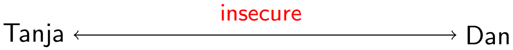
Accelerating Pre- and Post-Quantum Cryptography

Tung Chou

Cryptography

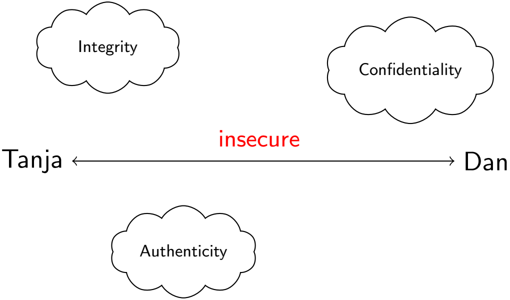


Tanja

insecure

Dan

Cryptography



Integrity

Confidentiality

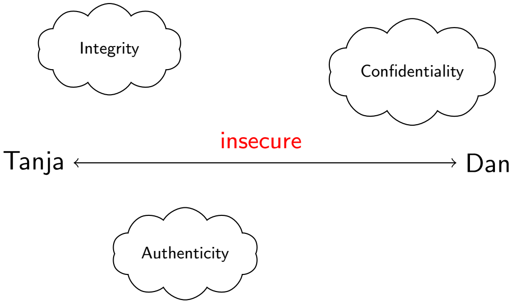
insecure

Tanja

Dan

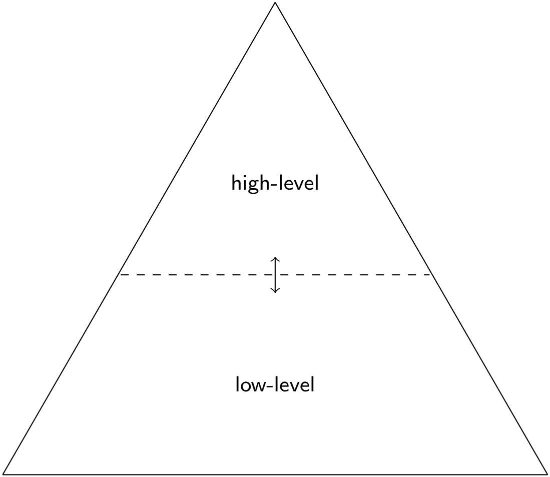
Authenticity

Cryptography

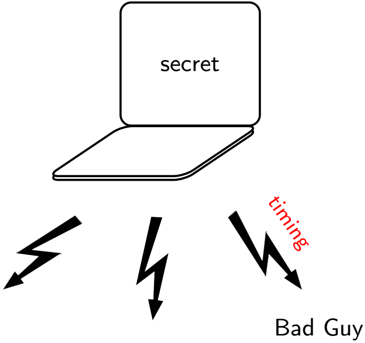


Challenge: Efficiency vs. Security

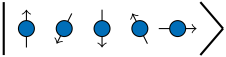
Optimization for efficiency



Secure computation



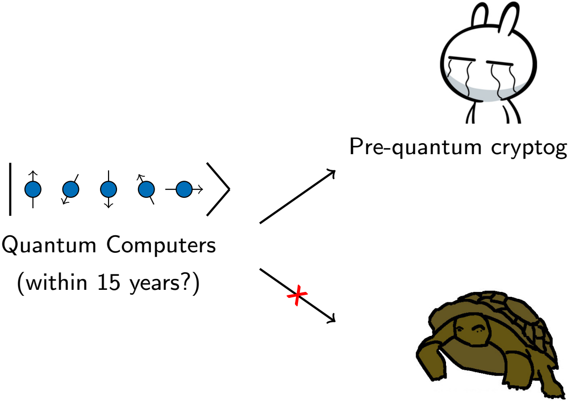
Post-quantum cryptography



Quantum Computers

(within 15 years?)

Post-quantum cryptography



Pre-quantum cryptography

Quantum Computers

(within 15 years?)

Post-quantum cryptography

Overview

	Pre-quantum	Post-quantum
Constructive	Sandy2x OT	McBits QcBits Auth256
Destructive	BADA55	XL