Efficient Lattice (H)IBE in the Standard Model from the BB_1 Framework

Dan Boneh   Xavier Boyen

Stanford University

Crypto'09 — Rump Session

2009/08/18

Lattice IBE w/o Random Oracles

pairing world	lattice world	ID processing
[CHK'03] $\longrightarrow\longrightarrow$	[AB'09] [CHK'09] [P'09]	bit by bit
$\downarrow$ $\downarrow$	$\downarrow$ $\downarrow$	
[BB'04] $\longrightarrow\longrightarrow$	[BB'09]	all at once

[CHK'03] — Canetti, Halevi, Katz

[BB'04] — Boneh, Boyen

[AB'09] — Agrawal, Boyen `crypto.stanford.edu/~xb/ab09/`

[CHK'09] — Cash, Hofheinz, Kiltz

[P'09] — Peikert

[BB'09] — Boneh, Boyen — this talk —

Efficient Lattice IBE : the Scheme

q — small prime $\quad$ n, m — matrix dimensions $\quad$ $m > 2\,n \log q$

Setup $A_0 \leftarrow \square \quad B_0 \leftarrow \square \quad R \leftarrow \square$ low norm $\quad u_0 \leftarrow \square$

$$\mathrm{PP} = \left(\, A = [A_0 \mid A_0\, R],\quad B_0 = [0 \mid B_0],\quad u_0 \,\right) \in \mathbb{Z}_q^{n\times 2m} \times \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n}$$

$$\mathrm{MK} = \left(\, T_{A_0} = \mathrm{Trapdoor}(A_0),\quad R \,\right)$$

Identity id uses matrix

$$F_{\mathrm{id}} := A + H(\mathrm{id})\, B = \left[A_0 \,\middle|\, A_0\, R + H(\mathrm{id})\, B_0\right] \in \mathbb{Z}_q^{n\times 2m}$$

Extract Use T_{A_0} to
output low-norm vector $d_{\mathrm{id}} \in \mathbb{Z}_q^{2m}$ solution of $F_{\mathrm{id}}\, d_{\mathrm{id}} = u_0$

Encrypt/Decrypt Regev w/ matrix F_{id} and adjusted noise vector

$$\mathrm{CT} = \left(\, c_0 = u_0^T\, s + x + b \left\lfloor \tfrac{q}{2} \right\rfloor,\quad c_1 = F_{\mathrm{id}}^T\, s + \left[\begin{smallmatrix} y \\ z \end{smallmatrix}\right] \,\right) \in \mathbb{Z}_q \times \mathbb{Z}_q^{2m}$$

$$\left\| c_0 - d_{\mathrm{id}}^T\, c_1 \right\| \overset{?}{>} \left\lfloor \tfrac{q}{4} \right\rfloor \quad \Rightarrow \text{decrypt as “1” else “0”}$$

Efficient Lattice IBE : the Reduction

LWE assumption $\mathcal{O}_s \equiv (\ a, \underbrace{a^T s + x}_{v})\ \approx_c\ \mathcal{U}(\ \mathbb{Z}_q^m \times \mathbb{Z}_q\ ) \equiv \mathcal{O}_\$$

Target   selective-ID security : $\mathcal{A}$ reveals id^* first

Setup $A_0, u_0 \leftarrow \mathcal{O}$ from LWE B_0 with $T_{B_0} = \mathrm{Trapdoor}(B_0)$

$$\mathrm{PP} = \Big(\ A = [\ A_0 \mid \underbrace{A_0\, R}_{\approx_s\, \mathcal{U}} - H(\mathrm{id}^*)\, B_0\ ],\ \ B = [\ 0 \mid B_0\ ],\ \ u_0\ \Big)$$

Queries   ($\mathrm{id} \neq \mathrm{id}^*$)   Use T_{B_0} to

output low-norm vector d_{id} solution of $F_{\mathrm{id}}\, d_{\mathrm{id}} = u_0$

(fails on id^* since for $F_{\mathrm{id}^*} = [A_0 \mid A_0\, R]$ the trapdoor cancels)

Challenge   w/ noise comp.

$$\mathrm{CT} = \Big(\ c_0 = \underbrace{v_0}_{\mathrm{LWE}} + b\lfloor \tfrac{q}{2} \rfloor,\ \ c_1 = \begin{bmatrix} 1 \\ R^T \end{bmatrix} \underbrace{[v_1 \ldots v_m]^T}_{\mathrm{LWE}} + \begin{bmatrix} y \\ -R^T y + z \end{bmatrix}\ \Big)$$

Efficient Identity Encoding

Only a few possible id $\in \mathbb{Z}_q$ so far...

How to get exponentially many?

Increase $q > 2^n$ but inefficient (wastes the appeal of small q)

Encode id not into $\mathbb{Z}_q$ but into $\mathbb{Z}_q^{n \times n}$

Encoding with Full-Rank Differences

$H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ s.t. $\forall \mathrm{id}_1 \neq \mathrm{id}_2 : \left| H(\mathrm{id}_1) - H(\mathrm{id}_2) \right| \neq 0$

Goals

Sub-expressions "$H(\mathrm{id})\, B_0$" : view as $n \times n$ matrix multiply

Trapdoor-ed $H(\mathrm{id})\, B_0 - H(\mathrm{id}^*)\, B_0$ must not vanish for $\mathrm{id} \neq \mathrm{id}^*$

$\longrightarrow$ requires $H(\mathrm{id}) - H(\mathrm{id}^*)$ non-singular

Result

- Have generic FRD encoding scheme w/ most possible q^n id-s

Conclusion

- First efficient IBE from lattices in standard model
  - comparable to random-oracle-model [GPV'08]
  - n times better than standard-model [AB'09] [CHK'09] [P'09]
- Lattice analogue to pairing BB_1 framework
  - supports HIBE delegation, etc.
- Nice use of general tool : full-rank-diff (FRD) matrix encoding

Why IBE from lattices?

hedge against quantum computing
simpler than pairings
etc.