Quantum Encryption with Certified Deletion

Anne Broadbent

Department of Mathematics and Statistics

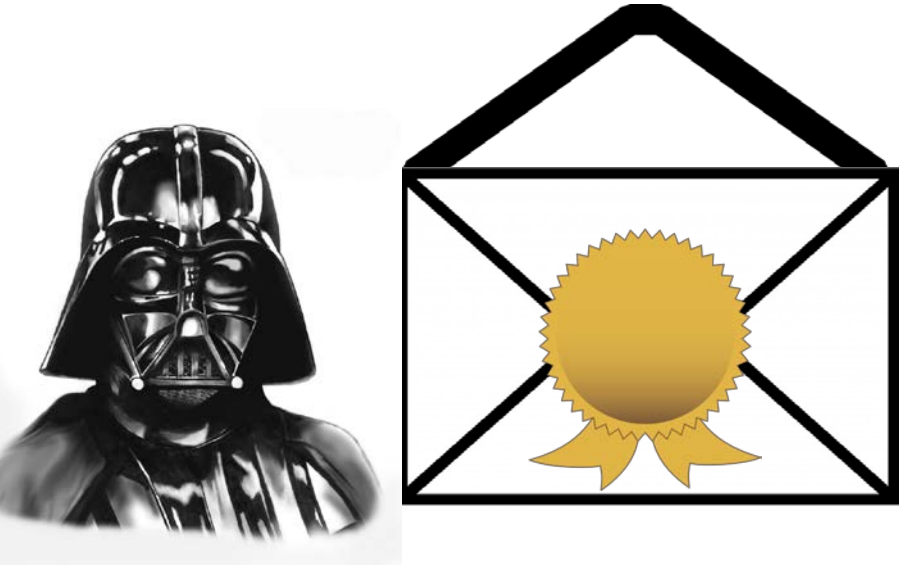
University of Ottawa

Based on joint work with Rabib Islam (arXiv:1910.03551)

INTRIQ, November 12, 2019

A “physical” type of encryption:

“Luke, I am your father.”



Luke decides

- Open & read the content

XOR

- return the sealed envelope as a proof that message was not read

Can we achieve this in a digital world?

Can we achieve this in a digital world?
No!
Proof by contradiction…

$\mathsf{Encode}_k(\text{“Luke, I am your father.”})$

“Luke, I am your father.”
$\mathsf{Encode}_k(\text{“Luke, I am your father.”})$

Luke can:

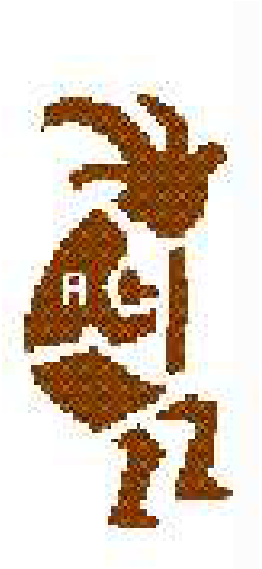
- Open & read the content (use copy #1)

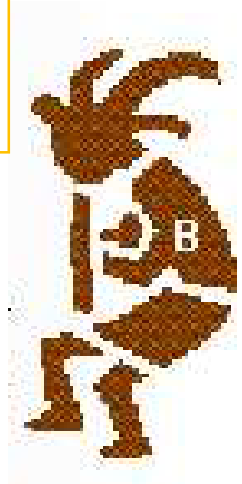
AND

- Convince Darth Vader that he did not read the message(use copy #2)

This talk: how quantum mechanics allows the best of the physical and digital worlds:

- encoding a classical message into a quantum state
- Bob can prove that he deleted the message by using a classical string





Quantum Encryption with Certified Deletion

Applications

- European Union's "right to be forgotten and to erasure'' (2012): legislation stating that a person should be able to have their data erased whenever its retention is no longer necessary.

- A trusted third party can be asked to prove deletion; this can be used as a building block for bit commitment


Erasable Bit Commitment from Temporary Quantum Trust

Norbert Lütkenhaus * Ashutosh S Marwah † Dave Touchette ‡

October 31, 2019

- A more general framework where the only attack possible would be break the protocol *during* its execution (c.f. "everlasting security'') [open question]

Related Work

Revocable Quantum Timed-Release Encryption

DOMINIQUE UNRUH, University of Tartu

quantum encodings can be used to certify that a ciphertext is completely "returned" (2015)

PHYSICAL REVIEW A **97**, 032324 (2018)

Local randomness: Examples and application

Honghao Fu[1] and Carl A. Miller[1,2]

proof of deletion is classical; device-independent; achieved for a single bit.

Proving Erasure

Xavier Coiteux-Roy
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland
xavier.coiteux.roy@usi.ch

Stefan Wolf
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland
stefan.wolf@usi.ch

idea of classical deletion certificate: gives a candidate scheme and breaks it. (2019)

Wiesner's conjugate coding

basis $\theta \in \{0,1\}$.
bit $r \in \{0,1\}$.
let $|r\rangle_\theta = H^\theta |r\rangle$

θ	r	$\|r\rangle_\theta$
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

Computational basis

Diagonal basis

Basic certified deletion scheme by example


Proving Erasure

Xavier Coiteux-Roy
Faculty of Informatics
la Svizzera italiana
Switzerland
eux.roy@usi.ch

Stefan Wolf
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland
stefan.wolf@usi.ch

θ random

r random

θ	0	1	0	1
r	0	1	1	0
$\|r\rangle_\theta$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$
r_{comp}	0		1	
r_{diag}		1		0

r_{comp} substring of r where $\theta = 0$

r_{diag} substring of r where $\theta = 1$

- To encrypt message $m \in \{0,1\}^2$, send $|r\rangle_\theta, m \oplus r_{comp}$
- To decrypt using key θ, measure qubits in position where $\theta = 0$, to get r_{comp}, then use $m \oplus r_{comp}$ to compute m.
- To delete the message, measure all qubits in diagonal basis to get $y = * 1 * 0$.
- To verify the deletion, check that the $\theta = 1$ positions of d equal r_{diag}.

Proof intuition

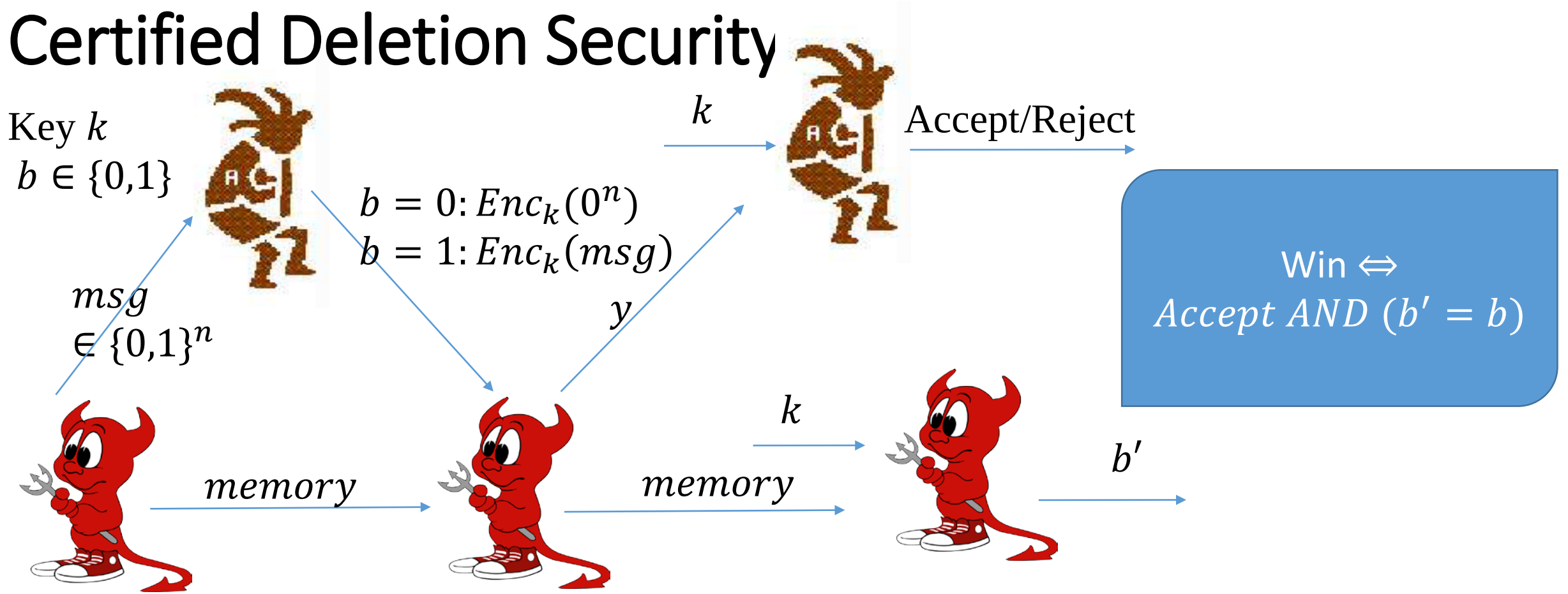
θ	0	1	0	1
r	0	1	1	0
$\|r\rangle_\theta$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$
r_{comp}	0		1	
r_{diag}		1		0

- A high success rate at predicting r_{diag} implies a low success rate of guessing r_{comp}.

$$H(X) + H(Z) \geq \log \frac{1}{c}$$

Maassen & Uffink, 1988

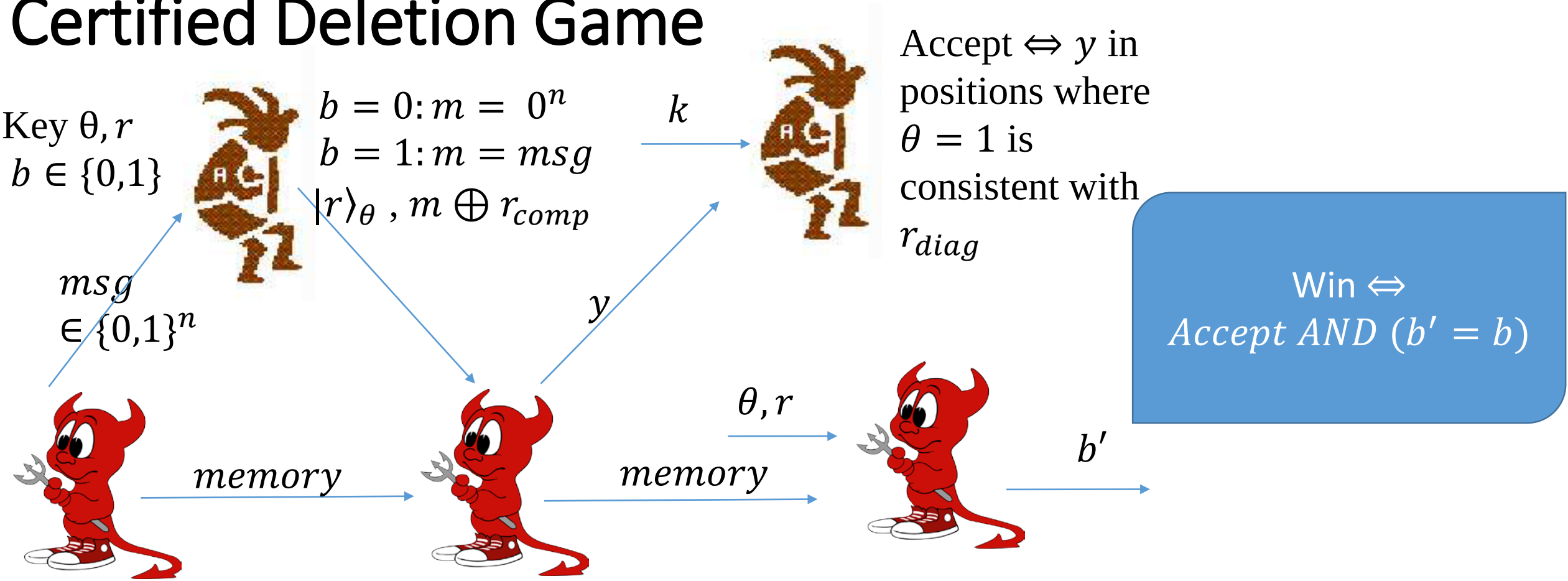
Certified Deletion Security



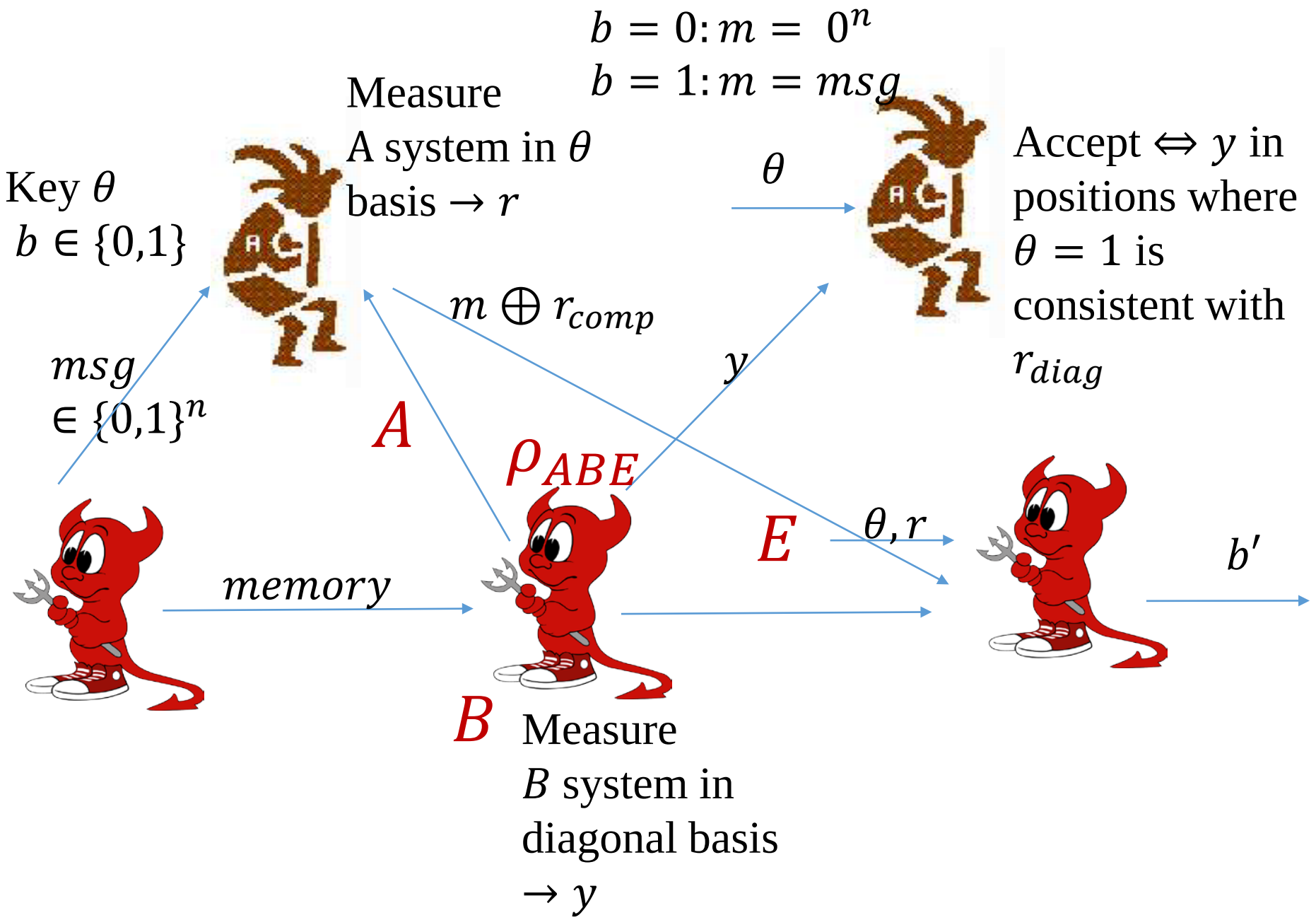
Win $\Leftrightarrow$
$Accept\ AND\ (b' = b)$

$$Certified\ Deletion\ Security \Leftrightarrow \Pr(Win) \leq \frac{1}{2} + \eta(\lambda)$$

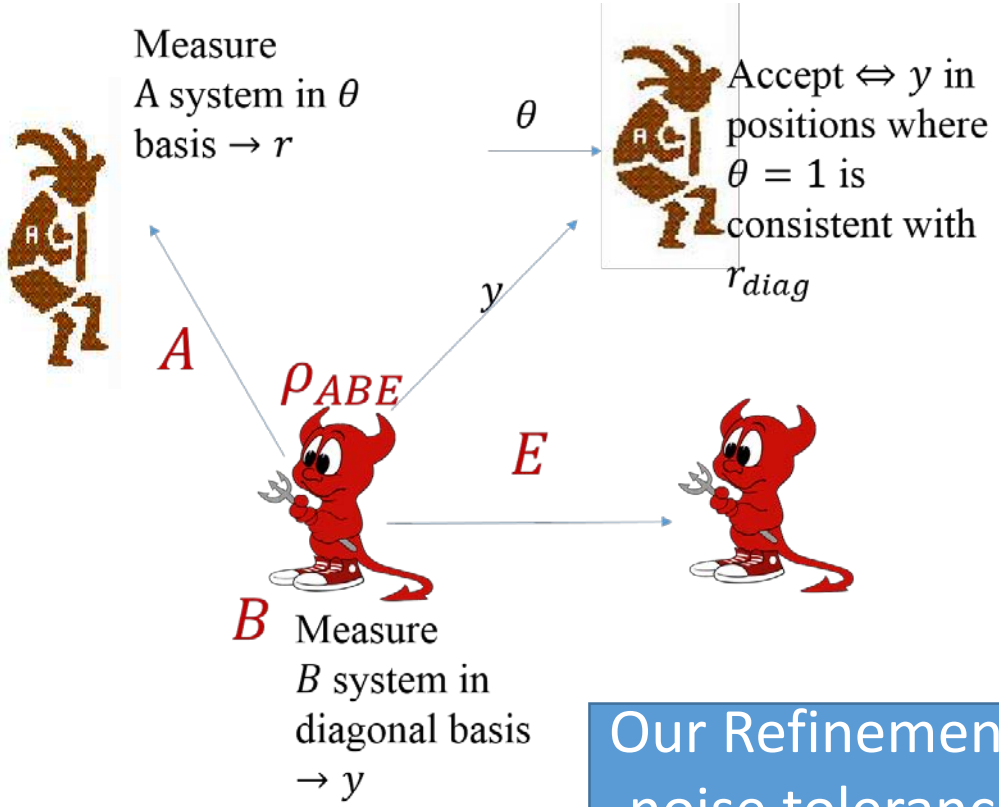
Certified Deletion Game



Certified Deletion Game (entanglement - based)



Win $\Leftrightarrow$ $Accept\ AND\ (b' = b)$



Entropic uncertainty relation (Tomamichel & Renner 2011):
X: outcome if Alice measures n qubits in computational basis
Z: outcome if Alice measures n qubits in diagonal basis
Z':outcome of Bob who measures n qubits in diagonal basis

$$H_{min}^{\epsilon}(X \mid E) + H_{max}^{\epsilon}(Z \mid Z') \geq n,$$

$H_{min}^{\epsilon}(X \mid E)$: average prob. that Eve guesses X correctly
$H_{max}^{\epsilon}(Z \mid Z')$: # of bits that are required to reconstruct Z from Z'.

Our Refinements of the protocol:
-noise tolerance: Accept y if less than $k\delta$ bits are wrong; send a syndrome to allow decoding.
-reduce and make uniform E's advantage: Use privacy amplification (2-universal hash function) to make r_{comp} exponentially close to uniform from E's point of view.

By giving an upper bound on the max-entropy, we obtain a lower bound on the min-entropy.
The conclusion is that $P(win) \leq \frac{1}{2} + negl(\lambda)$.

Summary

- Quantum encodings for classical messages allows the advantages of the physical world for certified deletion, with the convenience of digital communication.

Thank you!