Lecture 13

Tuesday, 10 January 2023 08:23

Countermeasures for bad randomness in signatures

- use secure PRNG
- use deterministic component in random number generator (include seed in secret key)
- use other signature scheme