UNIVERSITY OF TARTU
1632

Revocable Timed-Release Encryption

Dominique Unruh

University of Tartu

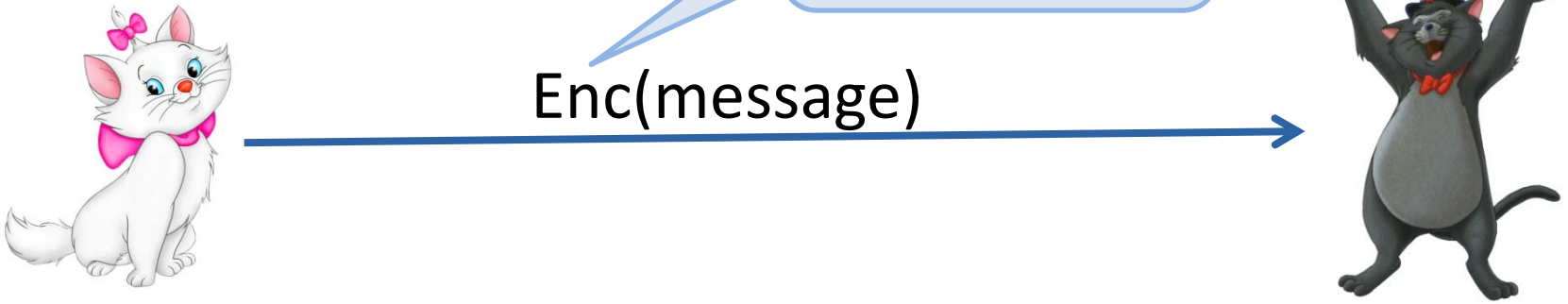
Motivation

- Want to send a message
- Opens at a particular date
- No earlier opening!

Time Vaults

Physical solution:

Digital solution:



Required properties

- Can be decrypted in time t
- Cannot be opened in time (much) smaller t

Challenges:

- Very precise hardness assumptions
- Knowledge of adversary hardware
- Non-parallelisable
- Quantum secure

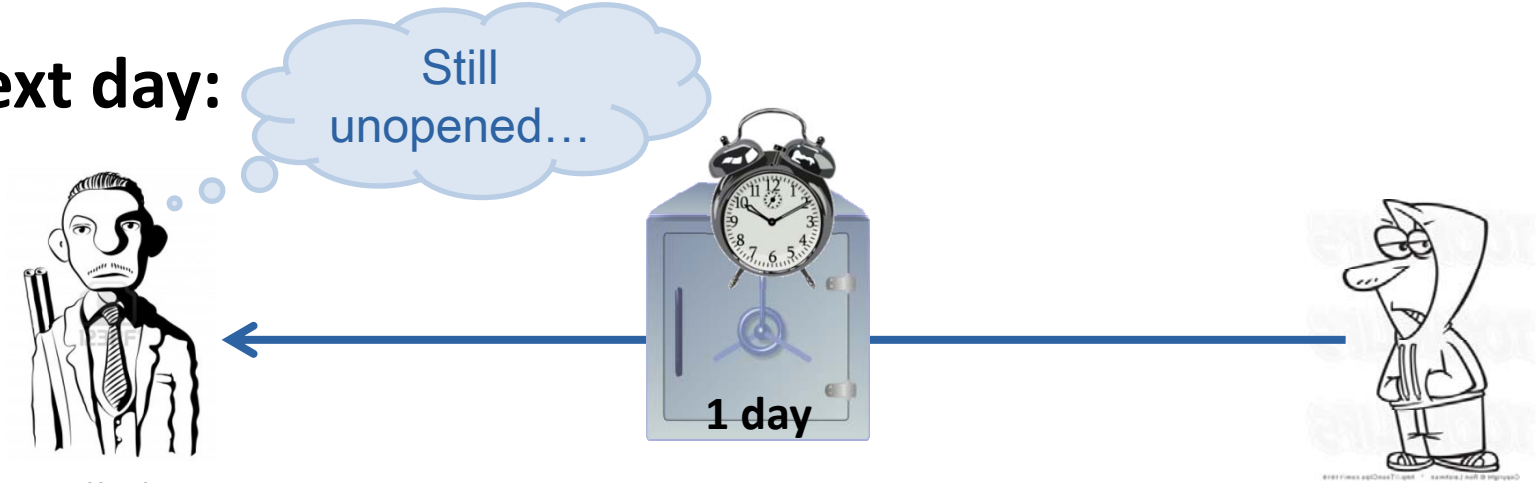
For this talk: Assume that's solved.

Another application

meets with mafia

"a friend"

Next day:



still alive

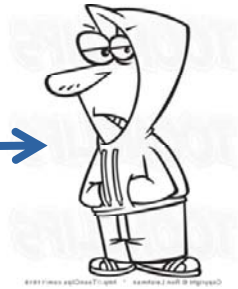
"a friend"

Using digital time vaults…

meets with mafia

Enc(msg)

(2 days)



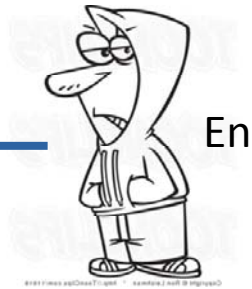
“a friend”

Next day:

still alive

Enc(msg)

(1 day)



Enc(msg)

“a friend”

Revocable time vaults

- Physical time vaults have “revocability”
  - Before timeout, possible to “give back”
  - Recipient can keep time vault, but will be detected
- Digital time vaults:
  - Recipient can always keep copy
  - And continue decrypting the copy

Quantum No Cloning?

Example applications

Deposits: Put digital money in TRE. Hand it back upon return.

- Useful for fair MPC also?

Data retention with verifiable deletion: Keep user data for legally mandated time, provably delete afterwards.

Unknown recipient encryption: Send a message to unknown recipient. Recipient knows no-one else got it.

- More unexpected applications of revocable TRE?

Quantum Time Vaults

$\mathbf{Enc}(B)$ $|msg\rangle_B$

- Message *msg*
- Random basis *B*

Classical time vault

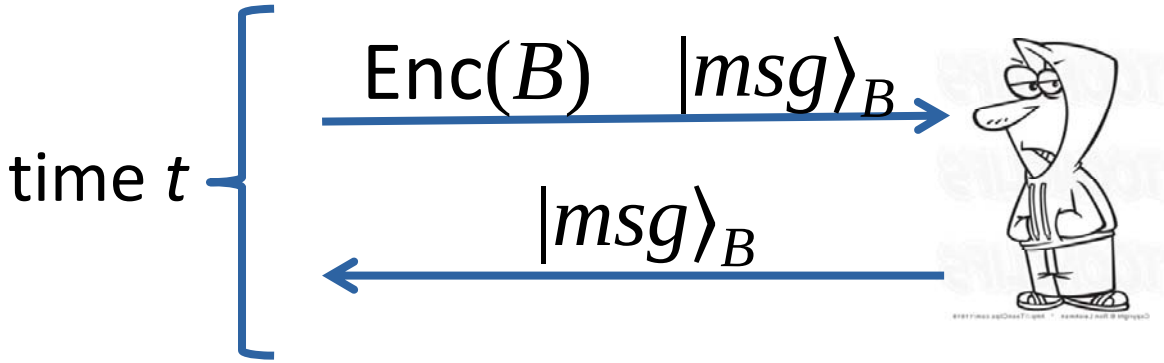
Quantum encoded msg

Revocation:

$|msg\rangle_B$

- Check if state unmodified

Naïve Proof



Recipient does not know B before time t

⇒ Can't copy msg before time t (no cloning)

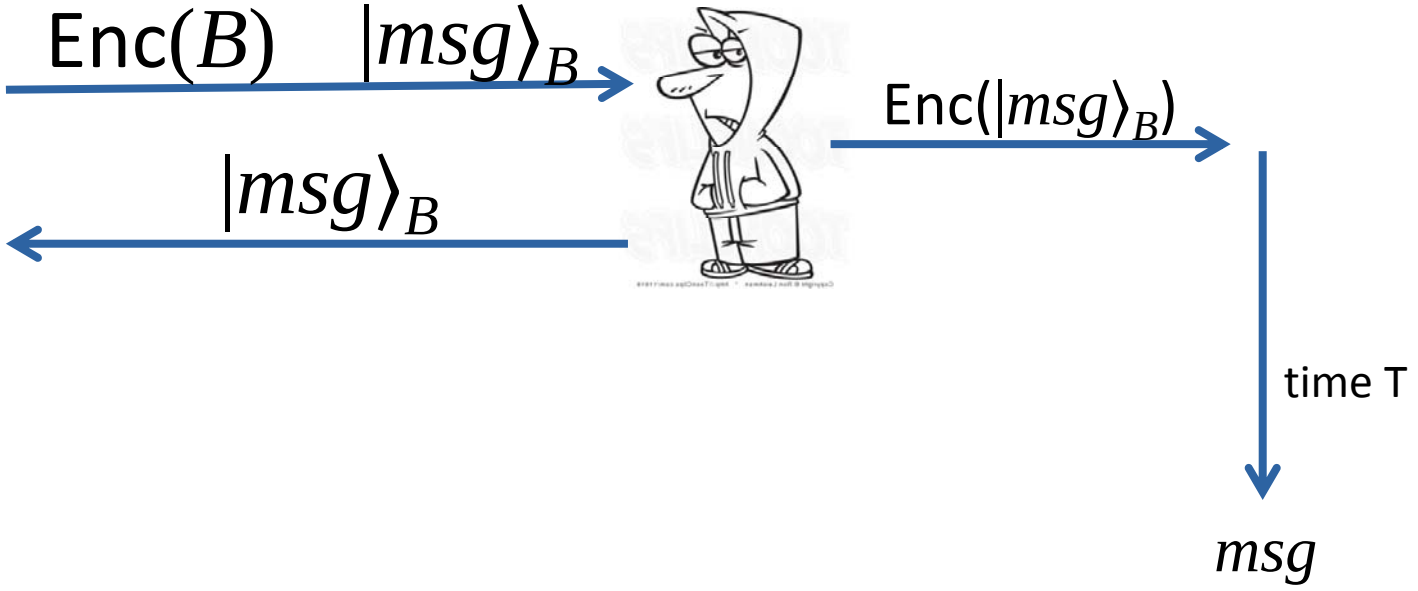
⇒ Won't have msg after revocation

⇒ Secure

"Theorem": Without knowing B, impossible to transform $|msg\rangle_B$ into $|msg\rangle_B, |msg\rangle_B$

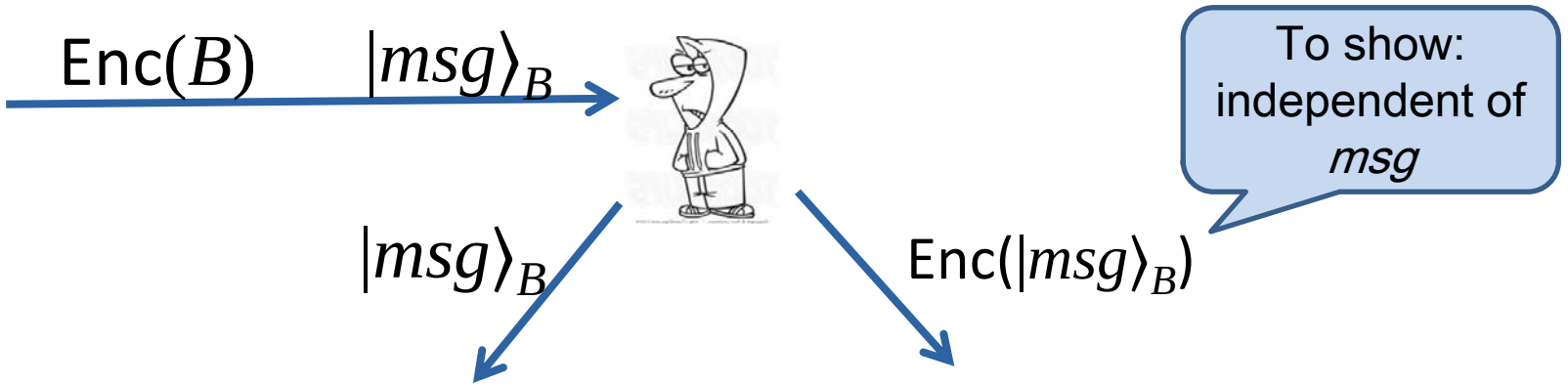
Naïve Proof – criticism

Perhaps “encrypted cloning” is possible?



Proof idea

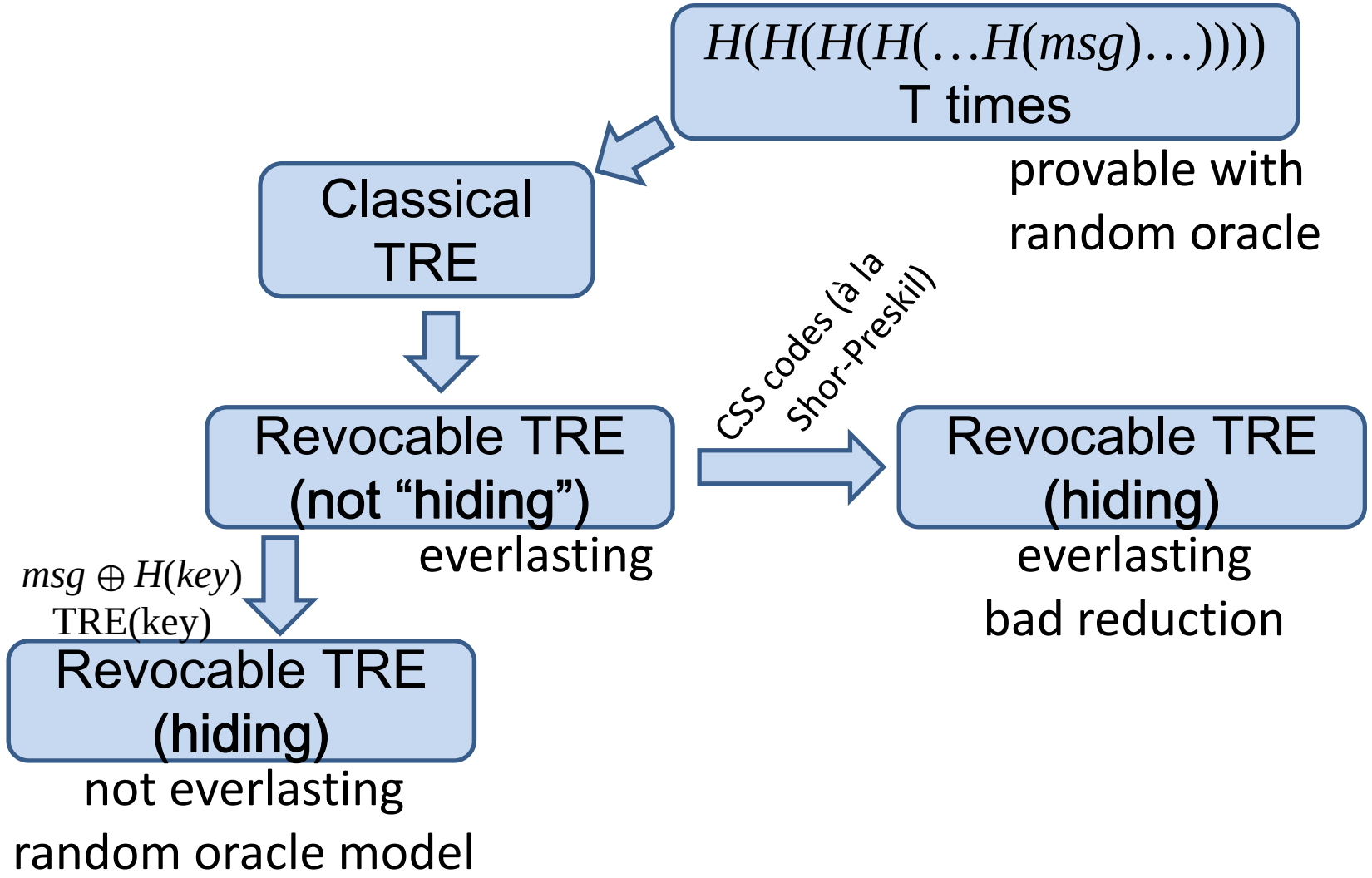
- Need to show: no "encrypted cloning"



- "Independence of msg": not T-time testable
- "$|msg\rangle_B$" maximally entangled with environment: T-time testable!

$\Rightarrow$ Unentangled with Enc($|msg\rangle_B$)

The big picture



Conclusions

- Revocable time vaults
  - Gap between quantum and classical crypto
- Useful building block in crypto protocols?
  - Unknown recipient encryption
- Technique: Giving back data → other applications?

Open questions

- Classical TRE schemes.
  - $H(H(H(H(\ldots H(msg)\ldots))))$: encryption takes long
  - Rivest-Shamir-Wagner: not quantum secure

- Efficient reduction for revocable hiding TRE in standard model.

I thank for your attention

Logo soup

This research was supported by European Social Fund's Doctoral Studies and Internationalisation Programme DoRa

European Union
European Social Fund

Investing in your future

ARCHIMEDES

DoRa

European Union
Regional Development Fund

Investing in your future

EXCS
ESTONIAN COMPUTING