Motivation & State-of-the-Art
- Crypto tools for secure multicast communications
- Broadcast Encryption (BE)
  - Transmit data to a dynamically changing set of recipients
  - Info about receivers is broadcast in the clear
- Receivers' identities are often sensitive. Secure communication ought to protect more than just transmitted content!
- Anonymous BE (AnoBE): also hides receiver set [BBW06]
  - Ciphertext linear in number of recipients
  - Security model against static adversary
  - Security of enhanced construction based on the ROM
- [LPQ12] recently removed ROM + active adversary

Applications
- Networking technology for military operations
  - AnoBE 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
  - AnoBE avoids disclosure of identities of 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 (SC) Framework [NNL01]
  - Goal: Define and analyze security of revocation schemes in the private-key setting
  - Users belong to multiple subsets with associated keys
  - To broadcast a message, first find the cover set, and then hybrid-encrypt the message under the keys of the coverset

[NNL01] presents two SC algorithms:
- Complete Subtree (CS) method
- Subset Difference (SD) method

Extension of the Subset Cover Framework to Public-Key Setting [DF02]
- [DF02] extends the CS and SD methods to the public-key setting
- Idea: Novel ID assignment + (Hierarchical) Identity-Based Encryption ((H)IBE)

Our Contribution (Published at PKC’12)
- 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 with enhanced decryption

Comparisons

<table>
<thead>
<tr>
<th>Scheme</th>
<th>PK Length</th>
<th>SK Length</th>
<th>CT Length</th>
<th>Decryption Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBW06</td>
<td>$O(N)$</td>
<td>$O(1)$</td>
<td>$O(N - r)$</td>
<td>$O(N - r)$</td>
</tr>
<tr>
<td>LPQ12</td>
<td>$O(N)$</td>
<td>$O(1)$</td>
<td>$O(N - r)$</td>
<td>$O(N - r)$</td>
</tr>
<tr>
<td>FP12a</td>
<td>$O(N)$</td>
<td>$O(1)$</td>
<td>$O(N - r)$</td>
<td>$O(N - r)$</td>
</tr>
<tr>
<td>FP12b</td>
<td>$O(N^2)$</td>
<td>$O(N)$</td>
<td>$O(r)$</td>
<td></td>
</tr>
</tbody>
</table>

Future Work
- [DF02] extends the CS and SD methods to the public-key setting
- Idea: Novel ID assignment + (Hierarchical) Identity-Based Encryption ((H)IBE)

Future Work
- [DF02] extends the CS and SD methods to the public-key setting
- Idea: Novel ID assignment + (Hierarchical) Identity-Based Encryption ((H)IBE)

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>AnoBE</th>
<th>oABE</th>
<th>BE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$O(N - r)$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$O(\log \frac{N}{2})$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$O(1)$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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