Cryptographic Group Actions and Digital Signatures

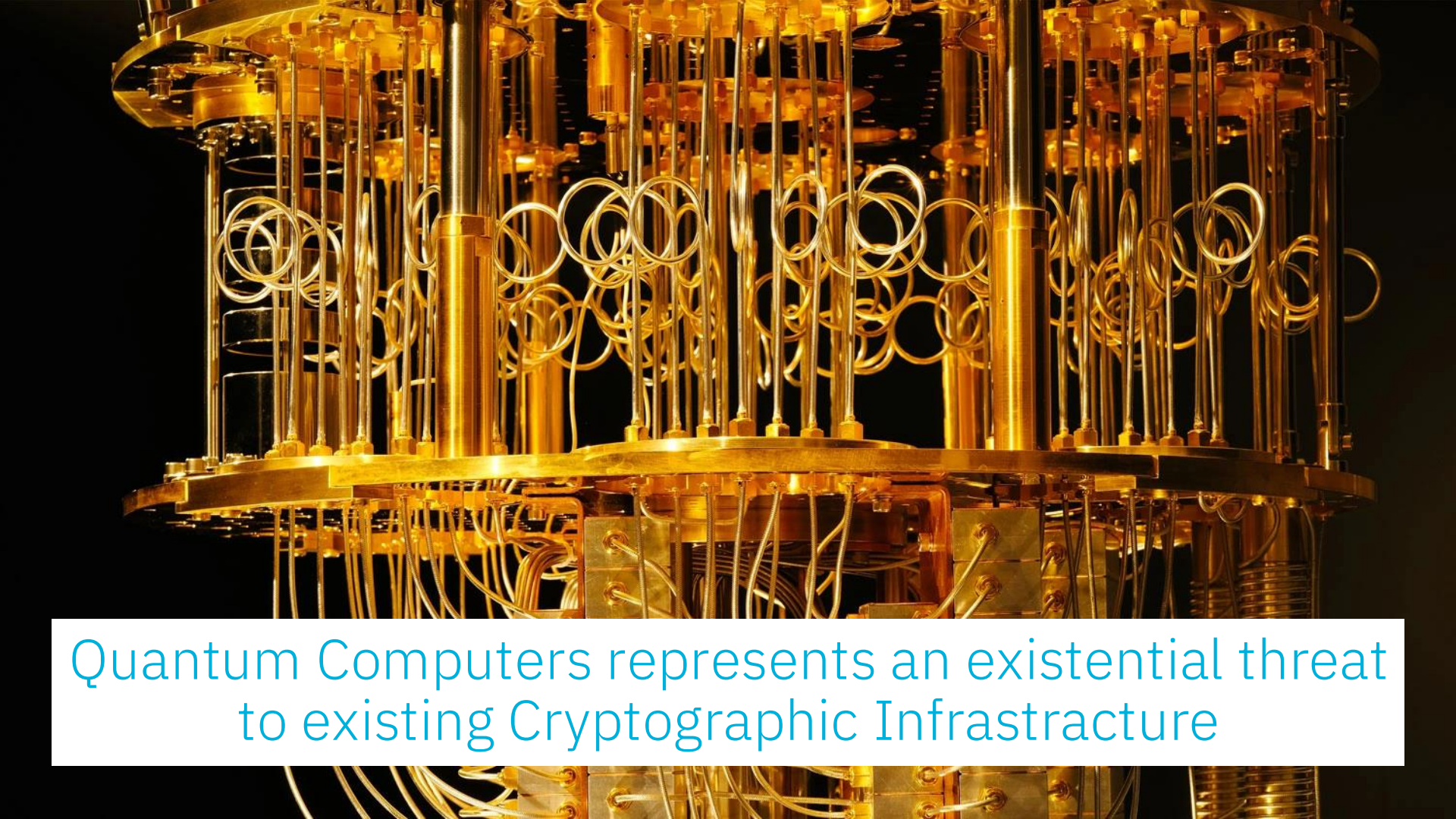
MsC Thesis supervised by Michele Battagliola, Alessio Meneghetti, Edoardo Persichetti
defended at Università di Trento

Giacomo Borin
IBM Research Zurich & University of Zurich

Opinions are my own!

Universität Zürich[UZH]

IBM



Quantum Computers represents an existential threat to existing Cryptographic Infrastracture

Post Quantum Cryptography

200* > people start researching

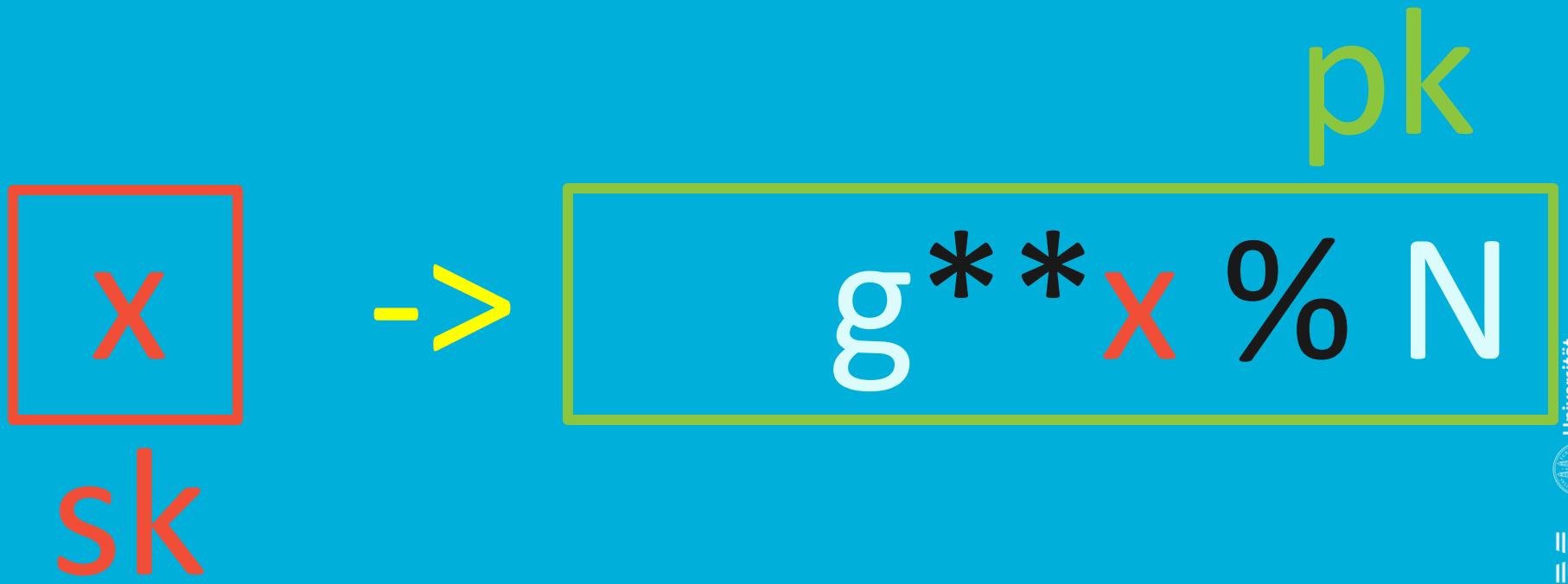
2016 > NIST opens PQC call

2024 > FIPS 203 – 204 – 205

202* > Ongoing Signature
‘on ramp’ call & more

There is still a lot of work

Discrete Logarithm Problem



Discrete Logarithm Problem

KEM, DS,

NIKE, Commitments, OT, RS,

OPRF, MPC, IBE…

Discrete Logarithm Problem

$$(g^{**}x \% N)*(g^{**}y \% N)$$

$$=$$

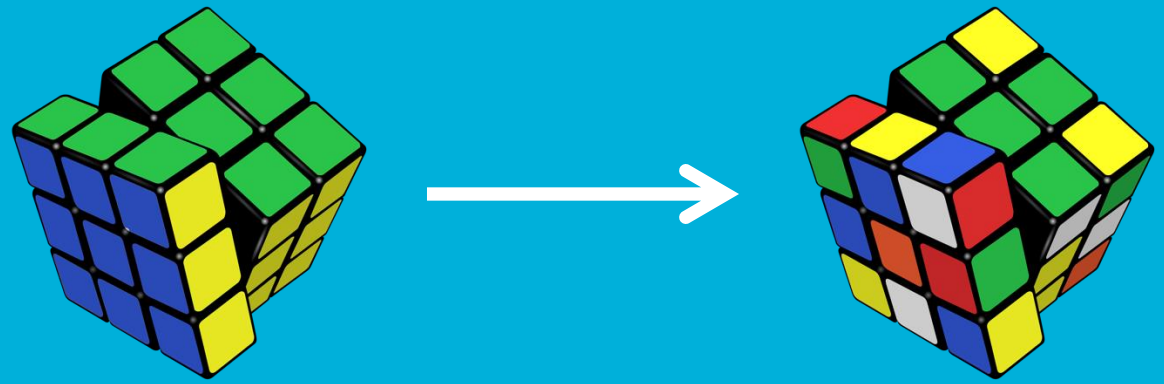
$$g^{**}(x+y) \% N$$

Cryptographic Group Actions

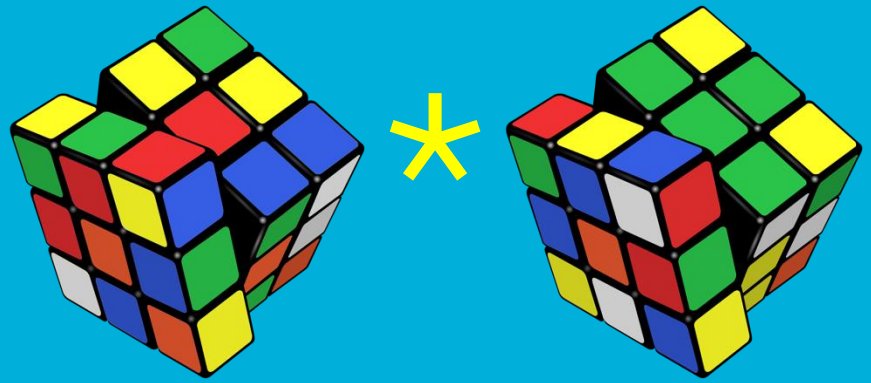
FBBDL

RRDD

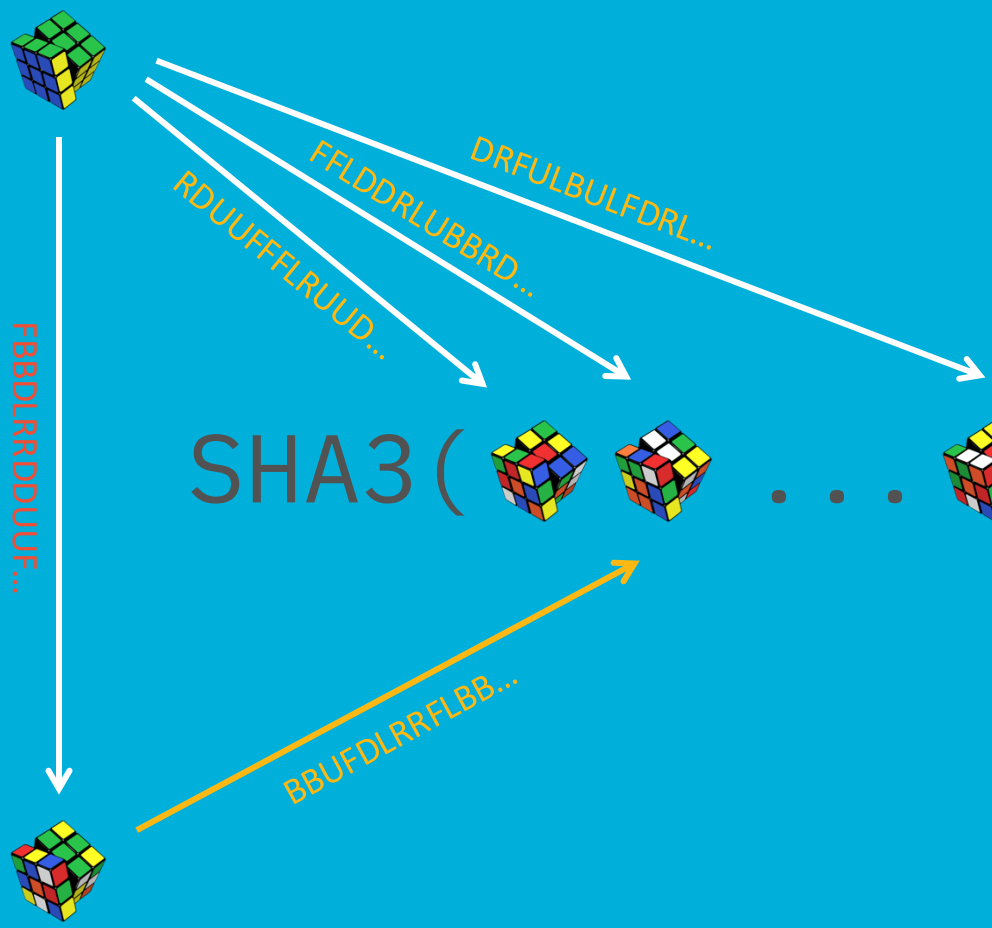
UUF…



Cryptographic Group Action



Group Actions to Digital Signatures

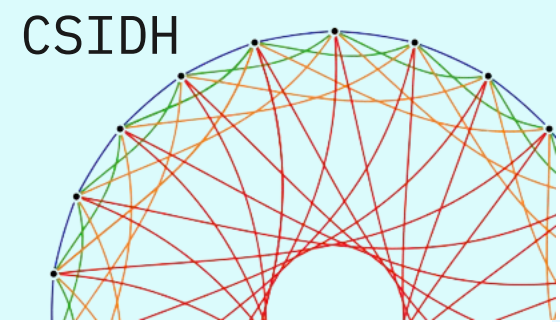


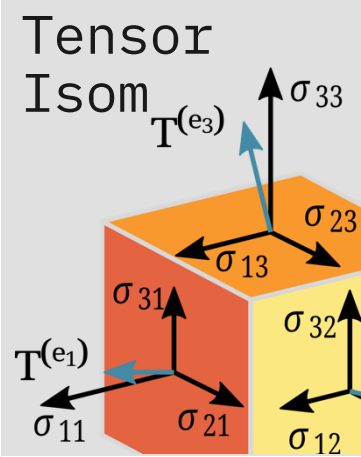
Stolbunov, Anton. "Cryptographic schemes based on isogenies." (2012).

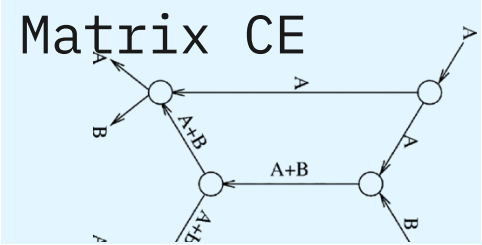
Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Re- port 2006/291, 2006

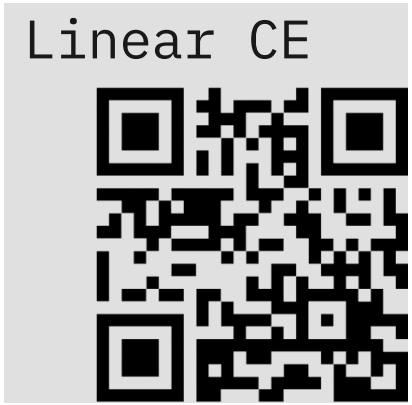
Cryptographic Group Actions

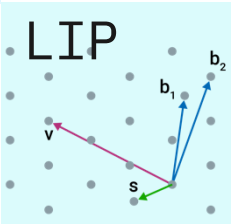
- Digital Signatures
- Ring S.
- Threshold S.
- Blind S.-*ish*
- Bit Commitments
- KEM
- NIKE
- OT





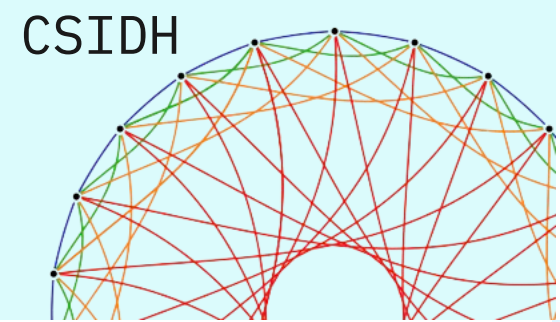


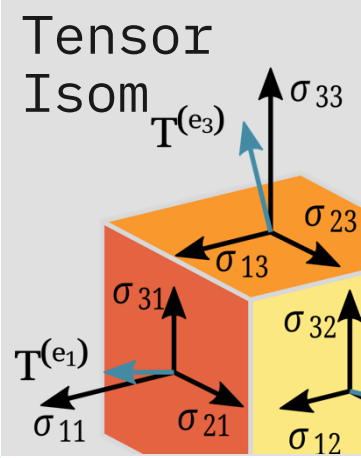


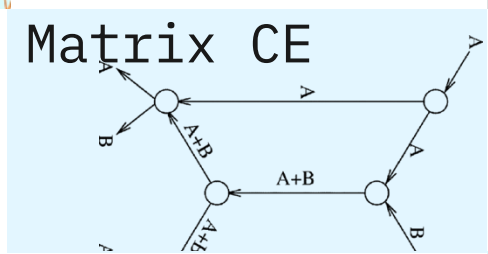


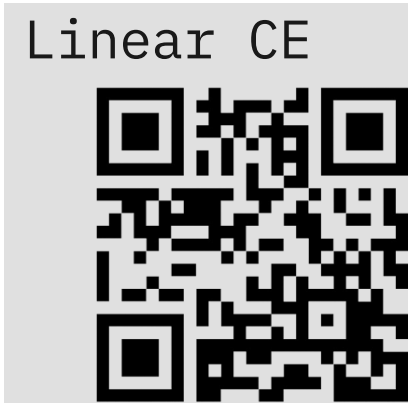
Cryptographic Group Actions

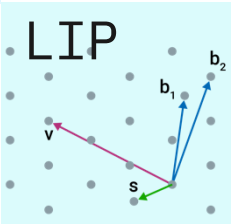
- Crtyptanalysis
- Improving efficiency (smaller and faster)
- New Constructions
- New Group Actions (?)











gbor.in/mscthesis