

PART 4 2D Future

SQLsign2D

Don't do "slow" translation of ideal into blocks of 1D-isogenies (SQLsign, AprèsSQL)

Don't do "fast" translation of ideal into slow 4D/8D isogenies (SQLsignHD)

Do use the previous section to translate ideal into 2D isogenies

✓
faster
primes!

✓
FASTER
signing!

✓
THE BEST
security!

✓
FAST
verification!

1

SQLsign2D-West

&

2

SQLsign2D-East

&

3

SQLPrime

PART 4 2D Future

SQLsign2D

Don't do "slow" translation of ideal into blocks of 1D-isogenies (SQLsign, AprèsSQL)

Don't do "fast" translation of ideal into slow 4D/8D isogenies (SQLsignHD)

Do use the previous section to translate ideal into 2D isogenies

✓
**faster
primes!**

✓
**FASTER
signing!**

✓
**THE BEST
security!**

✓
**FAST
verification!**

1

SQLsign2D-West

&

2

SQLsign2D-East

&

3

SQLPrime

concrete numbers

NIST SQLsign Level I

- **Public Key:** 64 bytes
- **Signature :** 177 bytes
- **Signing:** 2,400 MCycles
- **Verification:** 39 MCycles

SQLsign2D-West Level I

- **Public Key:** 66 bytes
- **Signature :** 148 bytes
- **Signing:** 160 MCycles
- **Verification:** 9 MCycles