypt scheme
  + Very computationally heavy
* Solution
  + Digital signature
  + Encryption
  + Operation will be performed simultaneously
* **Hybrid Signcryption**
  + **Digital signature**
  + **Encryption**
  + **Symmetric and asymmetric crptography**
  + **More efficient**
* Unsigncryption can be performed in either direction depending upon the scheme design
* Hybrid Signcryption
  + Symmetric key using public key
  + Let’s multiple users use their own public key to decrypt a broadcasted communication
  + Uses both symmetric and asymmetric approaches
* Traditional PKI
  + Each user generates own public and private key
  + Disadvantages
    - Certificate management overhead
    - Certificate revocation requires computation
  + Identity Based PKC
    - Some data as the id and data
    - Uses public key generator and encodes it with the public keys to send signed data to receiver
    - Disadvantages
      * What if public key generator was compromised
      * Key escrow problem
  + Certificateless based PKC
    - Sender sends ID to key generation center which will generate a partial private key
    - Sent back to sender
    - So that only part of private key is compromised

Problem Statement

* Signcryption scheme
  + ID-based PKC
  + Can lead to key escrow problem
* Contribution
  + Combination of asymmetric key and symmetric key
  + Multi-receiver key encapsulation mechanism (mKEM)
  + Data encapsulation mechanism (DEM)
* Assigns a pseudo-identity PID

Framework of AMCLHS

Before communication

* Key generation center
  + Trusted authority
  + Generates
    - Public parameters
    - Master secret key
    - Master public key
    - Partial private key
  + If KGC is compromised than partial key is compromised
* Registration Authority
  + Generates sk\_Ra, pk\_RA
  + Provides verification
* N users perform signcryption and unsigncryption

Security Model

* Type I adversity: if sender is compromised
  + Cannot access master security key
  + Cannot access ppk for any of the target ID
* Type II
  + Malicious KGC
  + Cannot compute/query pk replace pk and sv

Security Attacks

* Chosen ciphertext attack (CCA) – breaks confidentiality
  + Prove indistinguishability
  + Challenger
    - Respond to queries
    - Generates challenge
  + Adversary
    - Learn some information about encryption algorithm
  + Challenger sends query to adversary
  + Adversary sends encryption query
  + Challenger sends c\_b
  + Adversary tries to descrypt
  + Challenger sends message to adversary
  + Adversary tries to see if message matches encryption
* Chosen Message Attacks (CMA) – breaks
  + Prove unforgeability
  + Challenger
  + Adversary
  + Adversary presents a query
  + Adversary Sends signature
  + Challenger generates signature to adversary
  + Adversary sends signature to challenger
  + Test if signature is valid or invalid

AMCLHS

* Sender with PID sends arbitrary length m to t designated receivers
* Performance Analysis
  + Computation for AMCLHS (2n + 5)M
  + Main bottle neck is multiplication and exponents
* Communication Cost
  + Signcryption O(n)
  + Unsigncryption O(1)
  + AMCLHS fulfills all the requirements
* Things learned
  + Way to prove security
  + How public keys are generated
  + General cryptography information