# Annual Conference of ITA

## ACITA 2012

MINISTRY OF DEFENCE

# Protecting Receivers' Identities in Secure Data Distribution

**Nelly Fazio** (The Graduate Center & The City College, CUNY), **Irippuge Milinda Perera** (The Graduate Center, CUNY)

## Motivation & State-of-the-Art

Cryptographic tools for securing multicast communications:

- Broadcast Encryption (BE): transmit data to a dynamically changing set of recipients
  - Info about receivers is broadcast in the clear

Receivers' identities often sensitive. Secure communication ought to protect more than just transmitted content!

- Anonymous BE (ABE) [BBW06]: also hides receiver set

**Current best solution**

- Ciphertext linear in number of recipients
- Security model against **static** adversary
- Security of enhanced construction based on the ROM; [LPQ12] recently removed ROM from [BBW06]

**Networking technology at support of military operations**

- ABE enables secure distribution of tactical data in missions with ad-hoc team formation while concealing identities of operatives authorized to access content

**BE enables efficient encrypted file systems**

- ABE avoids disclosure of the identities of the authorized users, not only from outsiders, but also from one another

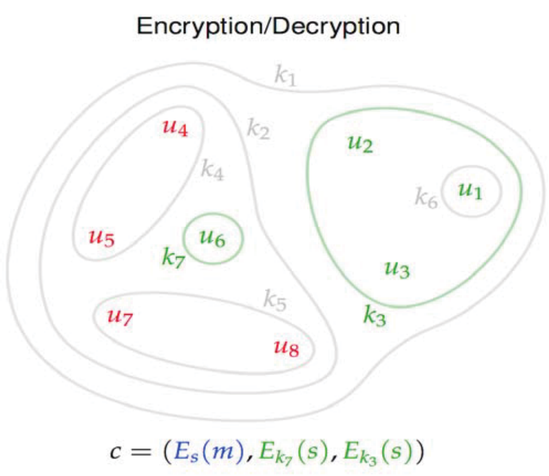
## Primitives

**Anonymous Identity-Based Encryption (AIBE)**

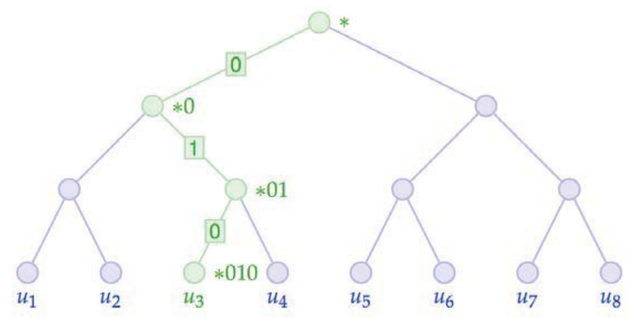
- A public-key encryption scheme where the user public key is an arbitrary bit-string
- Ciphertext hides the identity under which it is encrypted

**The Subset Cover Framework [NNL01]**

- Goal: Define and analyze the security of revocation schemes in the private-key setting
- Users belong to multiple subsets with associated keys




- To broadcast a message, first find the set of subsets covering the recipient set, and then encrypt the message under the keys of the coverset (*hybrid encryption*)
- [NNL01] provides two ways of defining subsets: Complete Subtree (CS) and Subset Difference (SD) method
- Dodis and Fazio (2002) extend the CS and SD methods to the public-key setting
- Idea: Novel ID assignment + (Hierarchical) Identity-Based Encryption ((H)IBE)




## Results

**Outsider Anonymous Broadcast Encryption (oABE)**: Relaxing receiver anonymity guarantees for better efficiency

- Recipient's identities hidden from outsiders…
- … but individual recipients might learn about each other
- Attain sub-linear ciphertexts in the number of recipients (in the standard model), and security against **active** adversary

**Our Constructions:**

- Idea: PK-CS method + Anonymous IBE = oABE
- Generic CPA + Generic CCA + CCA w/ enhanced decryption

| | Scheme | PK Length | SK Length | CT Length | Decryption Attempts |
|---|---|---|---|---|---|
| Regular | BBW06 | $\mathcal{O}(N)$ | $\mathcal{O}(1)$ | $\mathcal{O}(N-r)$ | $\mathcal{O}(N-r)$ |
| | LPQ12 | $\mathcal{O}(N)$ | $\mathcal{O}(1)$ | $\mathcal{O}(N-r)$ | $\mathcal{O}(N-r)$ |
| | FP12 | $\mathcal{O}(1)$ | $\mathcal{O}(\log N)$ | $\mathcal{O}\left(r\log\left(\frac{N}{r}\right)\right)$ | $\mathcal{O}\left(r\log\left(\frac{N}{r}\right)\log N\right)$ |
| Enhanced | BBW06 | $\mathcal{O}(N)$ | $\mathcal{O}(1)$ | $\mathcal{O}(N-r)$ | 1 |
| | LPQ12 | $\mathcal{O}(N)$ | $\mathcal{O}(1)$ | $\mathcal{O}(N-r)$ | 1 |
| | FP12 | $\mathcal{O}(N)$ | $\mathcal{O}(\log N)$ | $\mathcal{O}\left(r\log\left(\frac{N}{r}\right)\right)$ | 1 |
| | FP12 | $\mathcal{O}(N^2)$ | $\mathcal{O}(N)$ | $\mathcal{O}(2r)$ | 1 |

$N$: total number of users, $r$: number of revoked users.

## Long-Term Goals