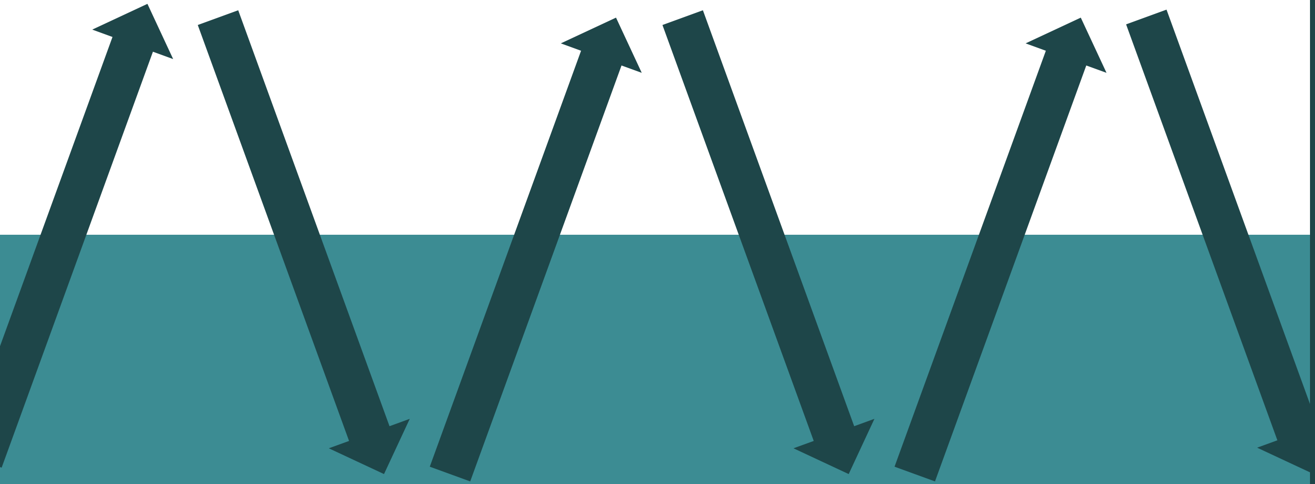
Bombs don’t explode, the forgers get rich:



an adaptive attack on Wiesner’s quantum $.

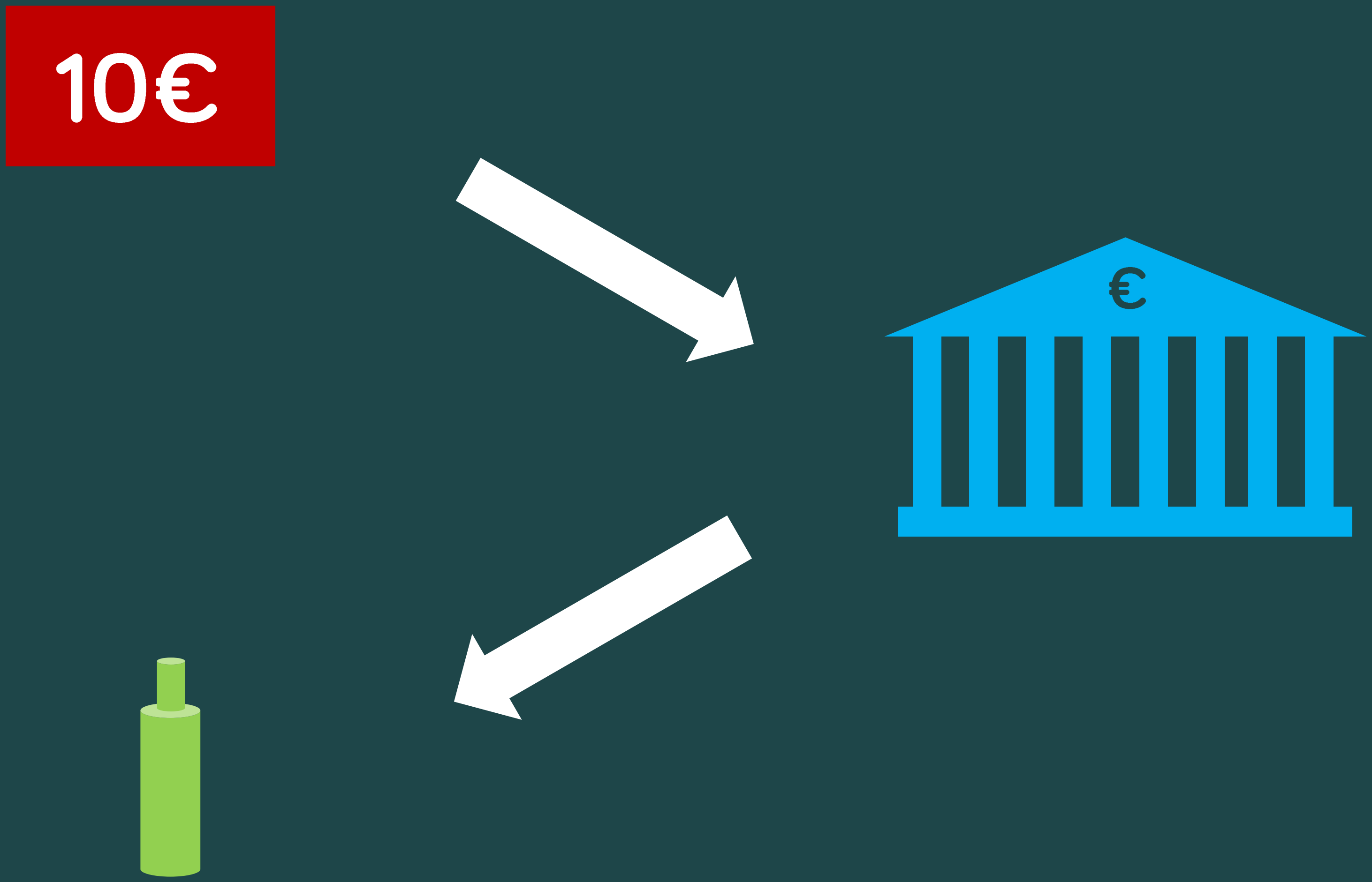
QCRYPT 2014

Or Sattath
Aharon Brodutch
Daniel Nagaj

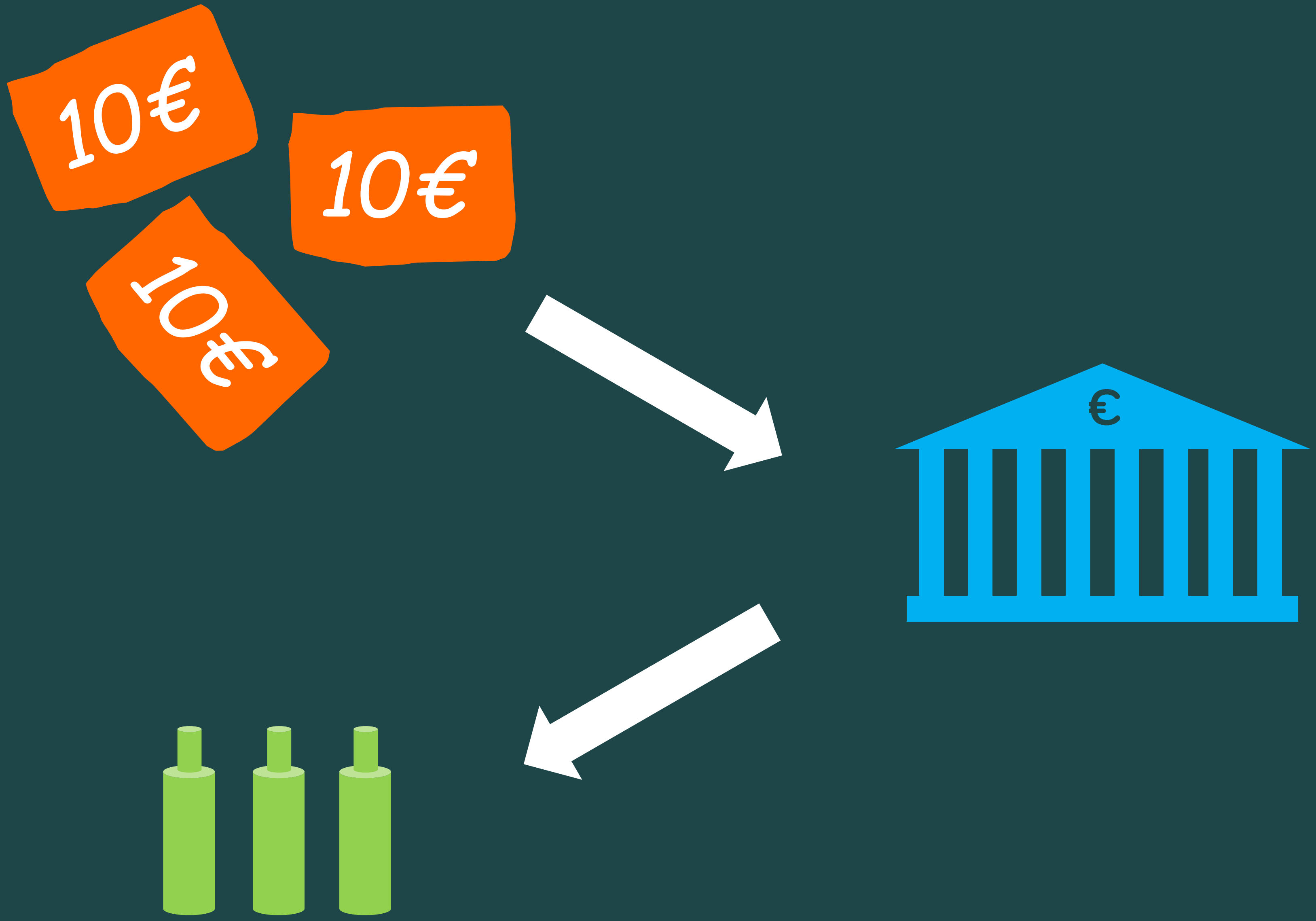
1404.1507

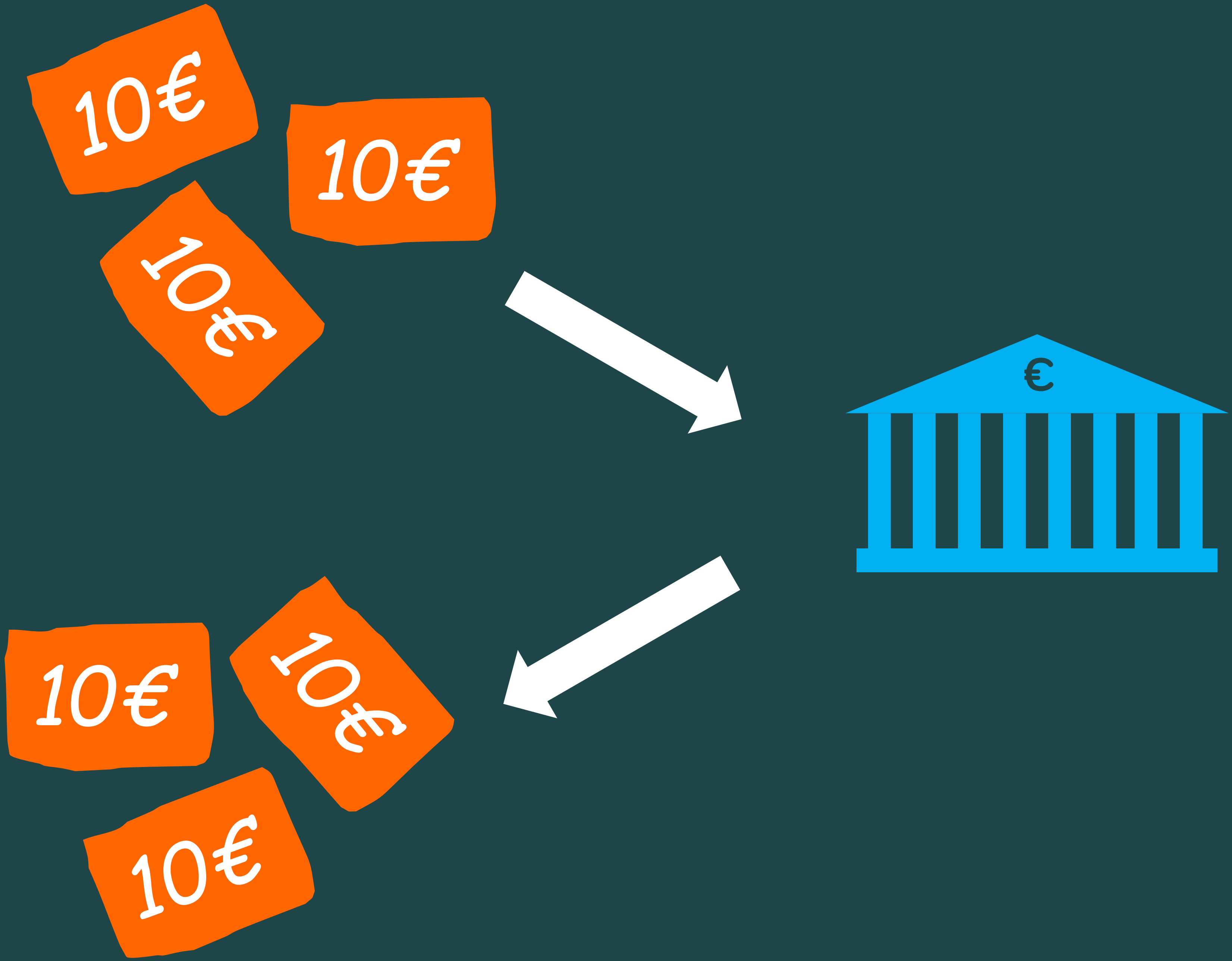
SAV

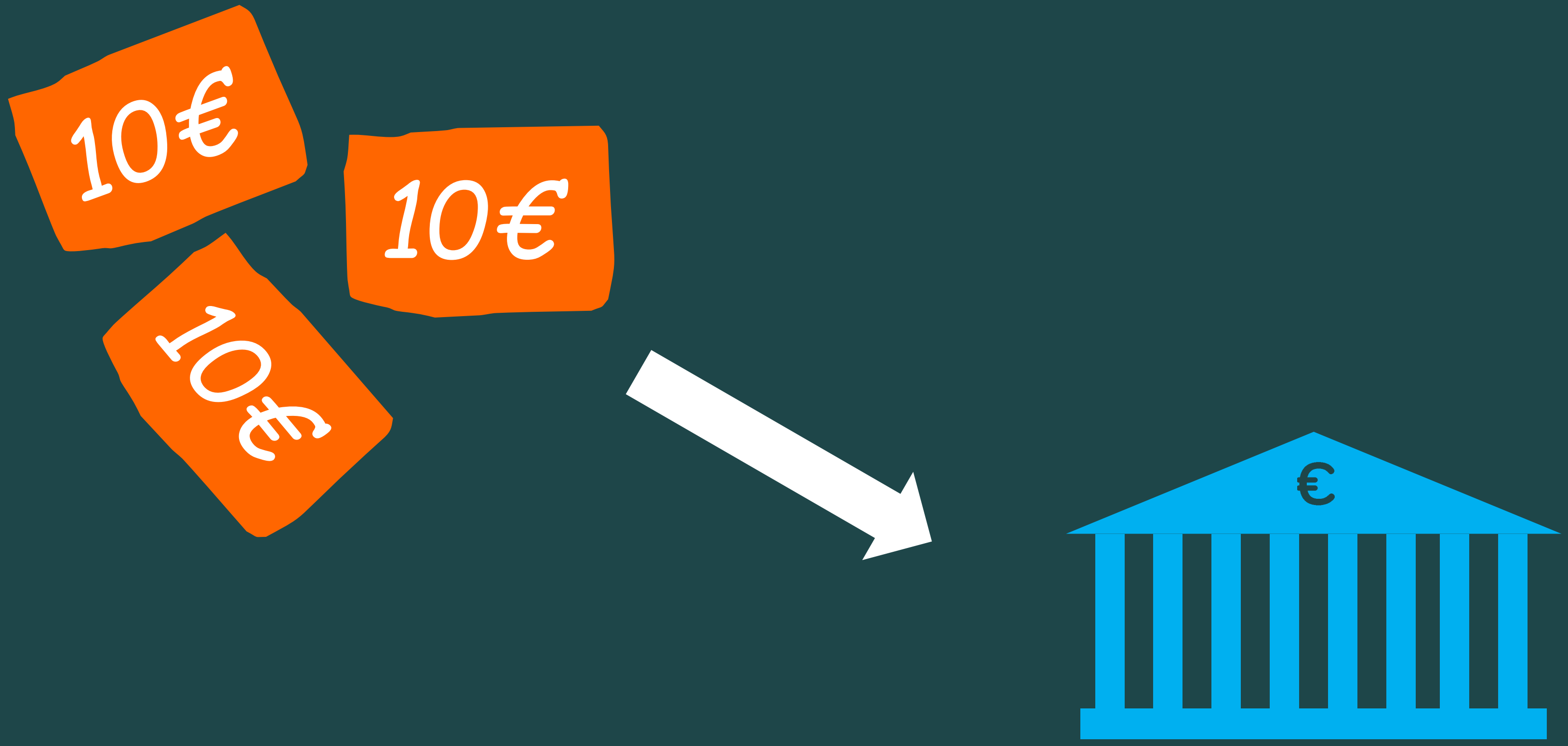
SIMONS INSTITUTE
for the Theory of Computing

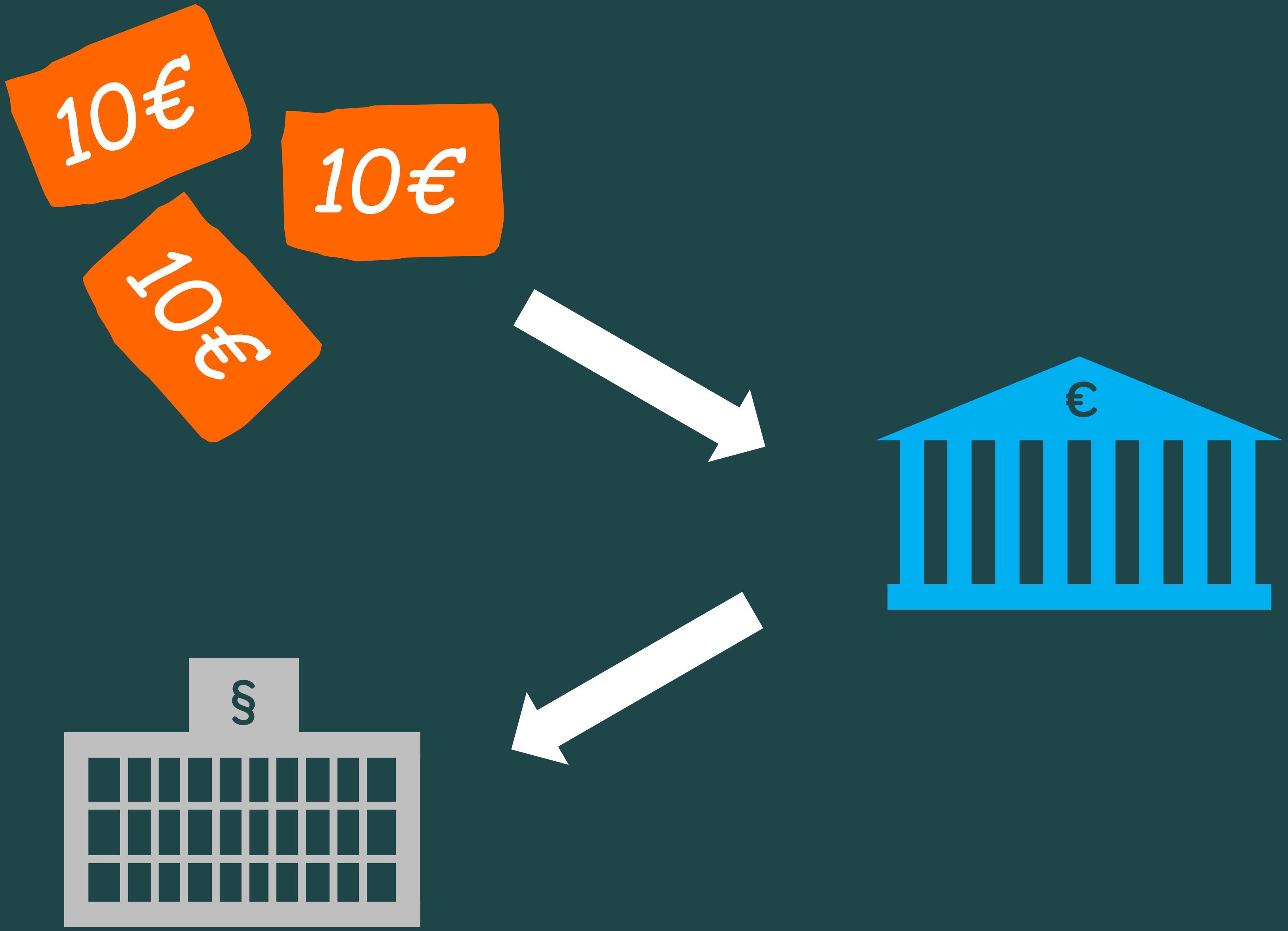


10€

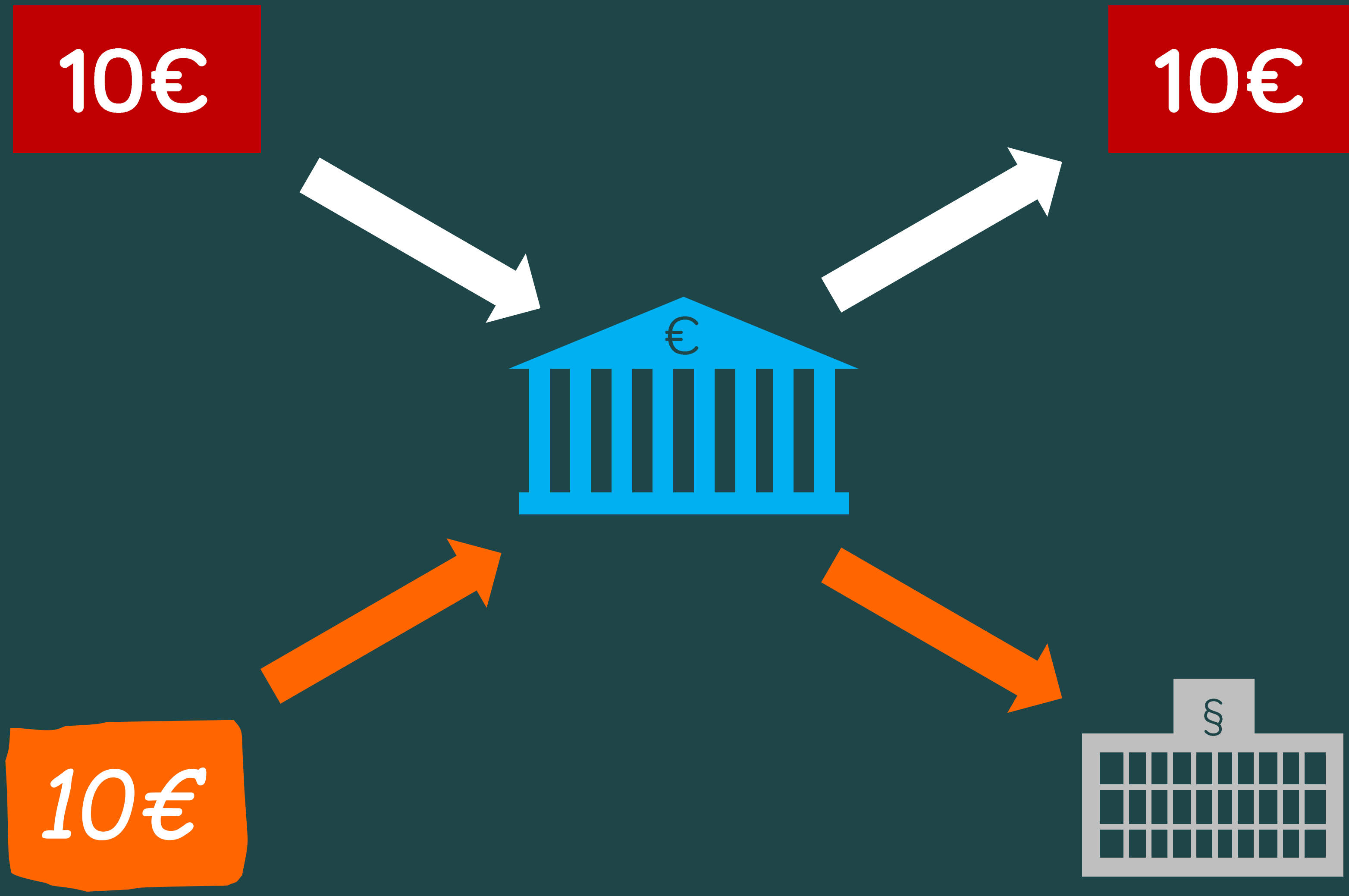

10€
10€
10€
€


10€
10€
10€
€
10€
10€
10€


10€
10€
10€
€


10€
10€
10€
€
§

strict testing



10€

10€

10€

1 expensive states

validity, (re)usability & strict testing

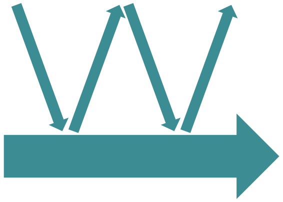
100€

2 money and bombs

quantum Zeno effect & successful forgery

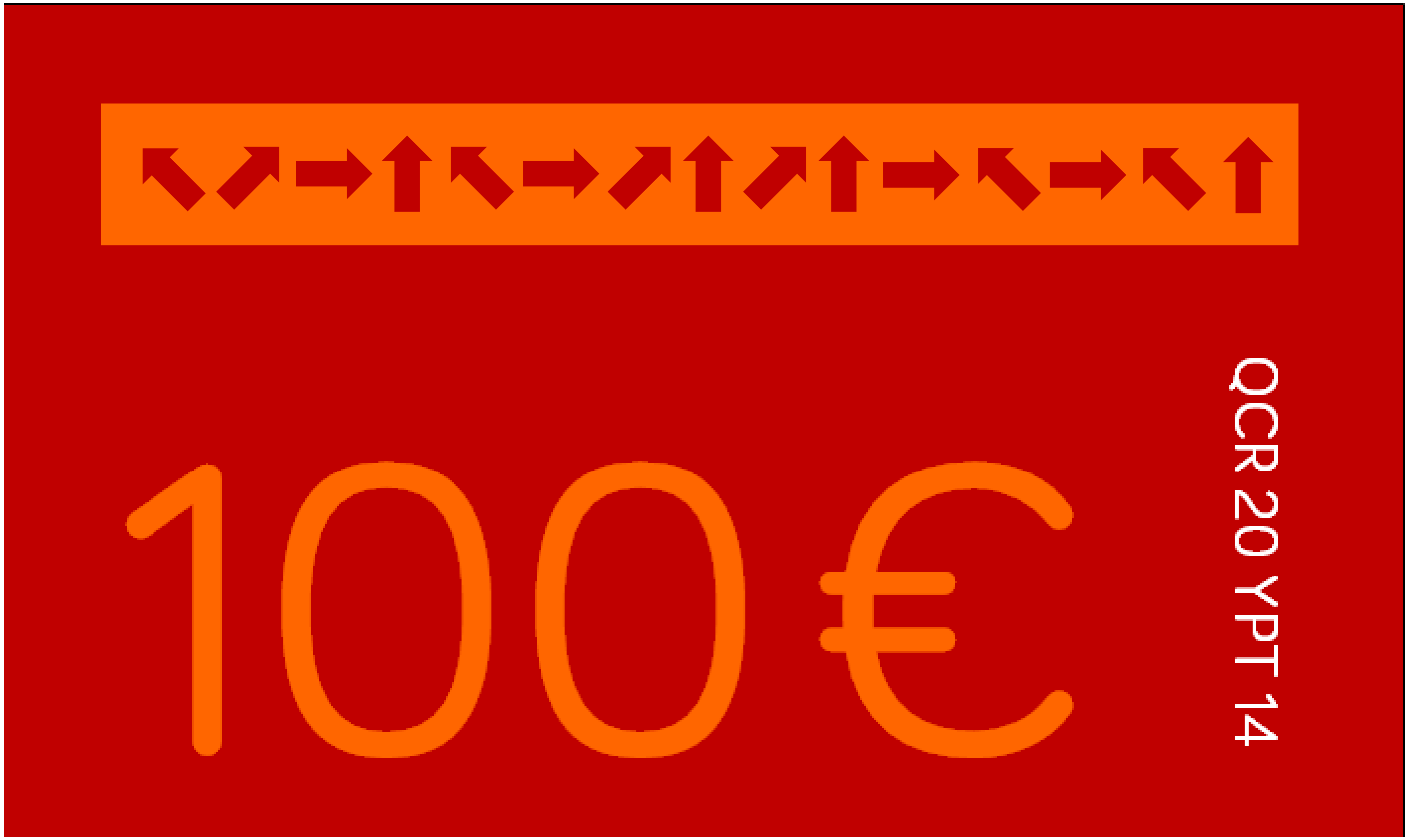
3 measuring weakly

strict testing & single-copy tomography



strict testing & Wiesner’s money

1 Wiesner's quantum money ['69, published '83]



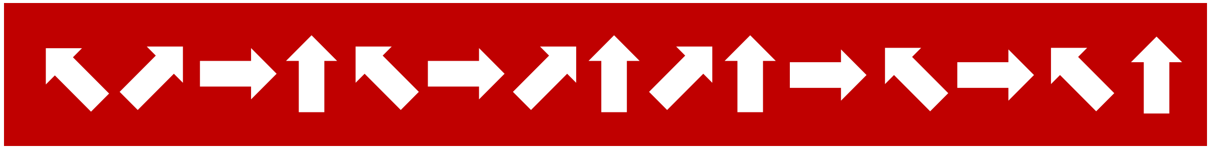
serial number s

secret state $|\psi_s\rangle = |c_1^s\rangle|c_2^s\rangle \cdots |c_n^s\rangle$

$$c_i^s \in \{0, 1, +, -\}$$

1 Is it secret? Is it safe?

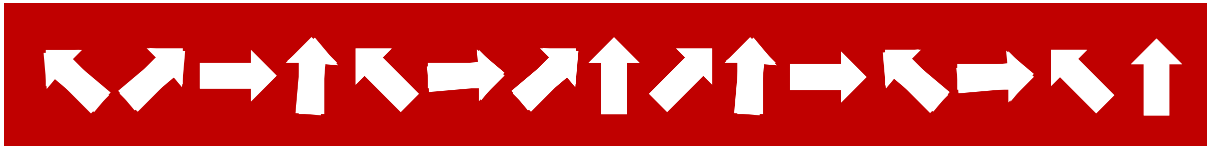
- verify-only memory, unforgeable tokens [BBBW ’83]



- guaranteed safe for a single use [Molina et al. ’12]

$\left(\frac{3}{4}\right)^n$

safest: 6 states $\left(\frac{2}{3}\right)^n$

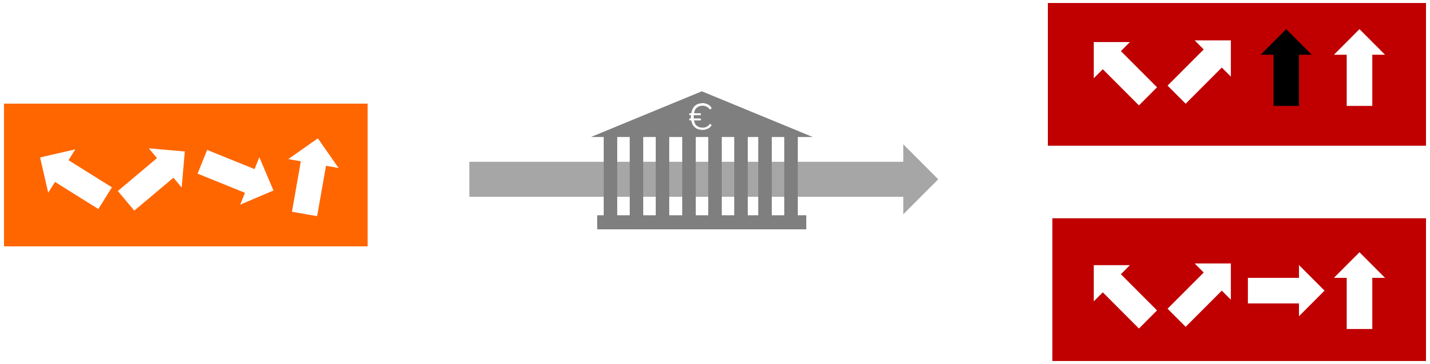


- OK with some noise [Pastawski et al. ’11]
  classical communication is enough [also Gavinsky ’11]

+ × + × × × + × + + × + + × +

1 Asking for “repairs” (and returns of bad states)

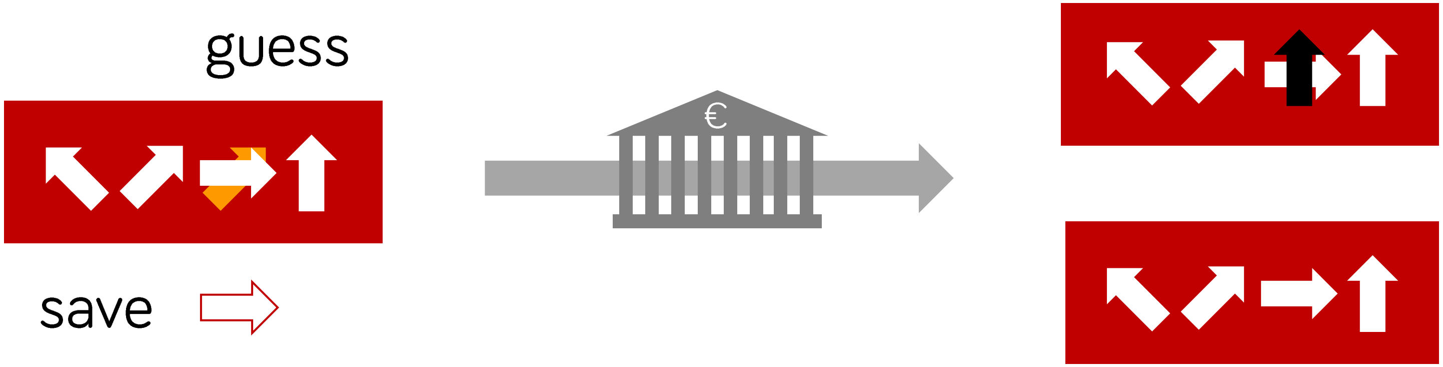
- validating “old” bills



bad $$$

OK

- Lutomirski’s attack



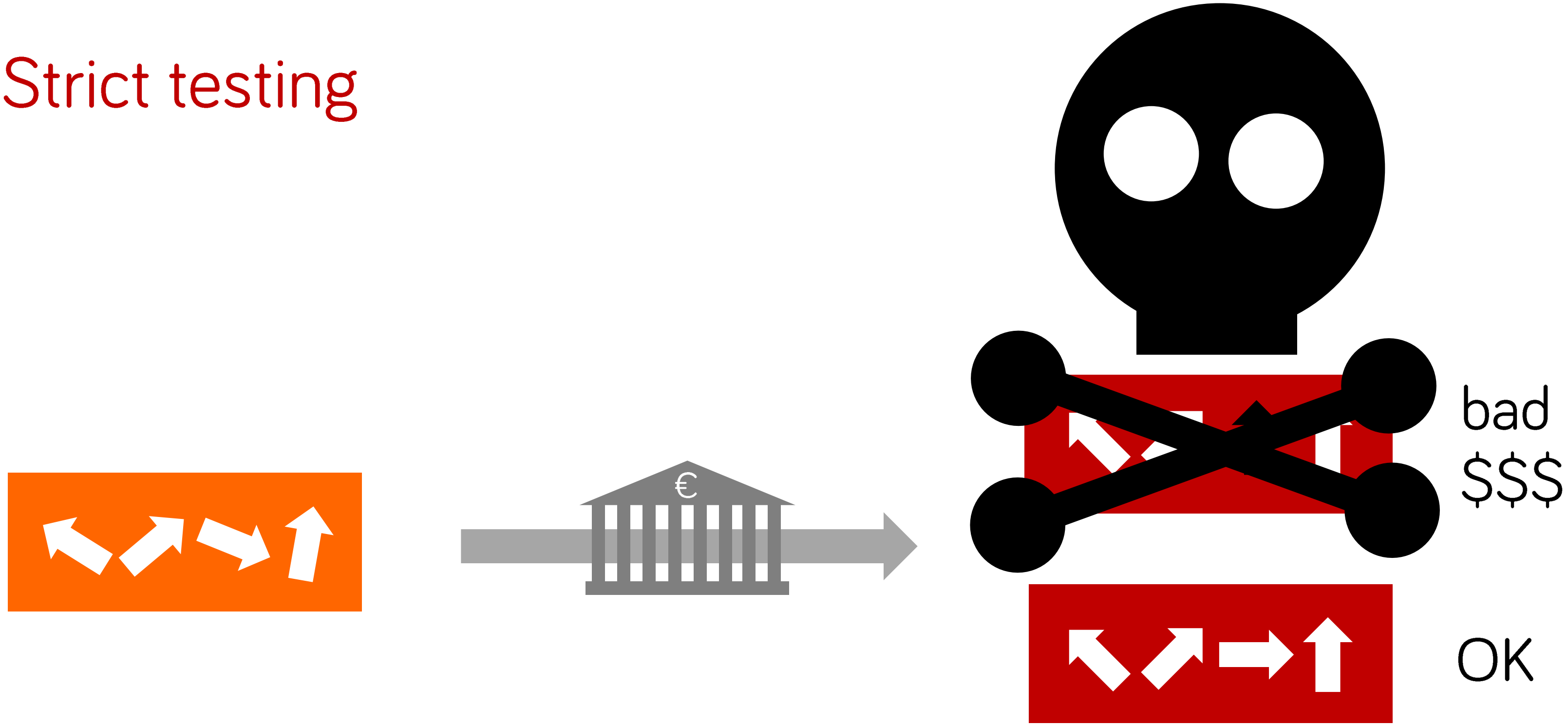
guess

save

flip & win!

win!

1 Strict testing



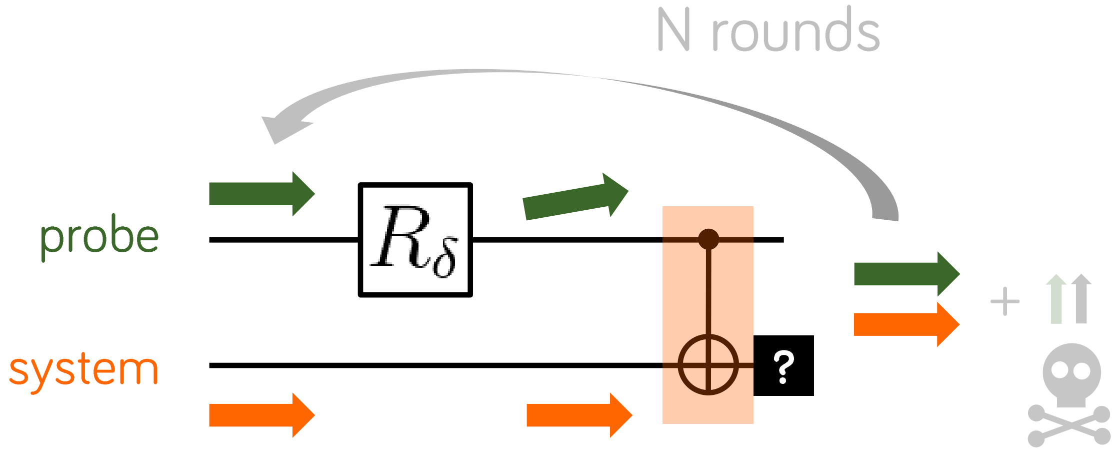
- is forgery still worth it?

We show an **efficient adaptive attack** on Wiesner's quantum money scheme (and its variant by Bennett et al.), when valid money is accepted and passed on, while invalid money is destroyed. Our approach is based on the quantum Zeno effect, also known as Elitzur-Vaidman's **bomb tester**. [1404.1507]

testing
quantum
bombs
carefully

2 The Elitzur-Vaidman bomb tester

- “bomb”



final state

→

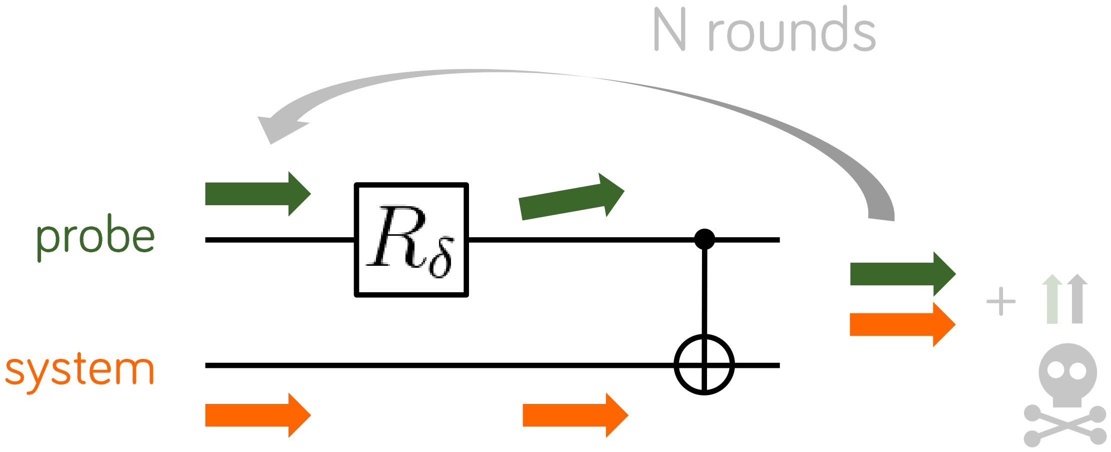
be careful!

$$\delta = \frac{\pi}{2N}$$

$$p_{☠} \propto N\delta^2 \propto \frac{1}{N}$$

2 The Elitzur-Vaidman bomb tester

- “bomb”



N rounds

probe

system

R_δ

final state

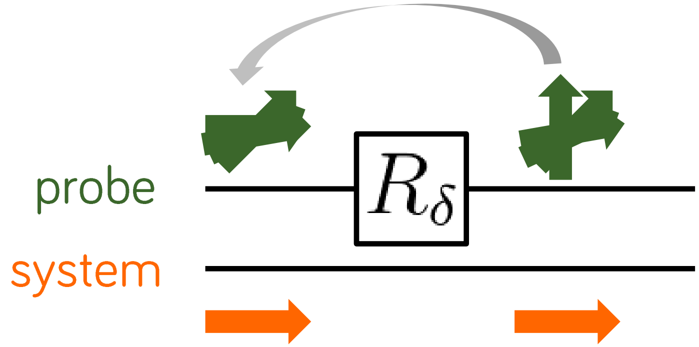
→

be careful!

$$\delta = \frac{\pi}{2N}$$

$$p_{\text{☠}} \propto N\delta^2 \propto \frac{1}{N}$$

- “no bomb”



probe

system

R_δ

final state

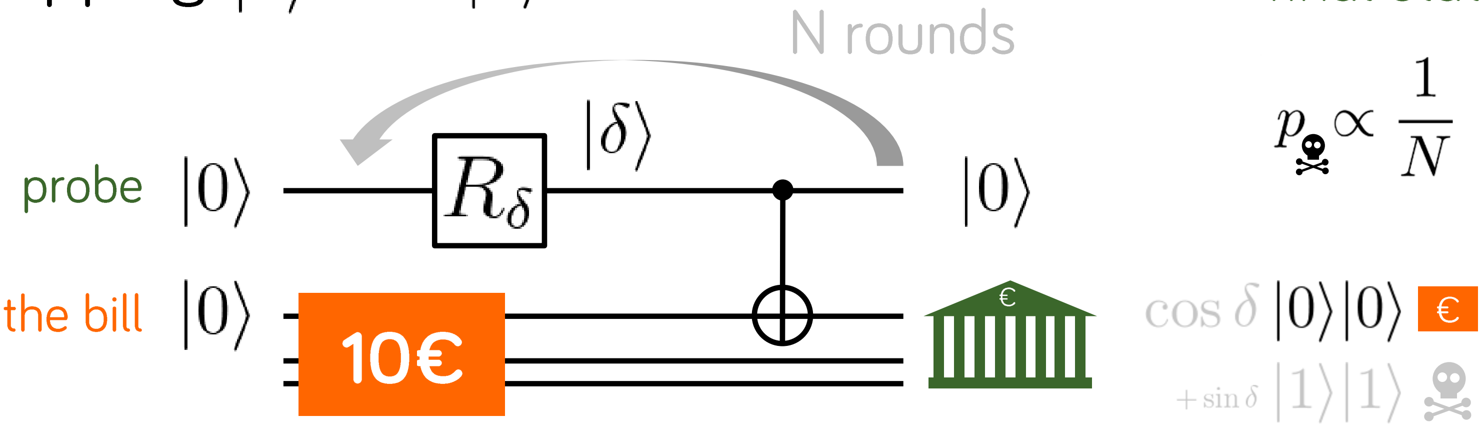
↑

all clear

2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$



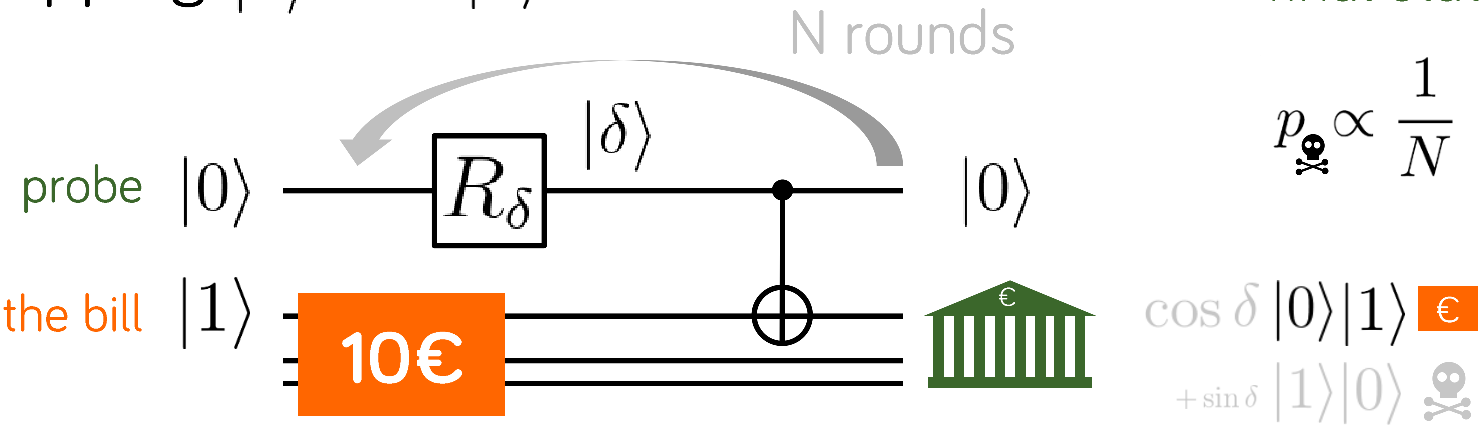
$p_{☠} \propto \frac{1}{N}$

2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$p_{☠} \propto \dfrac{1}{N}$

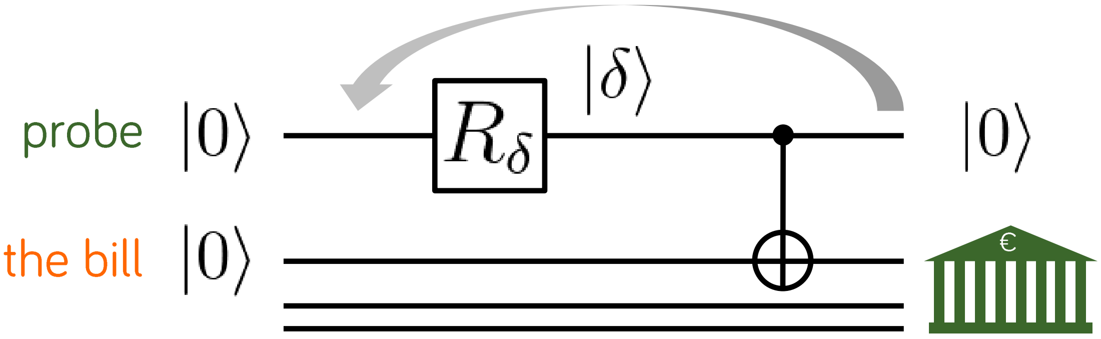


2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$p_{☠} \propto \frac{1}{N}$

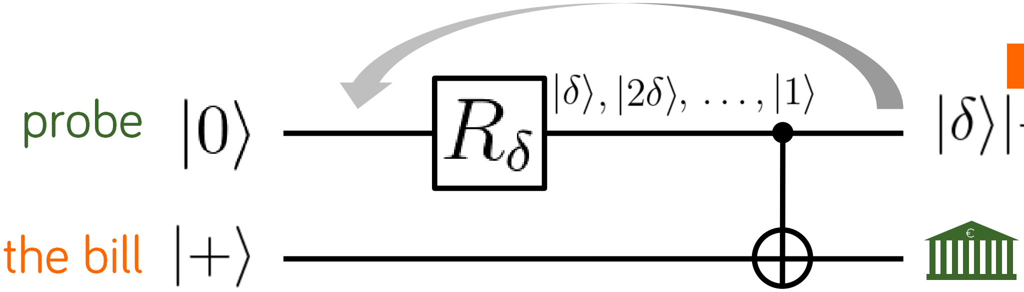


$\cos\delta\,|0\rangle|0\rangle$ €

$+\sin\delta\,|1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$



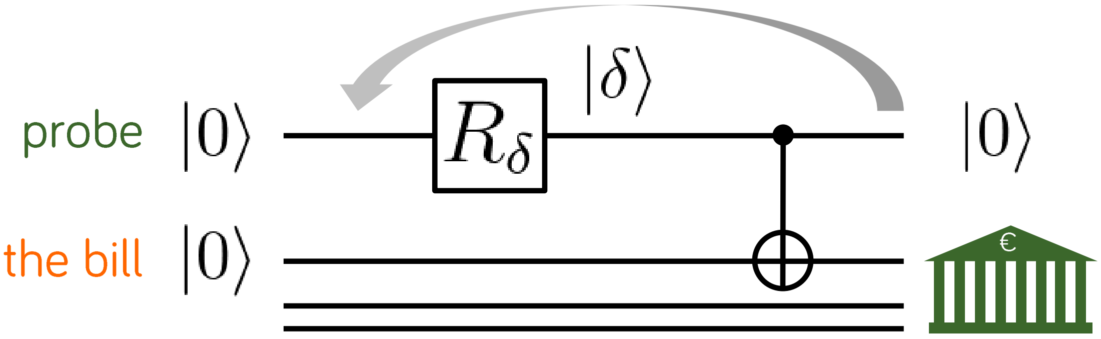
$|\delta\rangle\overset{€}{|+\rangle}, |2\delta\rangle\overset{€}{|+\rangle}, \ldots, |1\rangle\overset{€}{|+\rangle}$

2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$$p_{☠} \propto \frac{1}{N}$$



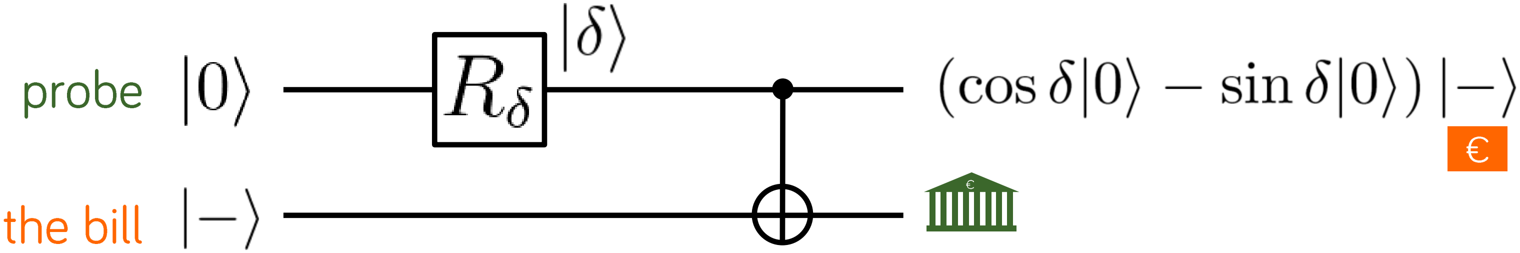
$\cos\delta\,|0\rangle|0\rangle$ €

$+\sin\delta\,|1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$



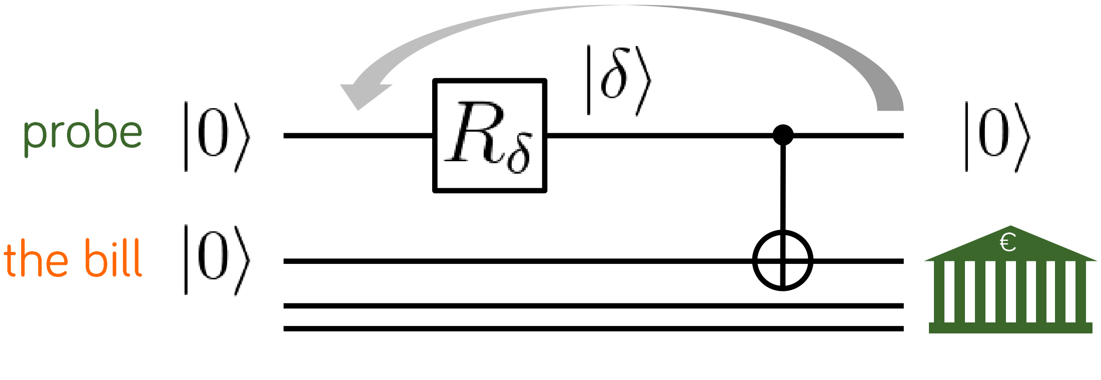
$(\cos\delta|0\rangle - \sin\delta|0\rangle)\,|-\rangle$ €

2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$p_{☠} \propto \frac{1}{N}$



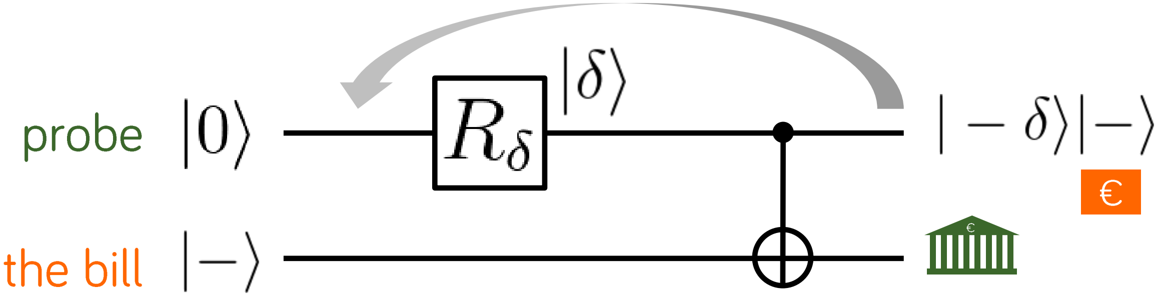
$\cos\delta\,|0\rangle|0\rangle$ €

$+\sin\delta\,|1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$

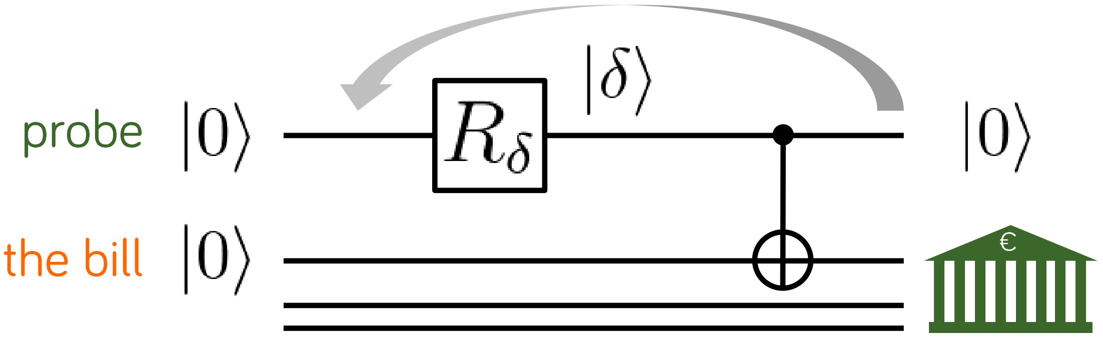


2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$$p_{☠} \propto \frac{1}{N}$$



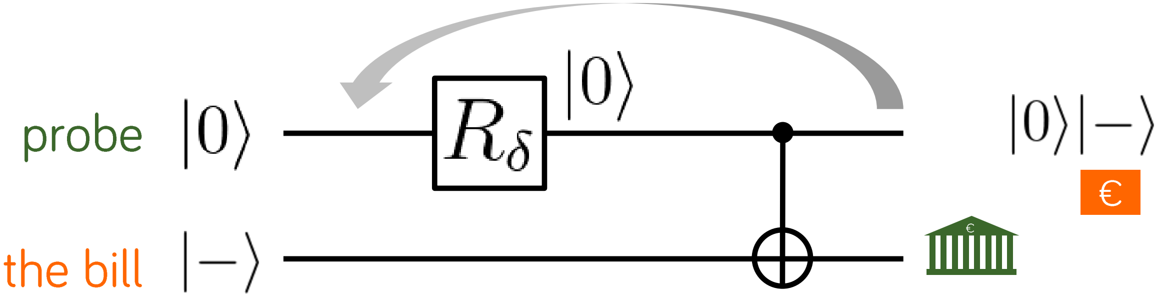
$\cos\delta\, |0\rangle|0\rangle$ €

$+\sin\delta\, |1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$

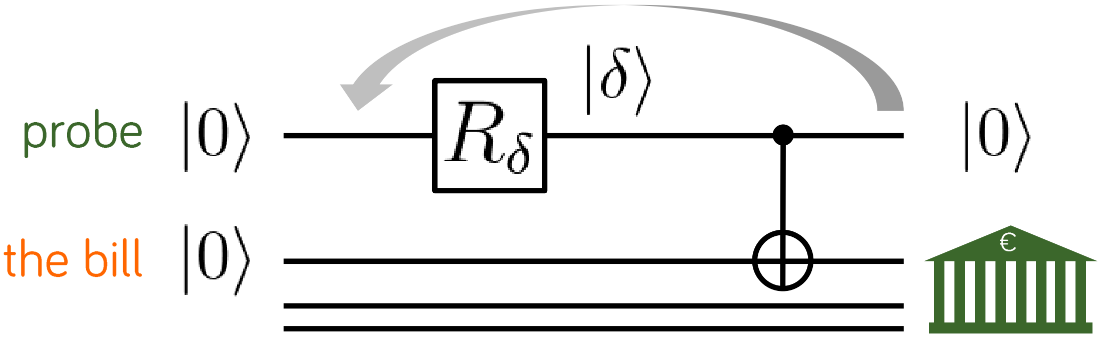


2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$p_{☠} \propto \frac{1}{N}$



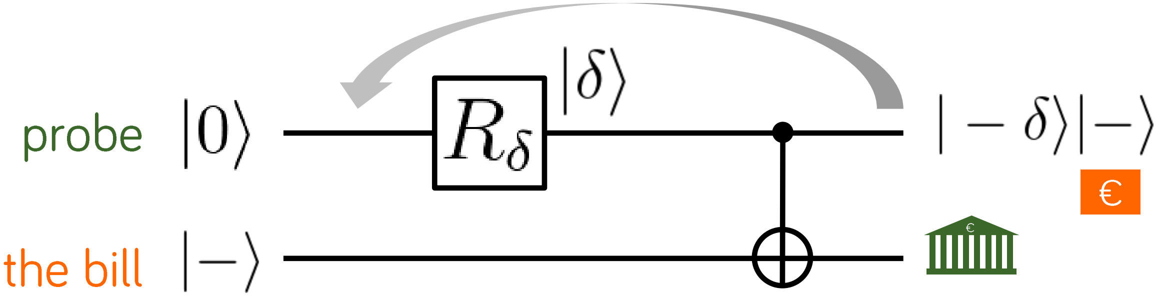
$\cos\delta\, |0\rangle|0\rangle$ €

$+\sin\delta\, |1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$

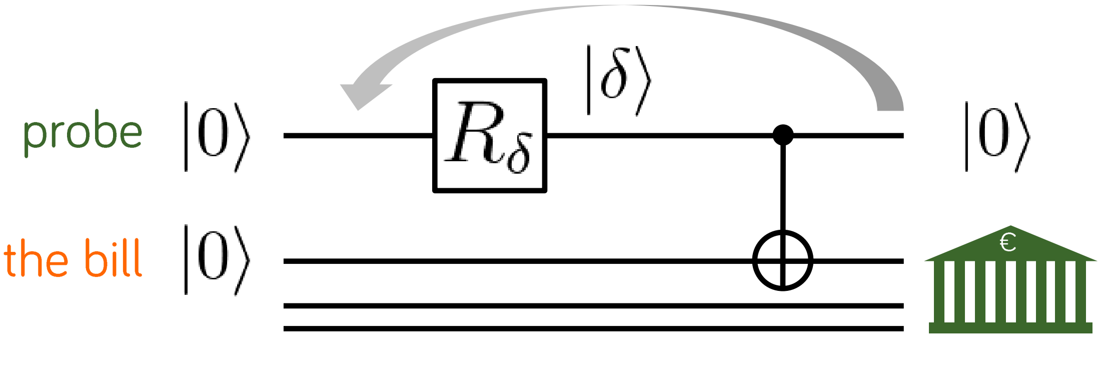


2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$p_{\text{☠}} \propto \frac{1}{N}$



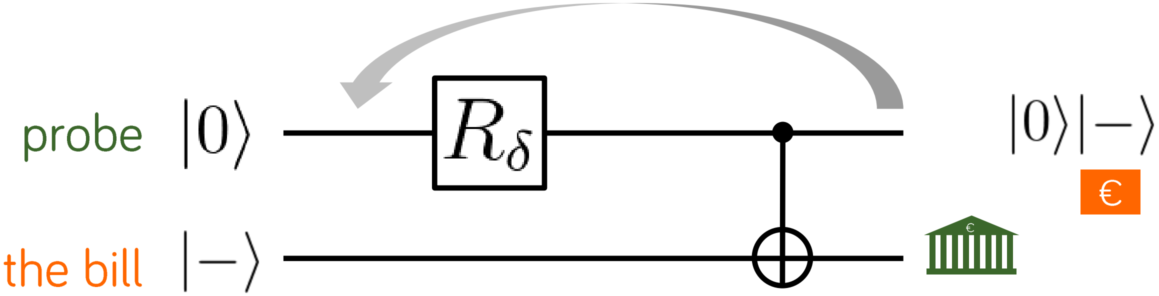
$\cos\delta\,|0\rangle|0\rangle$ €
$+\sin\delta\,|1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$

final state: $|0\rangle$

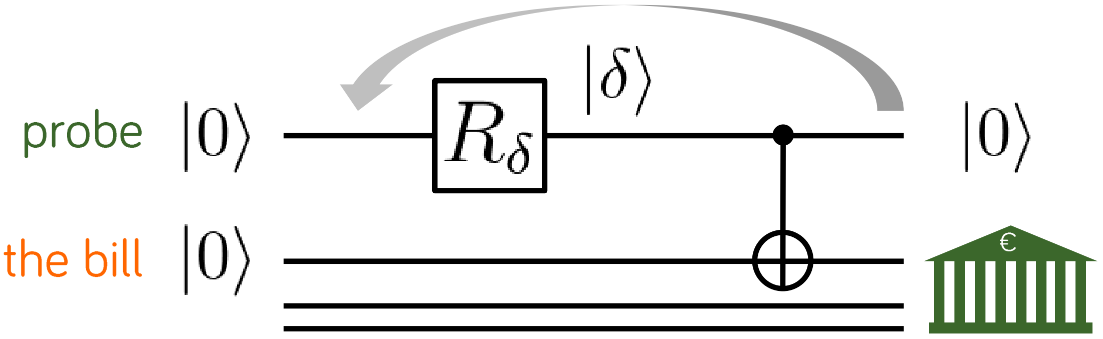


2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$$p_{☠} \propto \frac{1}{N}$$



$\cos\delta\, |0\rangle|0\rangle$ €
$+\sin\delta\, |1\rangle|1\rangle$ ☠

- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$

final state: $|0\rangle$

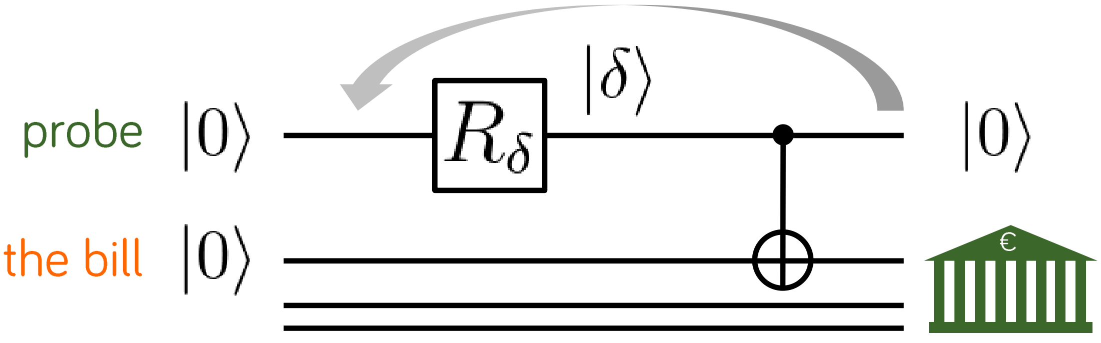
- identifying a state besides $|+\rangle$?

2 Validating slightly modified quantum money

- flipping $|0\rangle$ and $|1\rangle$

final state: $|0\rangle$

$p_{☠} \propto \frac{1}{N}$



$\cos\delta\, |0\rangle|0\rangle$ €

$+\sin\delta\, |1\rangle|1\rangle$ ☠

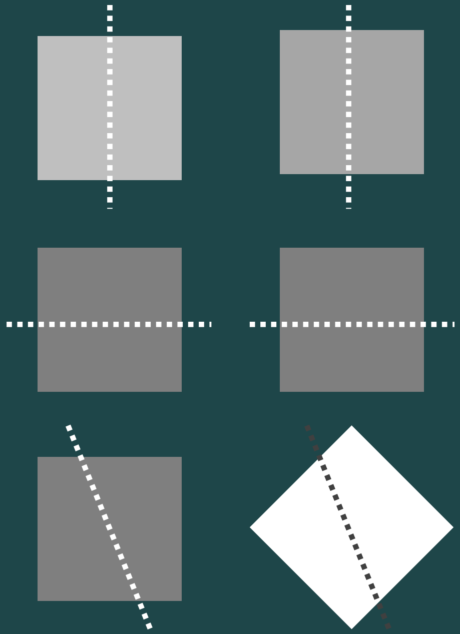
- keeping $|+\rangle$

final state: $|1\rangle$

- fun with phases on $|-\rangle$

final state: $|0\rangle$

adaptive verification + bomb-testing = $$$



single-copy tomography

from strict testing

3 Generalizing Wiesner's money

- a different list of states?

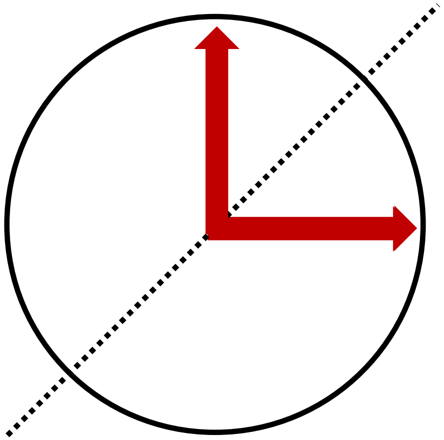
  $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |y+\rangle, |y-\rangle, \ldots\}$

  not a problem

- completely unknown states?

  guess an axis to flip about … imperfect bombs

a "bomb"



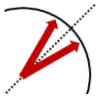
3 Generalizing Wiesner’s money

- a different list of states? $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |y+\rangle, |y-\rangle, \ldots\}$

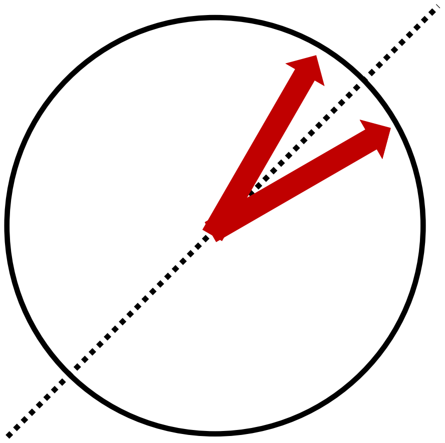
  not a problem

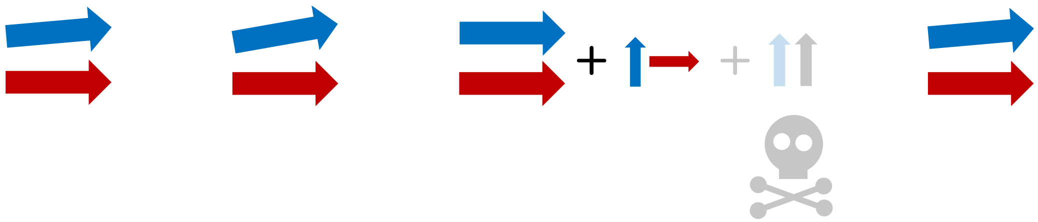
- completely unknown states?

  guess an axis to flip about … imperfect bombs



almost a “bomb”





the probe converges to a small fixed angle

3 Generalizing Wiesner's money

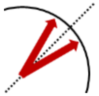
- a different list of states?

  $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |y+\rangle, |y-\rangle, \ldots\}$

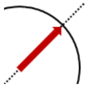
  not a problem

- completely unknown states?

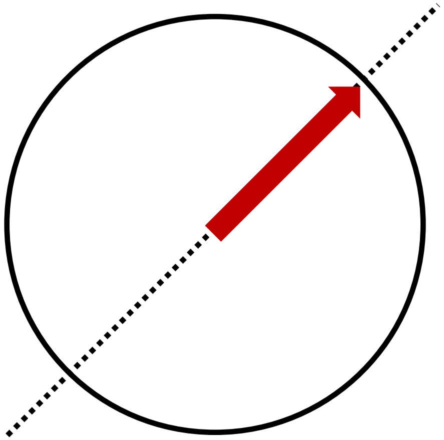
  guess an axis to flip about … imperfect bombs



almost a "bomb"



almost "no-bomb"



3 Generalizing Wiesner's money

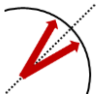
- a different list of states?

  not a problem

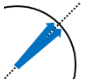
$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |y+\rangle, |y-\rangle, \ldots\}$

- completely unknown states?

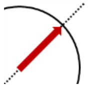
  guess an axis to flip about … imperfect bombs



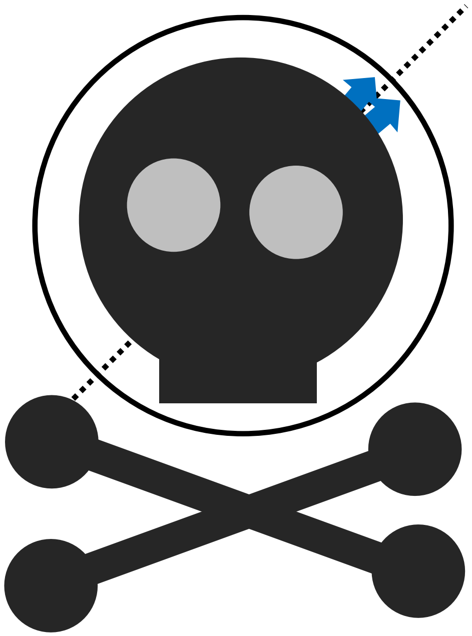
almost a “bomb”



a messy case



almost “no-bomb”



seems safe … probe more & more …

3 Generalizing Wiesner’s money

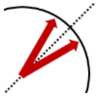
- a different list of states?

  not a problem

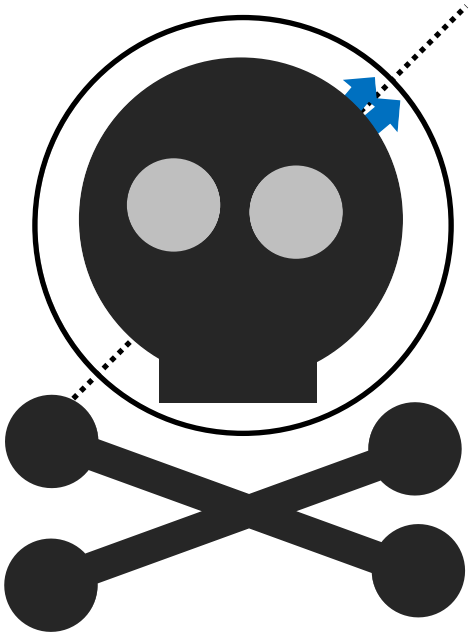
$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |y+\rangle, |y-\rangle, \ldots\}$

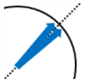
- completely unknown states?

  guess an axis to flip about … imperfect bombs

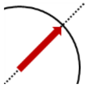


almost a “bomb”





a messy case

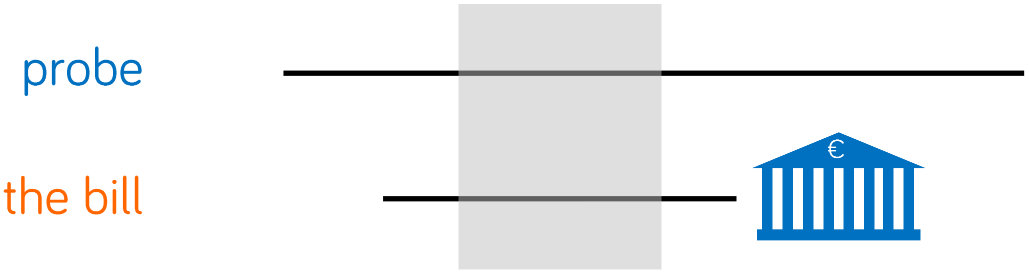


almost “no-bomb”

- tomography with strict testing?

3 Modular weak measurement

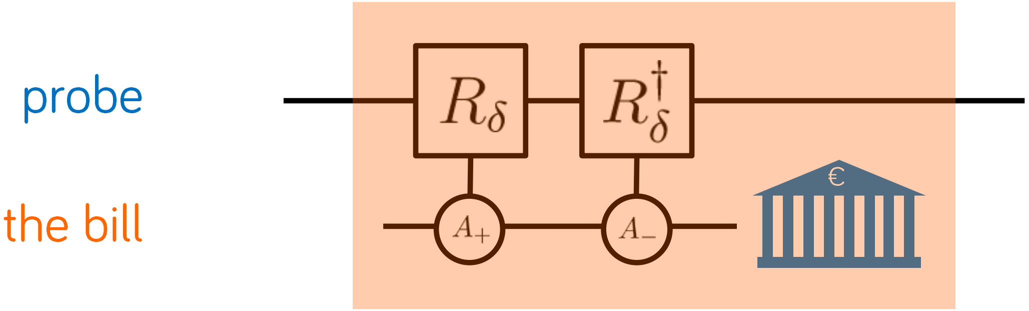
- an interaction that is always weak



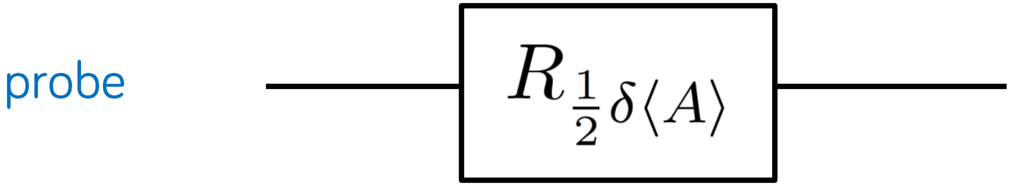
$$p_{\text{☠}} \propto \delta^2$$

3 Estimating $\langle A \rangle$ for a Pauli operator

- how much does A mess up the state?



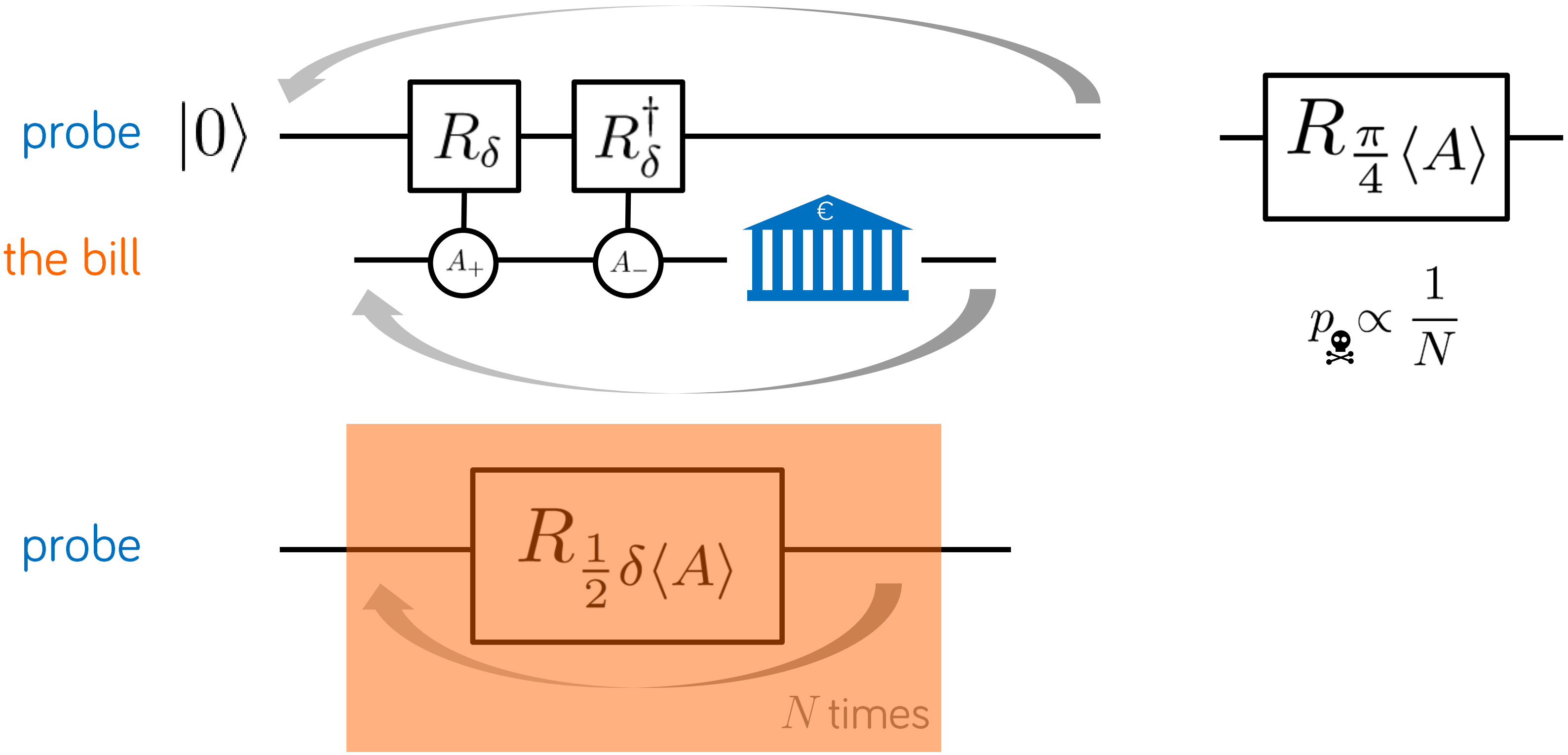
$p_{☠} \propto \delta^2$



if we don’t die
(approximately)

3 Estimating $\langle A \rangle$ for a Pauli operator

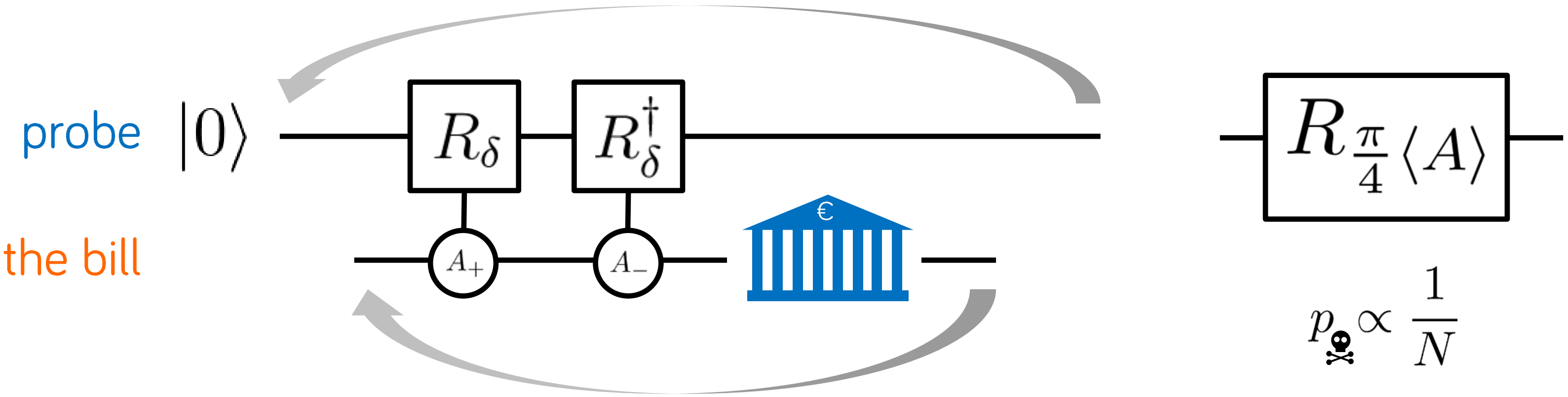
- how much does A mess up the state?


probe
$|0\rangle$
R_δ
$R_\delta^\dagger$
the bill
A_+
A_-
€
$R_{\frac{\pi}{4}\langle A\rangle}$
$p_{☠} \propto \frac{1}{N}$
probe
$R_{\frac{1}{2}\delta\langle A\rangle}$
N times

- phase estimation to required precision
- use operators A = { X, Y, Z } (or do it adaptively)

3 Estimating $\langle A \rangle$ for a Pauli operator

- how much does A mess up the state?


probe
$|0\rangle$
R_δ
$R_\delta^\dagger$
the bill
A_+
A_-
€
$R_{\frac{\pi}{4}\langle A \rangle}$
$p_{☠} \propto \frac{1}{N}$

single-copy tomography from strict testing

- phase estimation to required precision
- use operators A = { X, Y, Z } (or do it adaptively)

1 destroy bad bills

or print/prepare new ones!

100€

2 quantum Zeno

how to copy {0, 1, +, −} without dying

3 tomography

with a single copy and strict-testing