HOMOMORPHIC ENCRYPTION OF QUANTUM DATA

Christian Schaffner

UNIVERSITY OF COPENHAGEN

QMATH

(joint work with Yfke Dulek and Florian Speelman)
http://arxiv.org/abs/1603.09717

Institute for Logic, Language and Computation (ILLC)
University of Amsterdam

QuSoft
Research Center for Quantum Software

CWI
Centrum Wiskunde & Informatica

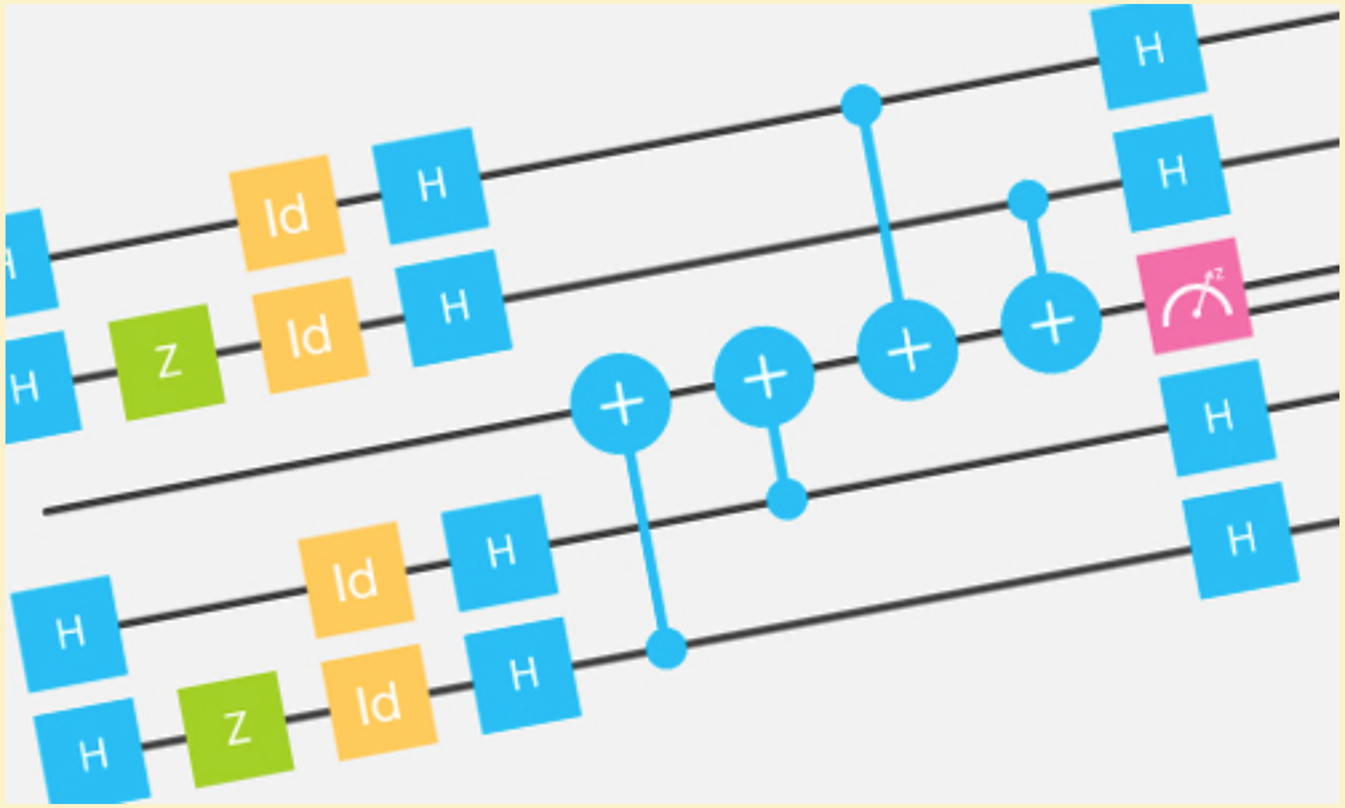
Colloquium KdVI, UvA, Wednesday 5 April 2017

EXAMPLE: IMAGE TAGGING

Classical homomorphic encryption: Gentry [2009]

What about quantum?

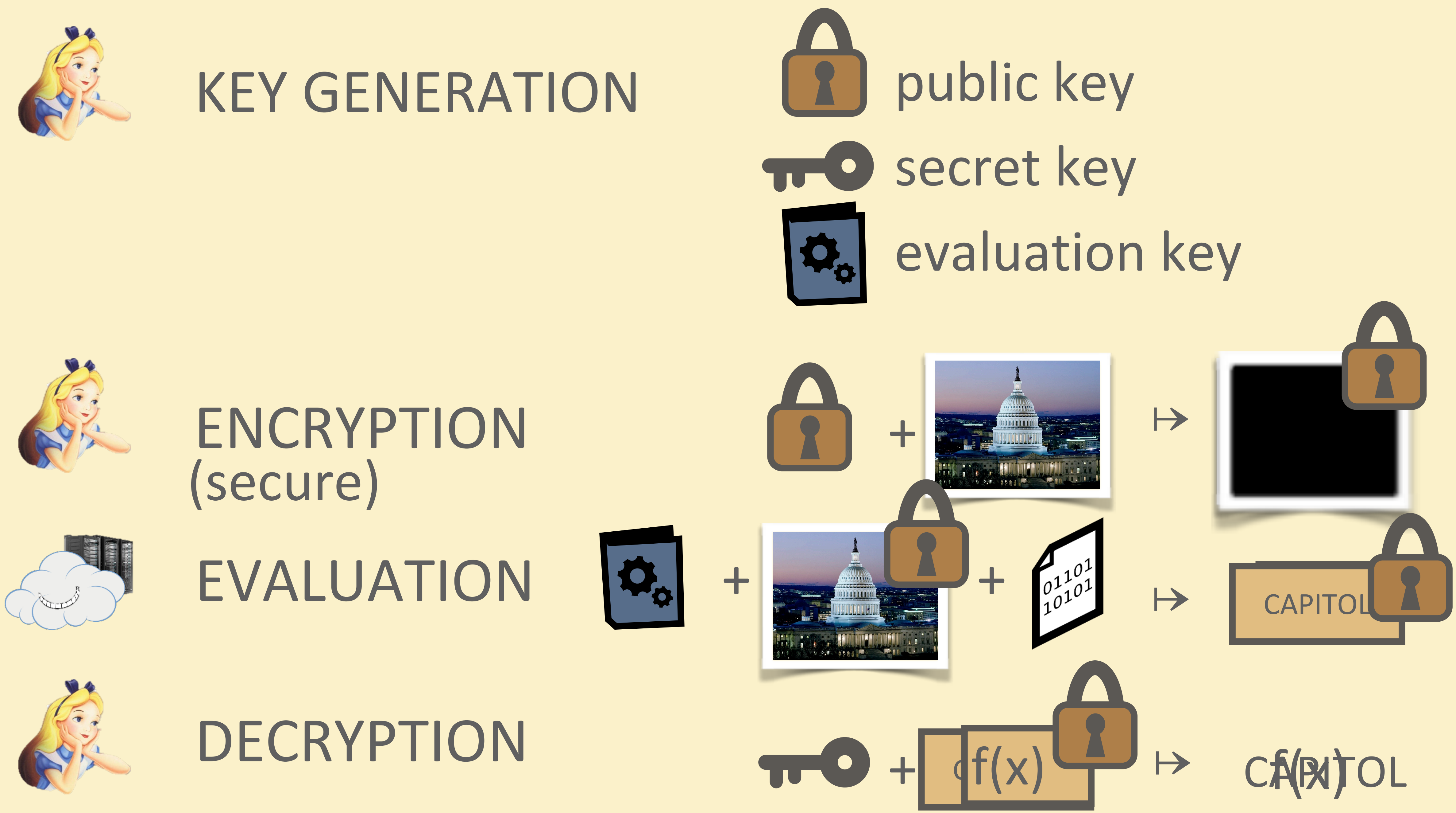
QUANTUM CLOUD COMPUTING



Google Microsoft intel

1. HOMOMORPHIC ENCRYPTION
2. PREVIOUS RESULTS: CLIFFORD SCHEME
3. NEW SCHEME

HOMOMORPHIC ENCRYPTION



Classical homomorphic encryption: Gentry [2009]

RSA IS MULTIPLICATIVE HOMOMORPHIC

- Public key: exponent e and modulus N
- Encryption of a message : $\mathrm{Enc}(x) = x^e \bmod N$

Given encryptions of messages x and y
possible to compute the encryption of the product:

$$(x^e \bmod N)(y^e \bmod N) = (xy)^e \bmod N$$

$$\mathrm{Enc}(x)\mathrm{Enc}(y) = \mathrm{Enc}(xy)$$

HOMOMORPHIC ENCRYPTION

KEY GENERATION

public key

secret key

quantum

evaluation key

ENCRYPTION
(secure)

+ $|\psi\rangle \mapsto |\psi\rangle$

EVALUATION

+ $|\psi\rangle$ + 01101 10101 $\mapsto U|\psi\rangle$

DECRYPTION

+ $U|\psi\rangle \mapsto U|\psi\rangle$

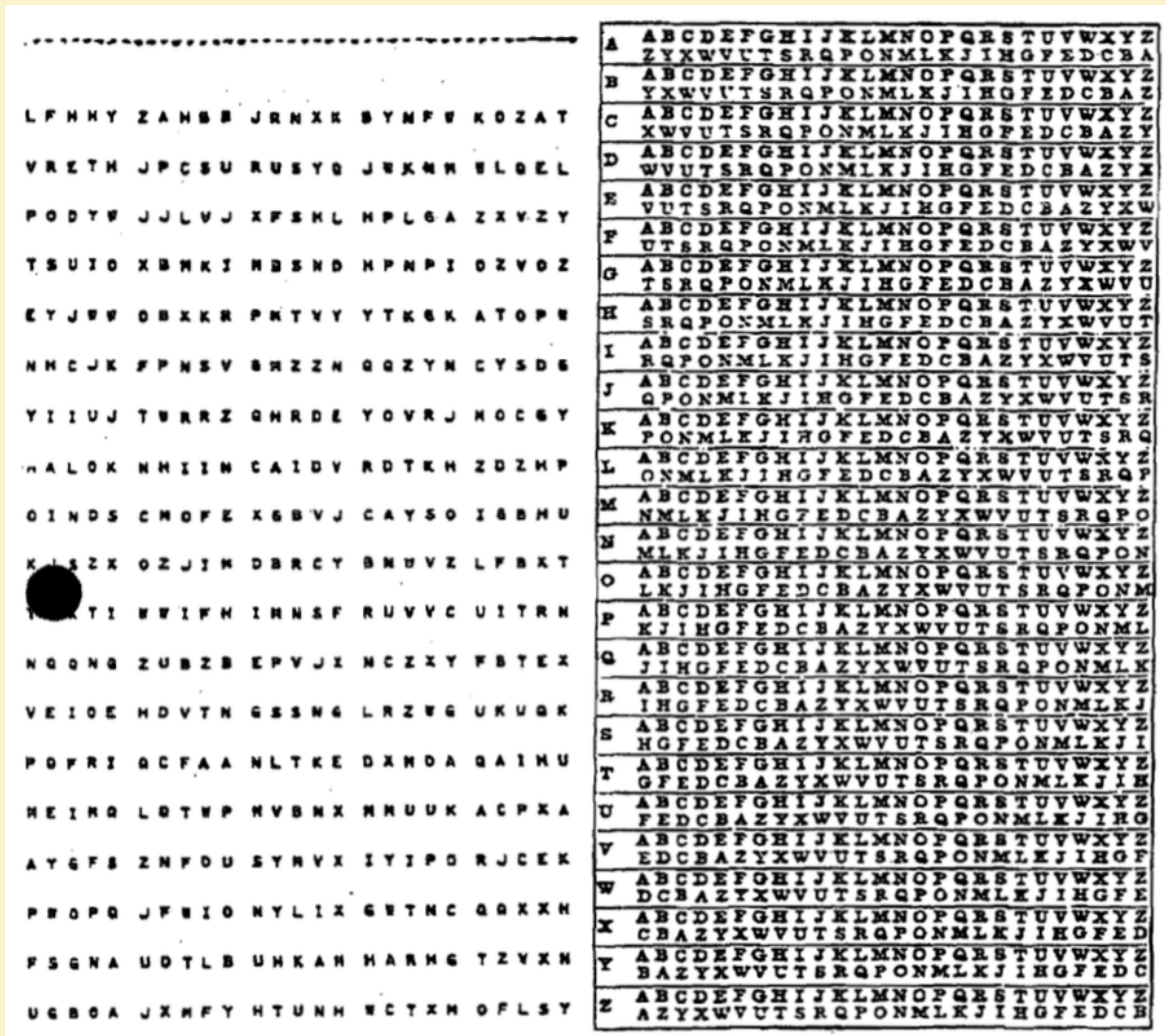
✓ HOMOMORPHIC ENCRYPTION

2. PREVIOUS RESULTS: CLIFFORD SCHEME

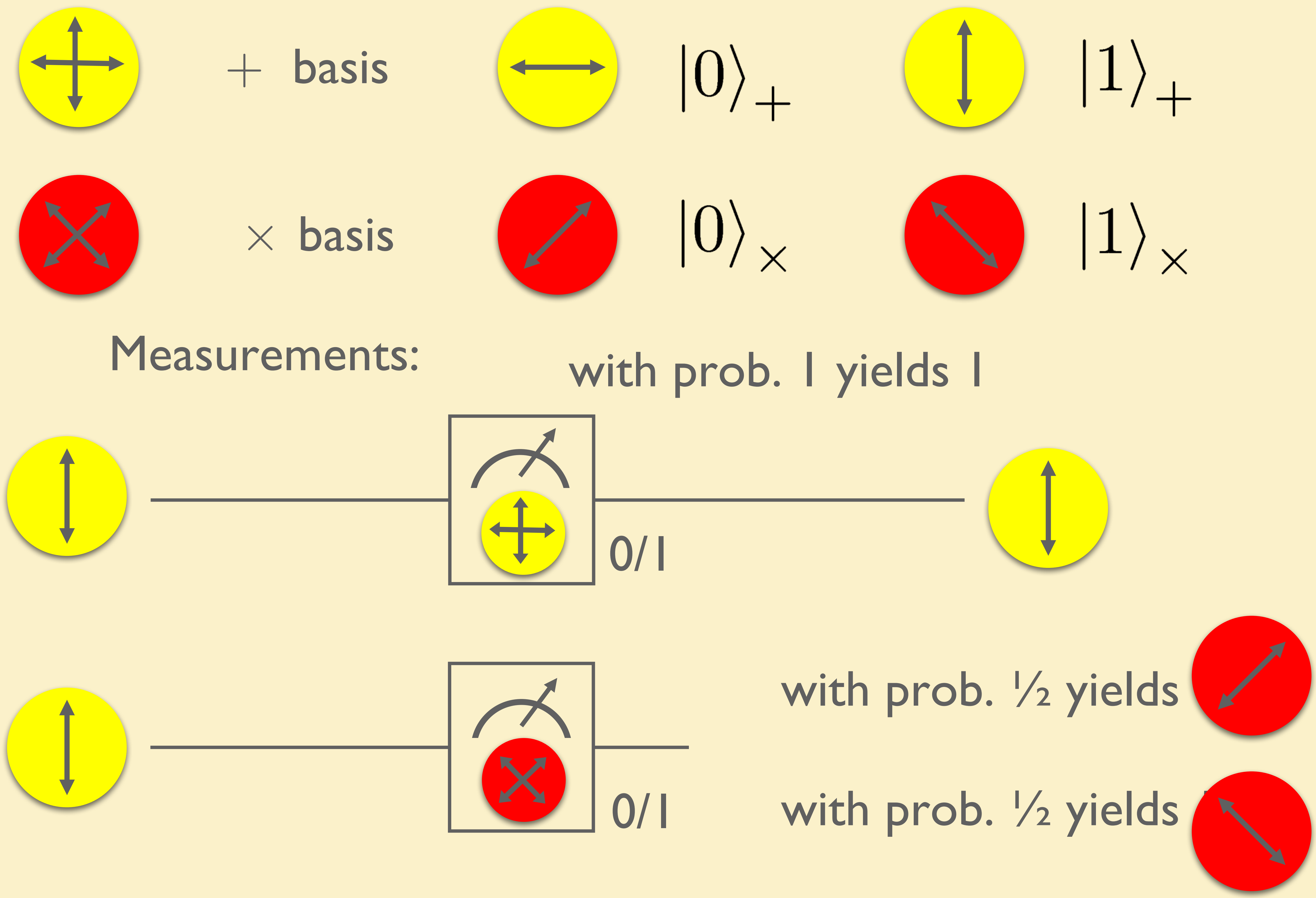
3. NEW SCHEME

CLASSICAL ONE-TIME PAD

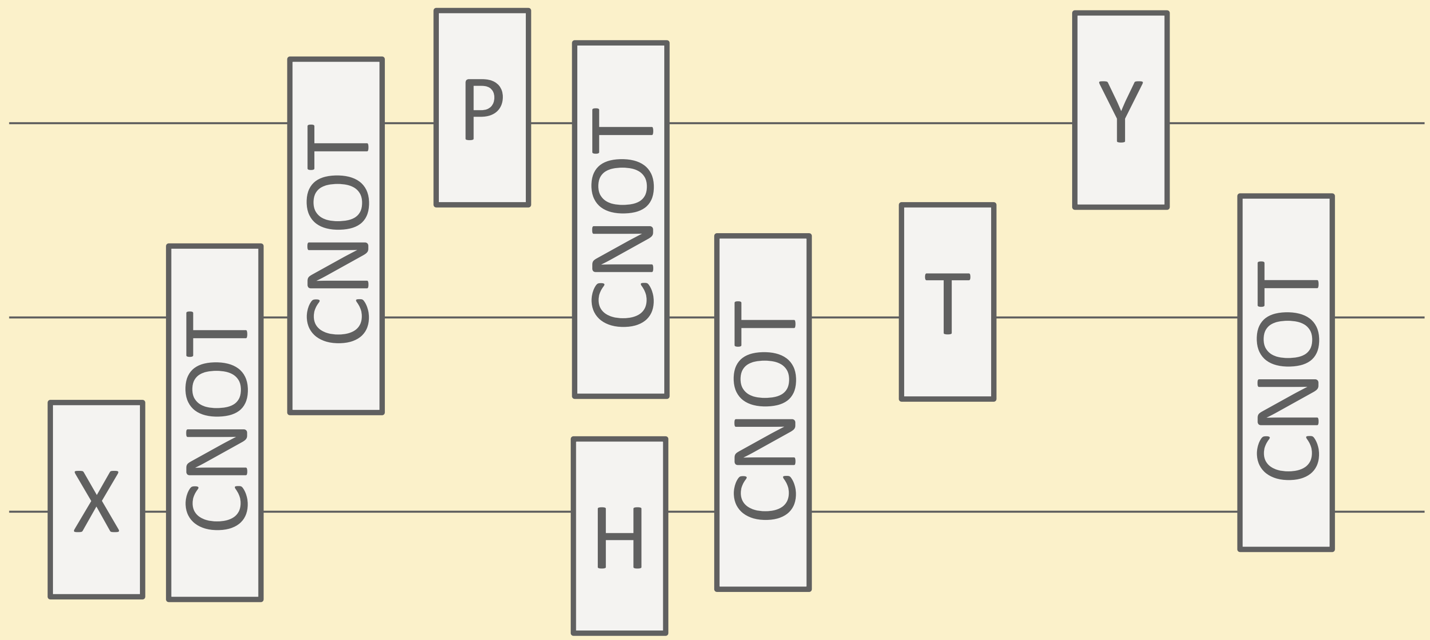
See explanations on black board



QUANTUM BITS



Q CIRCUITS AND PAULI GROUP



- Pauli operators $\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathrm{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- Self-inverse: $X^2 = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \ Y^2 = \mathbb{I},\ \ Z^2 = \mathbb{I}$
- Anti-commute: $XZ = -ZX,\ XY = -YX,\ YZ = -ZY$

QUANTUM ONE-TIME PAD

- Pauli operators $\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathrm{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Self-inverse: $X^2 = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; Y^2 = \mathbb{I}, \; Z^2 = \mathbb{I}$
- Anti-commute: $XZ = -ZX, \; XY = -YX, \; YZ = -ZY$
- Flip **two** random bits $a, b \leftarrow \{0,1\}$,
  encryption of a qubit $|\psi\rangle$: $X^a Z^b \, |\psi\rangle$
- Perfect security: not knowing a, b,
  the density matrix becomes *fully mixed*:
  $\frac{1}{4} \sum_{a,b} X^a Z^b \, |\psi\rangle\langle\psi| \, Z^b X^a = \mathbb{I}/2$

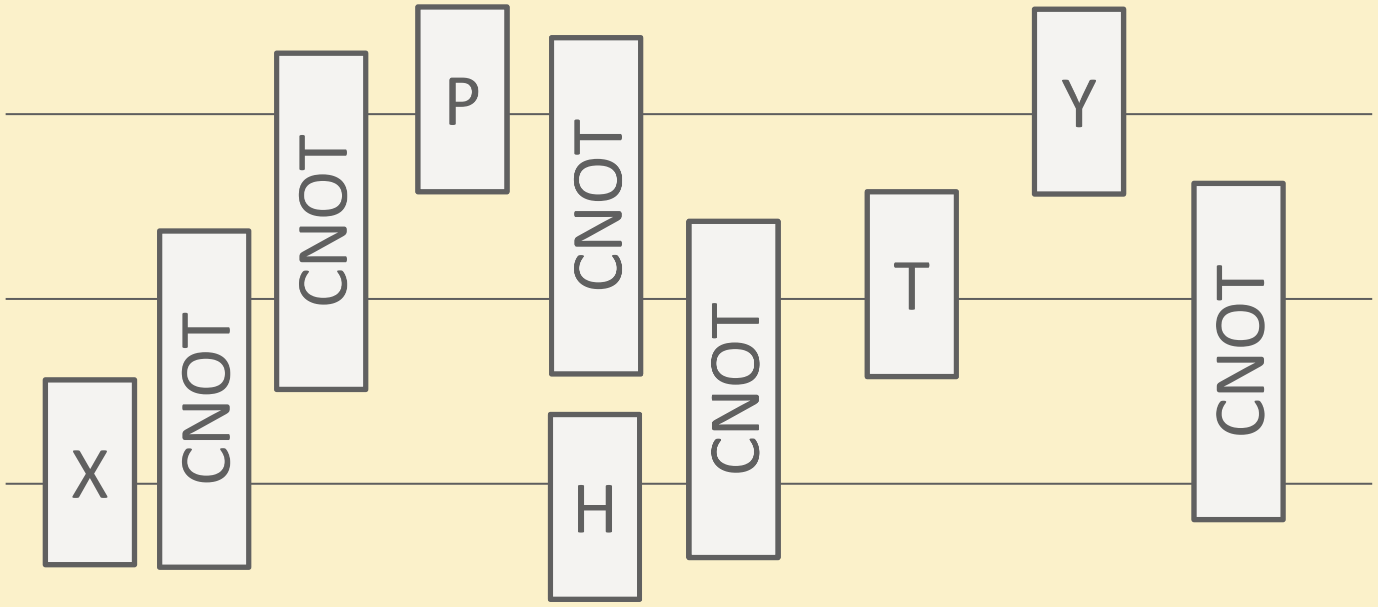
QUANTUM HOMOMORPHIC ENC

	homomorphic for	compactness	security
Not encrypting	Quantum circuits	yes	no
Quantum OTP	no	yes	yes
append evaluation description	Quantum circuits	Complexity of Dec prop to (# gates)	yes
Clifford Scheme	Clifford circuits	yes	computational

Quantum one-time pad:

pick a,b $\in_R \{0,1\}$

$|\psi\rangle \mapsto X^a Z^b \, |\psi\rangle$



THE CLIFFORD GROUP

Generated by $\{H, P, \text{CNOT}\}$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Commutation maps Pauli operators to Paulis (normalizer of Pauli group)

$$HX = ZH \qquad PZ = ZP$$

$$HZ = XH \qquad PX = XZP$$

$$\text{CNOT}(X \otimes I) = (X \otimes X)\text{CNOT}$$

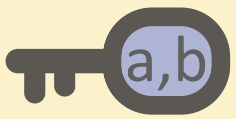
$$\text{CNOT}(I \otimes Z) = (Z \otimes Z)\text{CNOT}$$

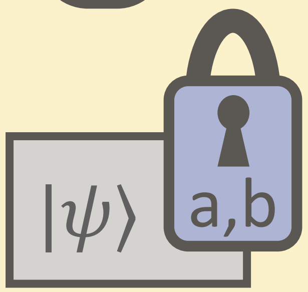
Not a universal gate set

(e.g. efficient classical simulation possible)

CLIFFORD SCHEME

Ingredient 1: quantum one-time pad

encryption: pick a,b $\in_R \{0,1\}$ 

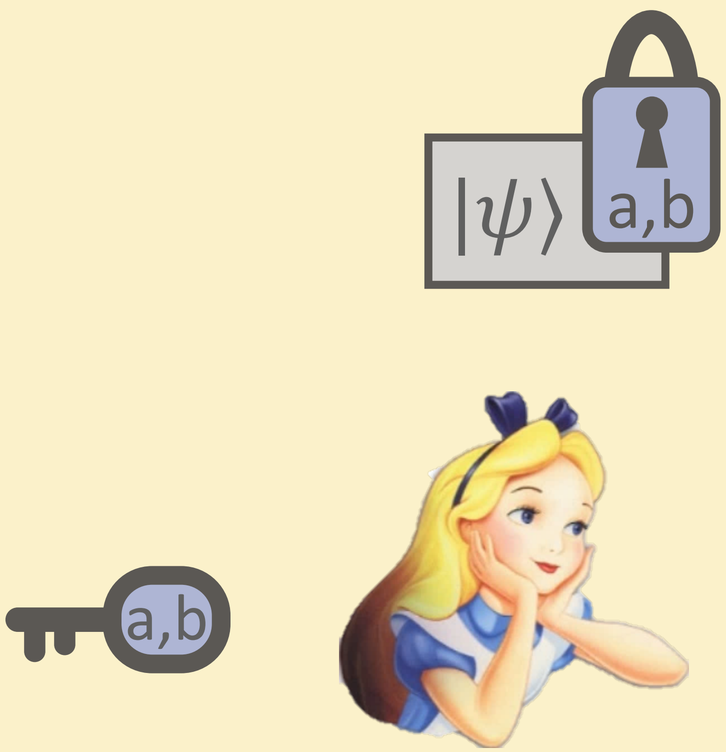
$|\psi\rangle \mapsto X^a Z^b |\psi\rangle$ = 

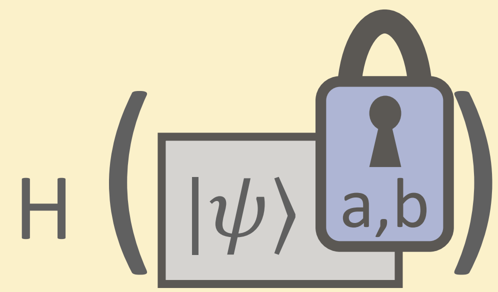
decryption: $X^a Z^b |\psi\rangle \mapsto |\psi\rangle$

Ingredient 2: classical homomorphic encryption (as black box)

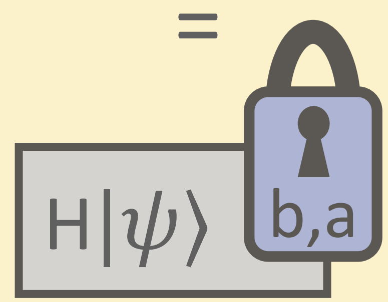
[AMTW00] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. FOCS'00
[Gentry 09] C. Gentry: Fully homomorphic encryption using ideal lattices. STOC'09

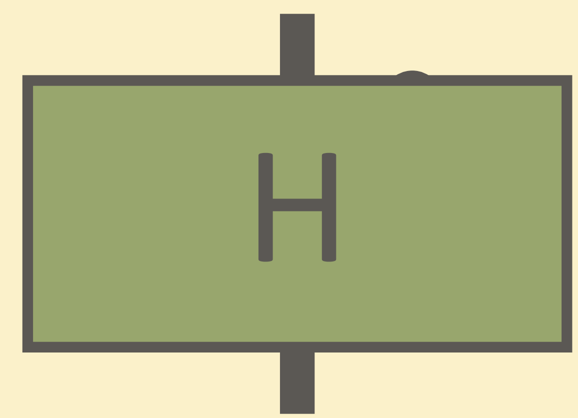
CLIFFORD SCHEME





$$= HX^aZ^b|\psi\rangle = X^bZ^aH|\psi\rangle =$$



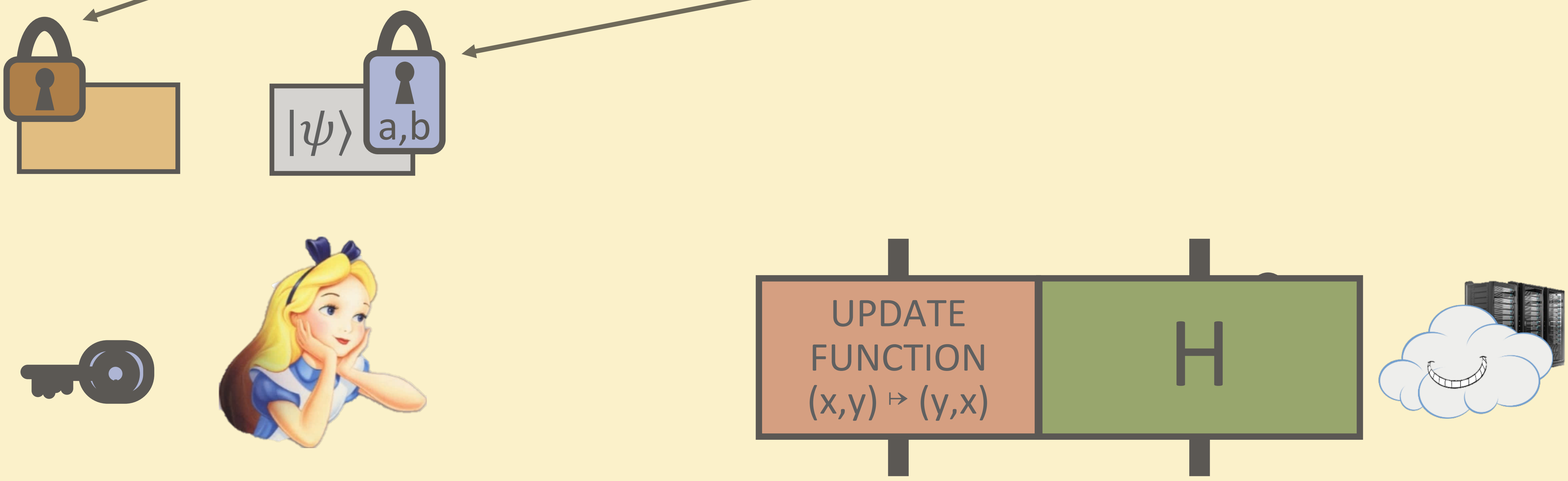


Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

CLIFFORD SCHEME

Classical homomorphic encryption

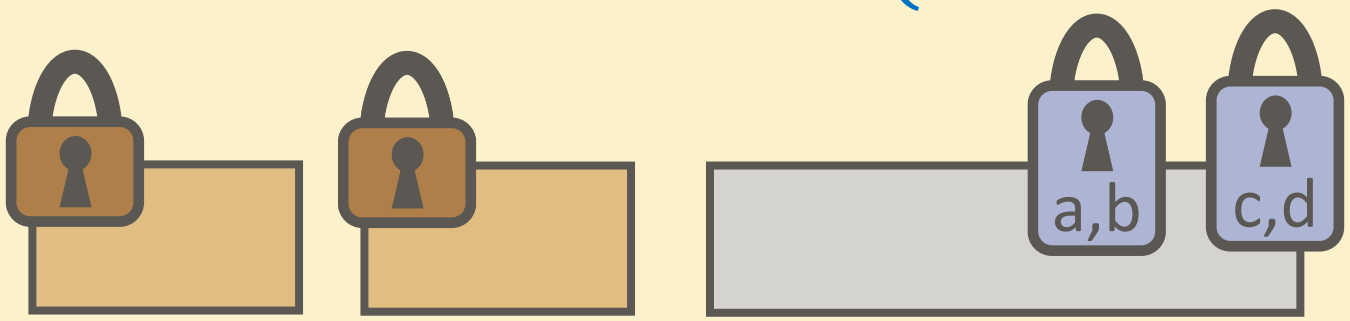
Quantum one-time pad



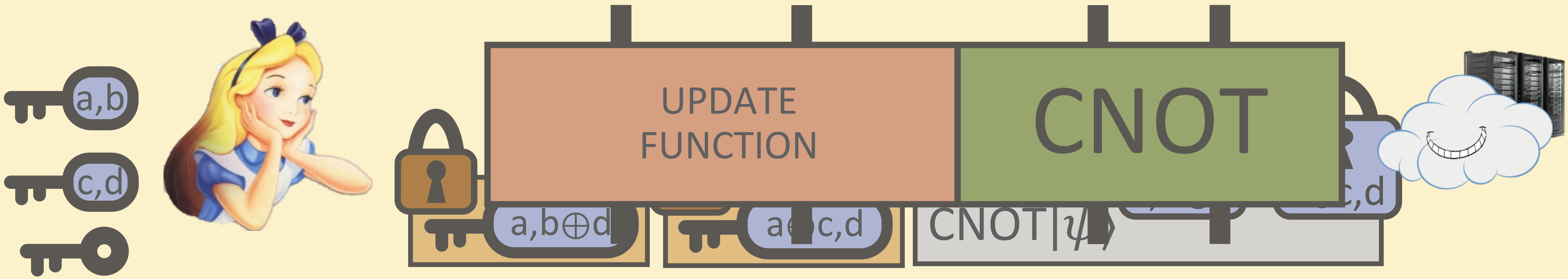
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

CLIFFORD SCHEME: CNOT

$$(X^aZ^b \otimes X^cZ^d)|\psi\rangle$$



2 qubit $|\psi\rangle$



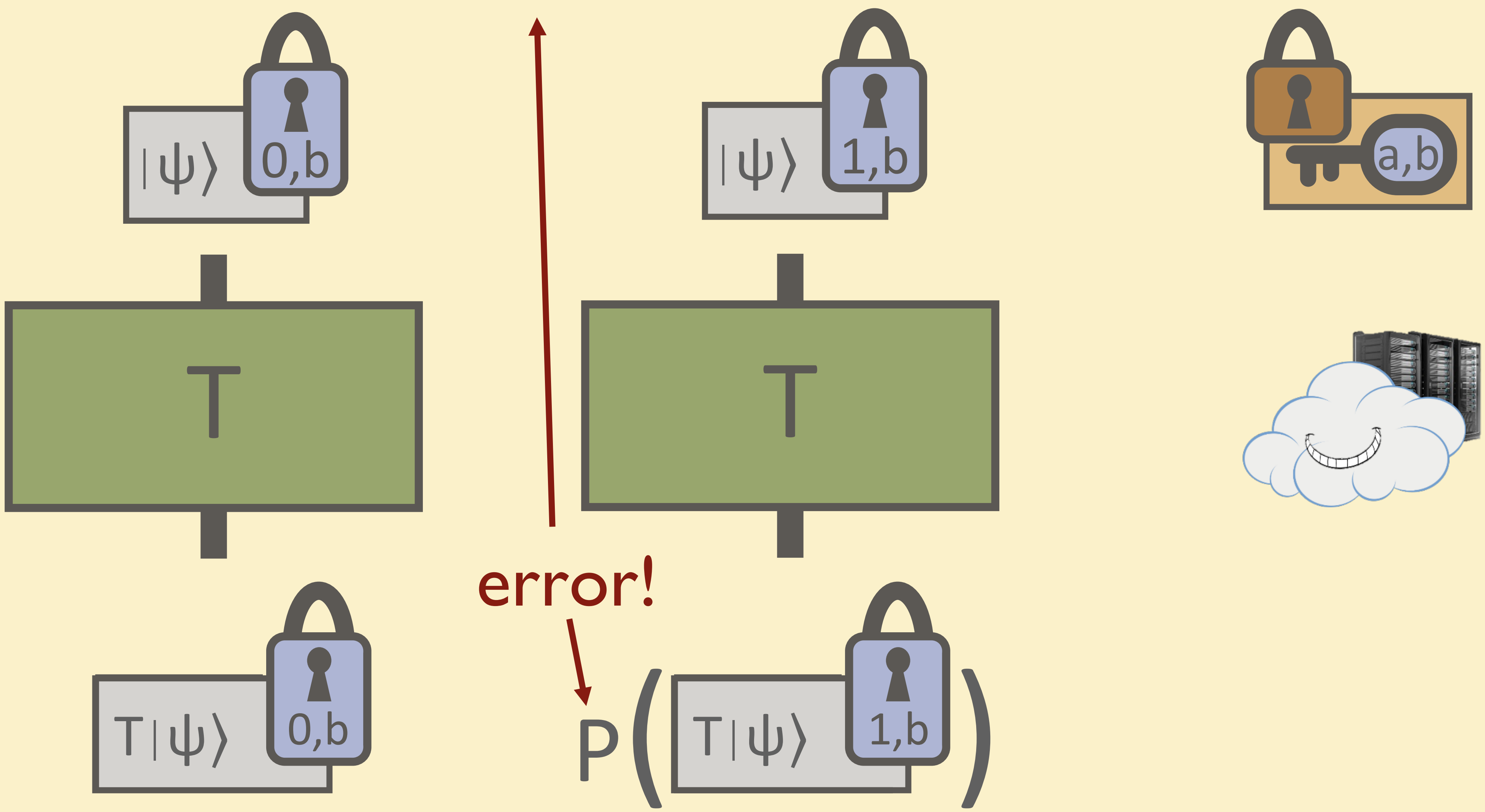
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

THE CHALLENGE: T GATE

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

TZ=ZT

TX=PXT



how to apply correction P^{-1} iff $a = 1$?

PREVIOUS RESULTS: OVERVIEW

	homomorphic for	compactness	security
Not encrypting	Quantum circuits	yes	no
Quantum OTP	No	yes	inf theoretic
append evaluation description	Quantum circuits	Complexity of Dec prop to (# gates)	yes
Clifford Scheme	Clifford circuits	yes	computational
[BJ15]: AUX	QCircuits with constant T-depth	yes	computational
[BJ15]: EPR	Quantum circuits	Comp of Dec is prop to (#T-gates)^2	computational
[OTF15]	QCircuits with constant #T-gates	yes	inf theoretic
Our result	QCircuits of polynomial size (levelled FHE)	yes	computational

(comparison based on Stacey Jeffery's slides)

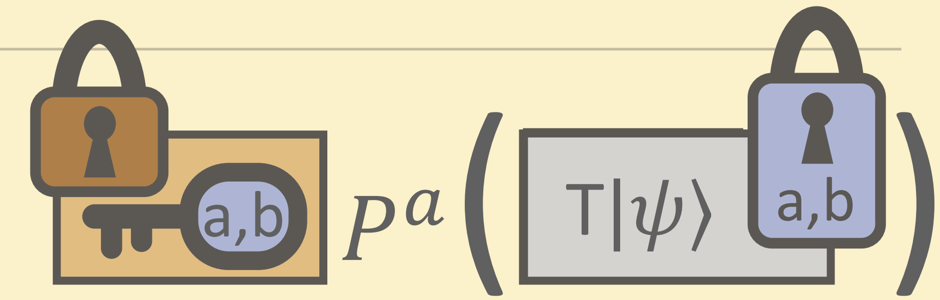
[BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015
[OTF15] Y. Ouyang, S-H. Tan, J. Fitzsimons. Quantum homomorphic encryption from quantum codes. arxiv:1508.00938

✓ HOMOMORPHIC ENCRYPTION

✓ PREVIOUS RESULTS: CLIFFORD SCHEME

3. NEW SCHEME

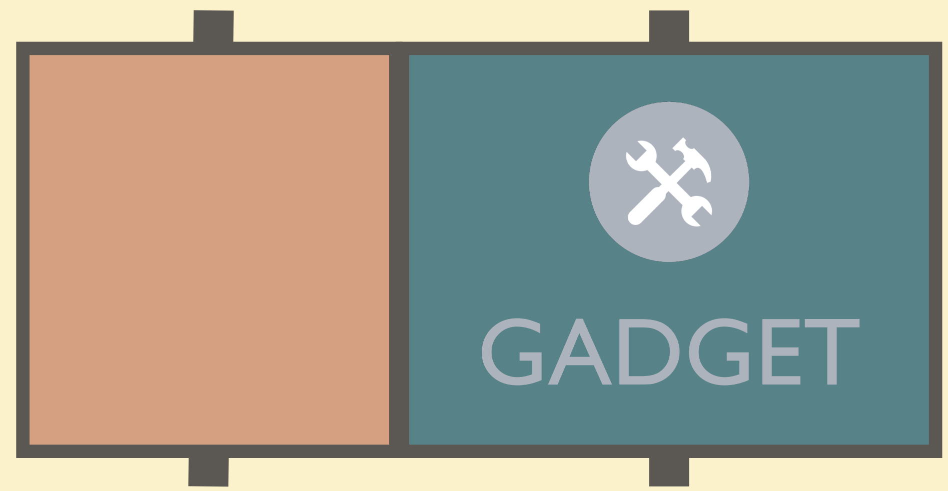
ERROR-CORRECTION 'GADGET'



- Build a 'gadget' that applies P^{-1} iff a = 1

- Apply correction iff :

  a=decrypt() = 1



Properties:

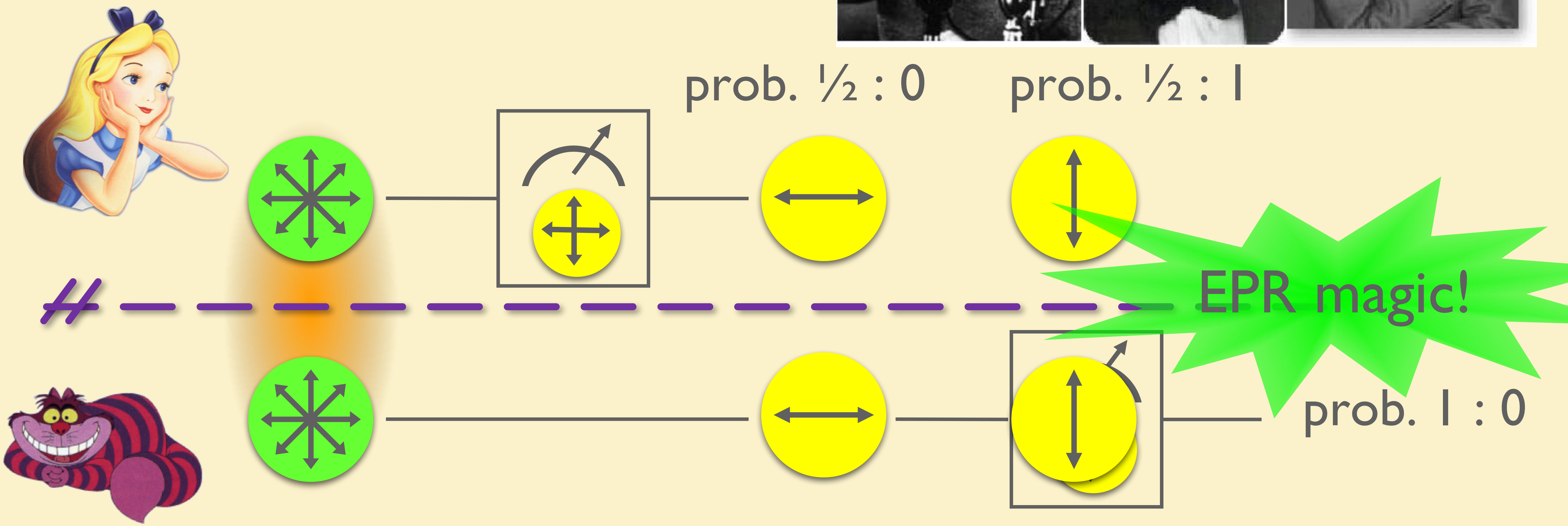
- Efficiently constructable
- Destroyed after single use

EXCURSION 1

Quantum Information Theory: Quantum Teleportation

EPR PAIRS

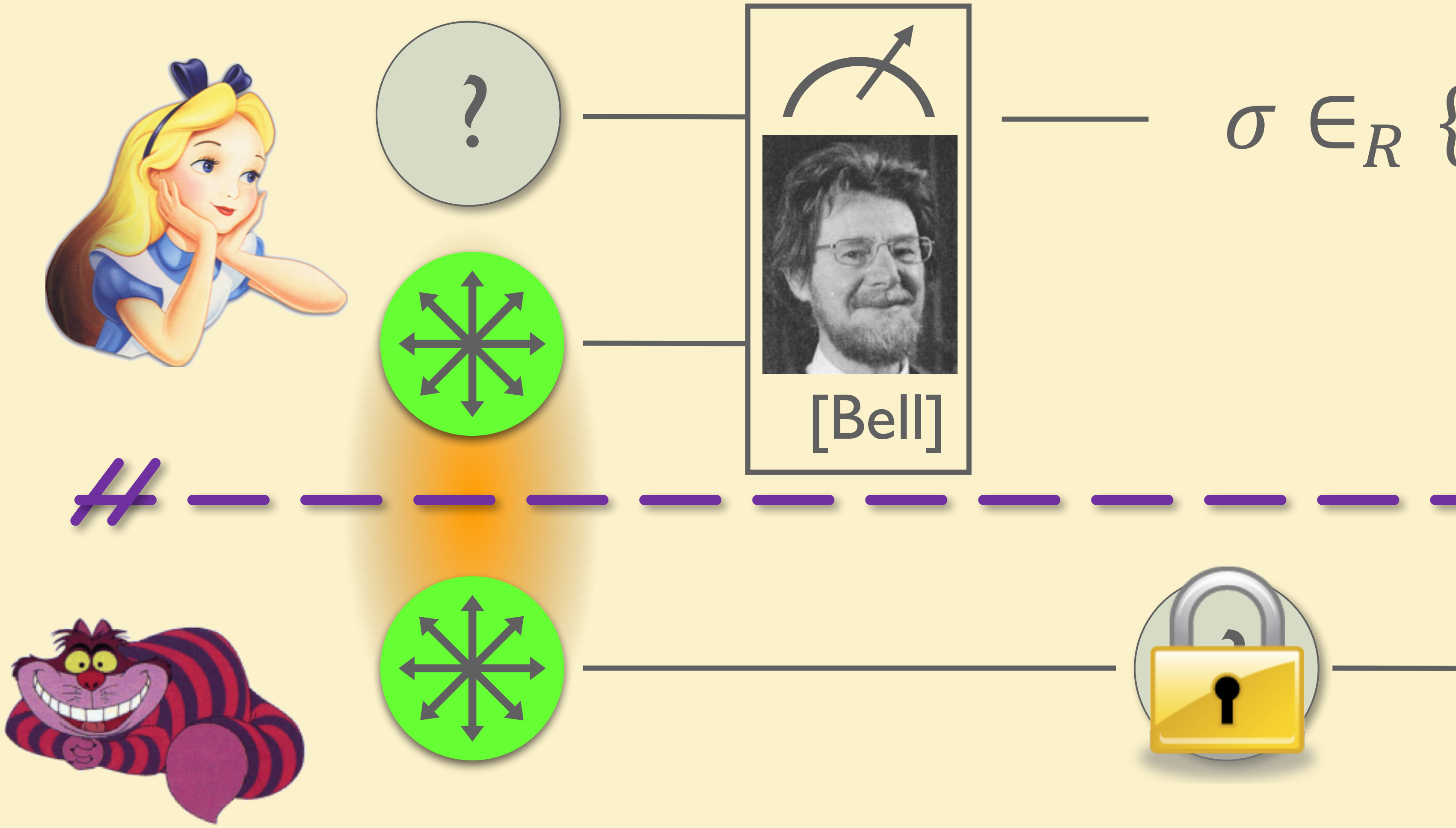
[Einstein Podolsky Rosen 1935]



- “spukhafte Fernwirkung” (spooky action at a distance)
- EPR pairs do not allow to communicate
  (no contradiction to relativity theory)
- can provide a shared random bit

QUANTUM TELEPORTATI

[Bennett Brassard Crépeau Jozsa Peres Wootters 19



- Bob's qubit is encrypted with quantum one-time pad
- Bob can only recover the teleported qubit after receiving the classical information σ

EXCURSION 2

Theoretical Computer Science: Barrington's Theorem

PERMUTATION BRANCHING PROGRAM

$f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$

- computes some Boolean function f(x,y)
- list of instructions: permutations of {1,2,3,4,5}

x_i	0: $\pi \in S_5$
	1: $\sigma \in S_5$
y_j	0: $\pi' \in S_5$
	1: $\sigma' \in S_5$
x_k	0: $\pi'' \in S_5$
	1: $\sigma'' \in S_5$

⋮

output: $\ldots \circ \sigma'' \circ \sigma' \circ \pi$

- id $\Rightarrow f(x,y) = 0$
- (fixed) cycle $\Rightarrow f(x,y) = 1$

length: # of instructions

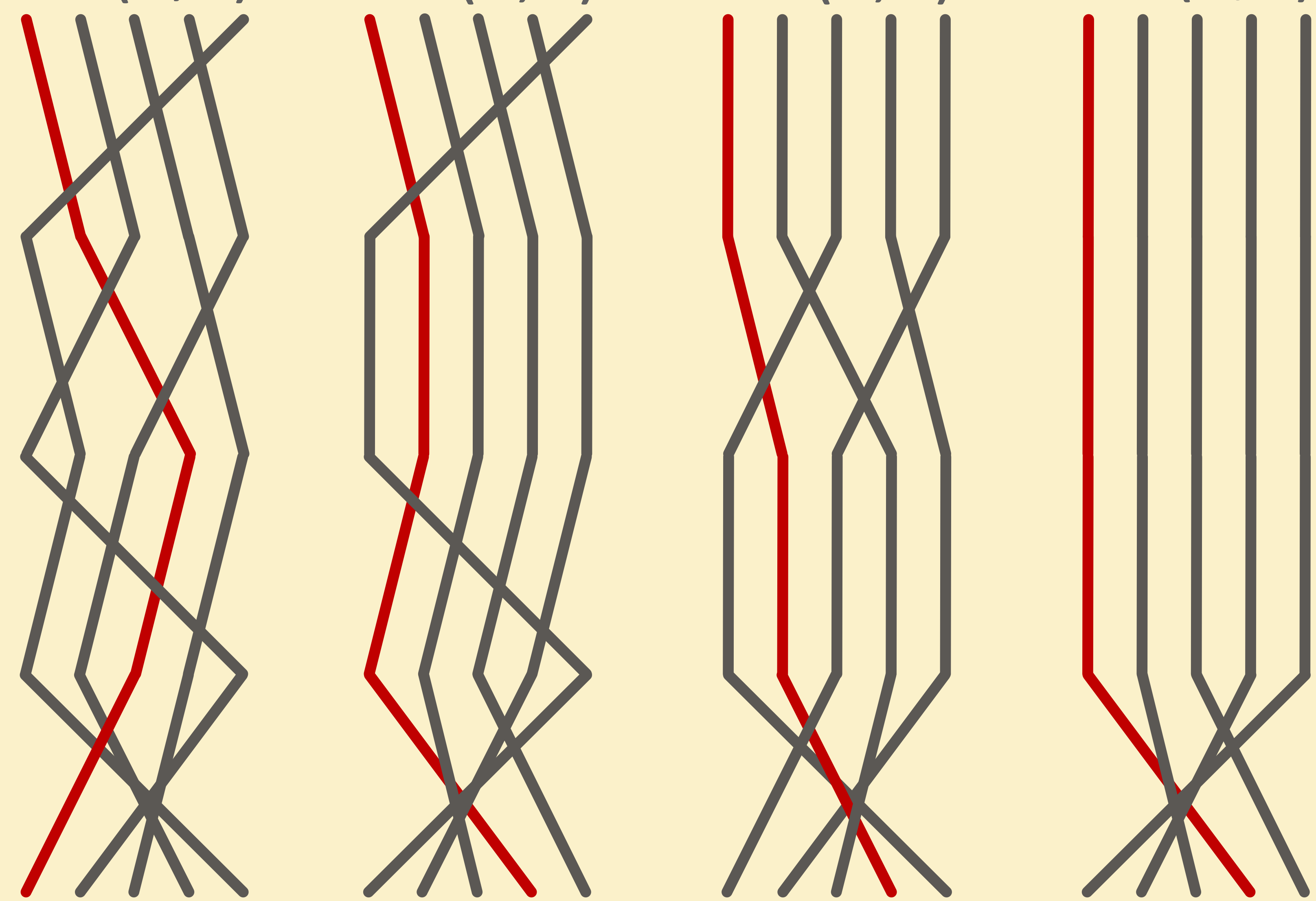
EXAMPLE PBP OR(x,y)

x	y	OR(x,y)
0	0	0
0	1	1
1	0	1
1	1	1

length 4:

x	0: (12345)	1: id
y	0: (12453)	1: id
x	0: (54321)	1: id
y	0: (15243)	1: (14235)

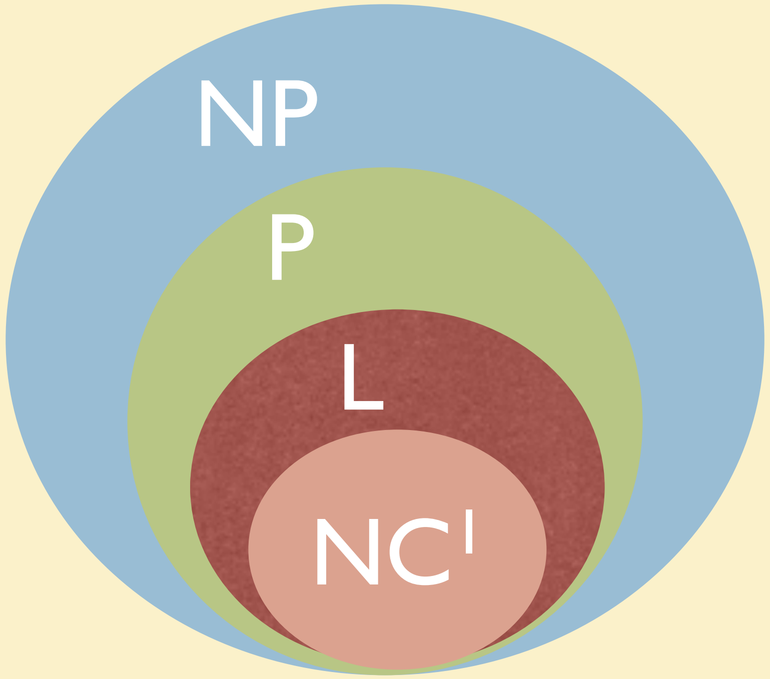
	OR(0,0)	OR(0,1)	OR(1,0)	OR(1,1)



output:	id	(14235)	(14235)	(14235)
	0	1	1	1

BARRINGTON'S THEOREM (1989)

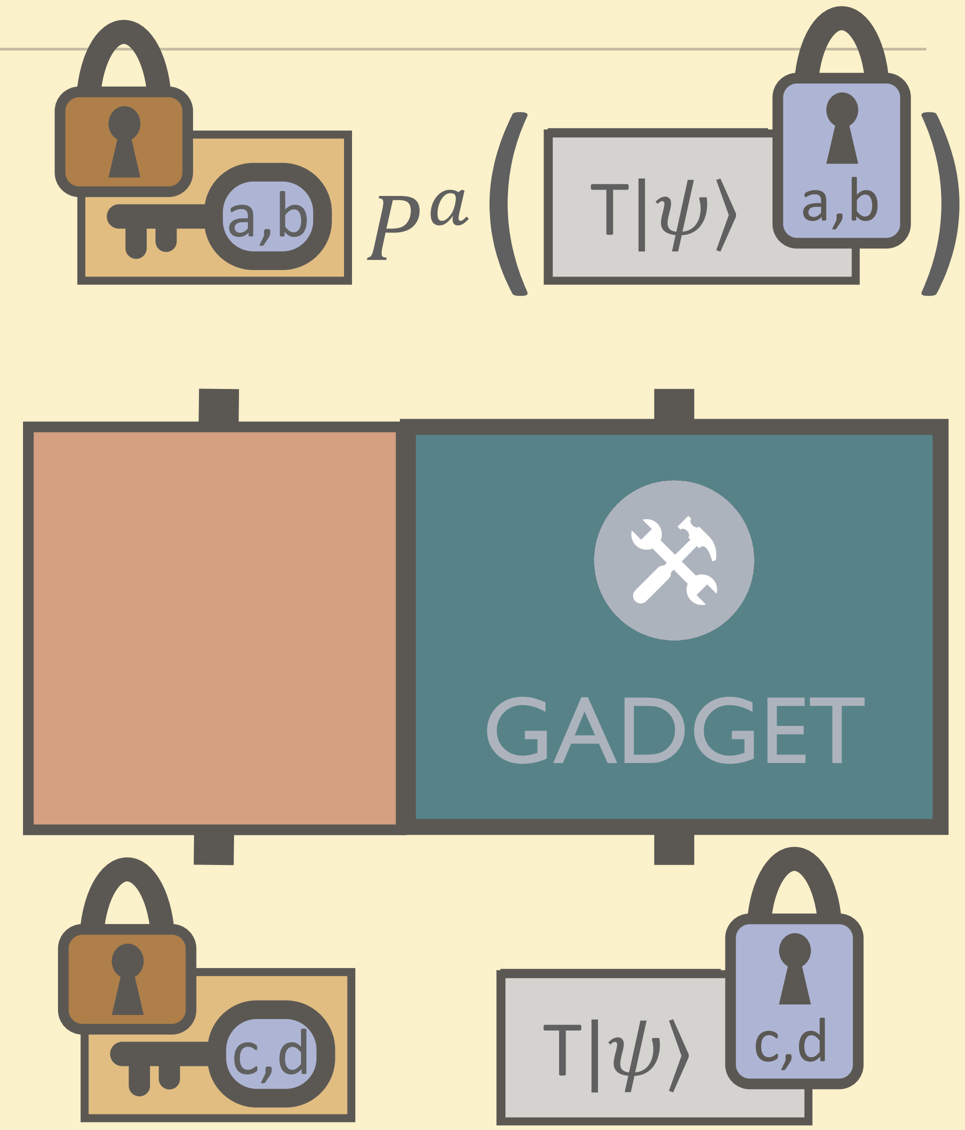
Theorem (variation): if f : $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ is in NC^1, then there exists a width-5 permutation branching program for f with length polynomial in n.



Classical homomorphic decryption functions happen to be in NC^1… [BV11]

[Barrington 89] Bounded-Width Polynomial-Size Branching Programs Recognize Exactly Those Languages in NC1, J. Comput. Syst. Sci. 38 (1): 150–164, 1989
[BV11] Z. Brakerski, V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. FOCS 2011

ERROR-CORRECTION GADGET



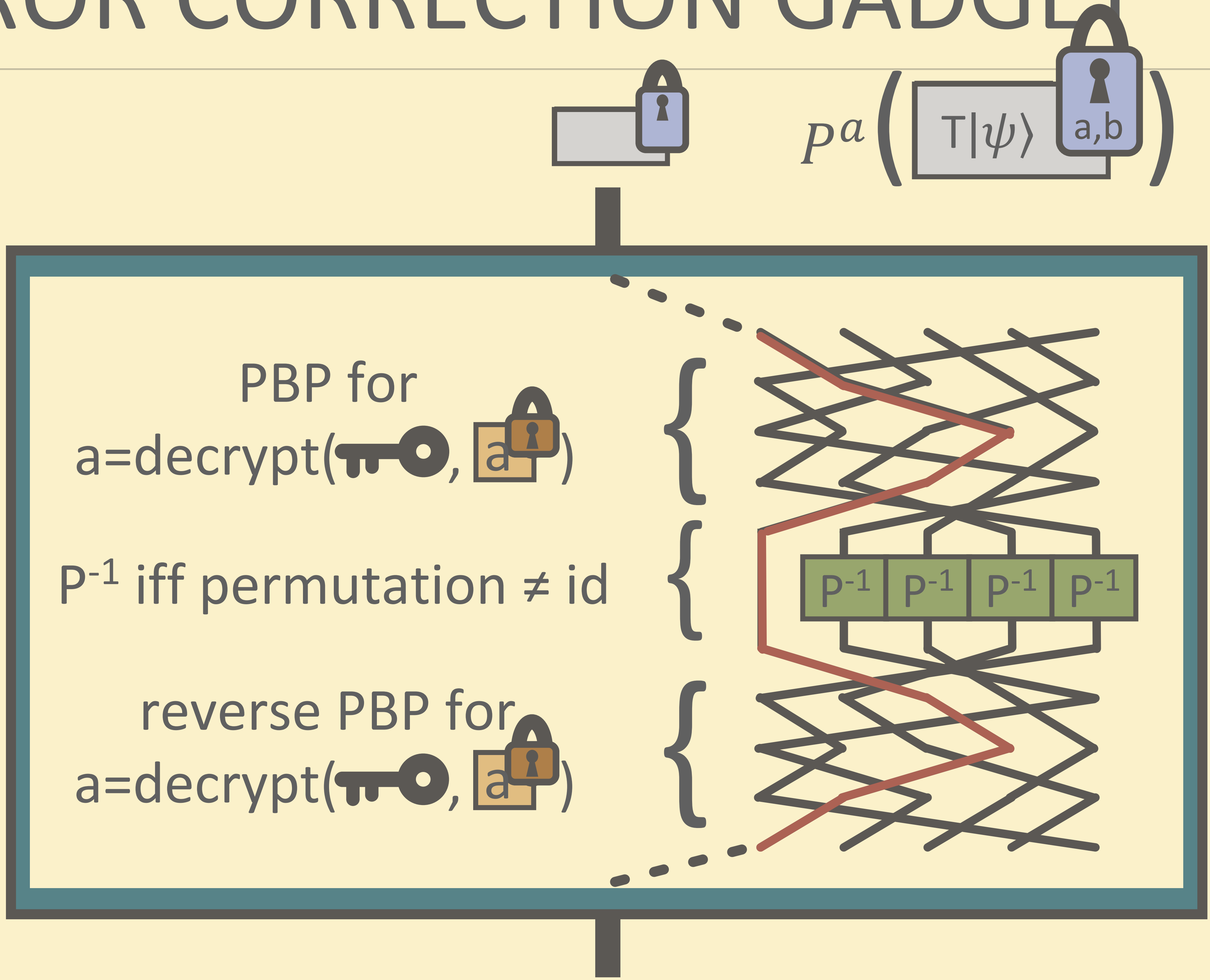
- Build a ‘gadget’ that applies P^{-1} iff a = 1

- Apply correction iff

a = decrypt(, a) = 1

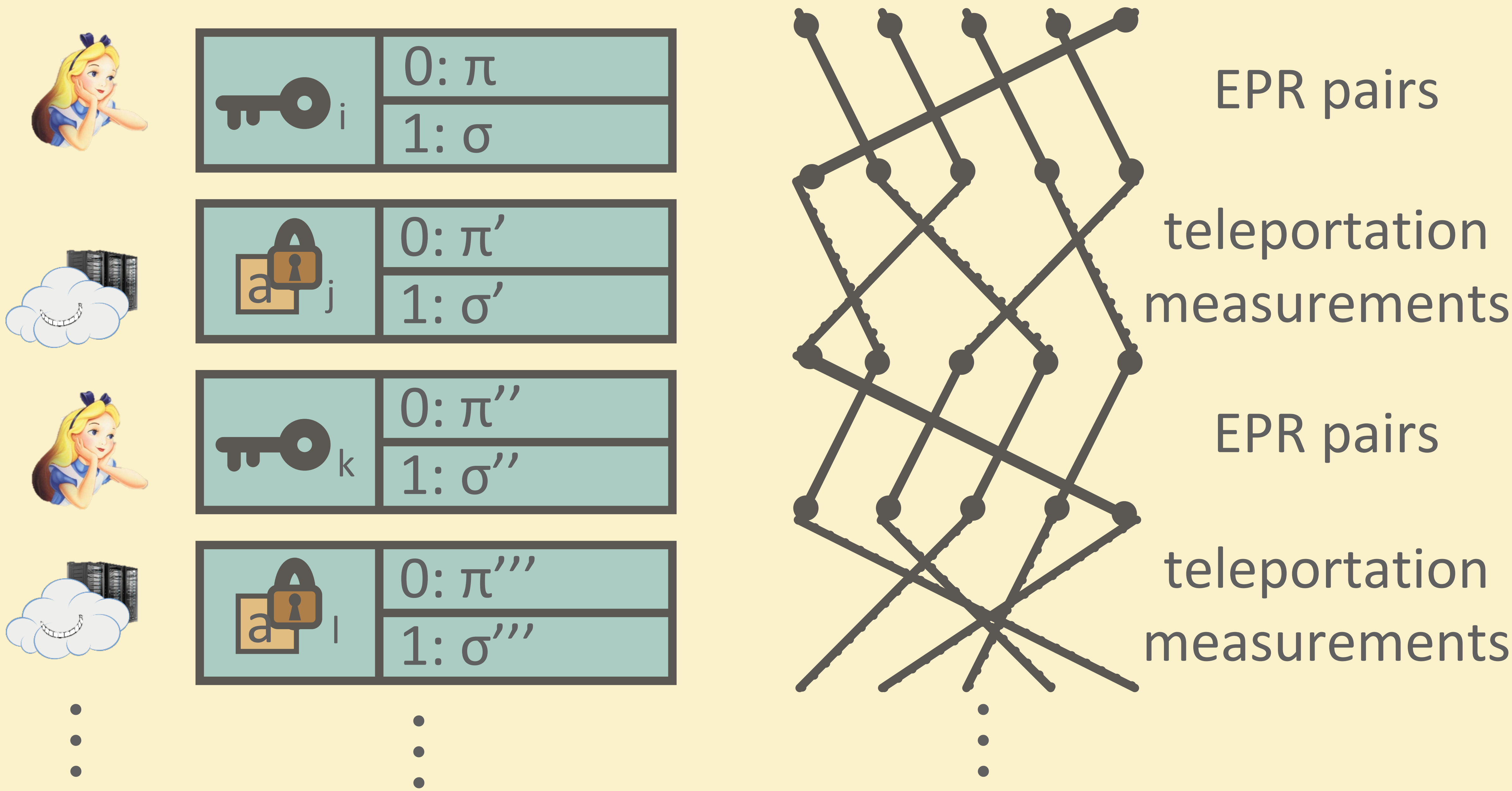
has a poly-size PBP

ERROR CORRECTION GADGET

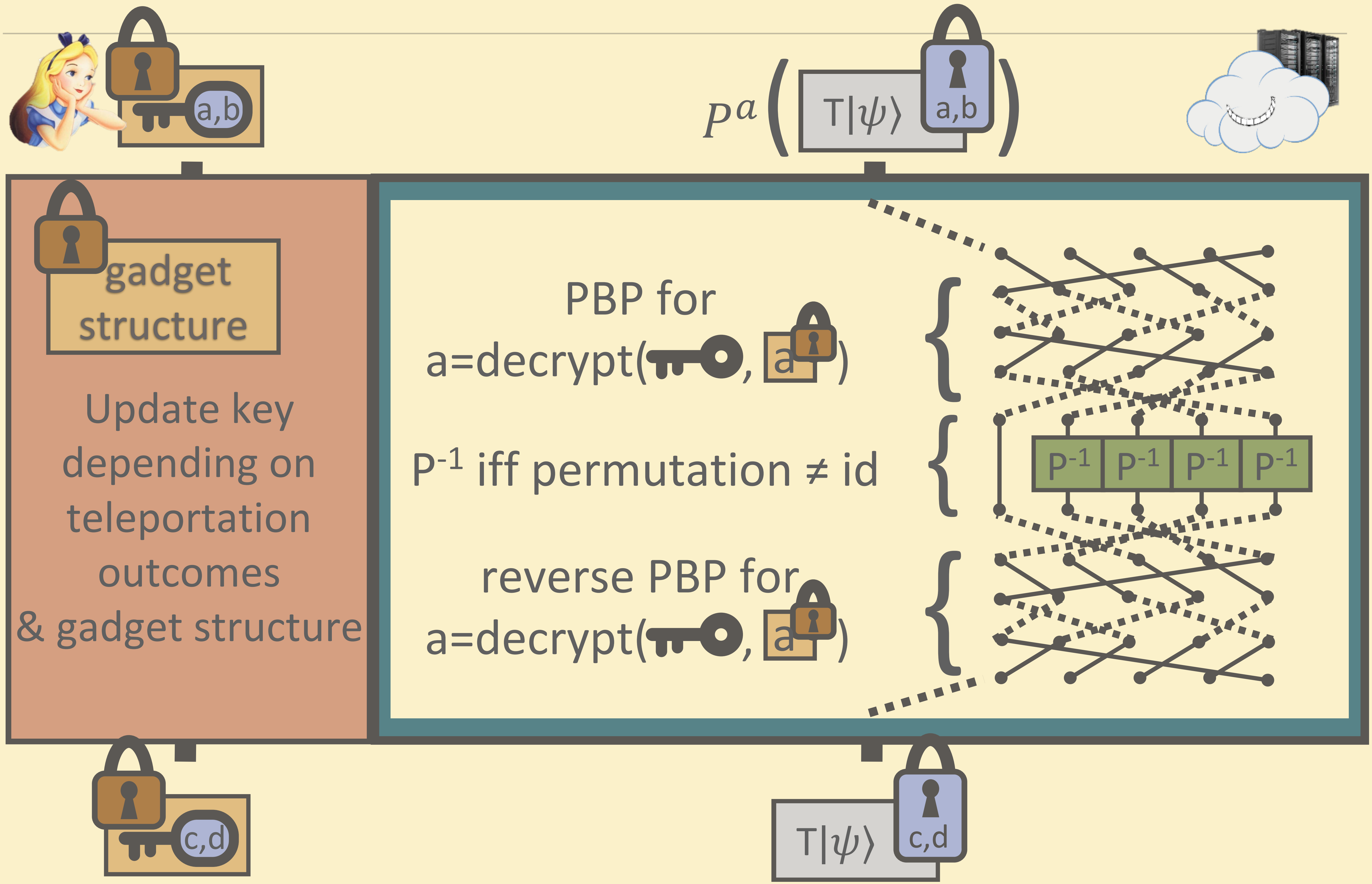


ERROR CORRECTION GADGET

Branching program for decrypt( )



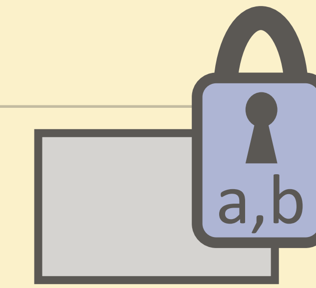
ERROR CORRECTION GADGET



SECURITY

All quantum information: quantum one-time pad

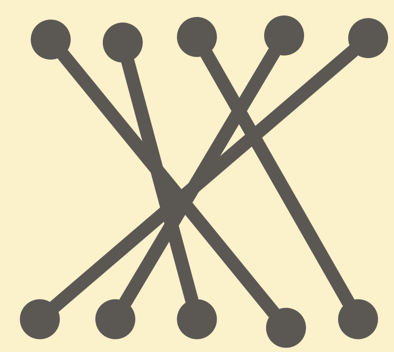
(perfectly secure if classical info is hidden)



Gadget structure, each ‘connection’:

Random choice out of 4 Bell states

(perfectly secure if classical info is hidden)



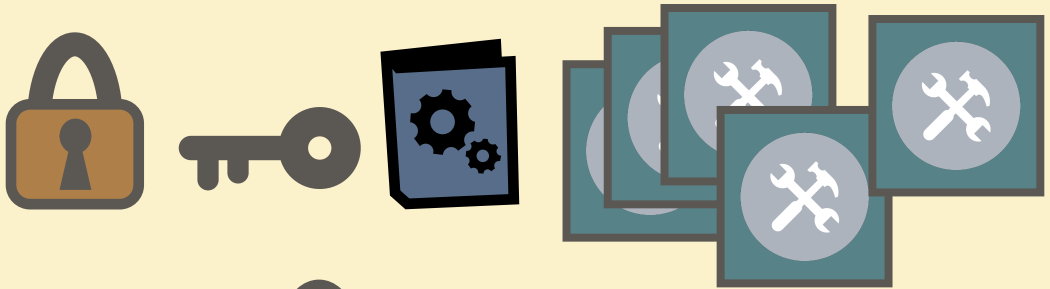
All classical information: classical homomorphic scheme

Security of classical scheme is the only assumption

NEW SCHEME: OVERVIEW

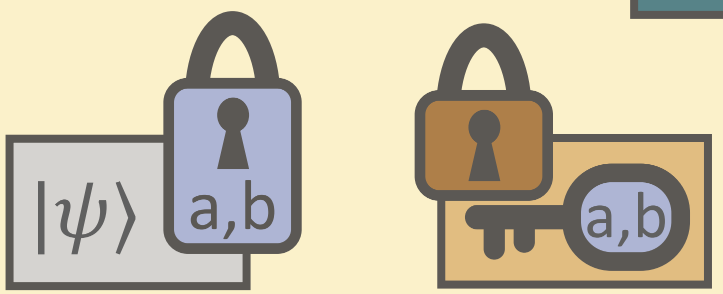
KEY GENERATION

- classical keys
- gadgets



ENCRYPTION

- apply quantum one-time pad
- classically encrypt pad keys

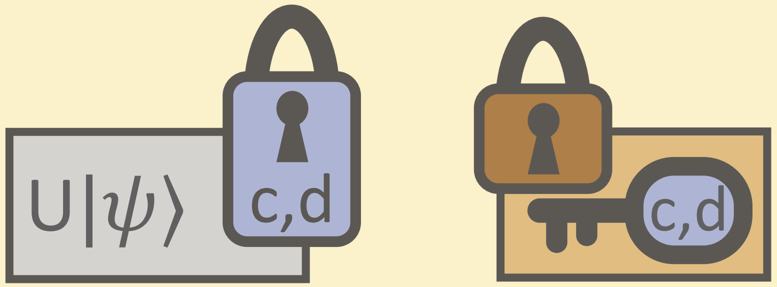


EVALUATION

- after H / P / CNOT : classically update keys
- after T : use 

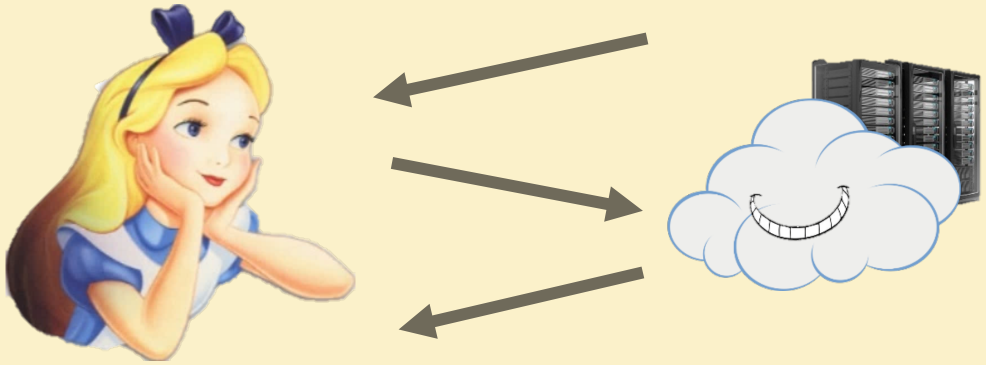
DECRYPTION

- classically decrypt pad keys
- remove quantum one-time pad



APPLICATIONS

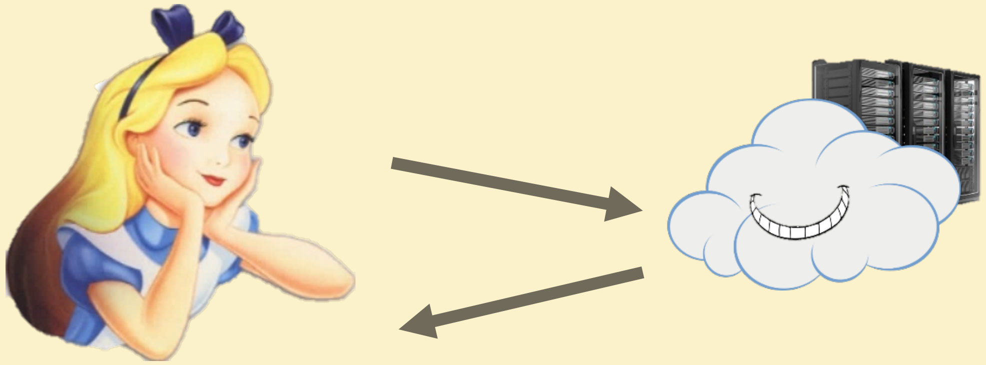
- Delegated quantum computation in two rounds
  - No memory needed on Alice's side
  - "Low-tech" generation of gadgets
- Gadget generation on demand
- Circuit privacy



FUTURE WORK

- non-leveled QFHE?

- verifiable delegated quantum computation



- quantum obfuscation?
- …

THANK YOU!