Weekly Lab Meeting

On the Multi-User Security of Short Schnorr Signatures with Preprocessing

Jeremiah Blocki and Seunghoon Lee

December 8, 2023

PURDUE UNIVERSITY

*Joint presentation of EUROCRYPT 2022 and ongoing work

01

Short Schnorr Signatures

02

Bridge-Finding Game

Multi-User Security of short Schnorr Signatures

03

Security against **Preprocessing Attacks**

From Bit-Fixing Model to Auxiliary-Input Model in Multiple Idealized Models