01

Md Shadnan Azwad Khan, Chin-Te LIAO, Christina Repou, Anne Marin, Flavia Voicu, Christian Meng, Sacha Ulysse Jeoffret

Secure Quantum Digital Payments

Motivation

WHY QUANTUM ENCRYPTION?

- Provides a more secure communication channel
- Realtime eavesdropping detection
- Various unique cryptographic methods
- Long time data security

Enhancing payment security through SquidASM-based quantum-digital transaction simulation

QUANTUM TOKEN

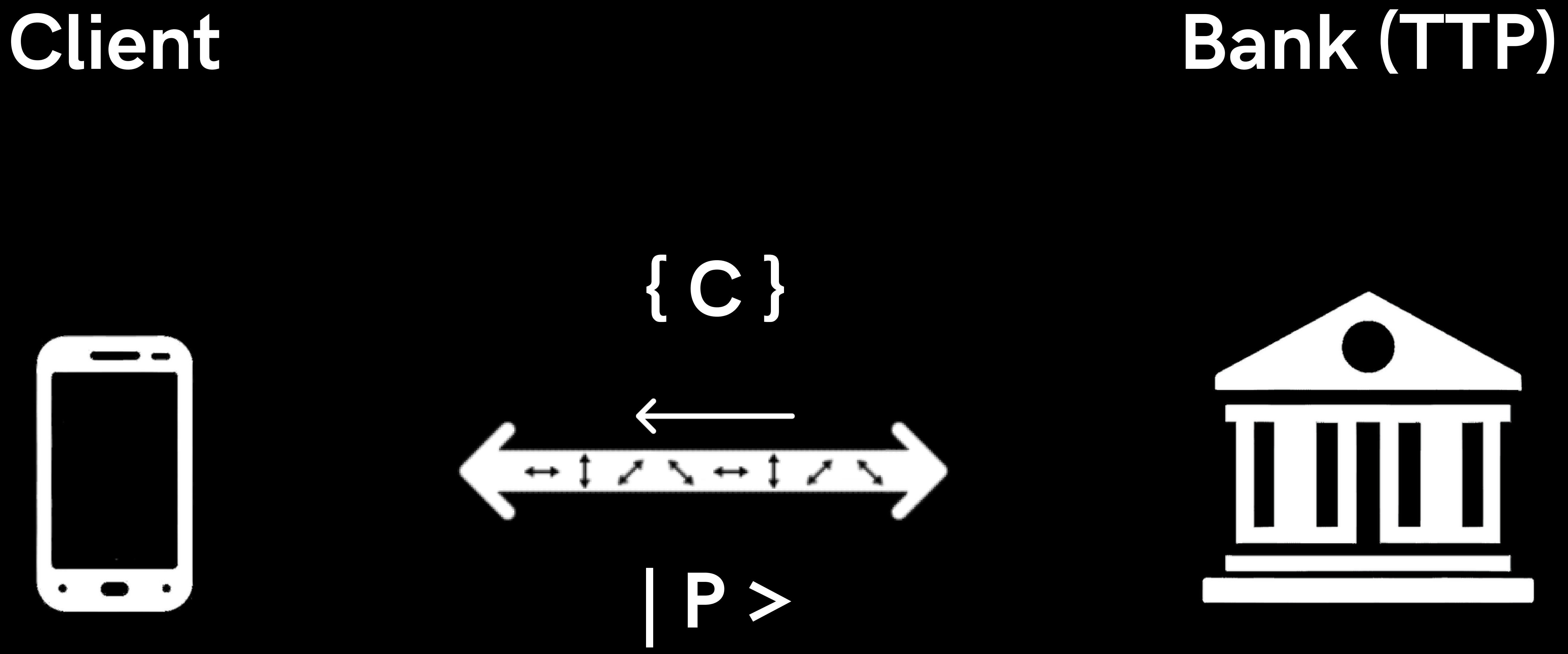
Quantum state with encoded data

MEASUREMENT CLIENT

Client side classical encryption

REQUEST + VERIFY TRANSACTION

Authentication by Trusted Third Party



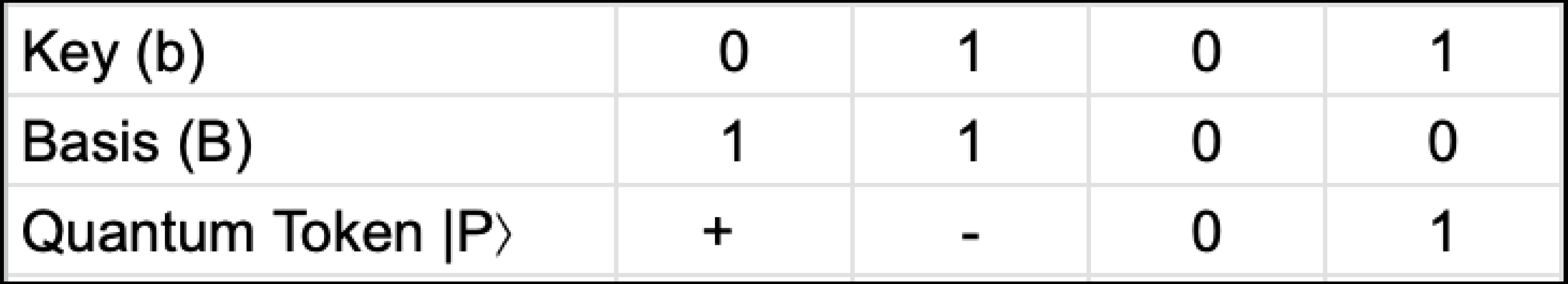
Client

Bank (TTP)

{ C }

| P >

Quantum token generation

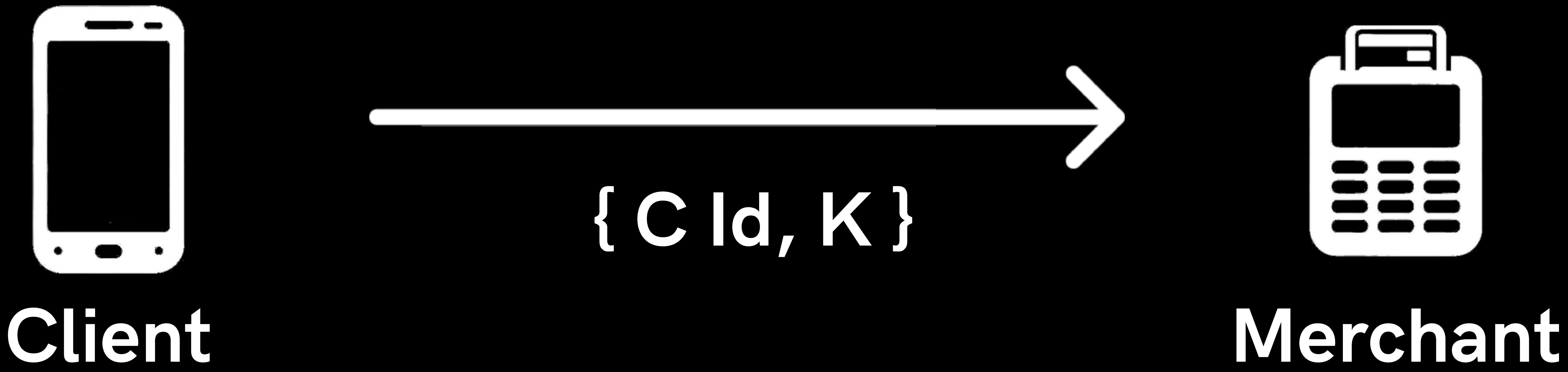


Key (b)	0	1	0	1
Basis (B)	1	1	0	0
Quantum Token |P⟩	+	-	0	1

|P⟩ = Payment Token (Quantum state)

b = random bit string

B = random conjugate basis-string (1=+/-, 0=0/1)

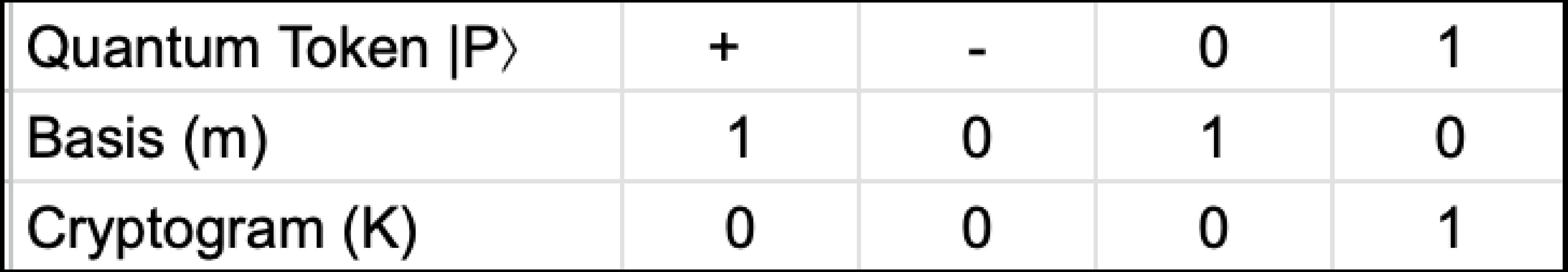


Client

{ C Id, K }

Merchant

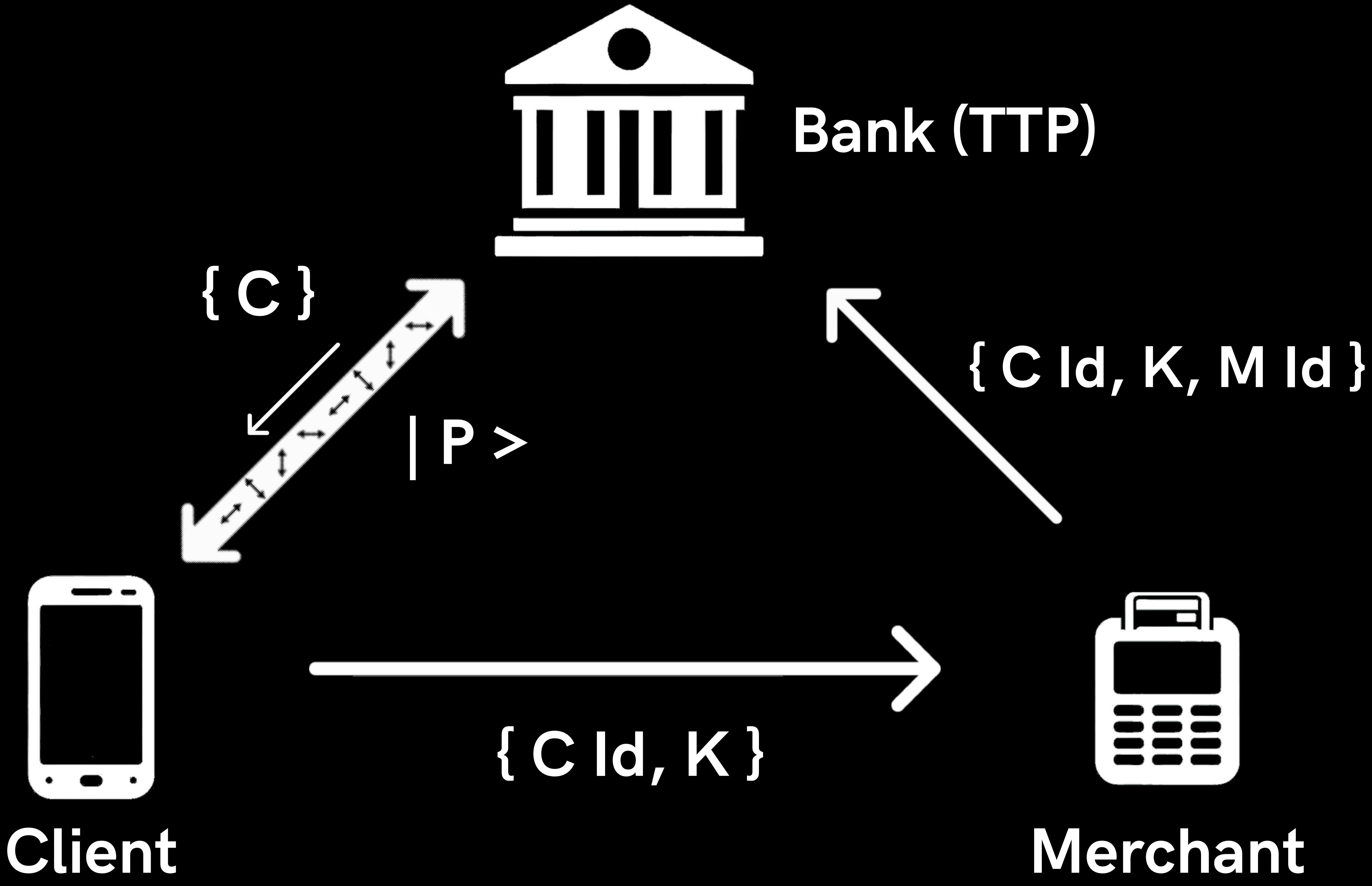
Cryptogram formation



Quantum Token |P⟩	+	-	0	1
Basis (m)	1	0	1	0
Cryptogram (K)	0	0	0	1

$$m_i = MAC(C, M_i)$$

$$\kappa_i \xleftarrow{m_i} |P\rangle$$


Bank (TTP)
{ C }
| P >
{ C Id, K, M Id }
{ C Id, K }
Client
Merchant

Transaction Authentication

Accept
Reject
BANK (TTP)