Attribute-Based Encryption from Lattices

Xavier Boyen

CRYPTO rump session - 2012/08/21
Attribute-based encryption

- Encrypt...
  - not to a key (PKE),
  - not to a name (IBE),
  - but to a formula on attributes.

“Law”

AND

OR

AND

5-out of-9

House

Senate

POTUS

SCOTUS
Regev's lattice PKE

**PK**: random \((A, u)\)  \(SK\): small \(e\) : \(A.e = u \ (q)\)

- Encrypt: pick \(s\), output : \(y = s^T A + \text{noise}\)
  \(x = M.\lfloor q/2 \rfloor + s^T A + \text{noise}\)

- Decrypt: \(x - y^T e = 0 + M.\lfloor q/2 \rfloor + \text{epsilon}\)
AB&CHKP’s lattice IBE

\[ A = f(Id) \]

\[ a \equiv u \pmod{q} \]

\[ y^T + \text{Noise} \]
ABVVW's lattice FuzzyIBE

\[ A = f(\text{Attr}) \]

\[ A = e_k \text{ Lagrange} \]

\[ s^T A_0 A A_k e_0 e e_k \]

\[ (\text{mod } q) \]

\[ y^T + \text{Noise} + \text{N.} + \text{M.} \]
Beyond Fuzzy? Danger!

Not independent; there be Rogue Basis!

Suppose $e_0 \neq e_1$
Idea: Split vectors bases

A

$\mathbf{s}^T \mathbf{A} \mathbf{e} \approx \mathbf{s}^T \mathbf{u}$

Public

Private key

$\mathbf{A}_1 \quad \mathbf{A}_2 \quad \mathbf{A}_i \quad \mathbf{A}_k$

$\lambda_{1,1} Z_1 \quad \lambda_{j,1} Z_j$

LSSS

Short Basis

$\lambda_{1,k} Z_1 \quad \lambda_{j,k} Z_j$
Conclusion

- /Basis Splitting /
  \Basis Sharing /
- KP-ABE
- CP-ABE
- Easy to simulate!
- (seemingly)
- VERY powerful indeed...

Regev