

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

Dan Boneh

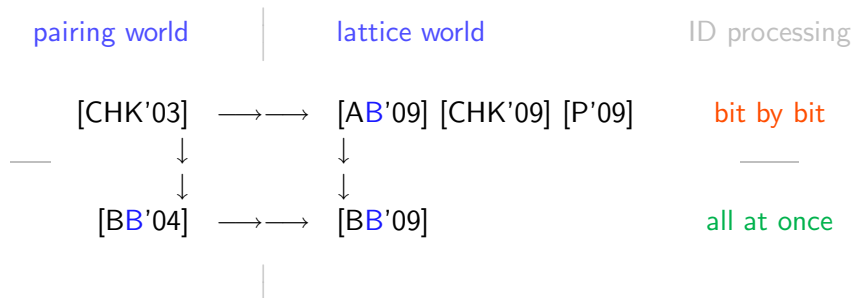
Xavier Boyen

Stanford University

Crypto'09 — Rump Session

2009/08/18

Lattice IBE w/o Random Oracles



[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 n, m — matrix dimensions $m > 2 n \log q$

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

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

MK = ($T_{A_0} = \text{Trapdoor}(A_0)$, R)

Identity id uses matrix

$$F_{\text{id}} := A + H(\text{id}) B = [A_0 \mid A_0 R + H(\text{id}) B_0] \in \mathbb{Z}_q^{n \times 2m}$$

Extract Use T_{A_0} to

output low-norm vector $d_{\text{id}} \in \mathbb{Z}_q^{2m}$ solution of $F_{\text{id}} d_{\text{id}} = u_0$

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

CT = ($c_0 = u_0^T s + x + b \lfloor \frac{q}{2} \rfloor$, $c_1 = F_{\text{id}}^T s + \lfloor \frac{y}{z} \rfloor$) $\in \mathbb{Z}_q \times \mathbb{Z}_q^{2m}$

$\|c_0 - d_{\text{id}}^T c_1\| \stackrel{?}{>} \lfloor \frac{q}{4} \rfloor \Rightarrow$ 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 $T_{B_0} = \text{Trapdoor}(B_0)$

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

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

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

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

Challenge w/ noise comp.

CT = $\left(c_0 = \underbrace{v_0}_{\text{LWE}} + b \left\lfloor \frac{q}{2} \right\rfloor, c_1 = \begin{bmatrix} 1 \\ R^T \end{bmatrix} \underbrace{[v_1 \dots v_m]}_{\text{LWE}}^T + \begin{bmatrix} -R^T y + z \end{bmatrix} \right)$

Efficient Identity Encoding

Only a few possible $\text{id} \in \mathbb{Z}_q$ 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

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

Goals

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

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

→ requires $H(\text{id}) - H(\text{id}^*)$ 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.