Dual-Form Signature Schemes

Michael Gerbush, Allison Lewko, Brent Waters
University of Texas at Austin

CL Signatures [CL04]

- Anonymous credentials[CL04, BCL04, BCS05], Group signatures[CL04, ACHM05], Ecash[CHL05], Uncloneable functions[CHKLM06], Batch Verification[CHP07], RFID encryption[ACM05]
- LRSW assumption
  - Interactive
  - Similar to scheme

Dual Form Signatures

- Algorithms: Sign_A, Sign_B
- Forgery Classes: Type_I, Type_{II}

Security Properties ⇒ EU-CMA

1. A-I Matching: $\text{Sign}_A \rightarrow \text{Type}_{II} = \text{negl}$
2. B-II Matching: $\text{Sign}_B \rightarrow \text{Type}_I = \text{negl}$
3. Invariance: $\text{Sign}_A \rightarrow \text{Type}_I = \text{Sign}_B \rightarrow \text{Type}_I$

Our Results

- CL from static assumptions
- BB IBE-derived signatures[BB04]
- KV fits dual form[KV09]