SESSION ID: CRYP-T07

Downgradable Identity-based Encryption and Applications

Olivier Blazy, Paul Germouty, Duong Hieu Phan
Associate Professor, Xlim, University of Limoges, France
http://www.blazy.eu
• Context
• Model
• Generic Transformations
• Construction
General Context
Identity-Based Encryption

Alice

C = \text{Encrypt}'Bob', M'

M

Bob

M = \text{Decrypt}(usk_{Bob}, C')
History of IBE

- Shamir ‘84
- Boneh-Franklin, Cocks ‘01
- Boneh-Boyen, Waters ’05
- Waters ’09,
- Chen-Wee, Blazy –Kiltz-Pan
- Context
- Model
- Generic Framework
- Construction
- Applications
So Many Variants

- Hierarchical IBE
- Wildcarded IBE
- Wicked IBE
- ...

#RSAC
Relations ?
Relations?
Model
Identity-Based Encryption

● 4 algorithms:
  – Keygen: Generates mpk, msk
  – USKGen(id, msk): Generates usk[id]
  – Enc(mpk,id): Generates a capsule C leading to a key K for id
  – Dec(C,usk[id]): Recovers K’ from C
Downgradable Identity-Based Encryption

- 5 algorithms:
  - Keygen: Generates mpk, msk
  - USKGen(id, msk): Generates usk[id]
  - Enc(mpk,id): Generates a capsule C leading to a key K for id
  - Dec(C,usk[id]): Recovers K’ from C
  - USKDown(usk[id],id’): Return usk[id’] if id’ << id

- Given a key for an id, one can deduce a key for id’ if id’ can be obtained by replacing some 1 in id by 0. (101 << 111)
Downgradable Identity-Based Encryption

**Procedure Initialize:**

\[(mpk, msk) \xleftarrow{\$} \text{Gen}(\mathcal{K})\]

Return mpk

**Procedure USKGen(id):**

\[Q_{ID} = Q_{ID} \cup \{\text{id}\}\]

Return usk[id] \xleftarrow{\$} USKGen(msk, id)

**Procedure Enc(id\*):** //one query

\[(sk\*, C\*) \xleftarrow{\$} \text{Enc}(mpk, \text{id}\*)\]

\[sk\* \xleftarrow{\$} \mathcal{K}; C\* \xleftarrow{\$} \mathcal{CS}\]

Return \((sk\*, C\*)\)

**Procedure Finalize(\(\beta\)):**

Return \((-\text{id}\* \leq Q_{ID})\) \land \(\beta\)
Transformations
Wildcard Identity-Based Encryption

- Allows * in targeted identities

\[
\text{id}[2i, 2i + 1] = \begin{cases} 
01 & \text{if wid}[i] = 0 \\
10 & \text{if wid}[i] = 1 \\
00 & \text{otherwise.}
\end{cases}
\]
Hierarchical Identity-Based Encryption

- Allows to derive keys for lower level
  - This means* at the end of original identities

\[ \text{id}[2i, 2i + 1] = \begin{cases} 
01 & \text{if } \text{hid}[i] = 0 \\
10 & \text{if } \text{hid}[i] = 1 \\
11 & \text{otherwise} (\text{hid}[i] = \bot).
\]
Wicked Identity-Based Encryption

- Allows to derive keys for lower level
  - This means * in the original identities

\[
id[2i, 2i + 1] = \begin{cases} 
01 & \text{if } \text{wkdid}[i] = 0 \\
10 & \text{if } \text{wkdid}[i] = 1 \\
11 & \text{if } \text{wkdid}[i] = *
\end{cases}
\]
Transformations

- All those transformations are tight
- However they use a space of size 4 for a ternary alphabet.
  - It could be improved, but would not drastically improve the tightness
Attribute-Based Encryption

- User keys have 1 where they have the attribute
- Ciphertext have a 0 where an attribute is not mandatory
- If the policy < attributes, a user can properly downgrade his key
Construction
Downgradable Identity-Based Encryption

- Can be constructed by adapting BKP’14
  - Can be instantiated under any k-MDDH assumption (SXDH, Dlin, ...)
  - Depending on the use case, it is possible to ensure that the downgraded key is indistinguishable from a fresh one.
  - Encapsulation is only k+1 elements (k=1 for SXDH)
  - Same goes for user keys
# Wicked / Wildcard Identity-Based Encryption

| Name          | |pk| | |usk| | |C| | |assump.| |Sec| | |Loss| |
|---------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| WKD [AKN07]   | n + 4 | n + 2 | 2 | BDDH | Sel. standard | O(nq_k) |
| WKD [AKN07]   | (n + 1)n + 3 | n + 2 | 2 | BDDH | Full standard | O(q^n_k) |
| WKD-DIBE      | 4n + 2 | 3n + 5 | 5 | DLin (any k – MDDH) | Full standard | O(q_k) |
| SWIBE [KLO18] | n + 4 | 2n + 3 | 4 | ROM | Full | O((n + 1)(q_k + 1)^n) |
| WIBE [BDNS07] | (n + 1)n + 3 | n + 1 | (n + 1)n + 2 | BDDH | Full standard | O(n^2q^n_k) |
| Wild-DIBE     | 4n + 2 | 3n + 5 | 5 | DLin (any k – MDDH) | Full standard | O(q_k) |
## Attribute-Based Encryption

| Name         | \(|pk|\) | \(|sk|\) | \(|C|\) | pairing   | exp G | exp G\(_2\) | Reduction Loss |
|--------------|---------|---------|---------|-----------|-------|-------------|----------------|
| [OT10]       | \(4U + 2\) | \(3U + 3\) | \(7m + 5\) | \(7m + 5\) | 0     | m           | \(O(q_k)\)     |
| [LW12]       | \(24U + 12\) | \(6U + 6\) | \(6m + 6\) | \(6m + 9\) | 0     | m           | \(O(q_k)\)     |
| [CGW15]      | \(6UR + 12\) | \(3UR + 3\) | \(3m + 3\) | 6         | 6m    | 0           | \(O(q_k)\)     |
| [Att16]      | \(6UR + 12\) | \(3UR + 3\) | \(3m + 3\) | 6         | 6m    | 0           | \(O(q_k)\)     |
| scheme 10    |         |         |         |           |       |             |                 |
| [Att16]      | \(96(M + TR)^2 + log(UR)\) | \(3UR + 6\) | \(3m + 6\) | 9         | 6m    | 0           | \(O(q_k)\)     |
| scheme 13    |         |         |         |           |       |             |                 |
| Our DNF-ABE  | \(4U + 2\) | \(3U + 3\) | \(3k + 2\) | 13        | 0     | 0           | \(O(q_k)\)     |
Conclusion

- Another IBE related primitive
  - However it can be tightly linked to the others
  - So any progress on DIBE should lead to progress to the other primitive

- Can DIBE be achieved in a Post Quantum world?

- How to avoid the DNF limitation for ABE
Thank you

Any questions?