PART 4

2D Future

- ✓ **faster primes!**
- ✓ **FASTER signing!**
- ✓ **THE BEST security!**
- ✓ **FAST verification!**

SQIsign2D

Don't do "slow" translation of ideal into blocks of 1D-isogenies (SQIsign, AprèsSQI)
Don't do "fast" translation of ideal into slow 4D/8D isogenies (SQIsignHD)

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

1. SQIsign2D-West **&**
2. SQIsign2D-East **&**
3. SQIPrime

concrete numbers

NIST SQIsign Level I		SQIsign2D-West Level I	
• **Public Key:**	64 bytes	• **Public Key:**	66 bytes
• **Signature :**	177 bytes	• **Signature :**	148 bytes
• **Signing:**	2,400 MCycles	• **Signing:**	160 MCycles
• **Verification:**	39 MCycles	• **Verification:**	9 MCycles

PART 4

2D Future