

short Short Signatures

01

02

03



Bridge-Finding Game

Security against Reproting Attacks



Multi-User Security of Short Schnorr Signatures

02

03

Bridge-Finding Game

Security against Reproting Attacks

From Bit-Fixing Model to Auxiliary-Input Model in Multiplicative Ideal Models



Multi-User Security of Short Schnorr Signatures