Predicate Encryption from LWE

Shweta Agrawal (UCLA)
David Mandell Freeman (Stanford)
Vinod Vaikuntanathan (U. Toronto)
Prediccate Encryption
[KSW08, OT09, LOSTW10]

Secret Keys
for functions $F$

Ciphertexts
for inputs $x$ & msg $m$

Decrypt iff $F(x) = 1$
PE for Inner Products

[KSW08, OT09, LOSTW10]

Secret Key for vector \(v\)

Ciphertexts for vector \(w\) & msg \(m\)

Decrypt iff \(<v, w> = 0\)
Predicate Encryption
[KSW08, OT09, LOSTW10]

**Theorem [AFV11]:** Predicate Encryption for Inner Products from Learning with Errors (LWE).

**Main Difficulty:**

- **Bilinear world:** same group for all keys/CT
- **Lattices:** Different lattice for every key/CT
Predicate Encryption
[KSW08, OT09, LOSTW10]

Solution: New algebraic technique (built on ABB10a IBE) that “matches” key lattice $L_v$ to ciphertext lattice $L_w$ iff $<v, w> = 0$.

However, only weakly attribute hiding (as in OT09, LOSTW10; not as in KSW08)
Why Lattices?

The Usual: Worst-case reduction, quantum security

The New: Inner products over small fields

The Future: More complex predicates?

Three wise men said:
“For predicate encryption…the inability to move beyond inner products stems from the ‘bi’ in Bilinear maps” - Boneh, Sahai, Waters, 2011

More at IACR ePrint 2011/410