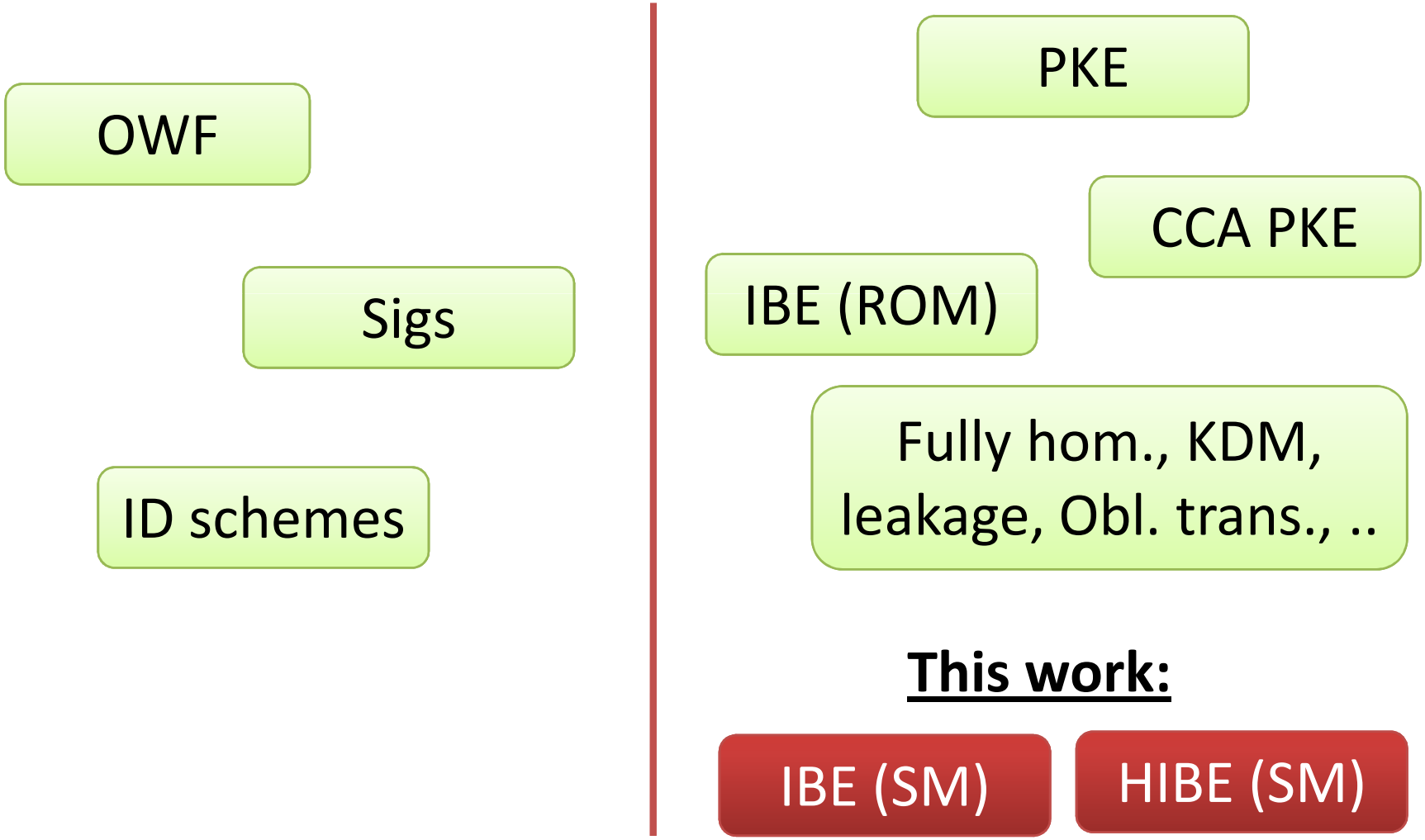
How to Delegate a Lattice Basis

David Cash, Dennis Hofheinz, Eike Kiltz

Cryptography from lattices



Encryption from lattices [AD97,R05,GPV08,…]

- **Public Key:**
  random basis for lattice L to encrypt

- **Secret Key:**
  short basis for lattice L to decrypt

New technique: basis delegation

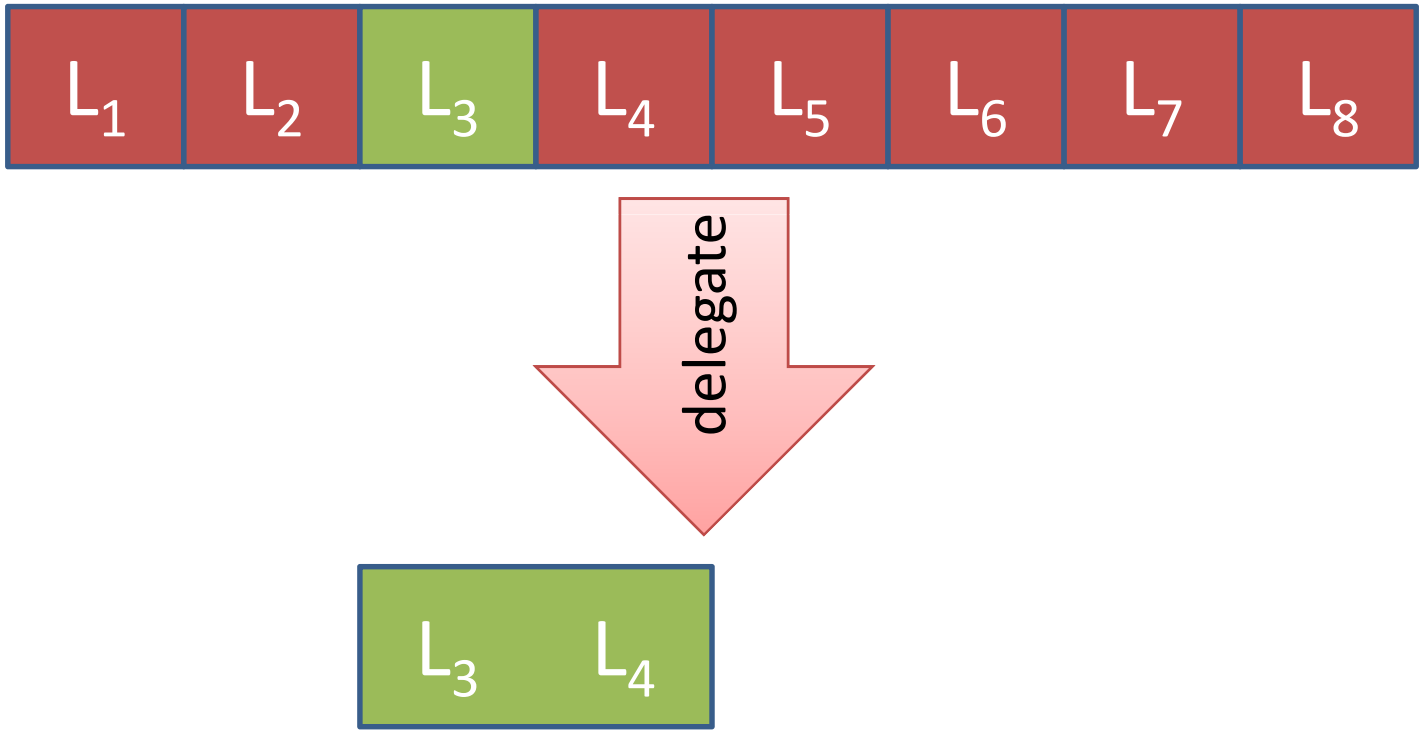
Red: random basis (PK)

Green: short basis (SK)

New technique: basis delegation

Red: random basis (PK)

Green: short basis (SK)

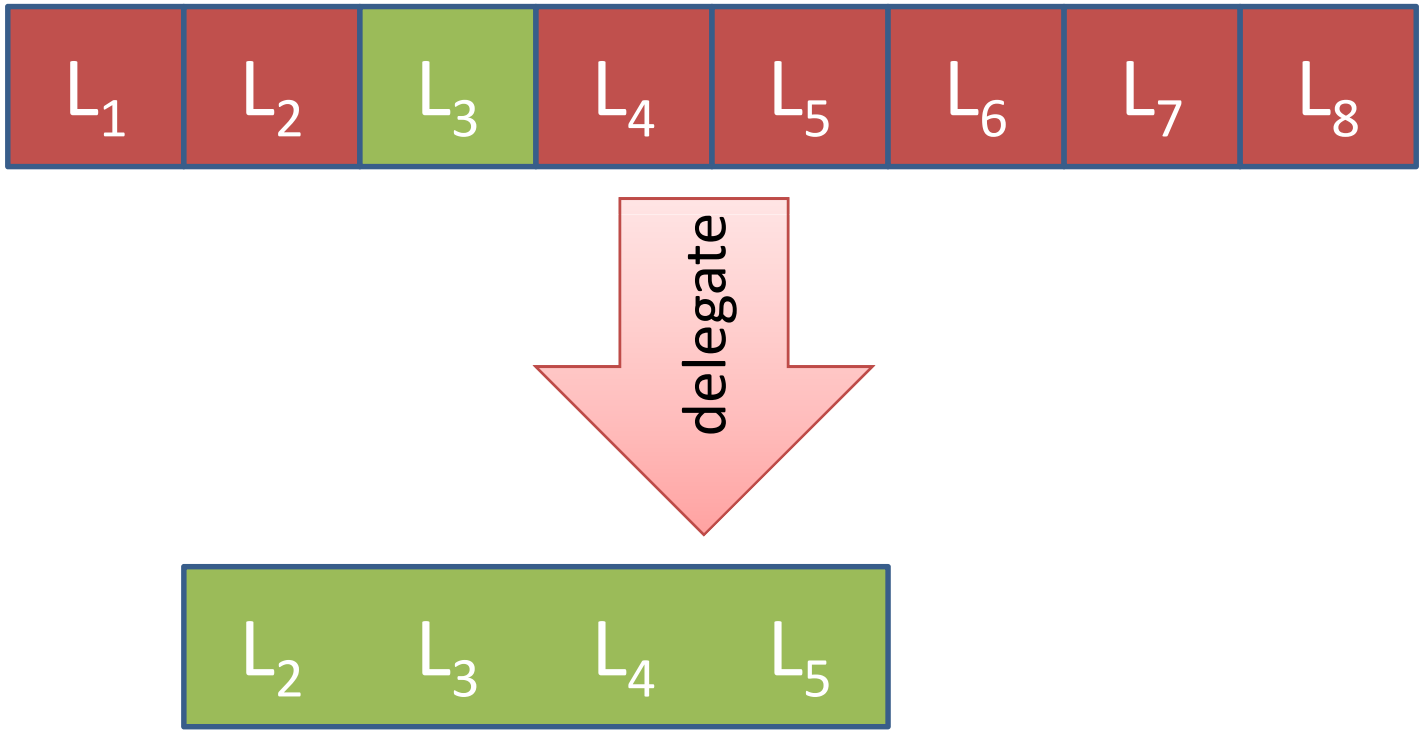


Short basis for higher-dim. joint lattice L_3 L_4

New technique: basis delegation

Red: random basis (PK)

Green: short basis (SK)

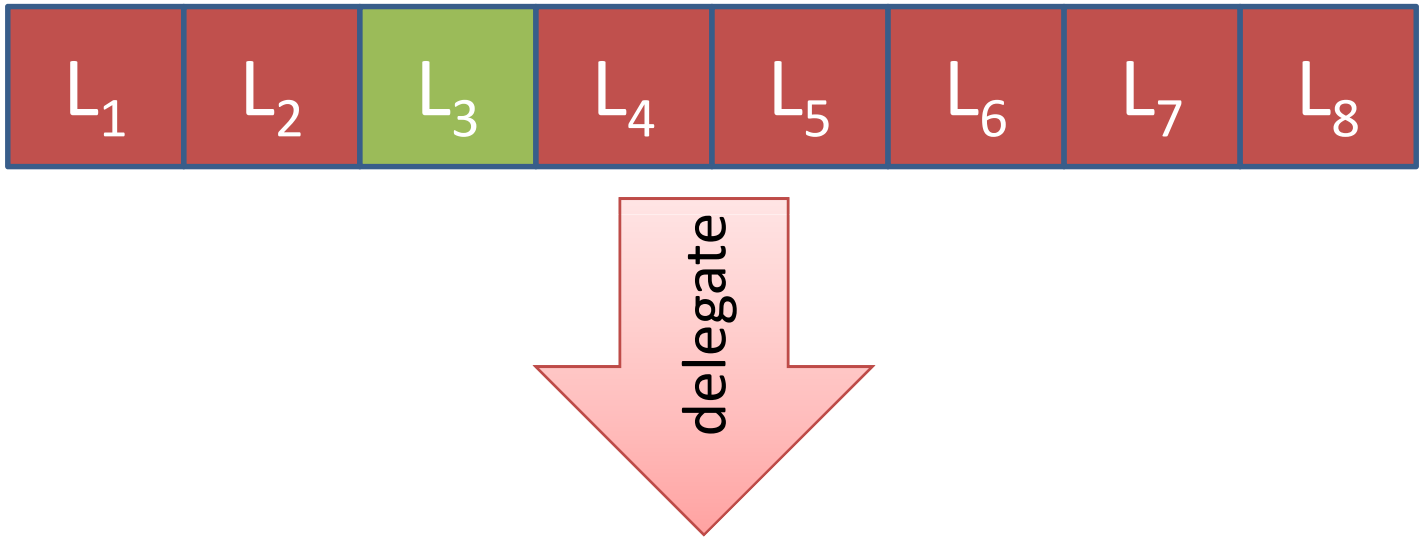


Short basis for higher-dim. joint lattice L_2 L_3 L_4 L_5

New technique: basis delegation

Red: random basis (PK)

Green: short basis (SK)



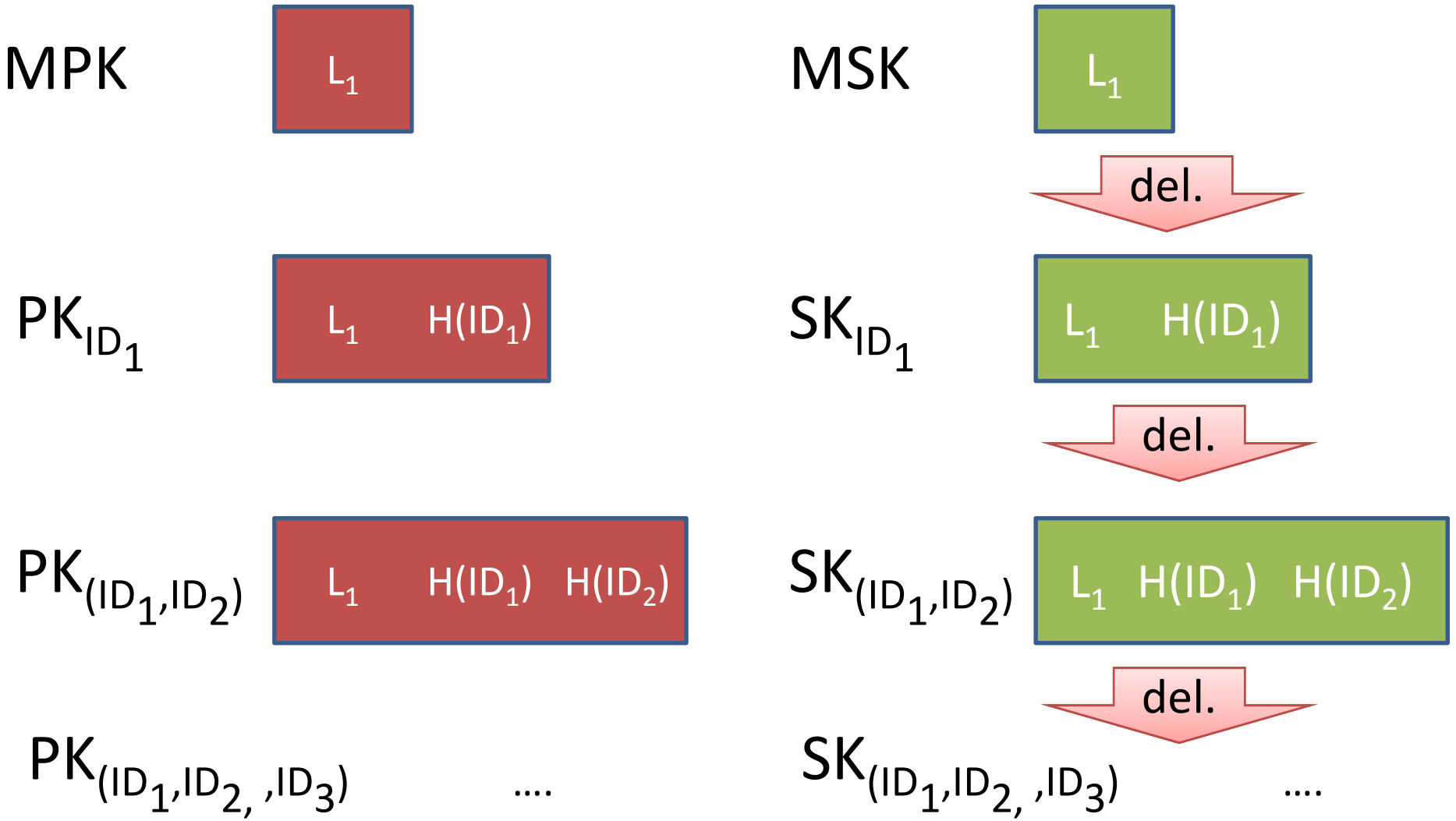
Short basis for joint lattice 

Application I: HIBE with random oracles

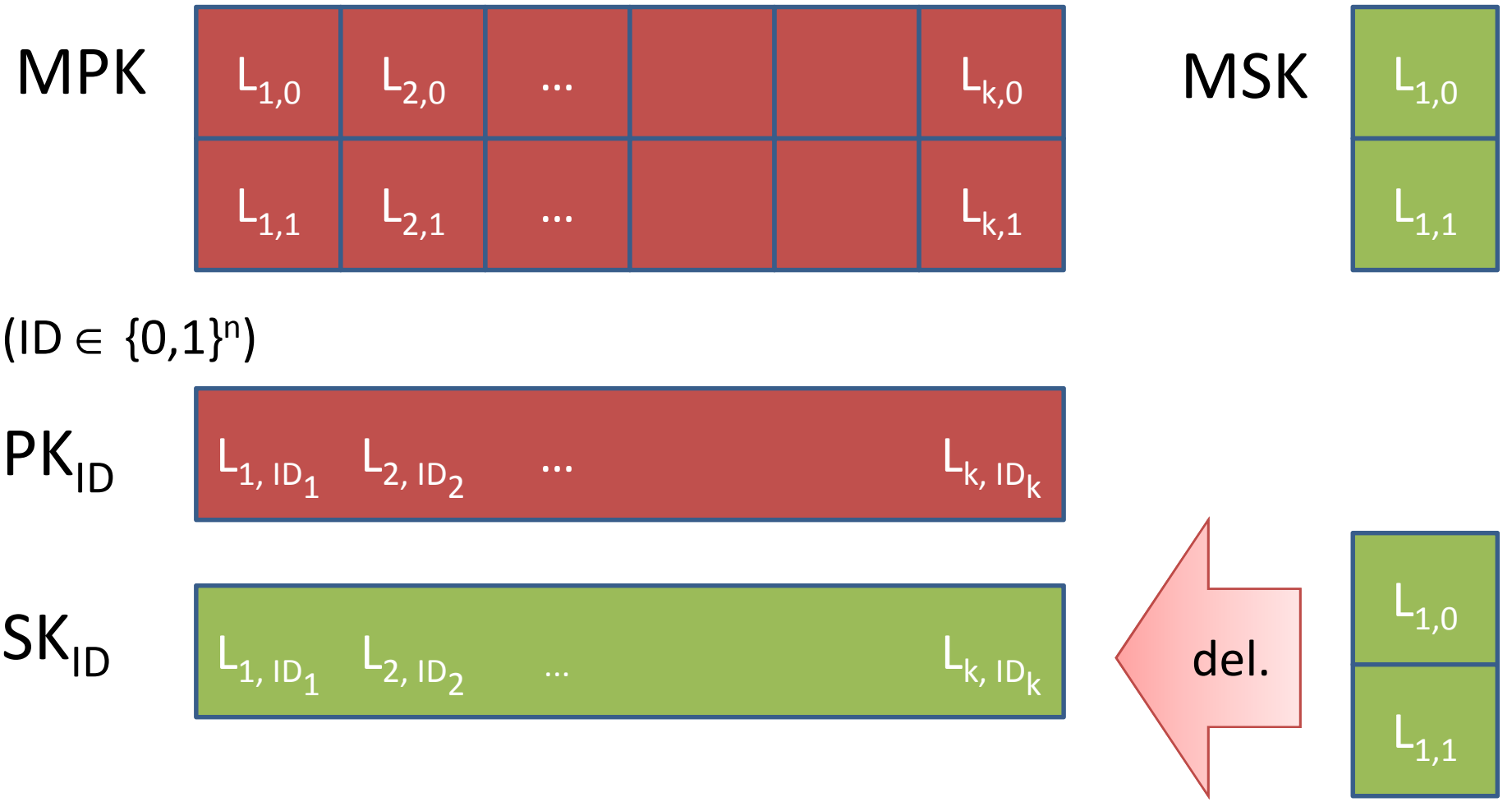
MPK 

MSK 

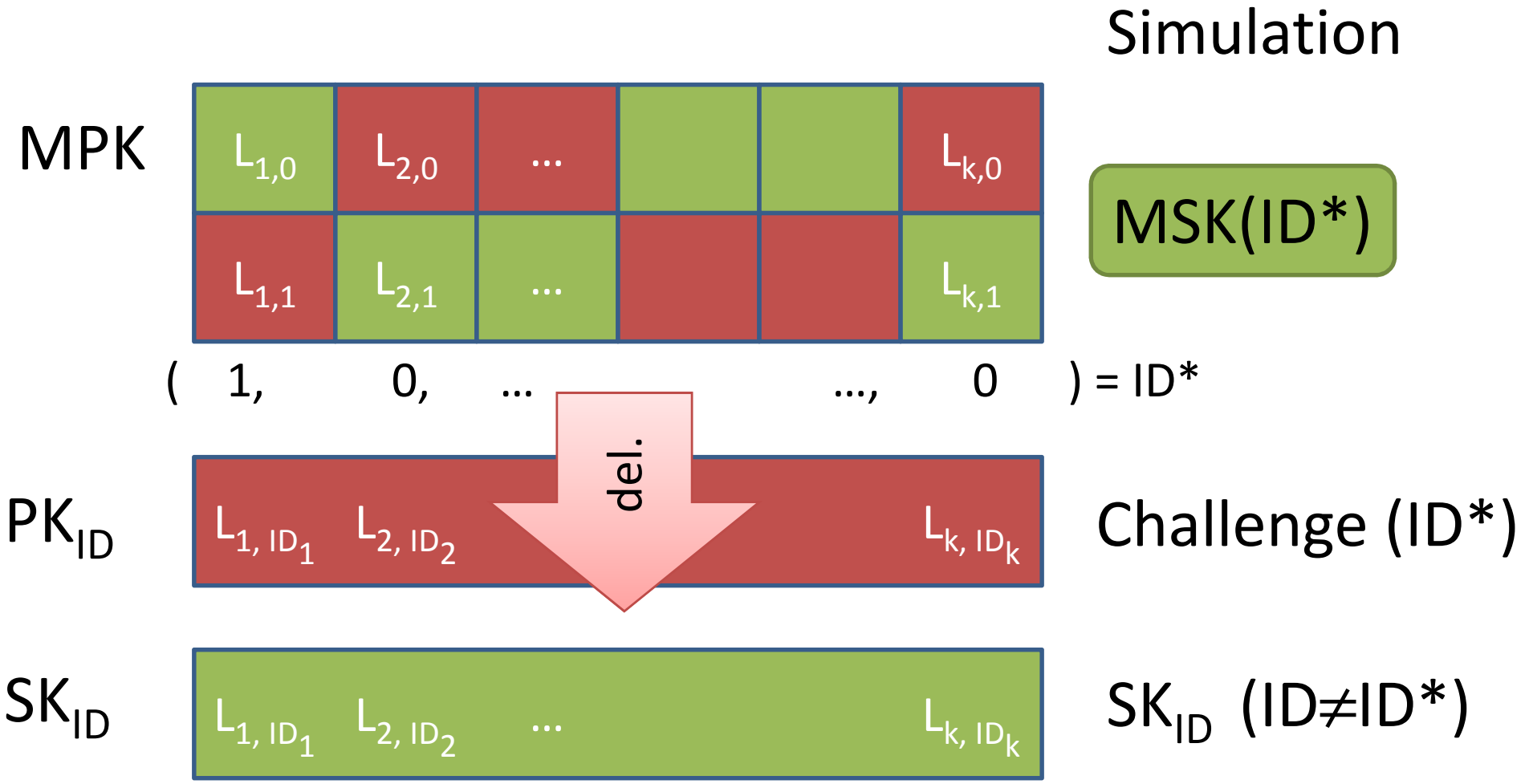
Application I: HIBE with random oracles



Application II: (H)IBE w/o ROs



Proof (selective-ID)



Summary

New short basis delegation technique for lattices

1. HIBE with random oracles
   - First HIBE w/o pairings!
2. sID secure HIBE w/o random oracles
   - Factor of k overhead
3. fully-secure HIBE w/o random oracle
   - Less efficient
4. Digital signatures w/o random oracle
5. …

More information

- Cash, Hofheinz, Kiltz: *How to Delegate a Lattice Basis*
  - Eprint 2009/351

Independent work

- Peikert: *Bonsai Trees (or, Arboriculture in Lattice-Based Cryptography)*
  - Eprint 2009/359, similar results, more efficient signatures

- Agrawal, Boyen: *Identity-based encryption from lattices in the standard model*
  - (sID) standard model IBE, no basis delegation/HIBE