Quantum Timed-Release & Unknown Recipient Encryption

Dominique Unruh
University of Tartu
Meeting the Mafia

meets with mafia

Compromising evidence

“a friend”
Meeting the Mafia

meets with mafia

Compromising evidence

“a friend”

Interesting....
Using “time capsules”

meets with mafia

2 days

“a friend”
Using “time capsules”

meets with mafia

“a friend”

Next day:

Still unopened…

still alive

“a friend”

Dominique Unruh
Digital: Using “timed-release enc”...

meets with mafia

Enc(msg)
(2 days)

“a friend”

Next day: ???

Enc(msg)
(1 day)

still alive

Enc(msg)

“a friend”
Quantum timed-release enc

Classical timed-release enc

Quantum encoded msg

Revocation:

|msg⟩_B
Unknown Recipient Encryption

$\text{Enc}(\text{msg})$

Only one can decrypt (before timeout)
I thank for your attention