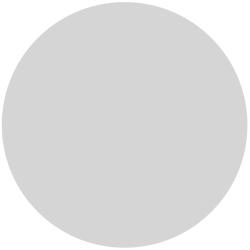
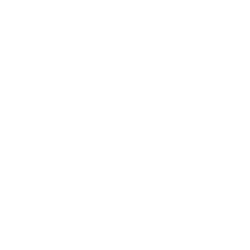
Short Schnorr Signatures











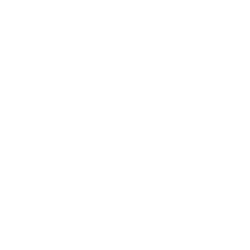
Bridge-Finding Game

Security against Preprocessing Attacks

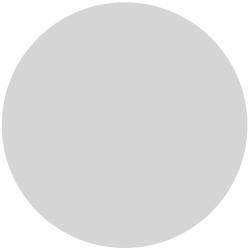
From Bit-Fixing Model to Auxiliary-Input Model in Multiple Idealized Models

Multi-User Security of short Schnorr Signatures

Short Schnorr Signatures









Bridge-Finding Game

Multi-User Security of short Schnorr Signatures