QUANTUM HOMOMORPHIC ENCRYPTION

Yfke Dulek

(joint work with Christian Schaffner and Florian Speelman)

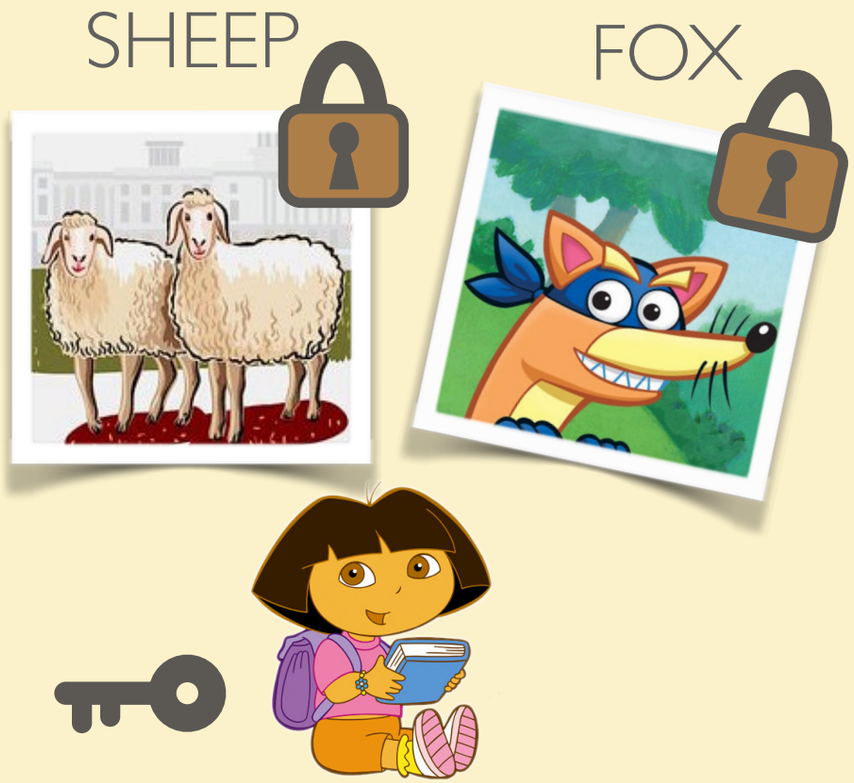
Institute for Logic, Language and Computation (ILLC)
University of Amsterdam

QuSoft
Research Center for Quantum Software

CWI
Centrum Wiskunde & Informatica

QCrypt 2016

EXAMPLE: IMAGE TAGGING



1. HOMOMORPHIC ENCRYPTION

2. PREVIOUS RESULTS

3. NEW RESULT

QUANTUM HOMOMORPHIC ENCRYPTION

KEY GENERATION

public key

secret key

quantum state

evaluation key

ENCRYPTION (secure)

quantum data

EVALUATION

quantum circuit

DECRYPTION (compact)

✓ HOMOMORPHIC ENCRYPTION

2. PREVIOUS RESULTS

3. NEW RESULT

PREVIOUS RESULTS: OVERVIEW

- Classical homomorphic encryption: solved [G09]

  under (quantum-safe) computational assumptions (e.g. LWE)

- Quantum homomorphic encryption: only partial results

C. Gentry: Fully homomorphic encryption using ideal lattices. STOC'09

PREVIOUS RESULTS: OVERVIEW

	homomorphic for	compact?	security
Not encrypting	all circuits	yes	none
Quantum one-time pad	none	yes	inf theoretic
Append circuit description	all circuits	no: proportional to (# gates)	inf theoretic
Clifford Scheme	Clifford circuits	yes	computational
[BJ15]: AUX	circuits with constant T-depth	yes	computational
[BJ15]: EPR	all circuits	no: proportional to (# T-gates)^2	computational
[OTF15]	circuit with constant # of T-gates	yes	inf theoretic
Our result	all circuits of polynomial size (levelled QHE)	yes	computational

Clifford gates: $P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ $H = 1/\sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Also need: $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

(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

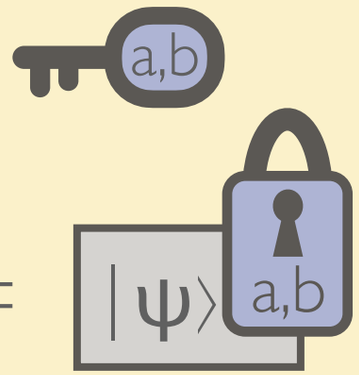
[YPDF14] L. Yu, C. Pérez-Delgado, J. Fitzsimons. Limitations on information-theoretically-secure quantum homomorphic encryption.

CLIFFORD SCHEME: P, H, CNOT

Ingredient 1: quantum one-time pad

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

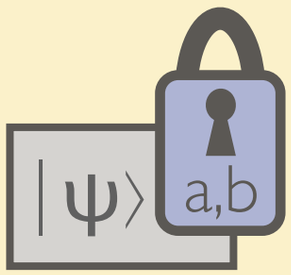
$$|\psi\rangle \mapsto X^a Z^b |\psi\rangle$$



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

Ingredient 2: classical homomorphic encryption

CLIFFORD SCHEME: P, H, CNOT

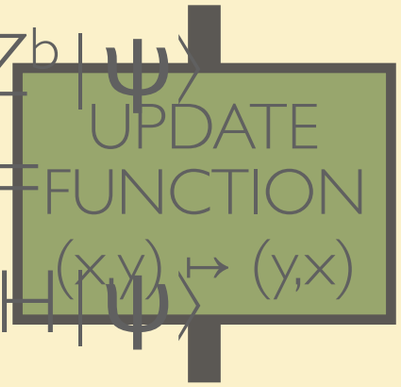


=

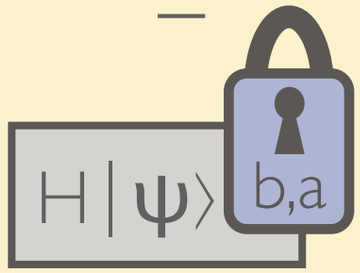
$HX^aZ^b|\psi\rangle$

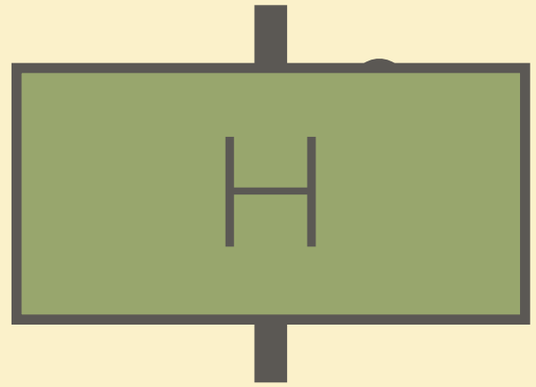
=

$X^bZ^aH|\psi\rangle$



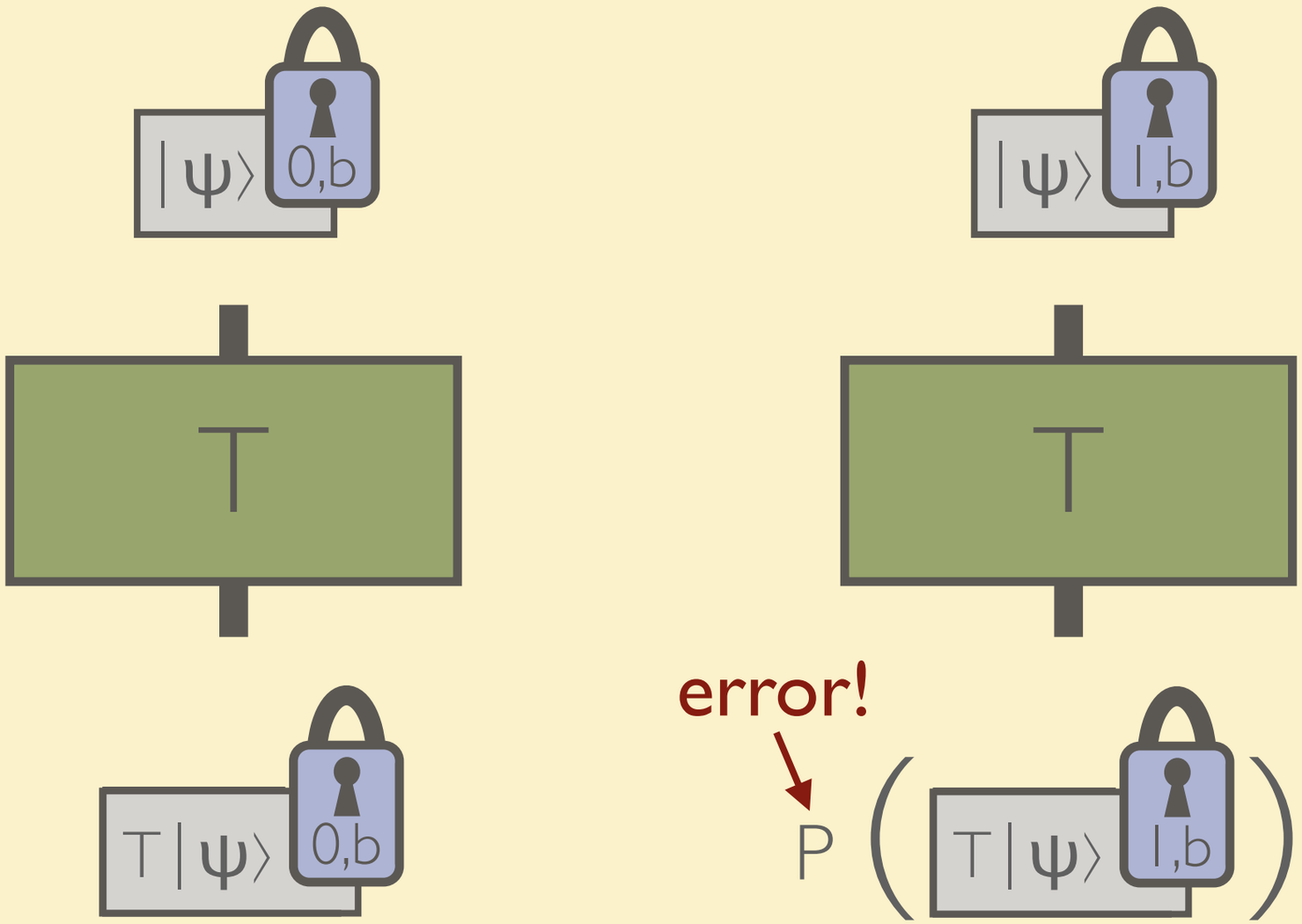
=





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

THE CHALLENGE: T GATE



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

✓ HOMOMORPHIC ENCRYPTION

✓ PREVIOUS RESULTS

3. NEW RESULT

NEW RESULT

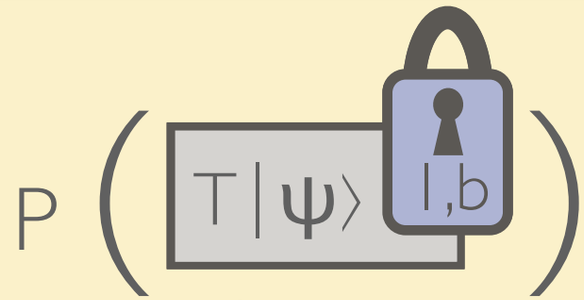
	homomorphic for	compact?	security
Not encrypting	all circuits	yes	none
Quantum one-time pad	none	yes	inf theoretic
Append circuit description	all circuits	no: proportional to (# gates)	inf theoretic
Clifford Scheme	Clifford circuits	yes	computational
[BJ15]: AUX	circuits with constant T-depth	yes	computational
[BJ15]: EPR	all circuits	no: proportional to (# T-gates)^2	computational
[OTF15]	circuit with constant # of T-gates	yes	inf theoretic
Our result	circuits of polynomial size (levelled QFHE)	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
[YPDF14] L. Yu, C. Pérez-Delgado, J. Fitzsimons. Limitations on information-theoretically-secure quantum homomorphic encryption.

ERROR-CORRECTION GADGET

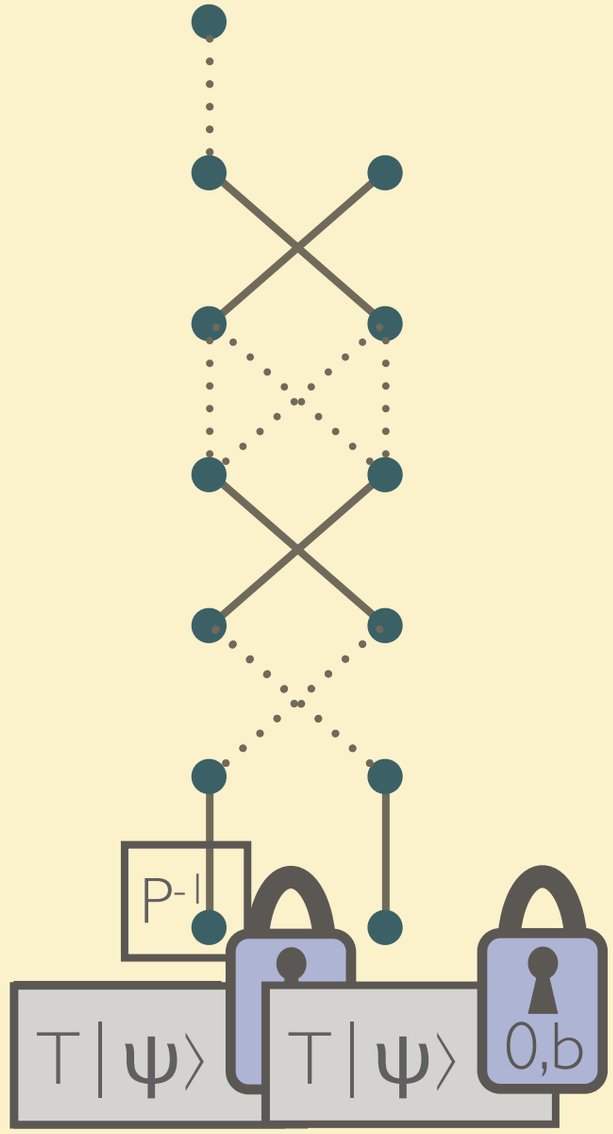
A quantum state (part of the evaluation key):



- Generation: entangle pairwise, according to 
- Usage: Bell measurements according to 

The gadget computes a permutation branching program for decrypt(

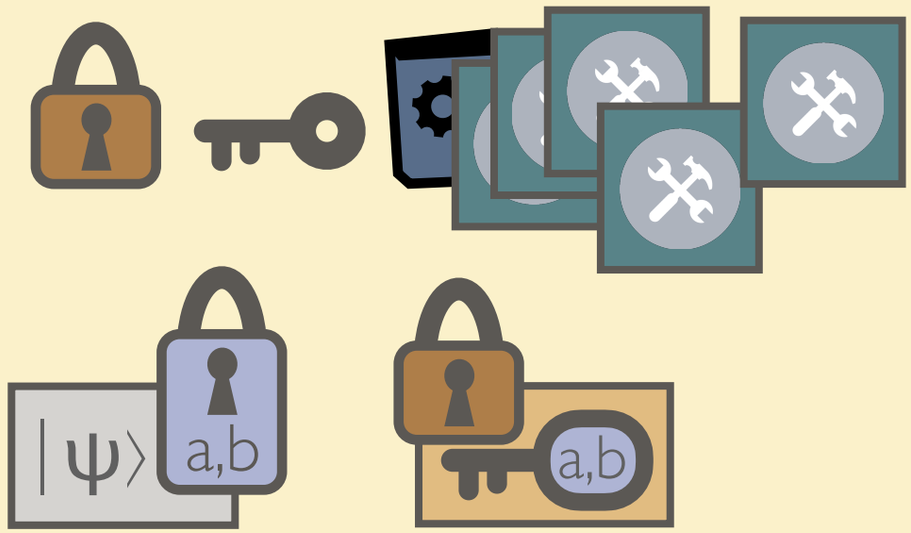
)



NEW SCHEME: OVERVIEW

KEY GENERATION

- classical keys
- gadgets



ENCRYPTION

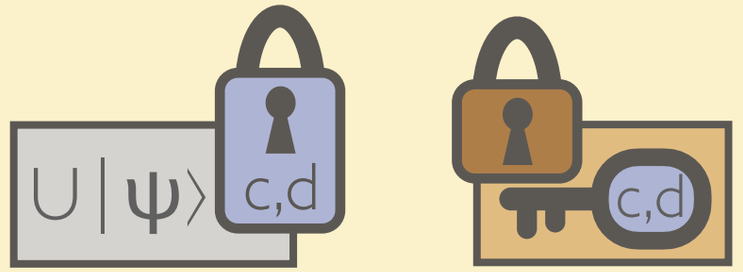
- apply quantum one-time pad
- classically encrypt pad keys

EVALUATION

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

DECRYPTION

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



FUTURE WORK

- non-leveled QFHE?
- multiparty quantum computation?
- quantum obfuscation?
- …


THANK YOU!