QUANTUM HOMOMORPHIC ENCRYPTION

Christian Schaffner

(joint work with Yfke Dulek and Florian Speelman)

http://arxiv.org/abs/1603.09717

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

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

QuSoft
Research Center for Quantum Software

CWI
Centrum Wiskunde & Informatica

Trustworthy Quantum Information 2016, Shanghai, China, Wednesday 29 June 2016

EXAMPLE: IMAGE TAGGING

EXAMPLE: IMAGE TAGGING

EXAMPLE: IMAGE TAGGING

EXAMPLE: IMAGE TAGGING

SKYLINE

JED

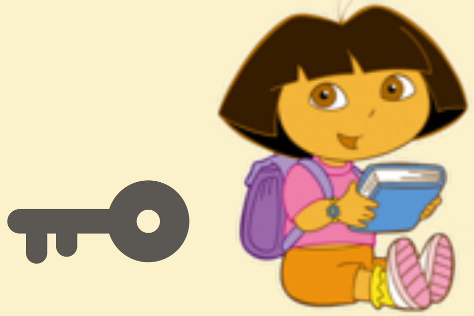
EXAMPLE: IMAGE TAGGING

EXAMPLE: IMAGE TAGGING

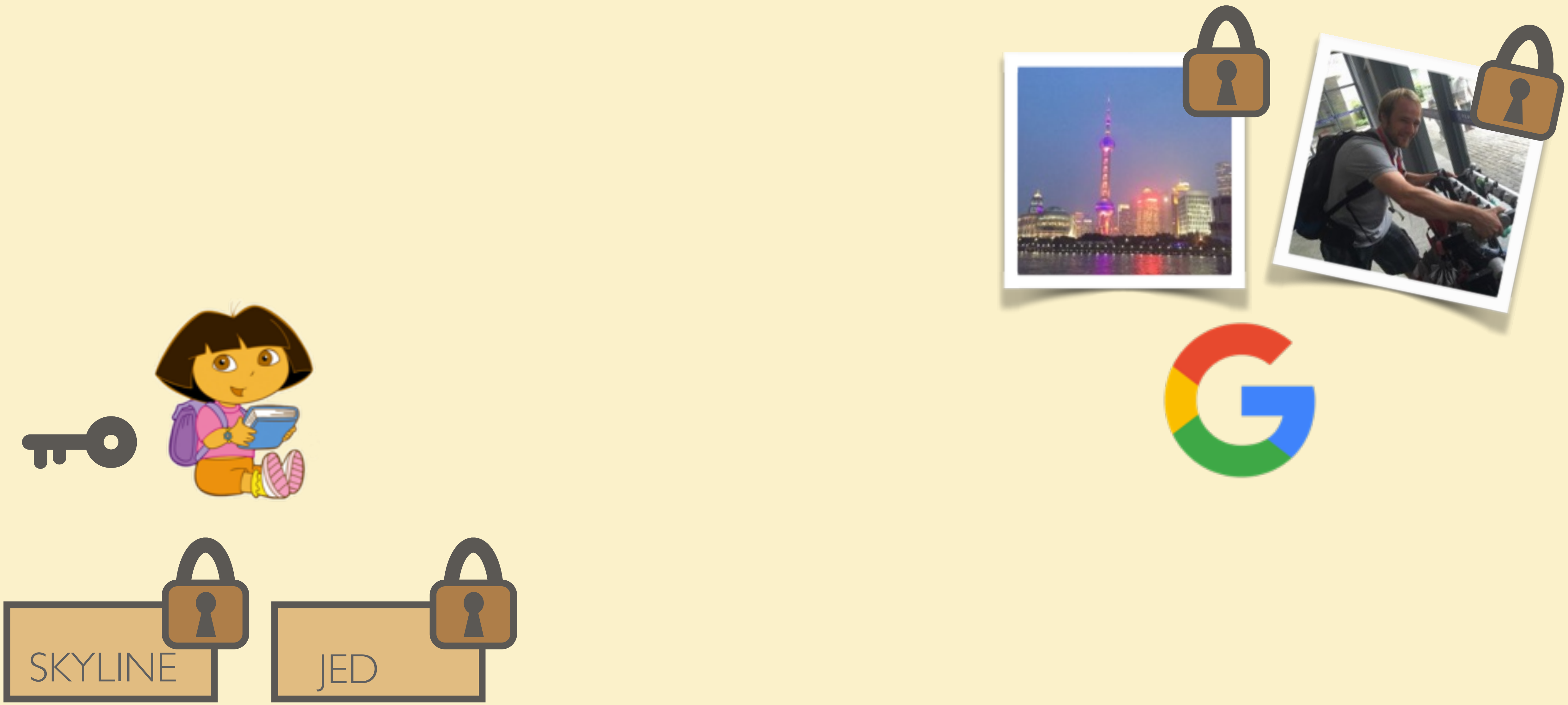
EXAMPLE: IMAGE TAGGING

EXAMPLE: IMAGE TAGGING

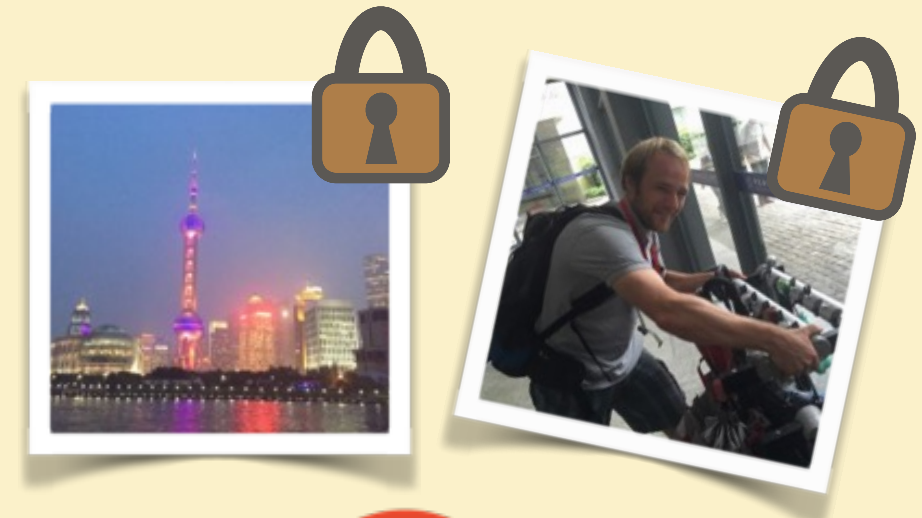
EXAMPLE: IMAGE TAGGING

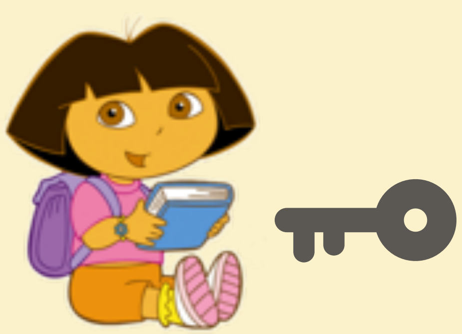


EXAMPLE: IMAGE TAGGING



EXAMPLE: IMAGE TAGGING





SKYLINE

JED

1. HOMOMORPHIC ENCRYPTION
2. PREVIOUS RESULTS
3. NEW RESULT

HOMOMORPHIC ENCRYPTION

HOMOMORPHIC ENCRYPTION

KEY GENERATION

HOMOMORPHIC ENCRYPTION

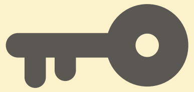
KEY GENERATION

public key

HOMOMORPHIC ENCRYPTION

KEY GENERATION

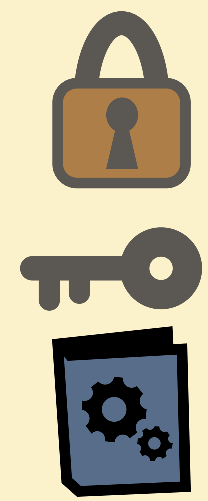
public key



secret key

HOMOMORPHIC ENCRYPTION

KEY GENERATION



public key

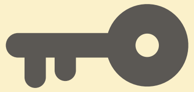
secret key

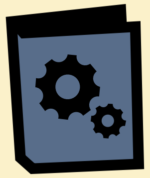
evaluation key

HOMOMORPHIC ENCRYPTION

KEY GENERATION


public key

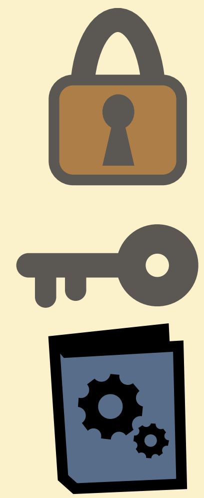

secret key


evaluation key

ENCRYPTION

HOMOMORPHIC ENCRYPTION

KEY GENERATION

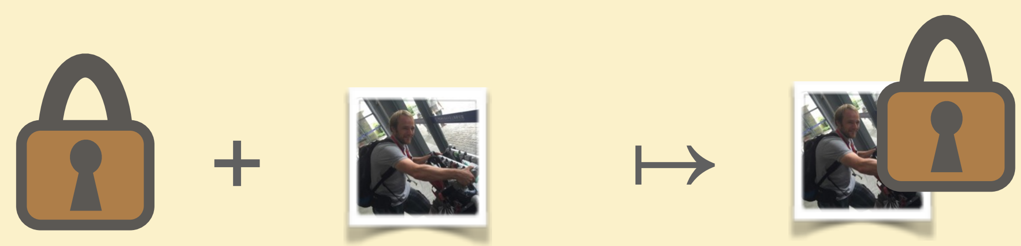


public key

secret key

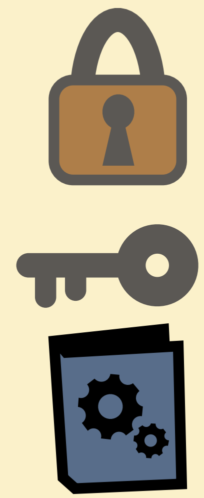
evaluation key

ENCRYPTION



HOMOMORPHIC ENCRYPTION

KEY GENERATION

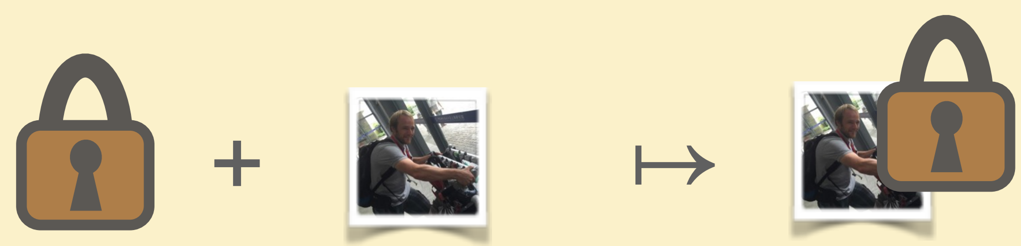


public key

secret key

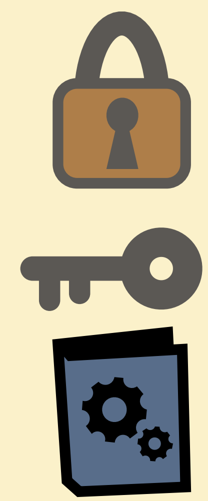
evaluation key

ENCRYPTION
(secure)



HOMOMORPHIC ENCRYPTION

KEY GENERATION



public key

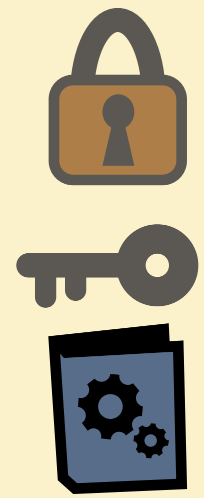
secret key

evaluation key

ENCRYPTION
(secure)

HOMOMORPHIC ENCRYPTION

KEY GENERATION

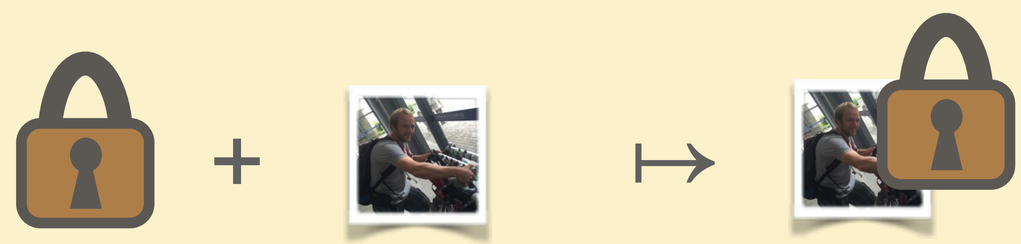


public key

secret key

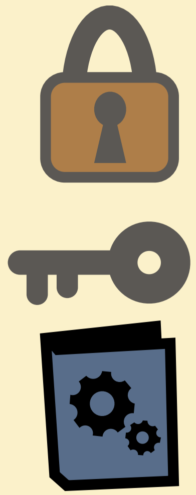
evaluation key

ENCRYPTION
(secure)



HOMOMORPHIC ENCRYPTION

KEY GENERATION

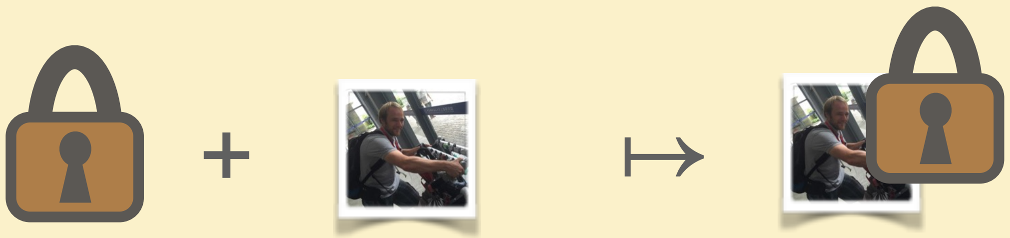


public key

secret key

evaluation key

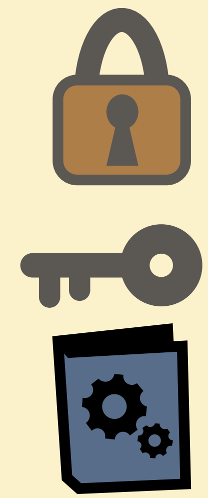
ENCRYPTION
(secure)



EVALUATION

HOMOMORPHIC ENCRYPTION

KEY GENERATION

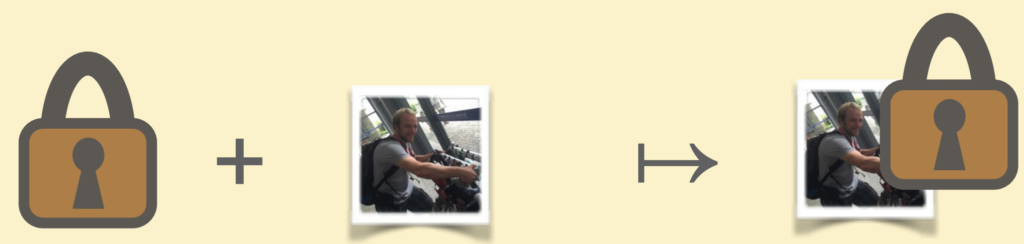


public key

secret key

evaluation key

ENCRYPTION
(secure)



EVALUATION

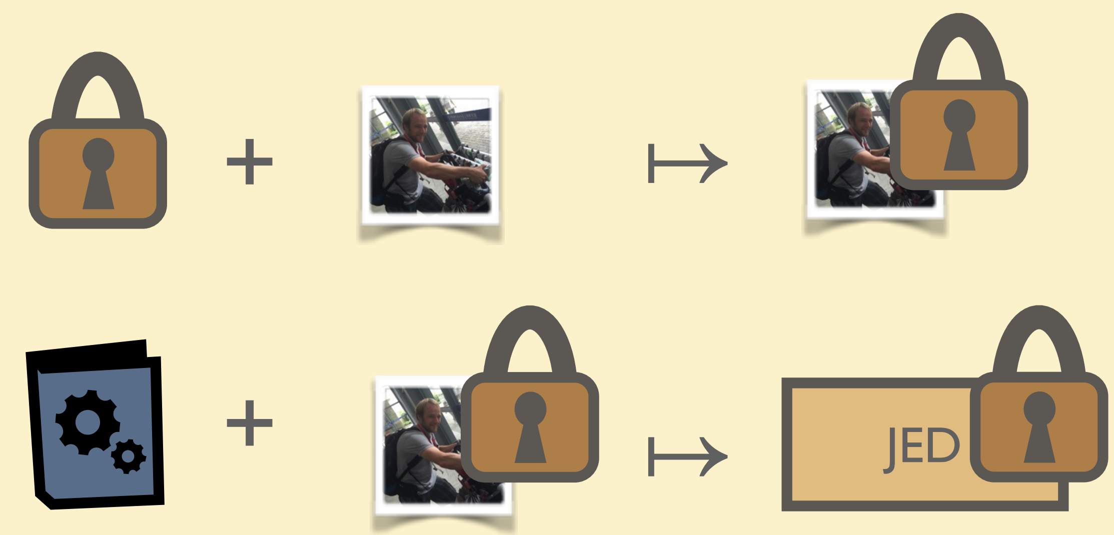
HOMOMORPHIC ENCRYPTION

KEY GENERATION

- public key
- secret key
- evaluation key

ENCRYPTION
(secure)

EVALUATION



DECRYPTION

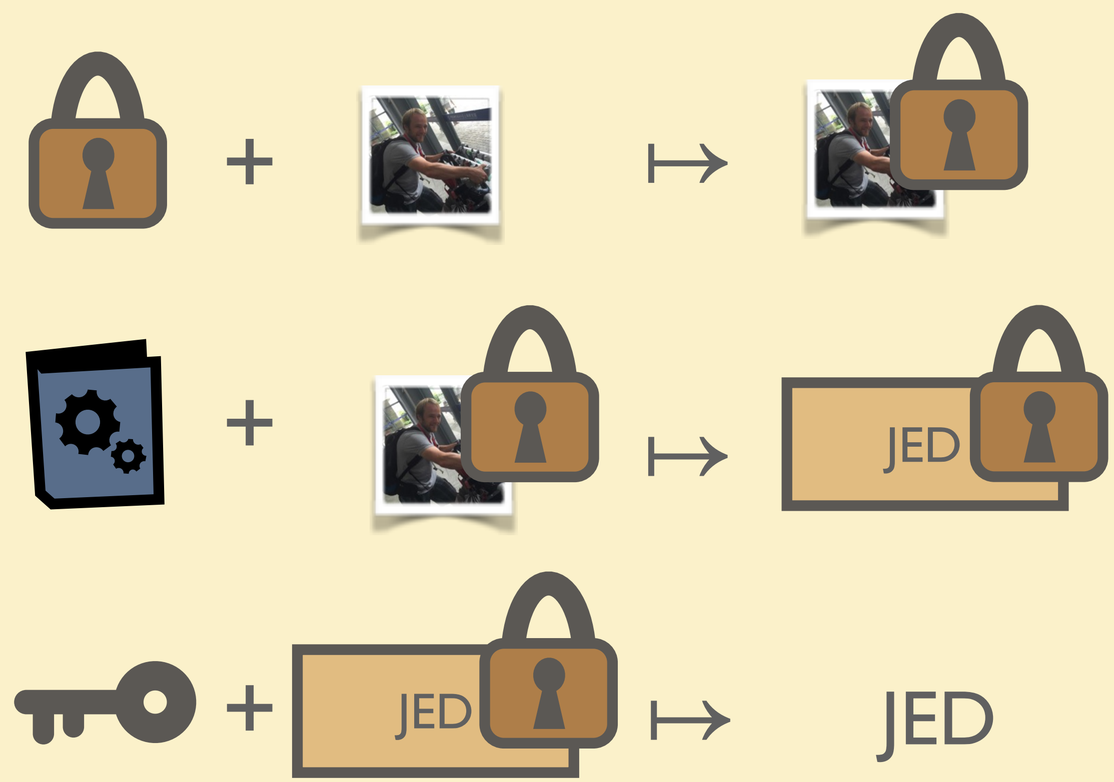
HOMOMORPHIC ENCRYPTION

KEY GENERATION
- public key
- secret key
- evaluation key

ENCRYPTION (secure)

EVALUATION

DECRYPTION



HOMOMORPHIC ENCRYPTION

KEY GENERATION		public key secret key evaluation key
ENCRYPTION (secure)		public key + x ↦ [x]
EVALUATION		evaluation key + [x] ↦ [f(x)]
DECRYPTION		secret key + [f(x)] ↦ f(x)

HOMOMORPHIC ENCRYPTION

KEY GENERATION

public key

secret key

evaluation key

ENCRYPTION (secure)

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

EVALUATION

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

DECRYPTION

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

HOMOMORPHIC ENCRYPTION

KEY GENERATION

ENCRYPTION
(secure)

EVALUATION

DECRYPTION

✓ HOMOMORPHIC ENCRYPTION

2. PREVIOUS RESULTS

3. NEW RESULT

PREVIOUS RESULTS: OVERVIEW

C. Gentry: Fully homomorphic encryption using ideal lattices. STOC’09
A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015
Y. Ouyang, S-H. Tan, J. Fitzsimons. Quantum homomorphic encryption from quantum codes. arxiv:1508.00938

PREVIOUS RESULTS: OVERVIEW

- Classical homomorphic encryption: solved! [Gentry 2009]

C. Gentry: Fully homomorphic encryption using ideal lattices. STOC'09
A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015
Y. Ouyang, S-H. Tan, J. Fitzsimons. Quantum homomorphic encryption from quantum codes. arxiv:1508.00938

PREVIOUS RESULTS: OVERVIEW

- Classical homomorphic encryption: solved! [Gentry 2009]
- Quantum homomorphic encryption: only partial results
  - Clifford scheme allowing evaluation of {P, H, CNOT}
  - schemes for {P, H, CNOT} + limited # of T gates

C. Gentry: Fully homomorphic encryption using ideal lattices. STOC'09
A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015
Y. Ouyang, S-H. Tan, J. Fitzsimons. Quantum homomorphic encryption from quantum codes. arxiv:1508.00938

PREVIOUS RESULTS: OVERVIEW

- Classical homomorphic encryption: solved! [Gentry 2009]
- Quantum homomorphic encryption: only partial results
  - Clifford scheme allowing evaluation of {P, H, CNOT}
  - schemes for {P, H, CNOT} + limited # of T gates

C. Gentry: Fully homomorphic encryption using ideal lattices. STOC'09
A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015
Y. Ouyang, S-H. Tan, J. Fitzsimons. Quantum homomorphic encryption from quantum codes. arxiv:1508.00938

SCHEME FOR {P, H, CNOT}

[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

SCHEME FOR {P, H, CNOT}

Ingredient 1: quantum encryption (one-time pad)

[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

SCHEME FOR {P, H, CNOT}

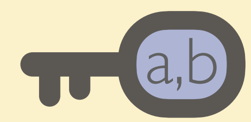
Ingredient 1: quantum encryption (one-time pad)

encryption:

[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

SCHEME FOR {P, H, CNOT}

Ingredient 1: quantum encryption (one-time pad)

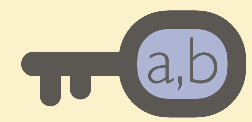
encryption: pick a,b $\in_R$ {0,1} 

[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

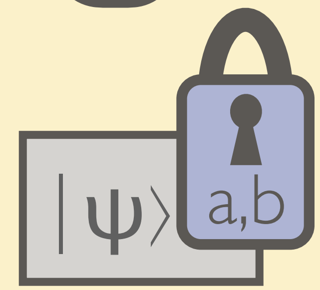
SCHEME FOR {P, H, CNOT}

Ingredient 1: quantum encryption (one-time pad)

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



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

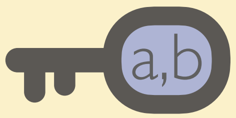


[AMTW00] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. FOCS'00
[Gentry 09] C. Gentry: Fully homomorphic encryption using ideal lattices. STOC'09

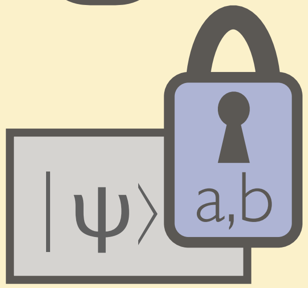
SCHEME FOR {P, H, CNOT}

Ingredient 1: quantum encryption (one-time pad)

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



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



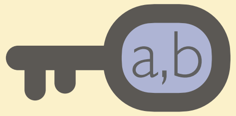
decryption:

[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

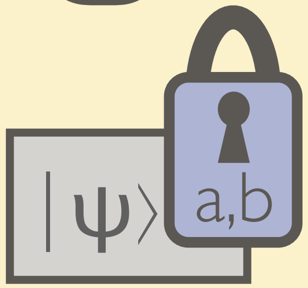
SCHEME FOR {P, H, CNOT}

Ingredient 1: quantum encryption (one-time pad)

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



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



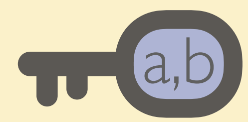
decryption: $X^a Z^b |\psi\rangle \mapsto |\psi\rangle$

[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

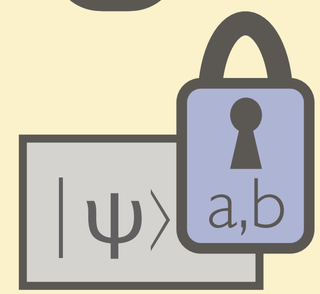
SCHEME FOR {P, H, CNOT}

Ingredient 1: quantum encryption (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

[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

SCHEME FOR {P, H, CNOT}

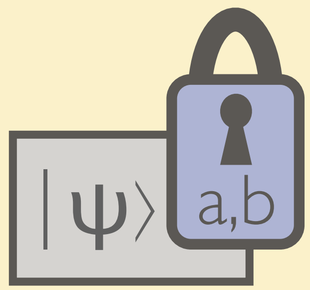
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

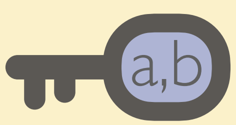
SCHEME FOR {P, H, CNOT}

$|\psi\rangle$

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

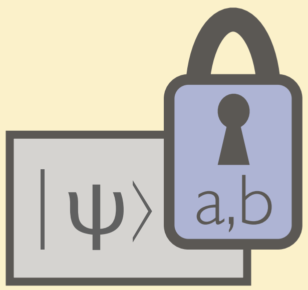
SCHEME FOR {P, H, CNOT}

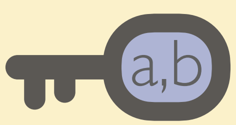




Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

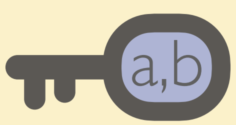
SCHEME FOR {P, H, CNOT}

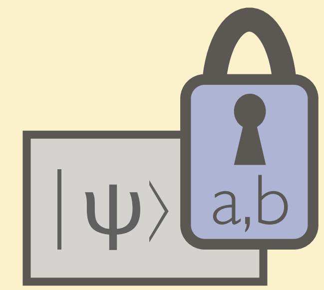


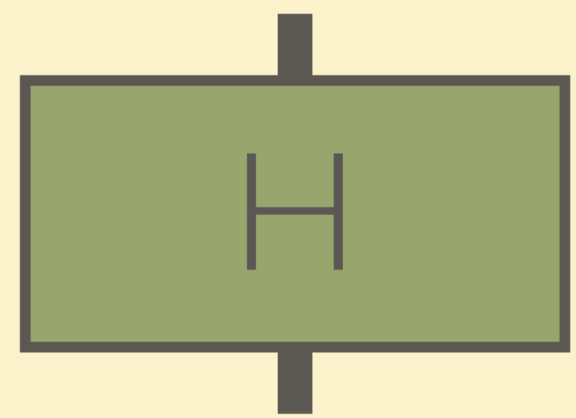


Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

SCHEME FOR {P, H, CNOT}

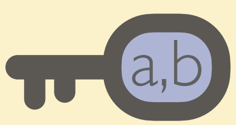


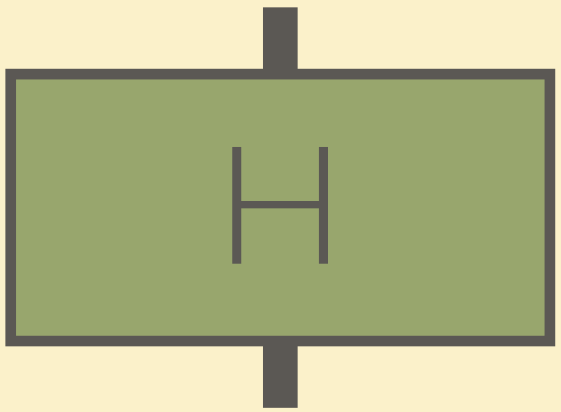


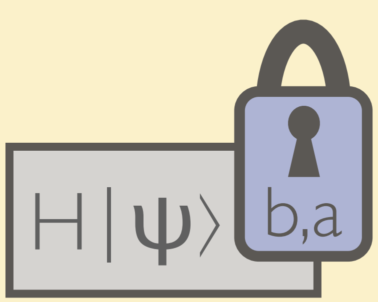


Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

SCHEME FOR {P, H, CNOT}

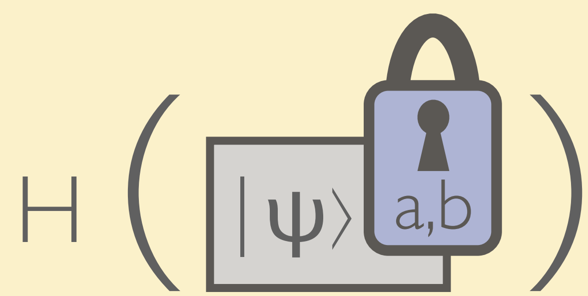




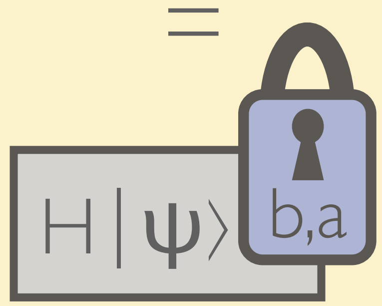


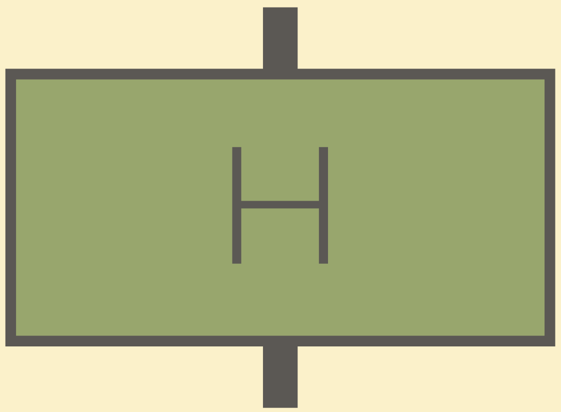
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

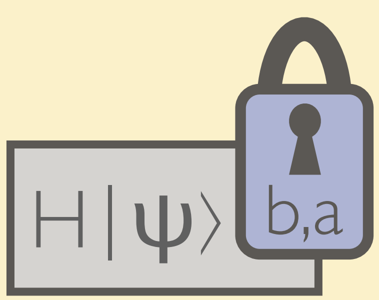
SCHEME FOR {P, H, CNOT}



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

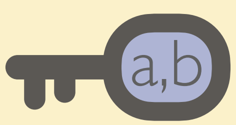


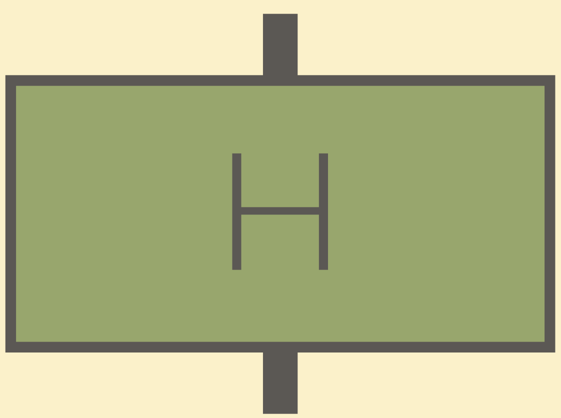


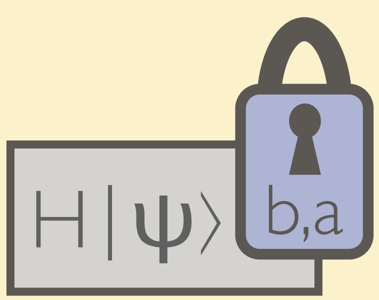


Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

SCHEME FOR {P, H, CNOT}

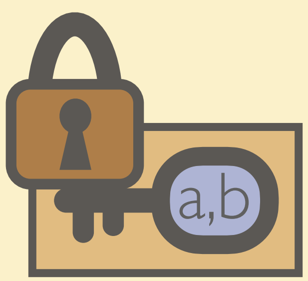


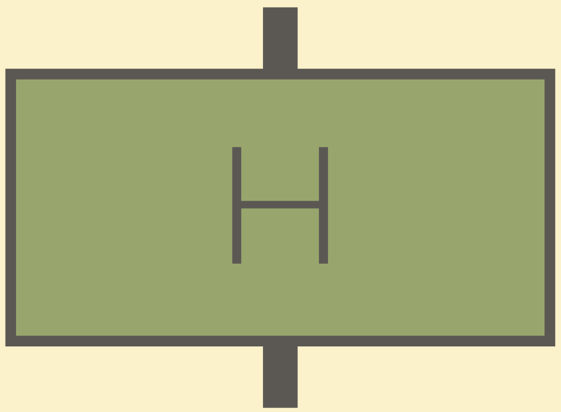


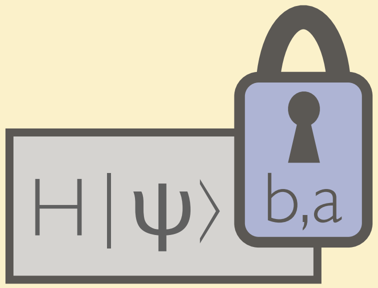


Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

SCHEME FOR {P, H, CNOT}

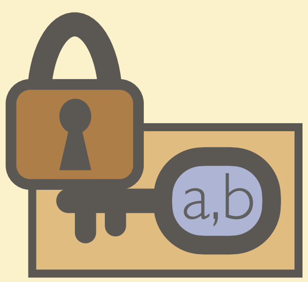


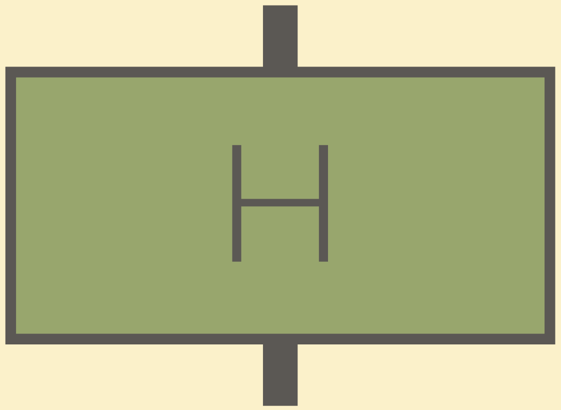


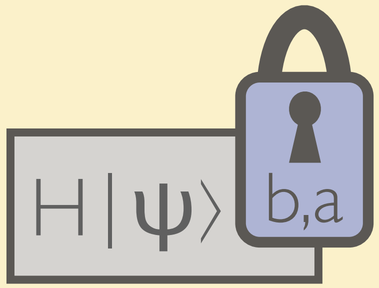


Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

SCHEME FOR {P, H, CNOT}

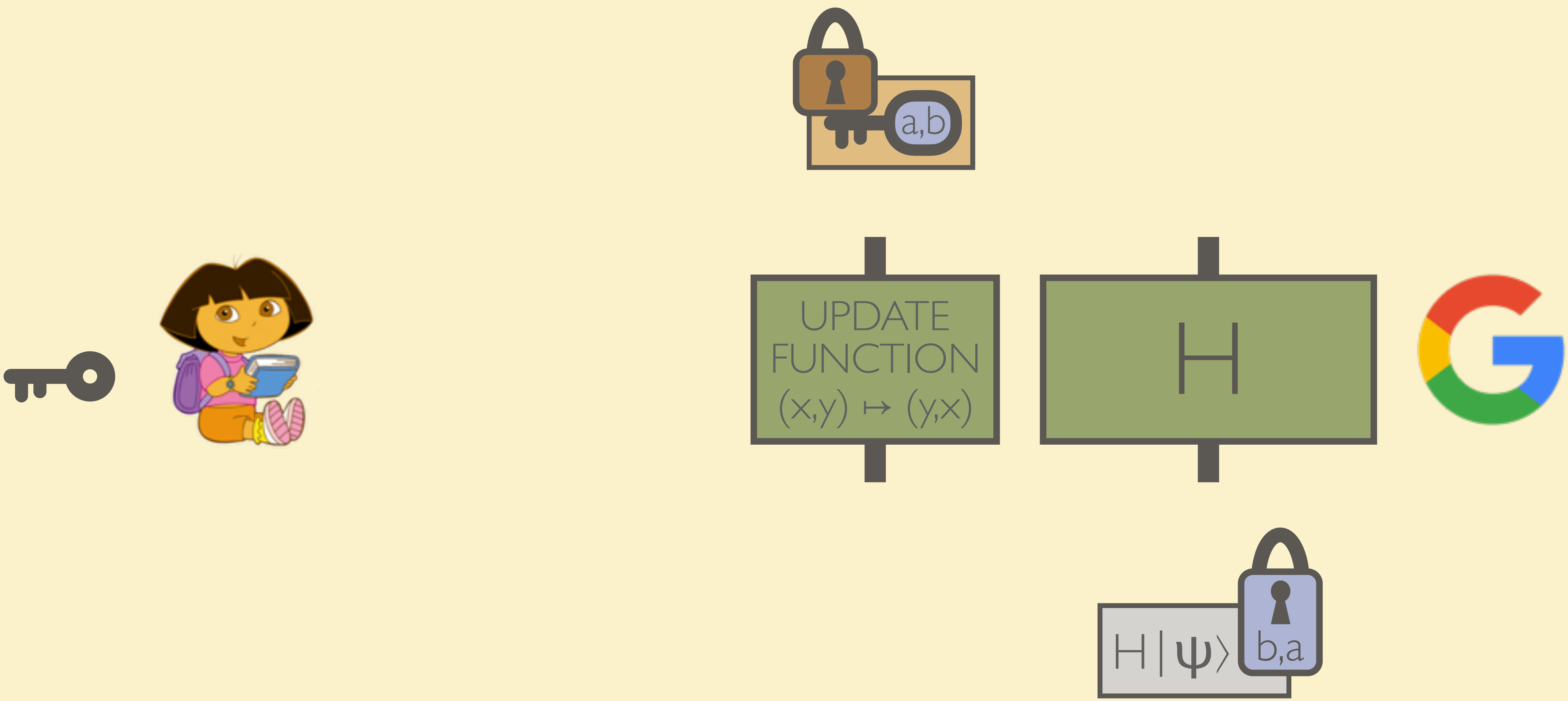






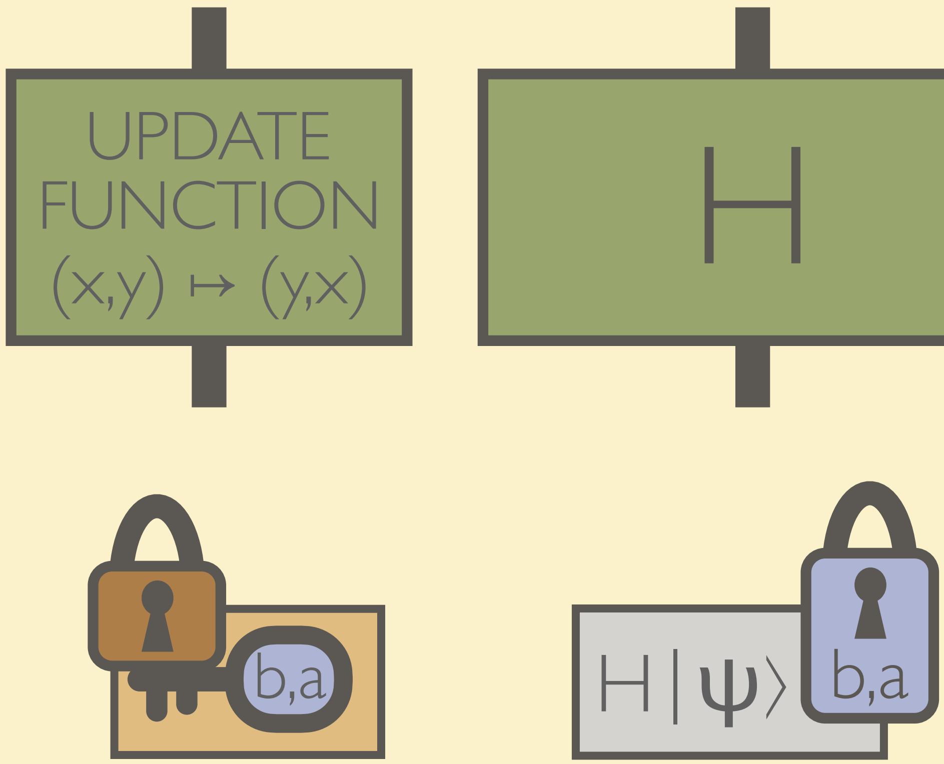
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

SCHEME FOR {P, H, CNOT}



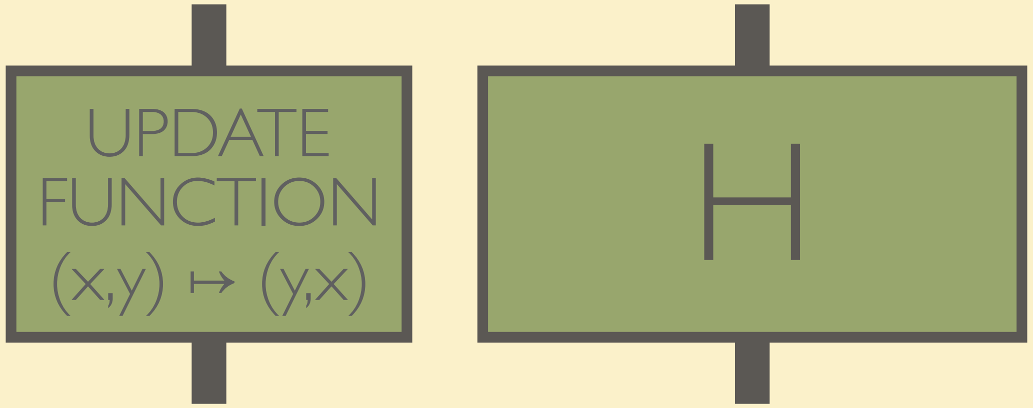
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

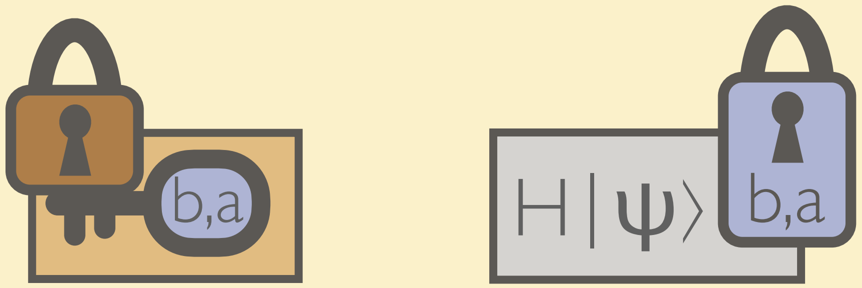
SCHEME FOR {P, H, CNOT}



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

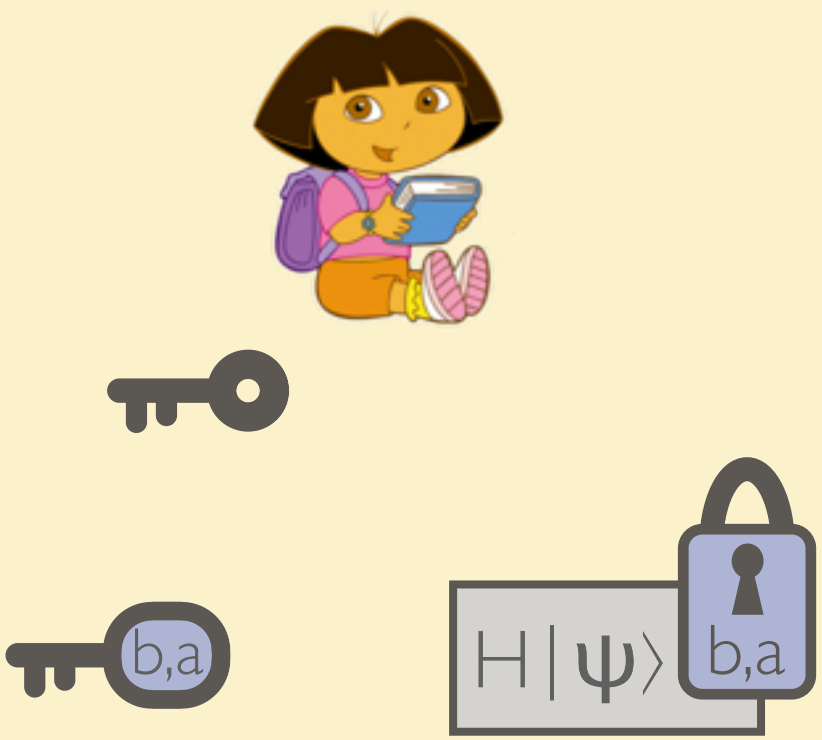
SCHEME FOR {P, H, CNOT}





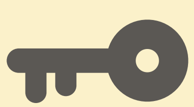
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

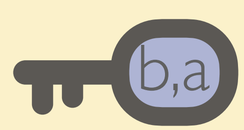
SCHEME FOR {P, H, CNOT}



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

SCHEME FOR {P, H, CNOT}



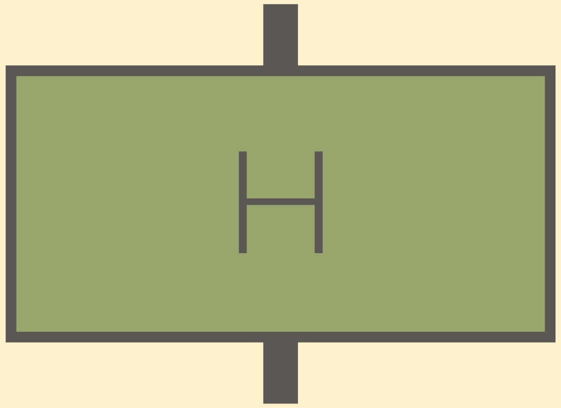


$H|\psi\rangle$

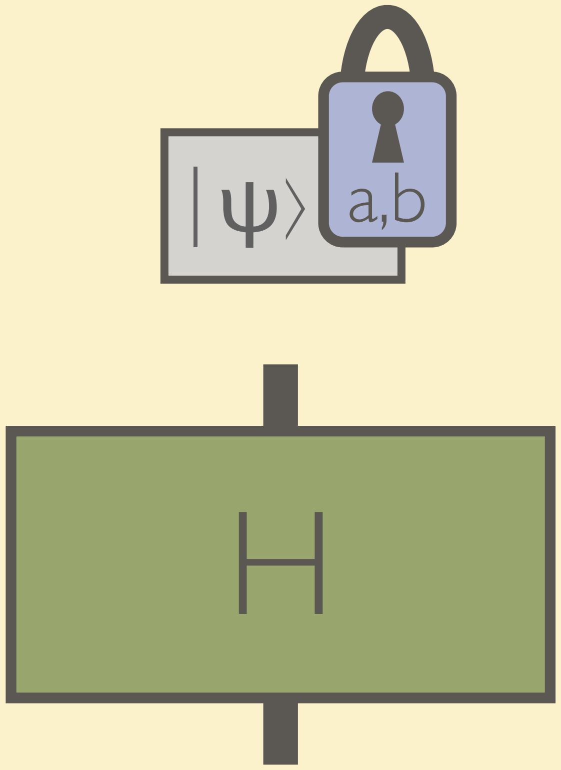
Folklore, last formalized by [BJ15] A. Broadbent, S. Jeffery. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. CRYPTO 2015

THE CHALLENGE: T GATE

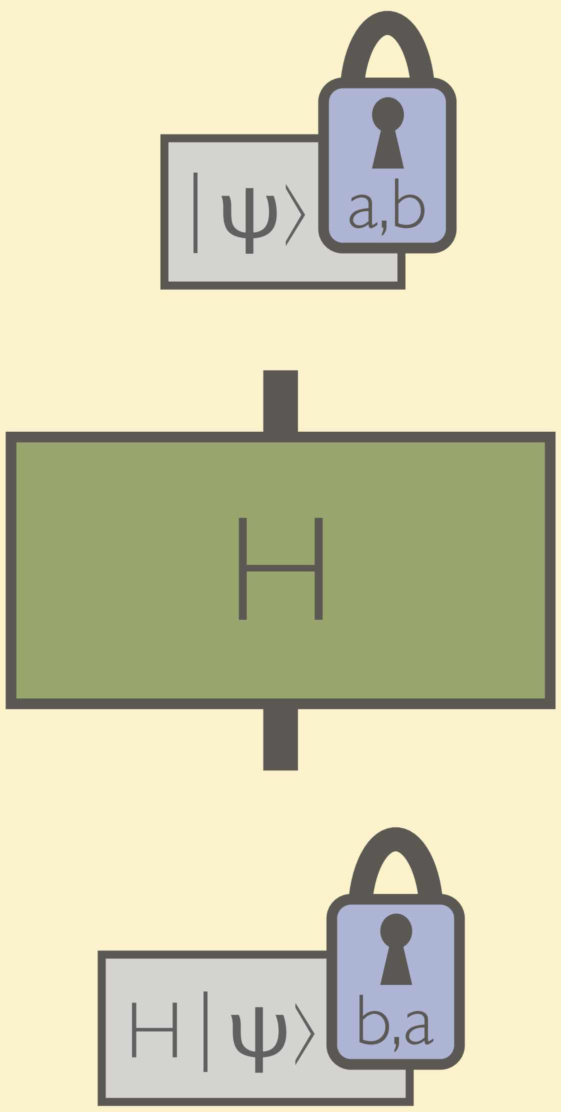
THE CHALLENGE: T GATE



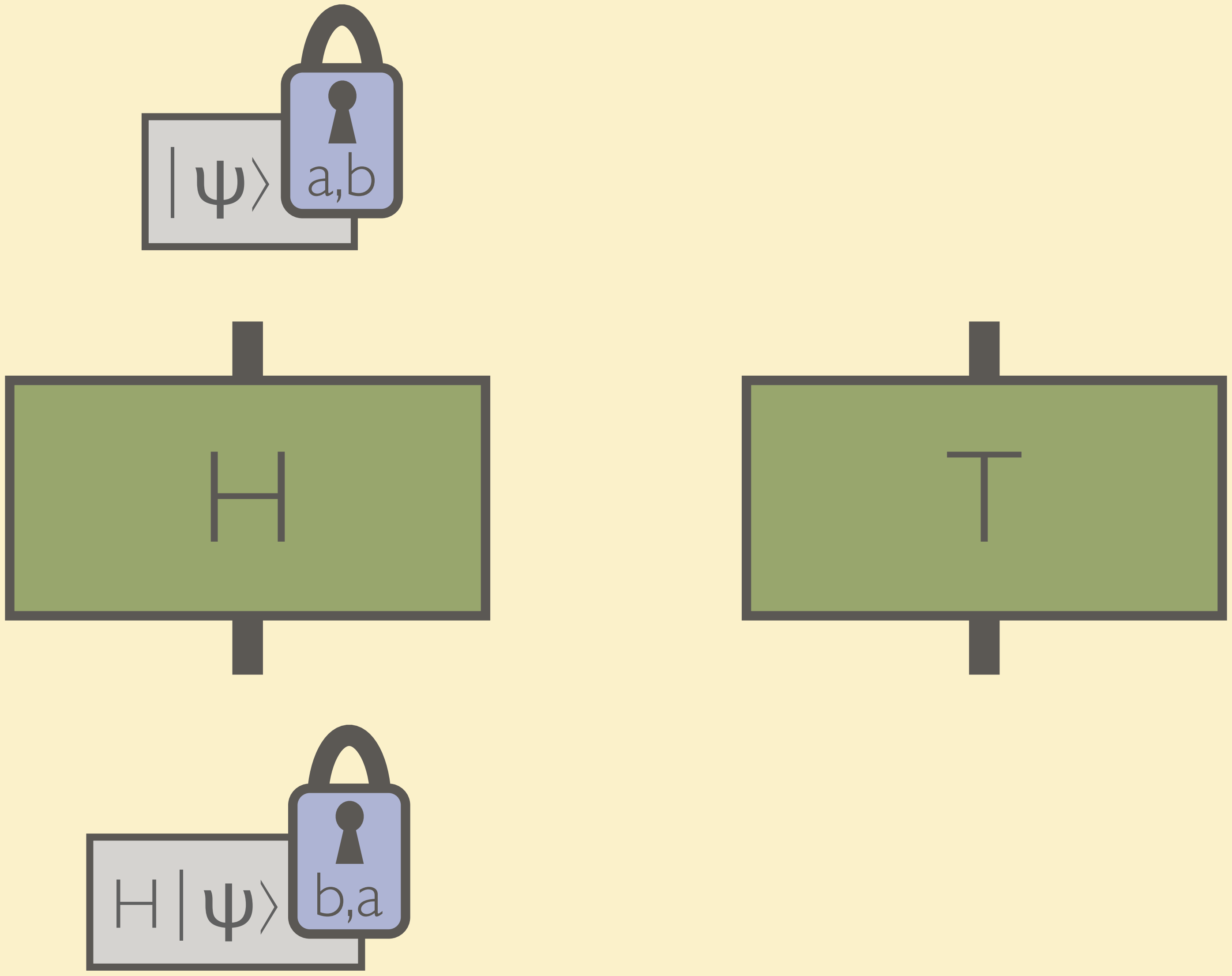
THE CHALLENGE: T GATE



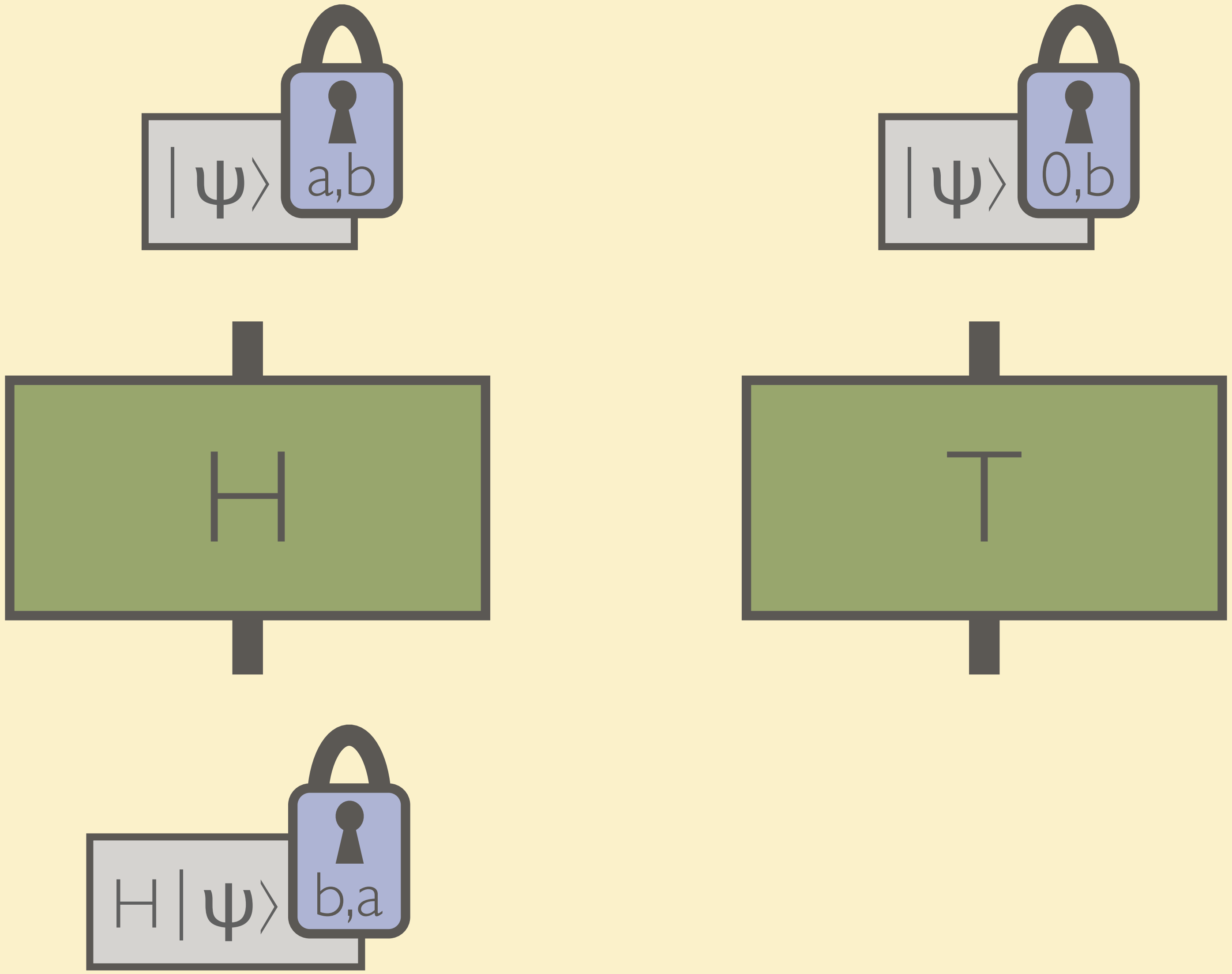
THE CHALLENGE: T GATE



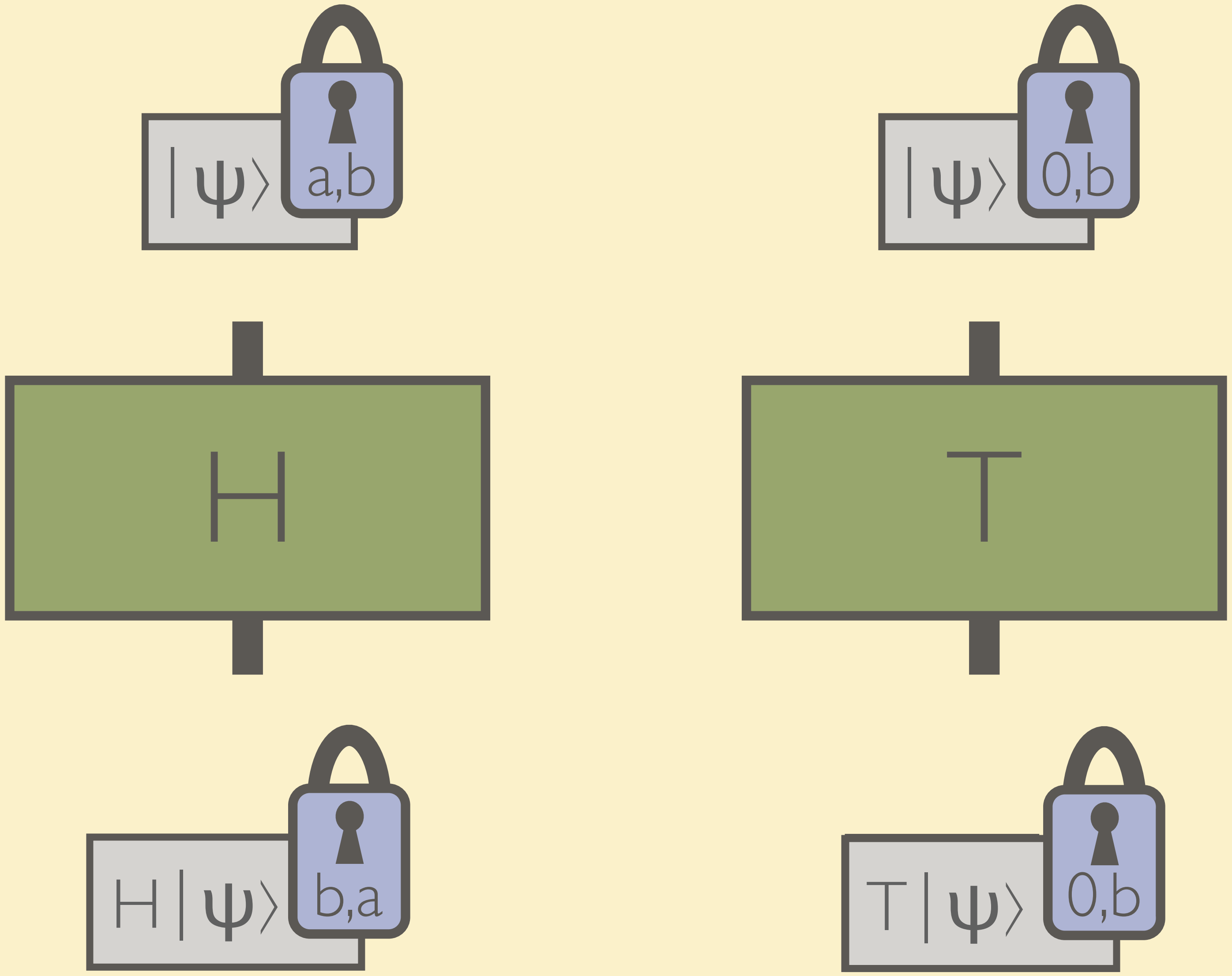
THE CHALLENGE: T GATE



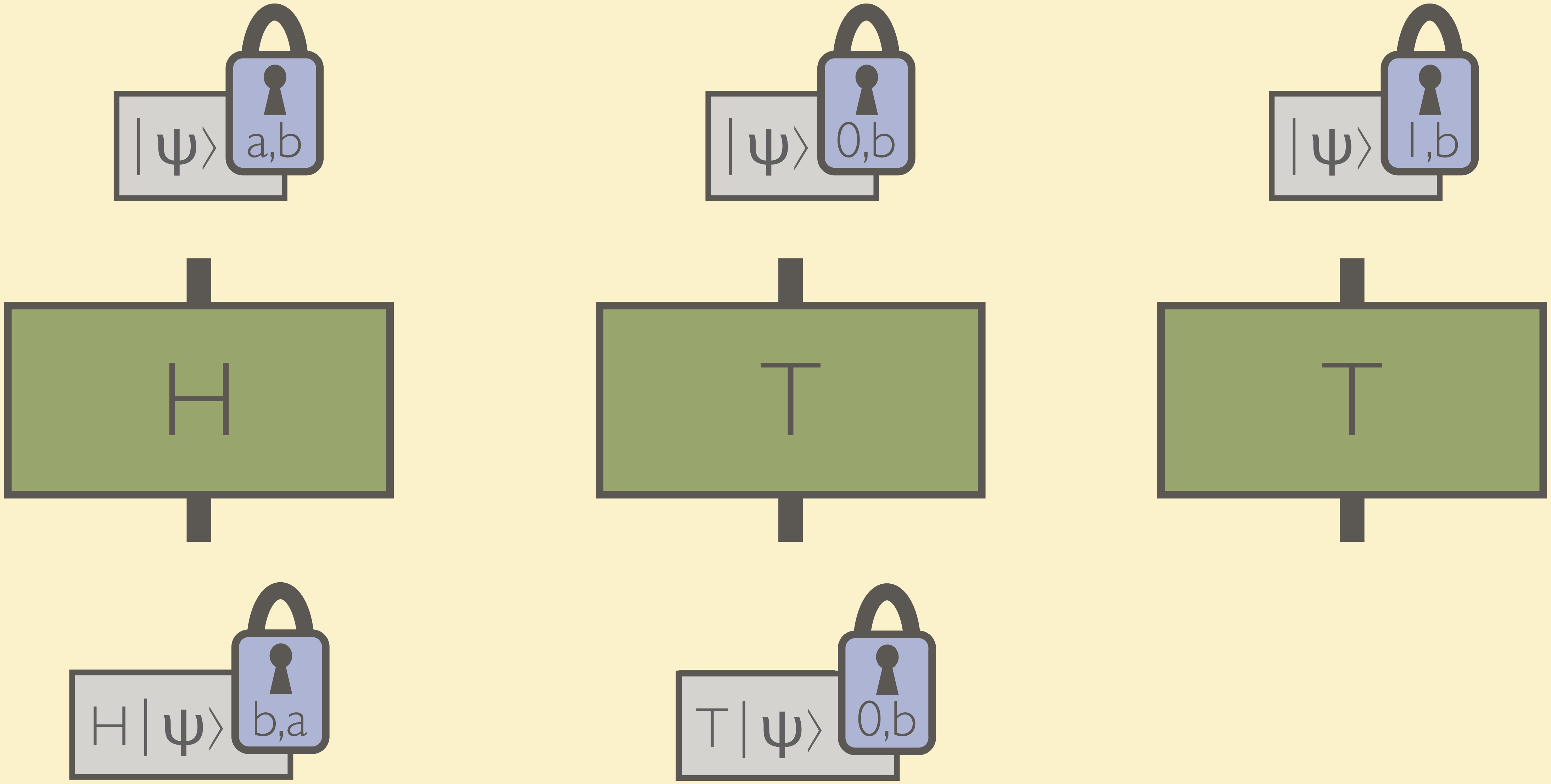
THE CHALLENGE: T GATE



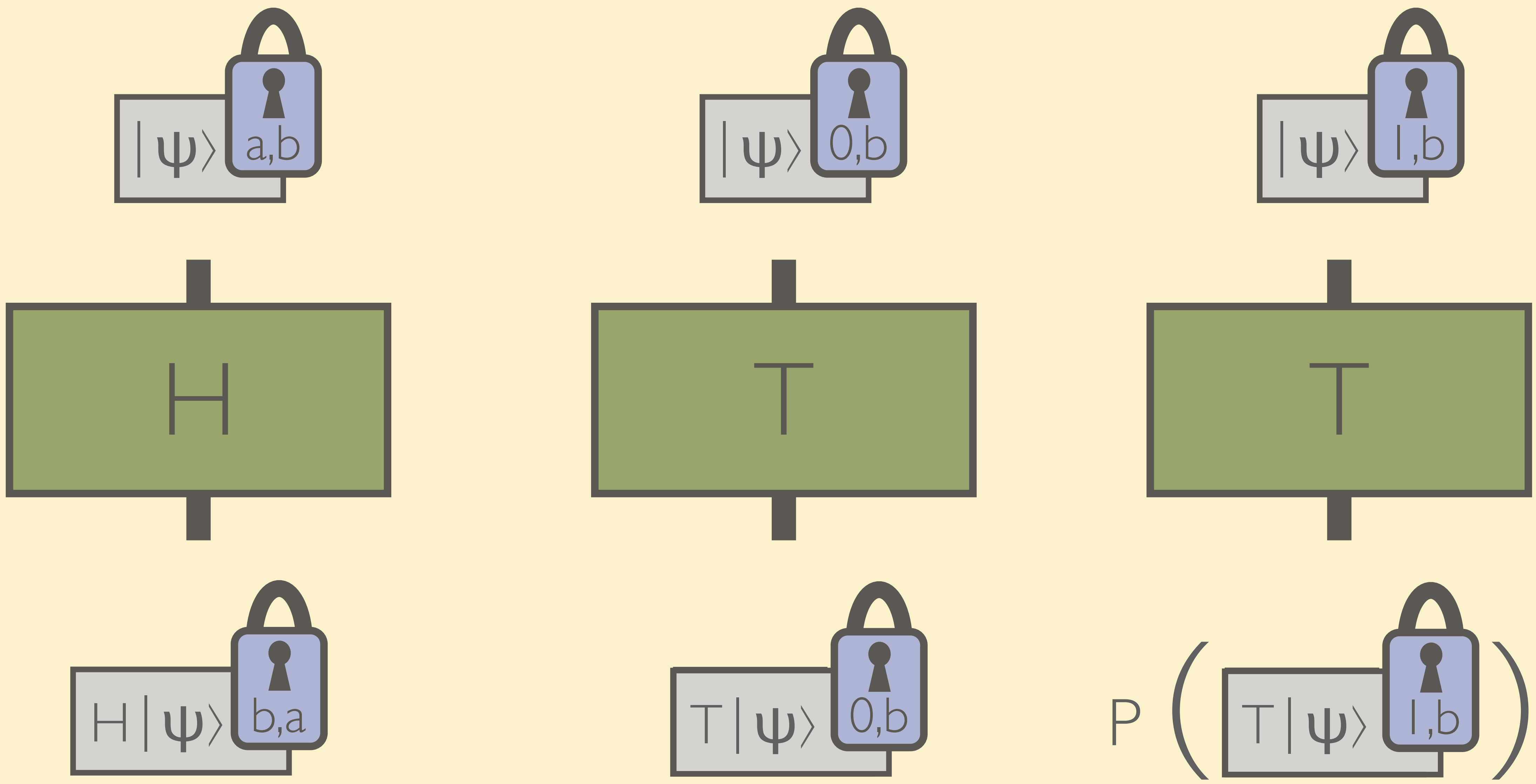
THE CHALLENGE: T GATE



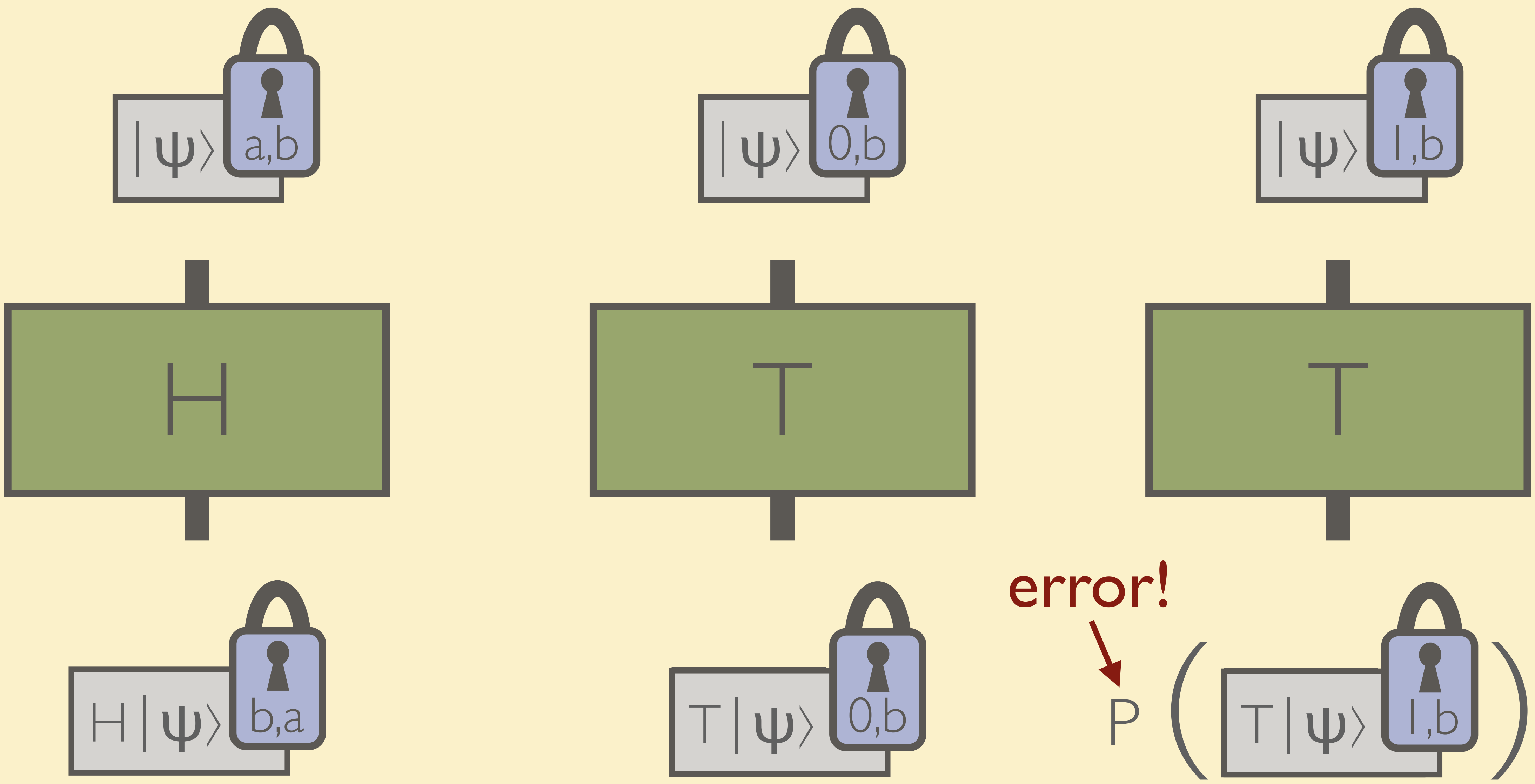
THE CHALLENGE: T GATE



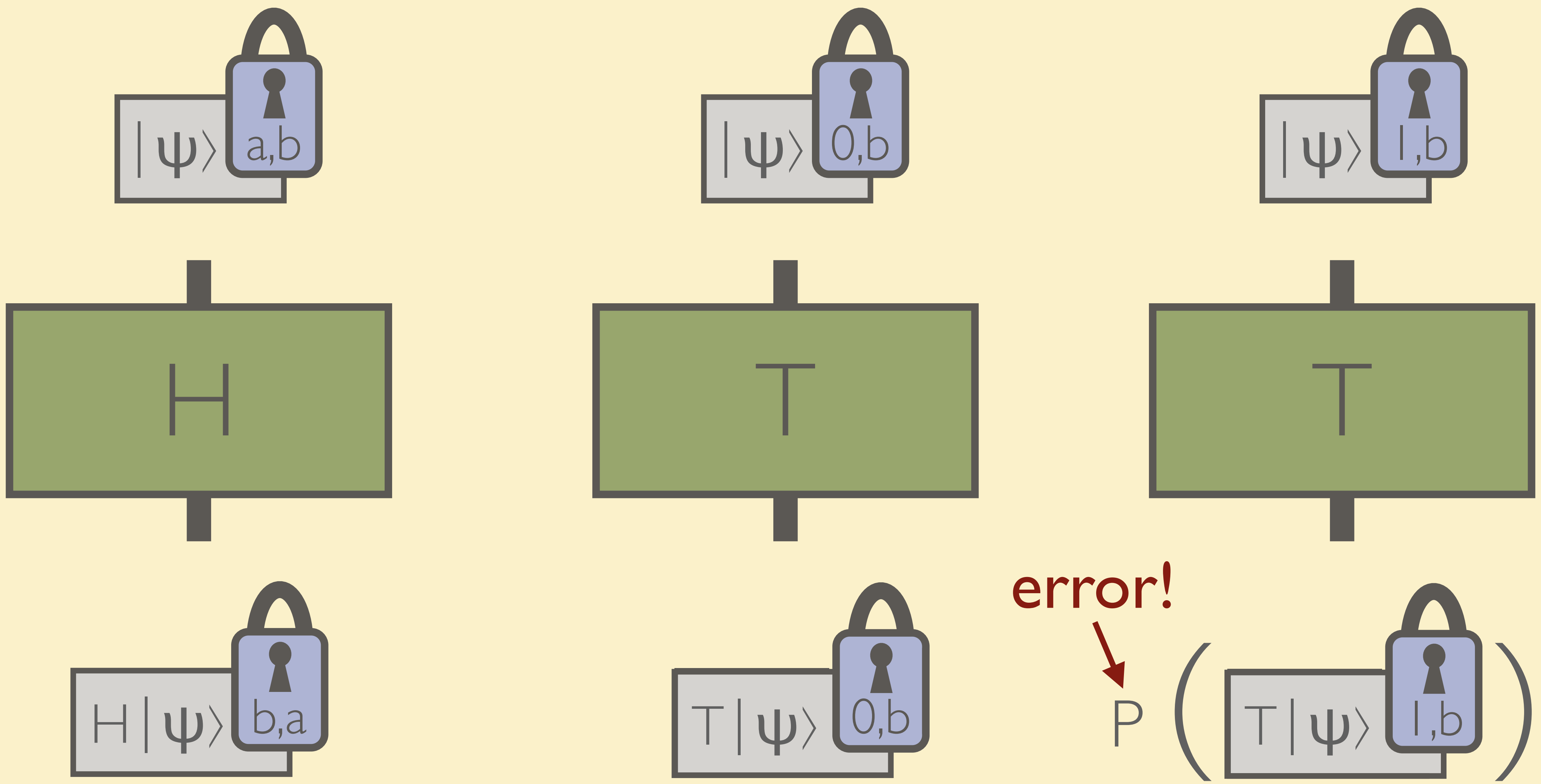
THE CHALLENGE: T GATE



THE CHALLENGE: T GATE



THE CHALLENGE: T GATE



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

PREVIOUS RESULTS: OVERVIEW

(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

PREVIOUS RESULTS: OVERVIEW

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

PREVIOUS RESULTS: OVERVIEW

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

(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

PREVIOUS RESULTS: OVERVIEW

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

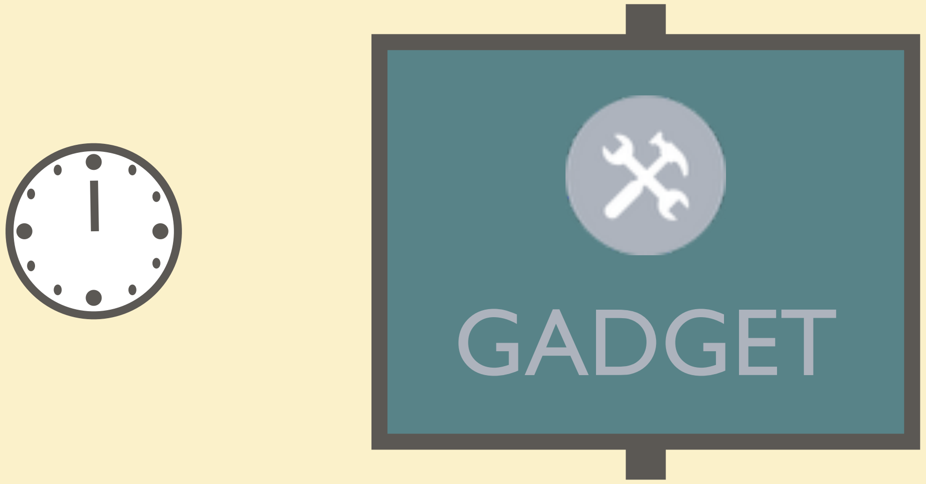
- ✓ HOMOMORPHIC ENCRYPTION
- ✓ PREVIOUS RESULTS
3. NEW RESULT

ERROR-CORRECTION “GADGET”

ERROR-CORRECTION "GADGET"

A quantum state that:

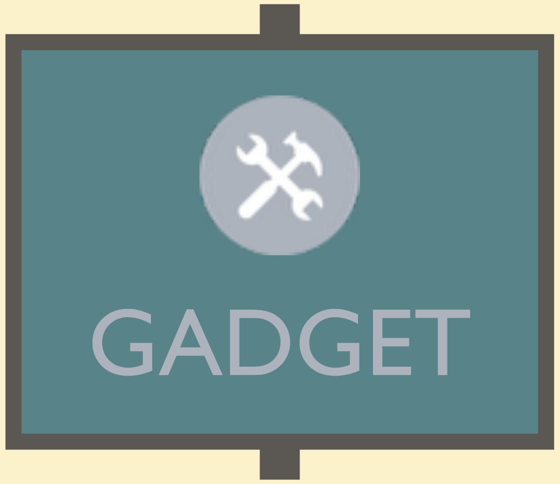
- can be efficiently constructed and used



ERROR-CORRECTION "GADGET"

A quantum state that:

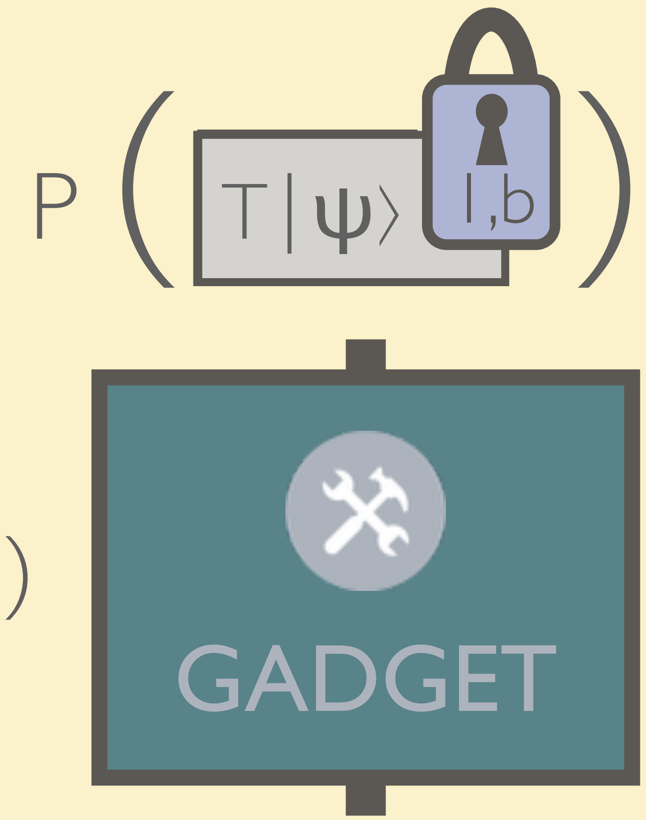
- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)



ERROR-CORRECTION "GADGET"

A quantum state that:

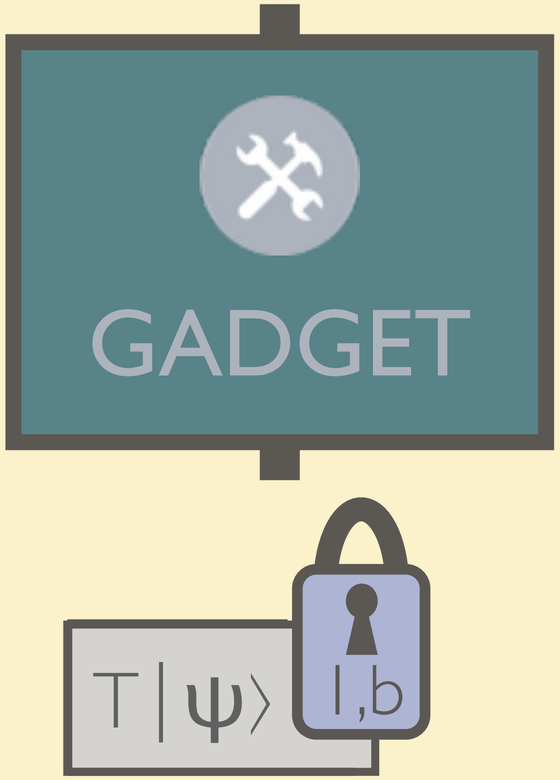
- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)



ERROR-CORRECTION "GADGET"

A quantum state that:

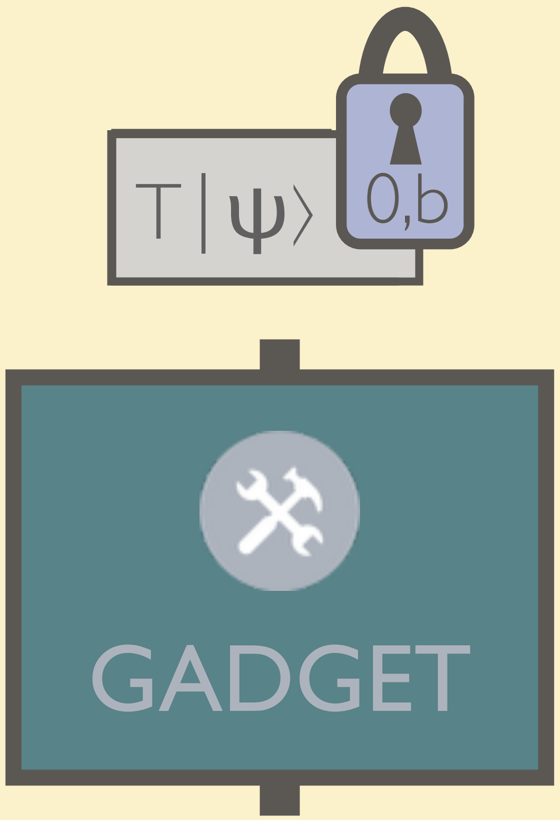
- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)



ERROR-CORRECTION "GADGET"

A quantum state that:

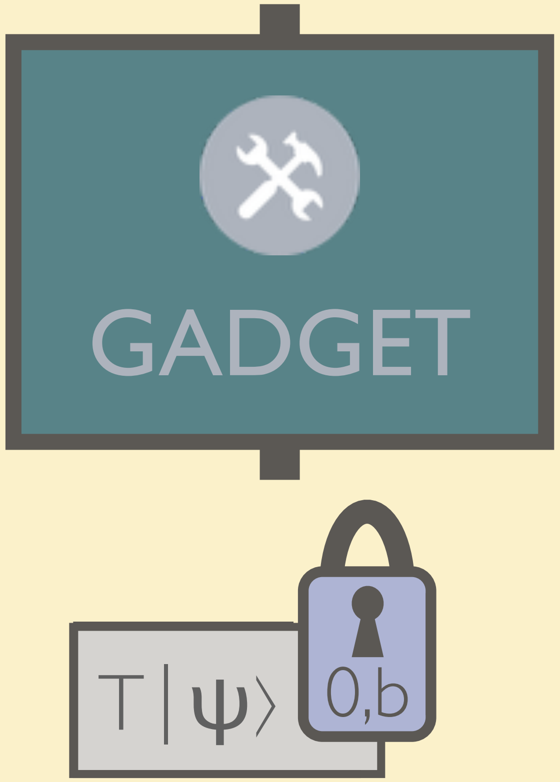
- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)



ERROR-CORRECTION "GADGET"

A quantum state that:

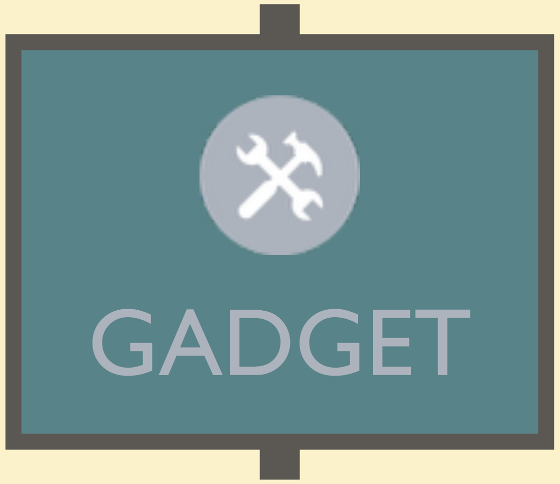
- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)



ERROR-CORRECTION "GADGET"

A quantum state that:

- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)
- is destroyed after a single use



ERROR-CORRECTION "GADGET"

A quantum state that:

- can be efficiently constructed and used
- applies correction iff error was present (iff a = 1)
- is destroyed after a single use

EXCURSION

Theoretical Computer Science

PERMUTATION BRANCHING PROGRAM

PERMUTATION BRANCHING PROGRAM

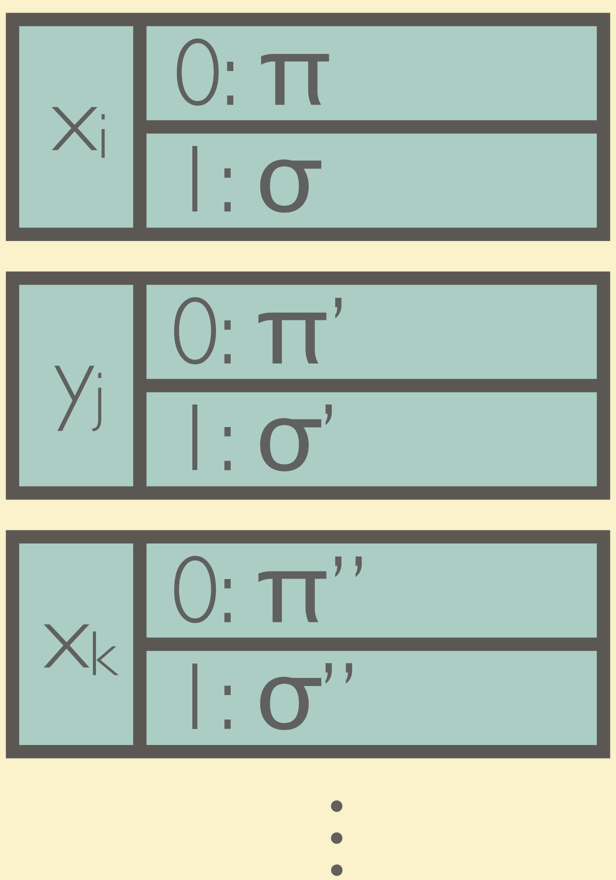
- computes some Boolean function $f(x,y)$

PERMUTATION BRANCHING PROGRAM

- computes some Boolean function f(x,y)
- list of instructions:

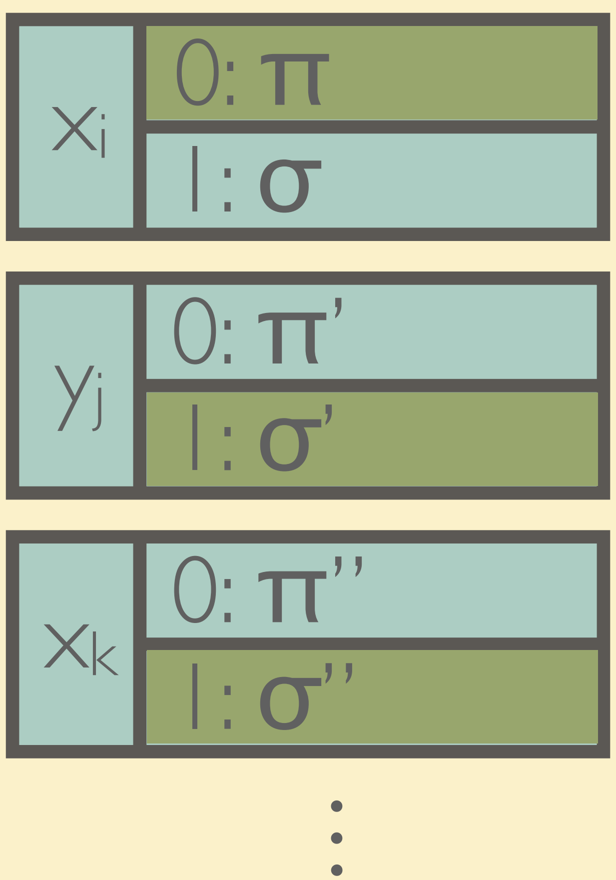
PERMUTATION BRANCHING PROGRAM

- computes some Boolean function f(x,y)
- list of instructions:



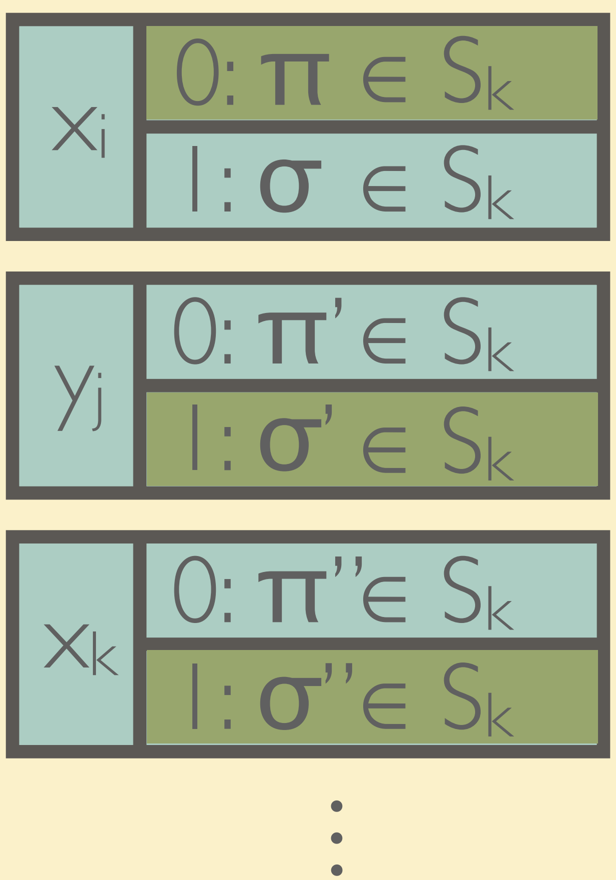
PERMUTATION BRANCHING PROGRAM

- computes some Boolean function f(x,y)
- list of instructions:



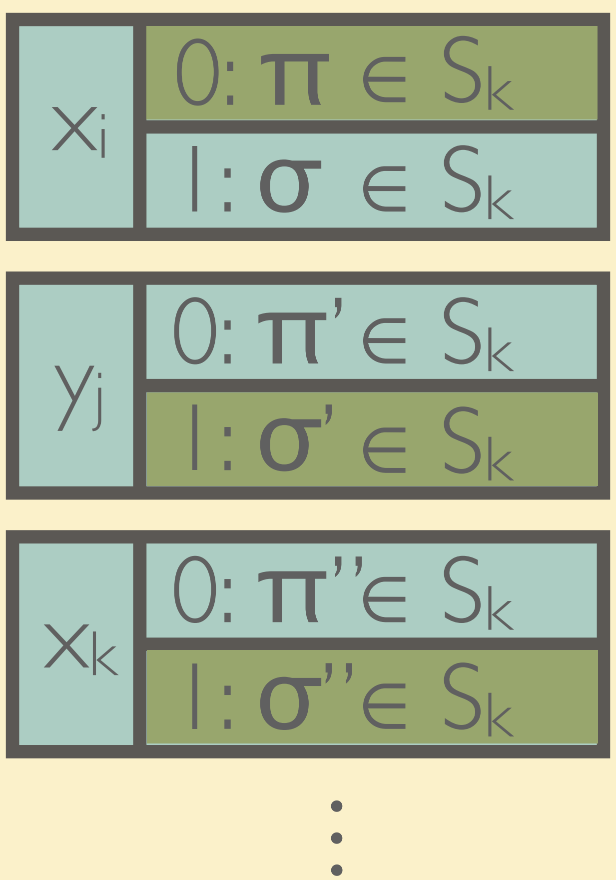
PERMUTATION BRANCHING PROGRAM

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



PERMUTATION BRANCHING PROGRAM

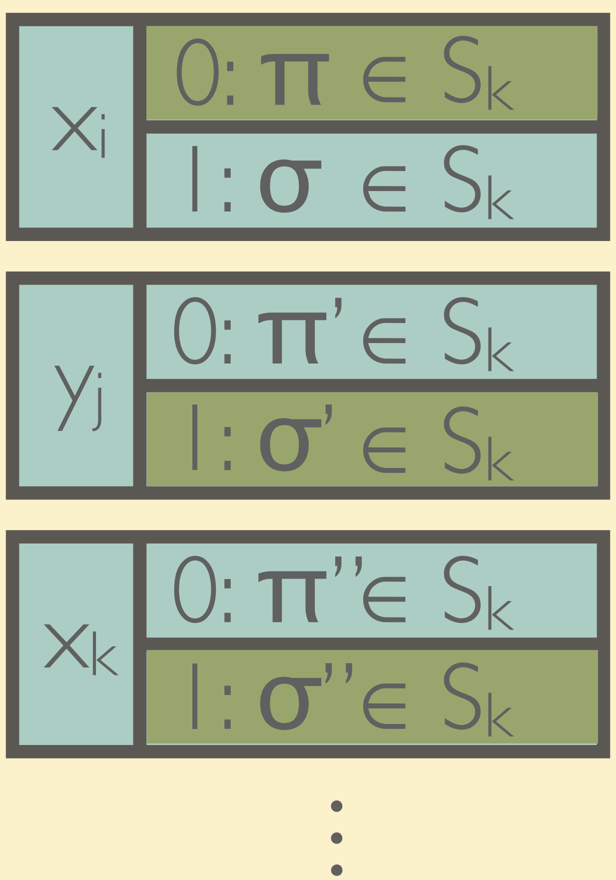
- computes some Boolean function f(x,y)
- list of instructions: permutations of {1,2, …, k}



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

PERMUTATION BRANCHING PROGRAM

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

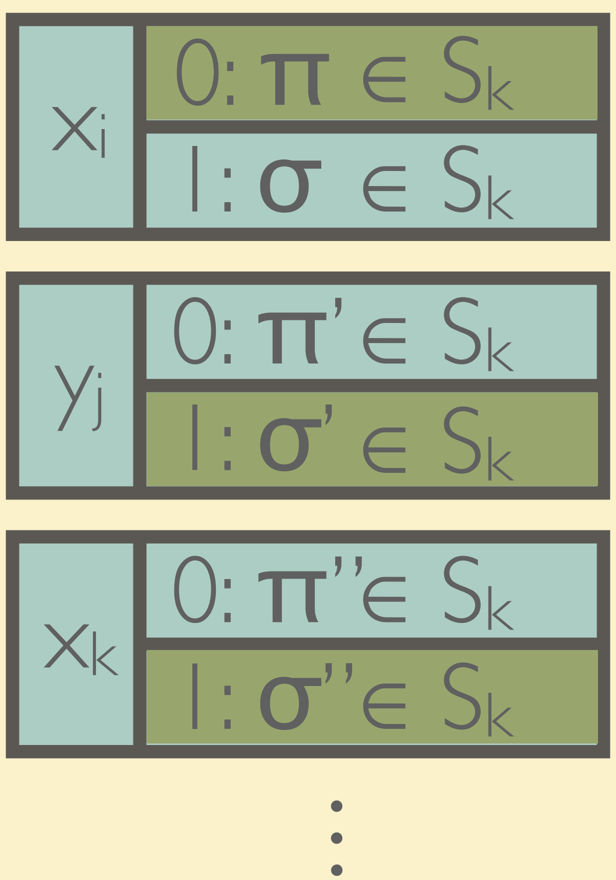


output: $\ldots \circ \sigma'' \circ \sigma' \circ \pi$

- id

PERMUTATION BRANCHING PROGRAM

- computes some Boolean function $f(x,y)$
- list of instructions: permutations of $\{1,2, \ldots, k\}$

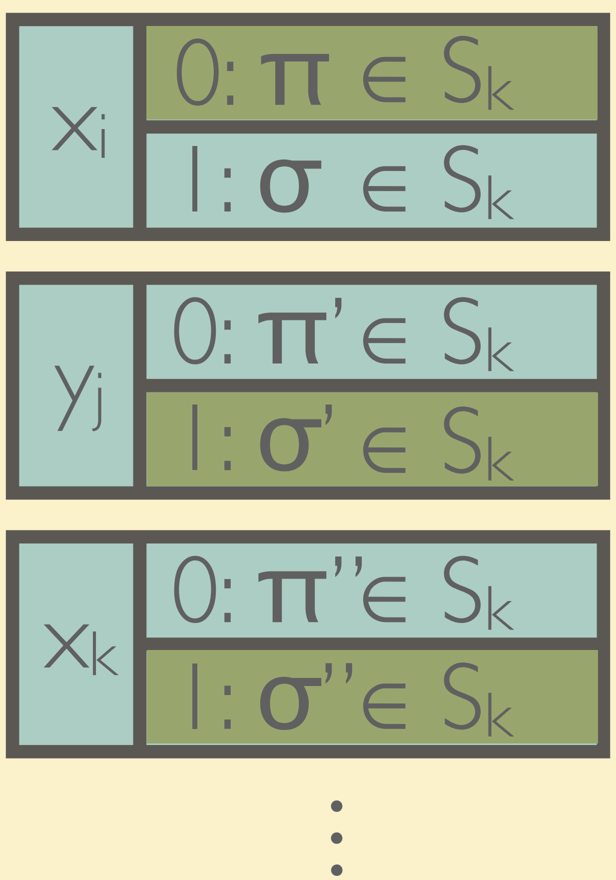


output: $\ldots \circ \sigma'' \circ \sigma' \circ \pi$

- id
- (fixed) cycle

PERMUTATION BRANCHING PROGRAM

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

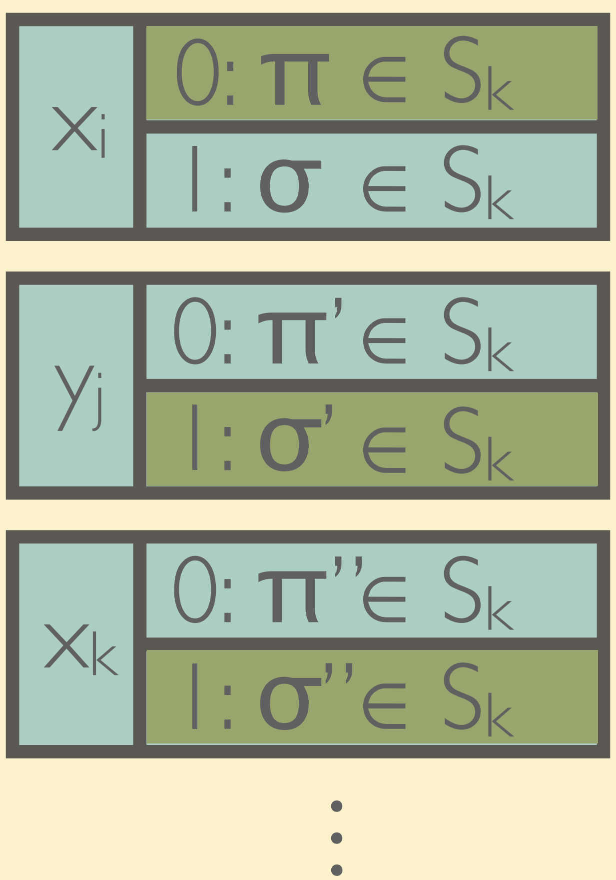


output: $\ldots \circ \sigma'' \circ \sigma' \circ \pi$

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

PERMUTATION BRANCHING PROGRAM

- computes some Boolean function $f(x,y)$
- list of instructions: permutations of $\{1,2, \ldots, k\}$

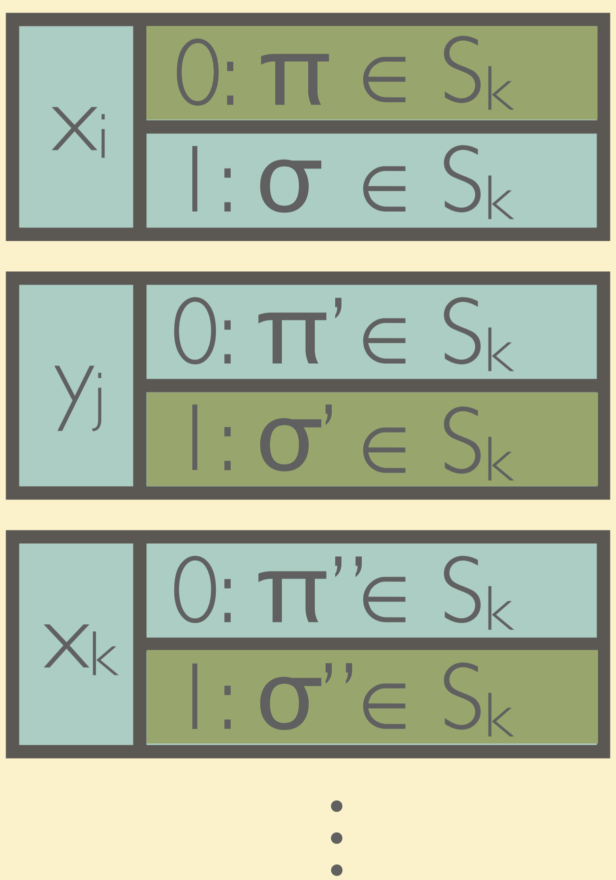


output: $\ldots \circ \sigma'' \circ \sigma' \circ \pi$

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

PERMUTATION BRANCHING PROGRAM

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



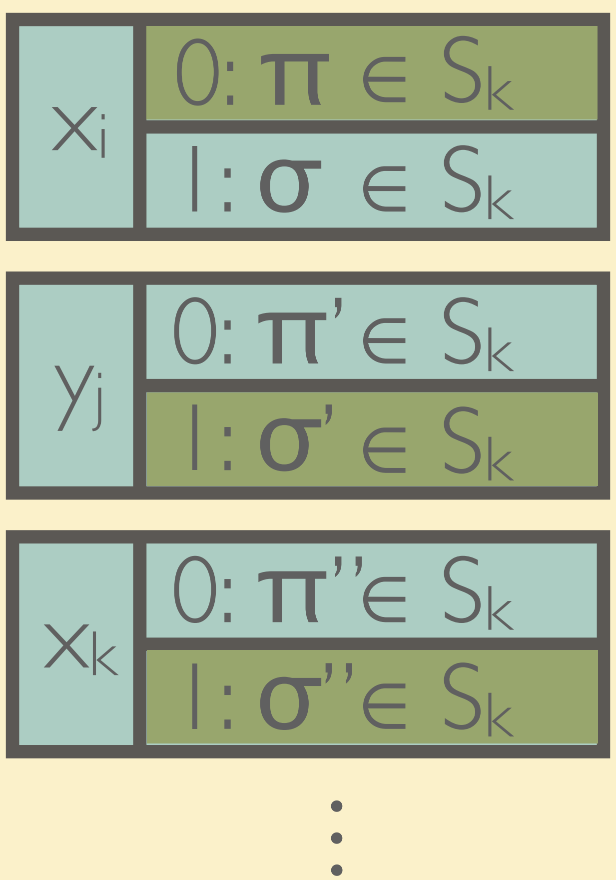
output: … ∘ **σ**’’ ∘ **σ**’ ∘ **π**

- id ⇒ f(x,y) = 0
- (fixed) cycle ⇒ f(x,y) = 1

length: # of instructions

PERMUTATION BRANCHING PROGRAM

- computes some Boolean function $f(x,y)$
- list of instructions: permutations of $\{1,2, \ldots, k\}$



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

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

length: # of instructions

width: k

EXAMPLE PBP (OR)

length 4, width 5:

EXAMPLE PBP (OR)

length 4, width 5:

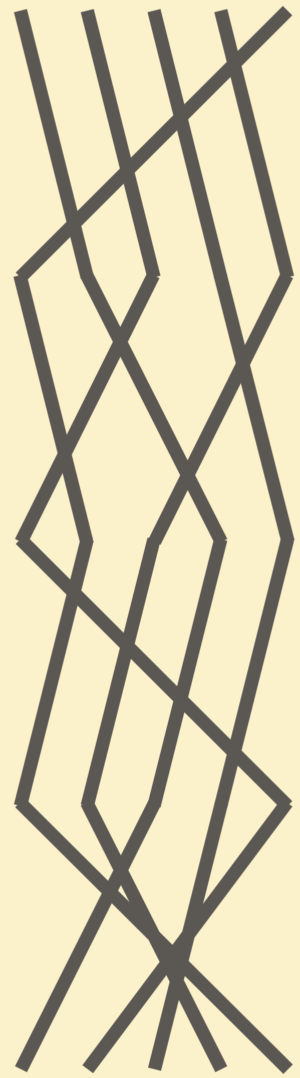
x_1	0: (12345)	1: id
y_1	0: (12453)	1: id
x_1	0: (54321)	1: id
y_1	0: (15243)	1: (14235)

EXAMPLE PBP (OR)

length 4, width 5:

x_1	0: (12345)
	1: id
y_1	0: (12453)
	1: id
x_1	0: (54321)
	1: id
y_1	0: (15243)
	1: (14235)

OR(0,0)



output: id

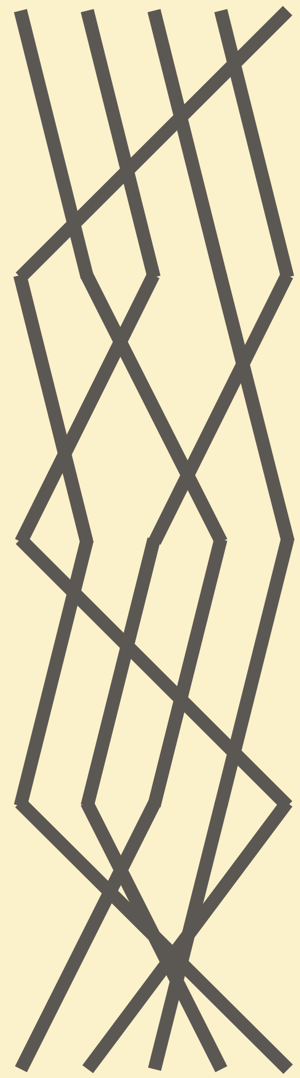
0

EXAMPLE PBP (OR)

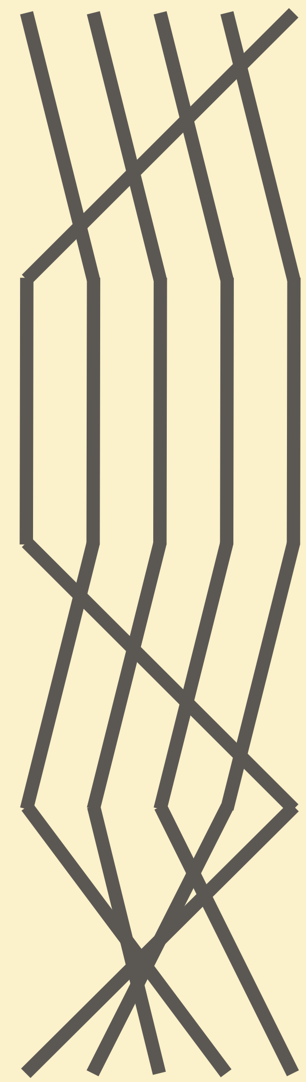
length 4, width 5:

x_1	0: (12345)	1: id
y_1	0: (12453)	1: id
x_1	0: (54321)	1: id
y_1	0: (15243)	1: (14235)

OR(0,0)



OR(0,1)



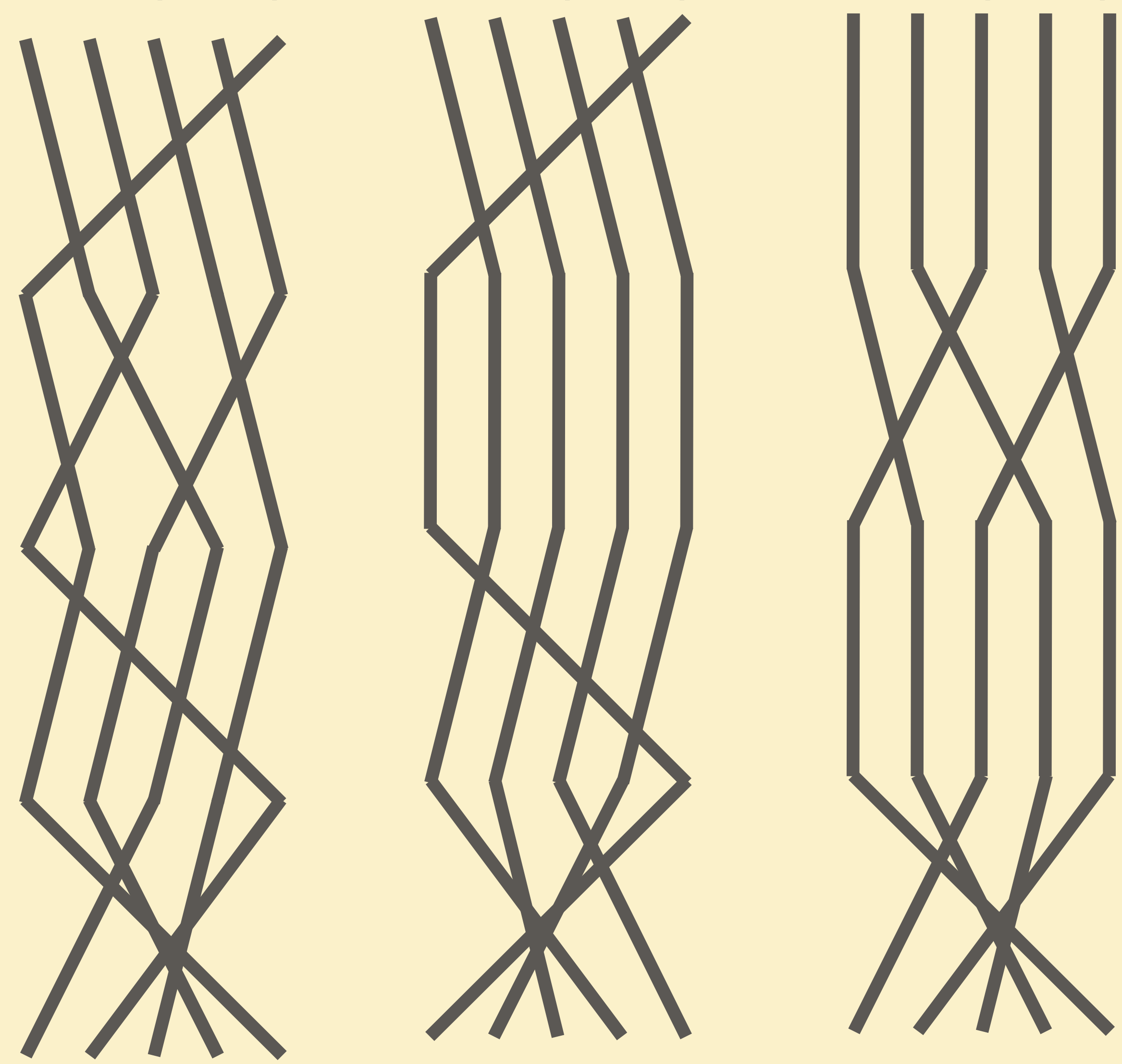
	OR(0,0)	OR(0,1)
output:	id	(14235)
	0	1

EXAMPLE PBP (OR)

length 4, width 5:

x_1	0: (12345)	1: id
y_1	0: (12453)	1: id
x_1	0: (54321)	1: id
y_1	0: (15243)	1: (14235)

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



output:

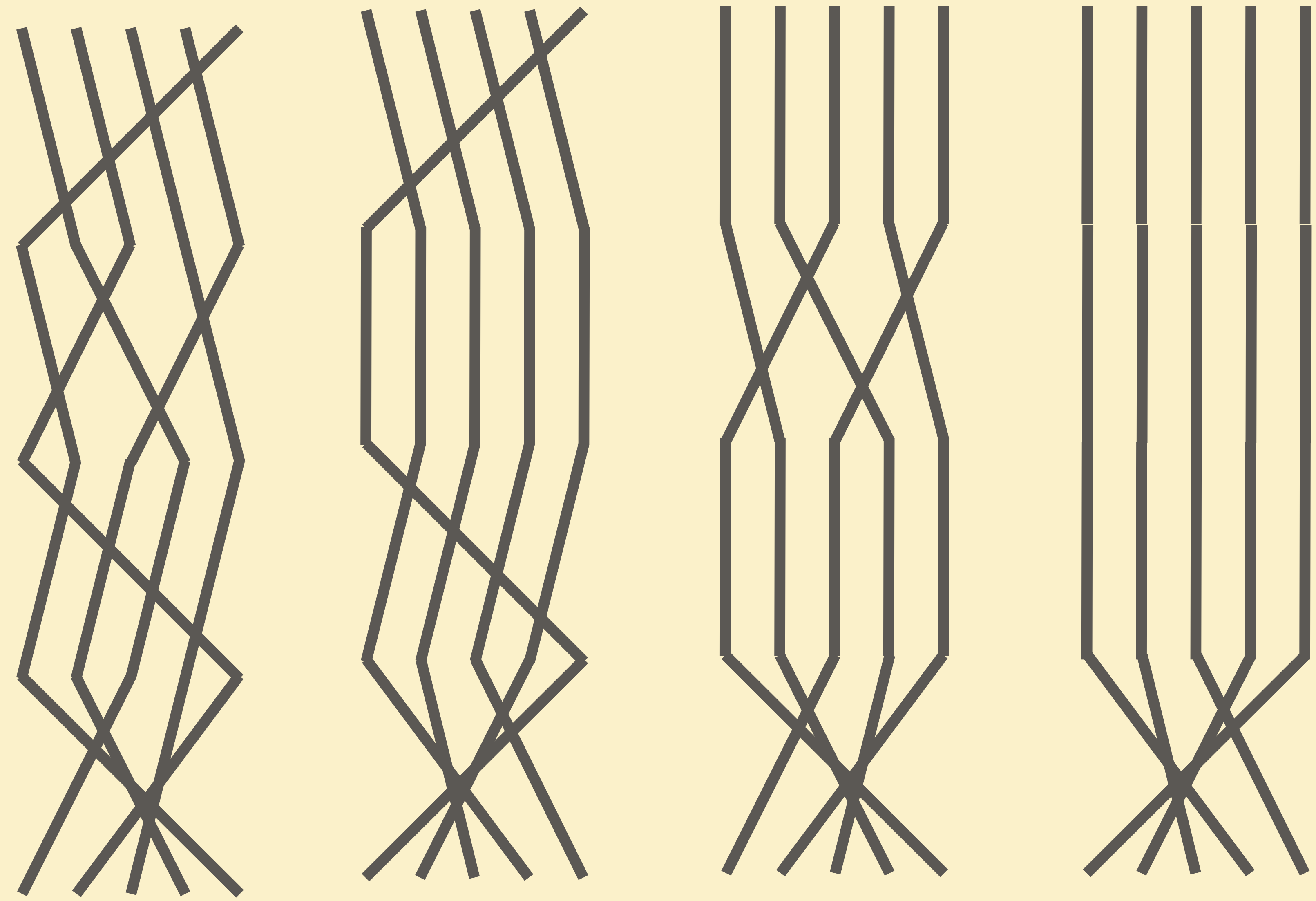
OR(0,0)	OR(0,1)	OR(1,0)	OR(1,1)
id	(14235)	(14235)	
0	1	1	

EXAMPLE PBP (OR)

length 4, width 5:

x_1	0: (12345)	1: id
y_1	0: (12453)	1: id
x_1	0: (54321)	1: id
y_1	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

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

[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

BARRINGTON'S THEOREM

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

- width 5

[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

BARRINGTON'S THEOREM

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

- width 5
- length polynomial in (n+m)

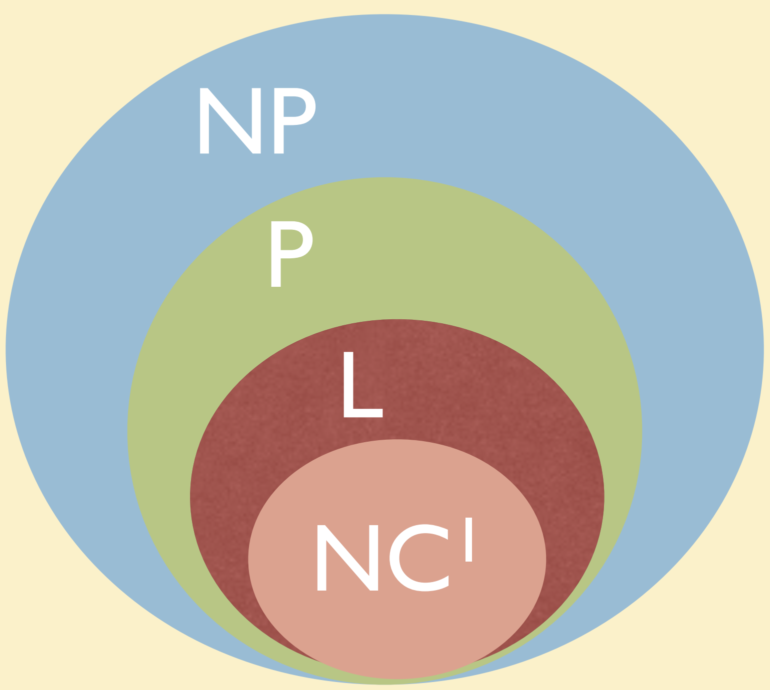
[Barrington 89] Bounded-Width Polynomial-Size Branching Programs Recognize Exactly Those Languages in NC1, J. Comput. Syst. Sci. 38 (1): 150–164, 1989
[BV11] Z. Brakerski, V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. FOCS 2011

BARRINGTON'S THEOREM

Theorem (variation): if $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ is in NC^1, then there exists a permutation branching program for f with:

- width 5
- length polynomial in (n+m)

no proof that $NP \neq NC^1$



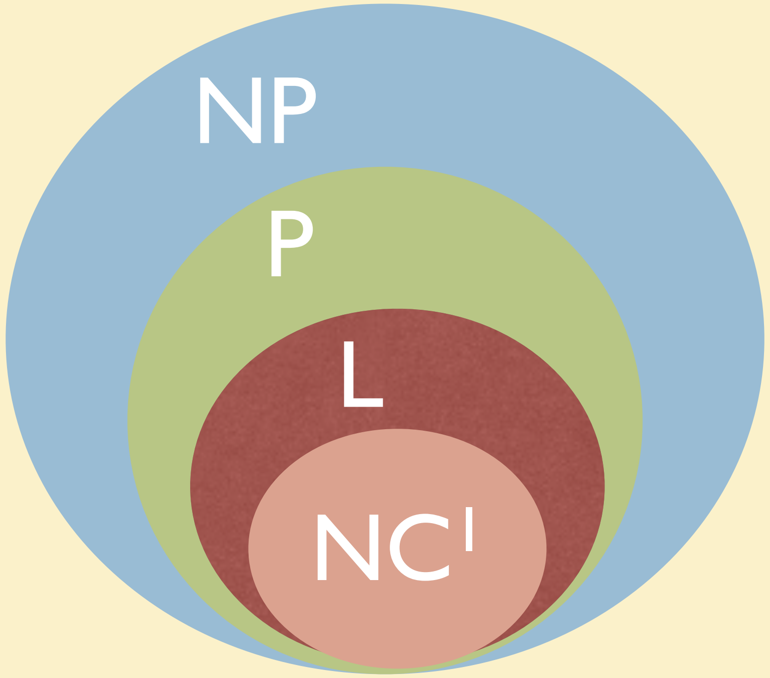
[Barrington 89] Bounded-Width Polynomial-Size Branching Programs Recognize Exactly Those Languages in NC1, J. Comput. Syst. Sci. 38 (1): 150–164, 1989
[BV11] Z. Brakerski, V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. FOCS 2011

BARRINGTON'S THEOREM

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

- width 5
- length polynomial in (n+m)

no proof that $NP \neq NC^1$

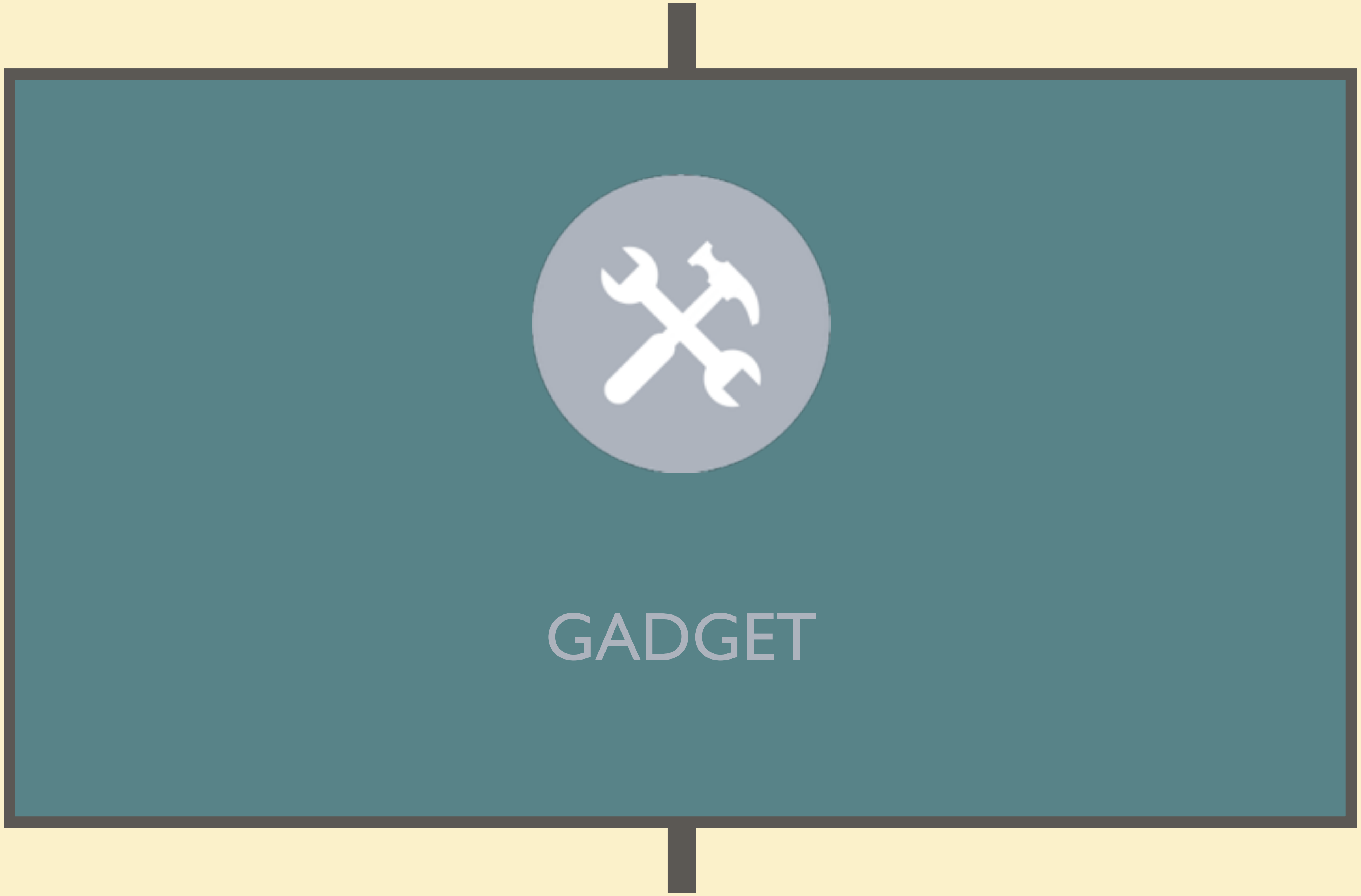


Classical homomorphic decryption functions happen to be in NC^1… [BV11]

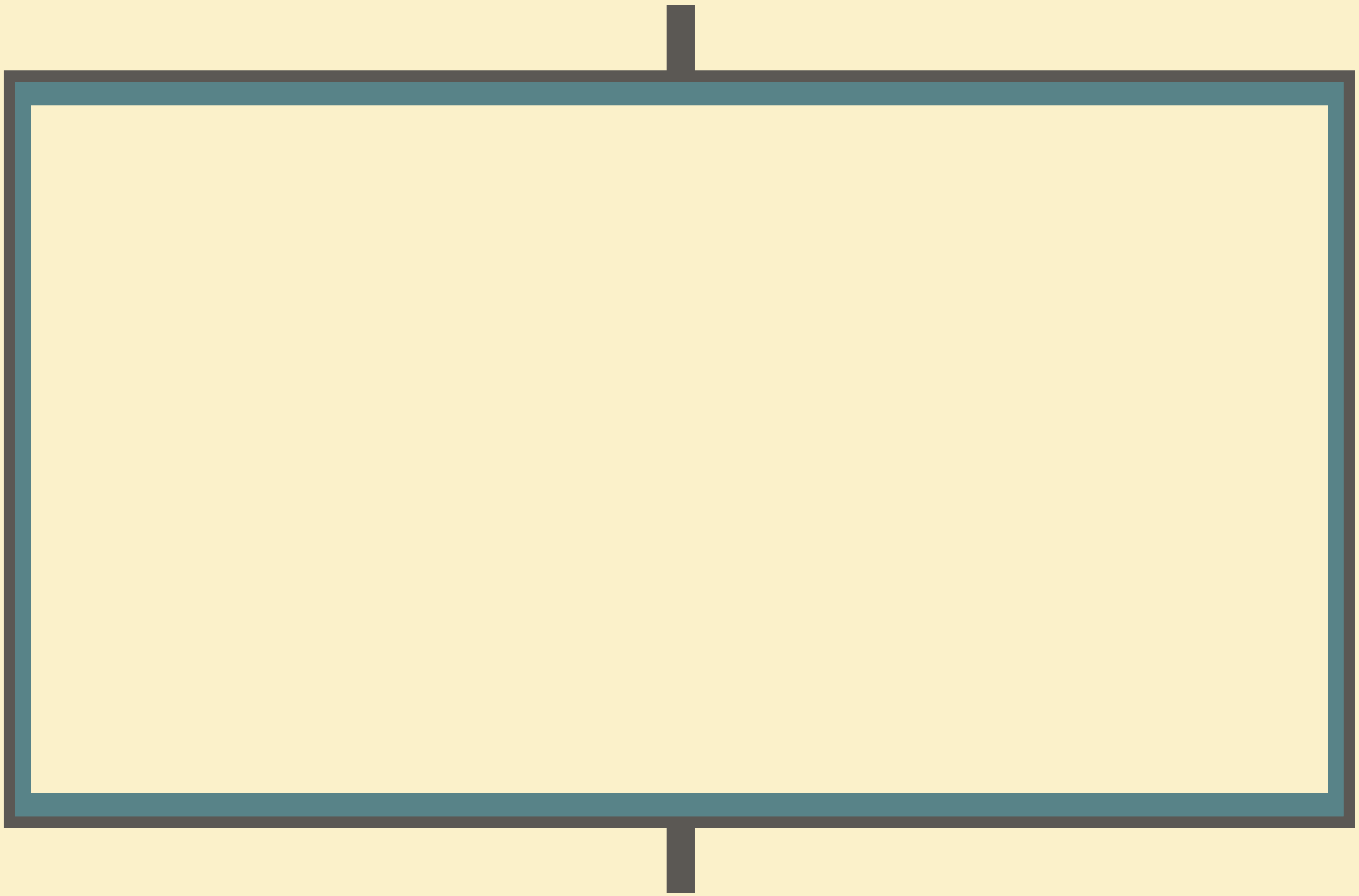
[Barrington 89] Bounded-Width Polynomial-Size Branching Programs Recognize Exactly Those Languages in NC1, J. Comput. Syst. Sci. 38 (1): 150–164, 1989
[BV11] Z. Brakerski, V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. FOCS 2011

ERROR CORRECTION GADGET

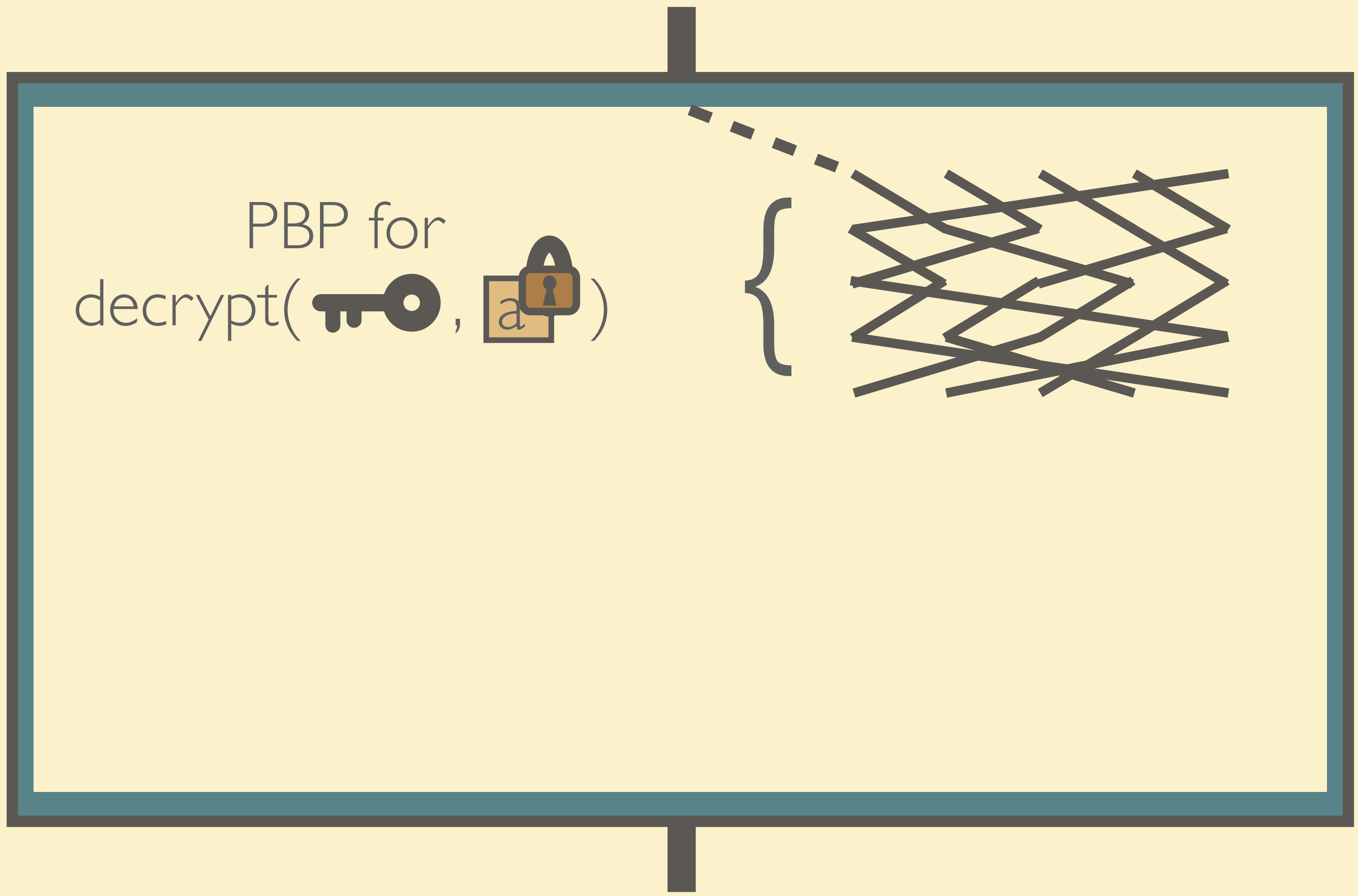
ERROR CORRECTION GADGET



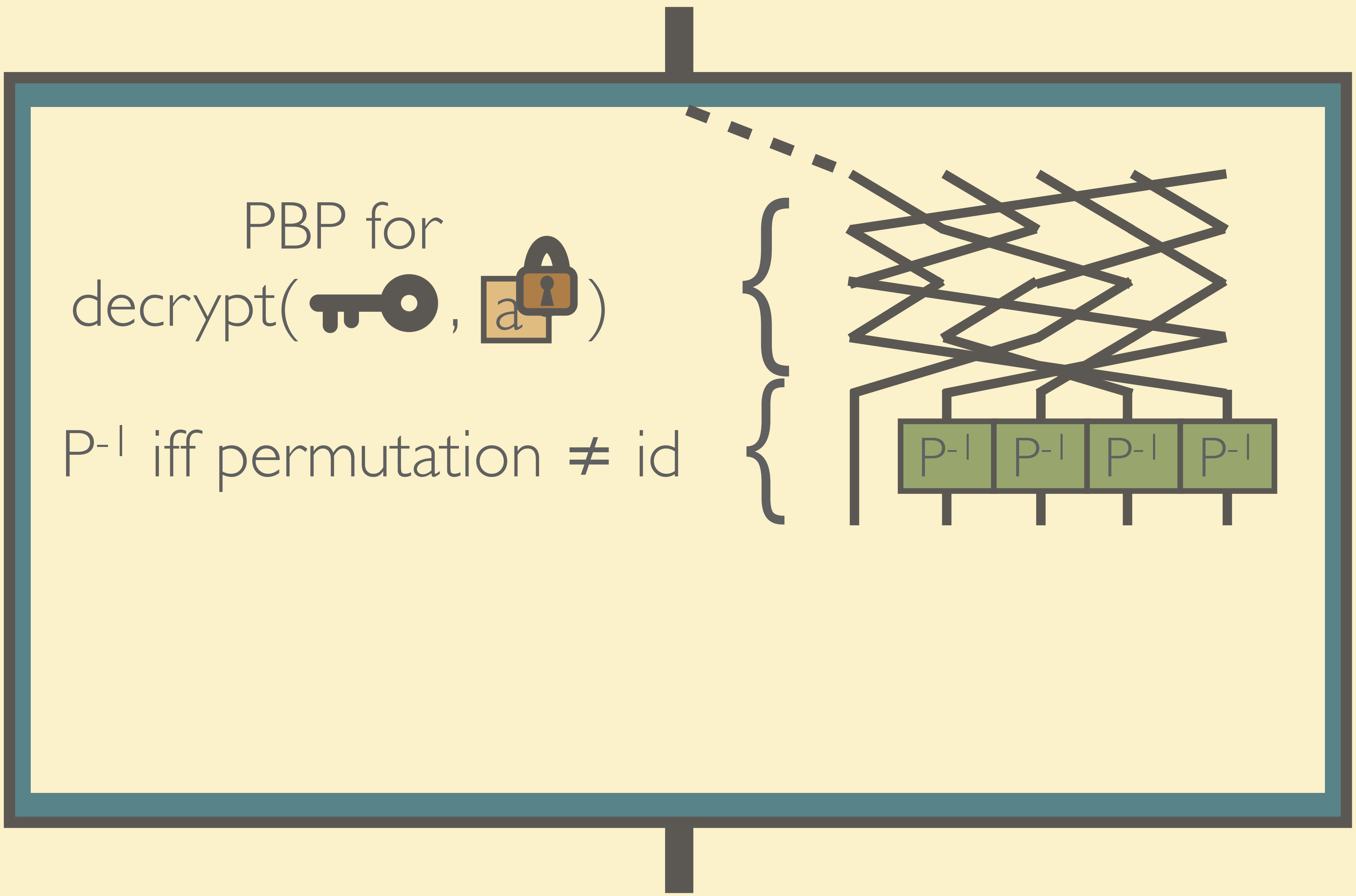
ERROR CORRECTION GADGET



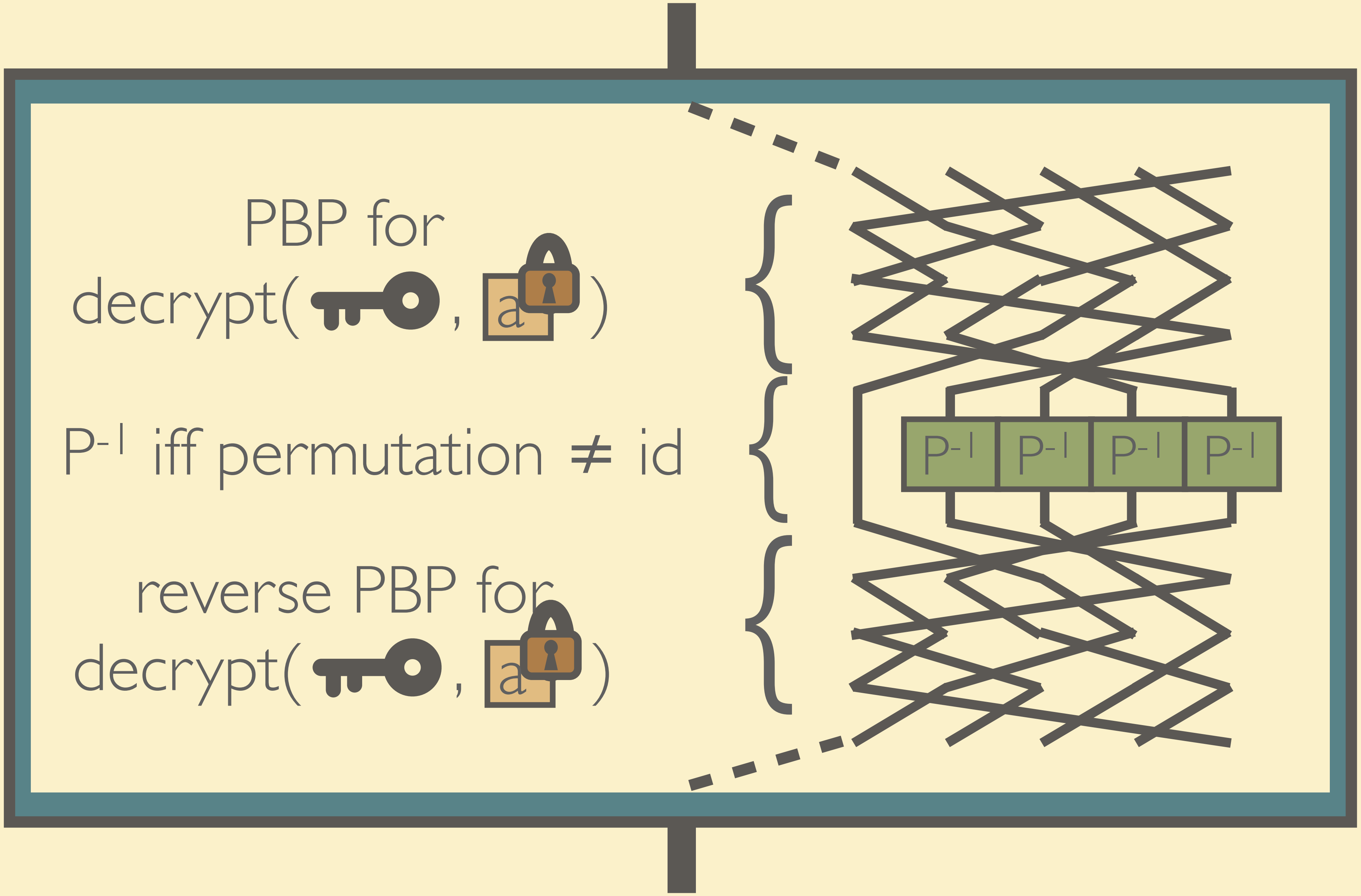
ERROR CORRECTION GADGET



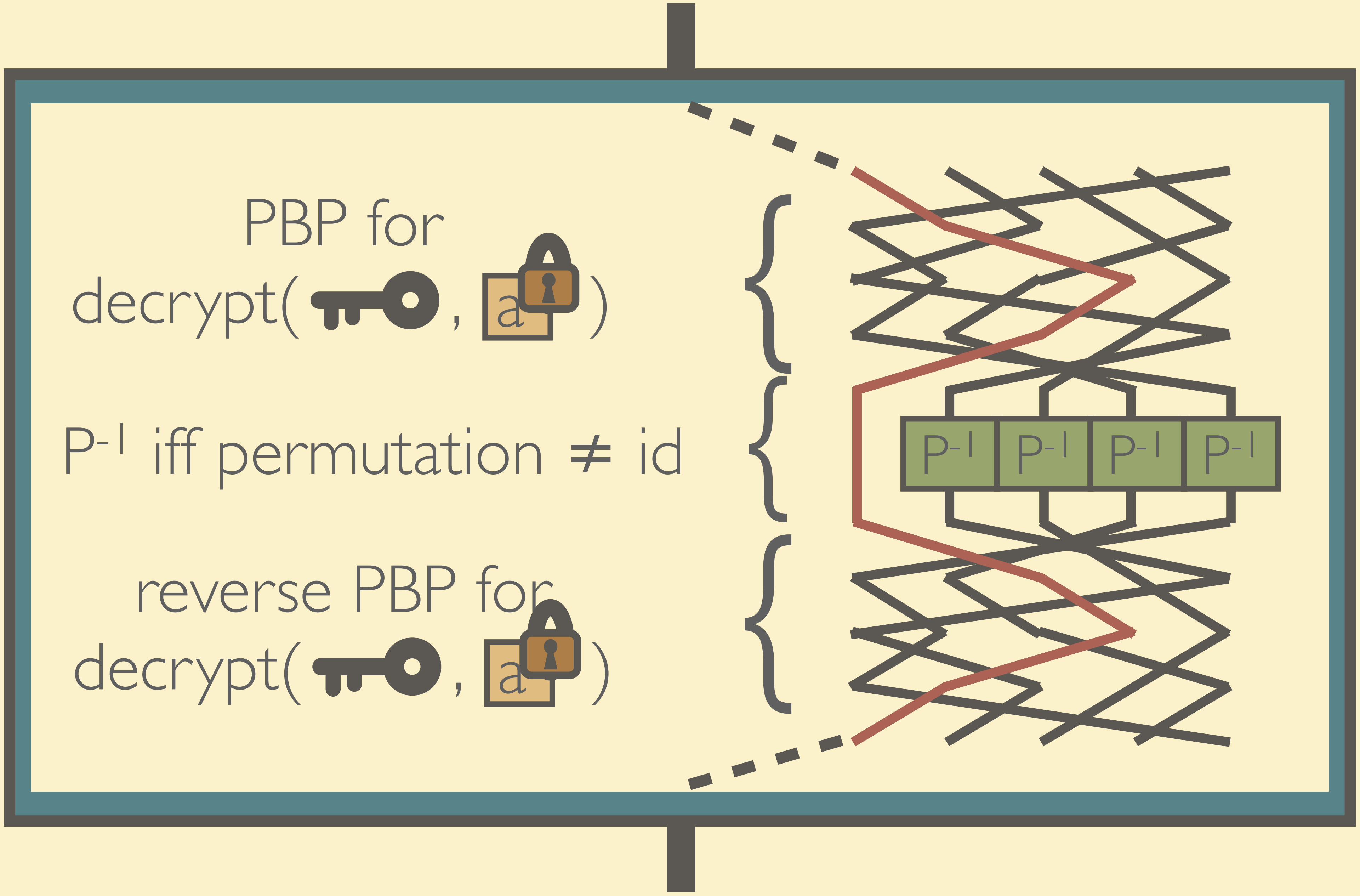
ERROR CORRECTION GADGET



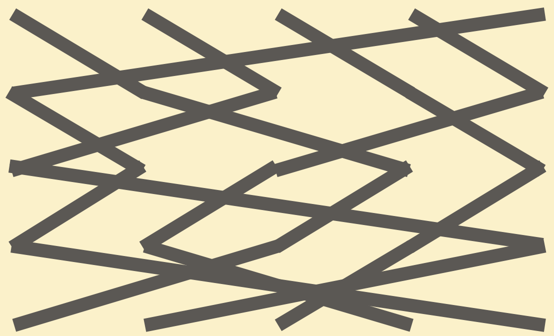
ERROR CORRECTION GADGET



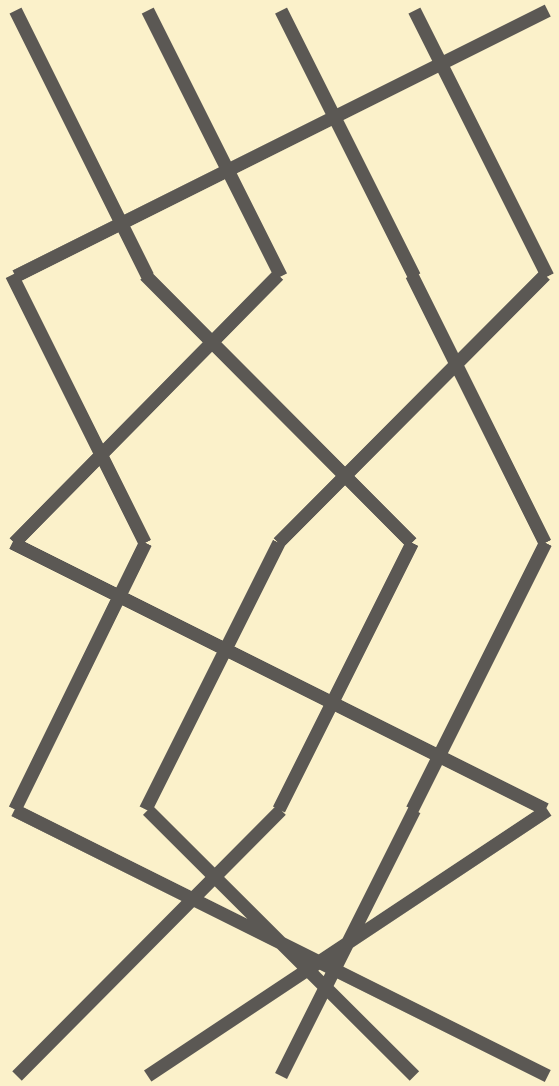
ERROR CORRECTION GADGET



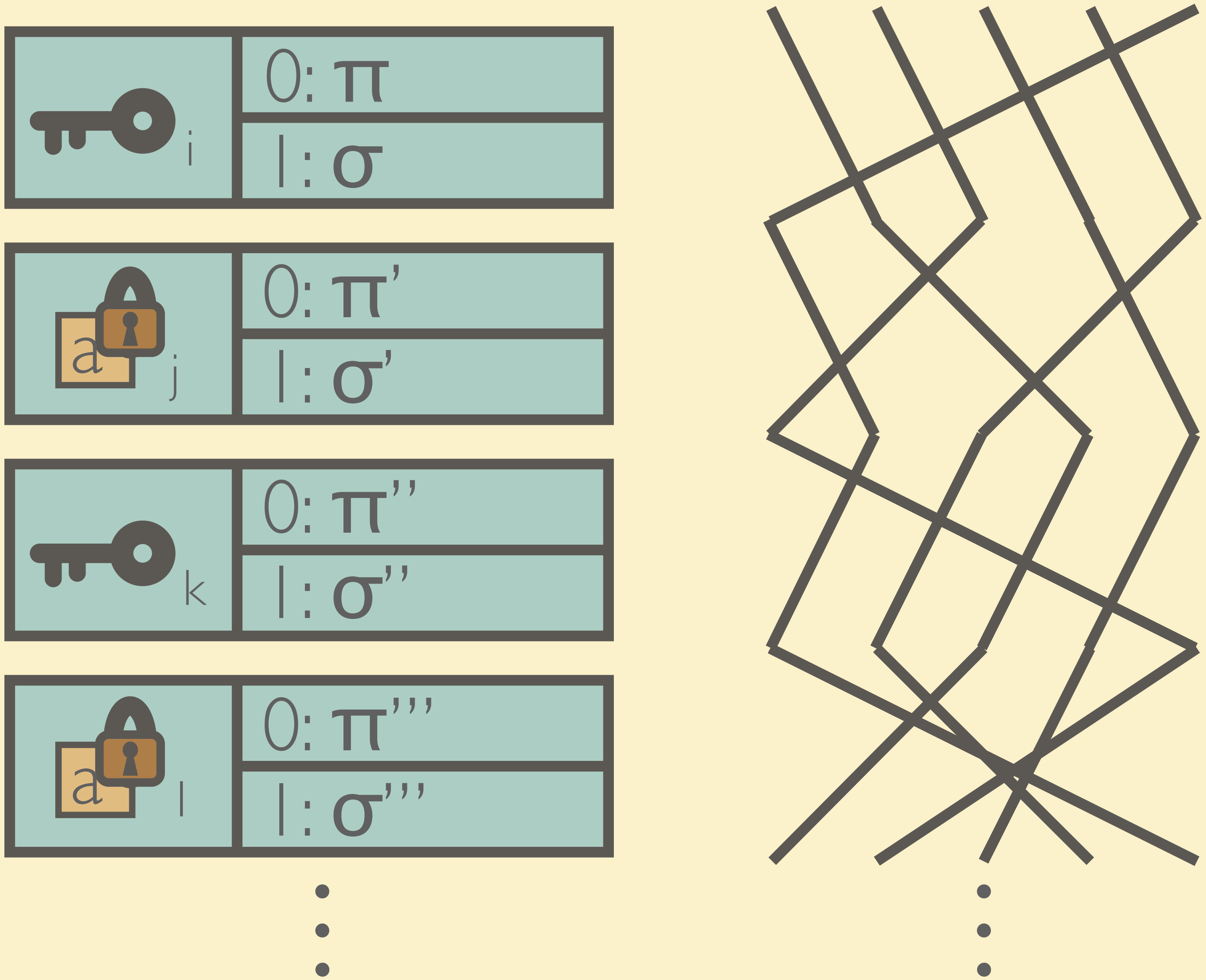
ERROR CORRECTION GADGET



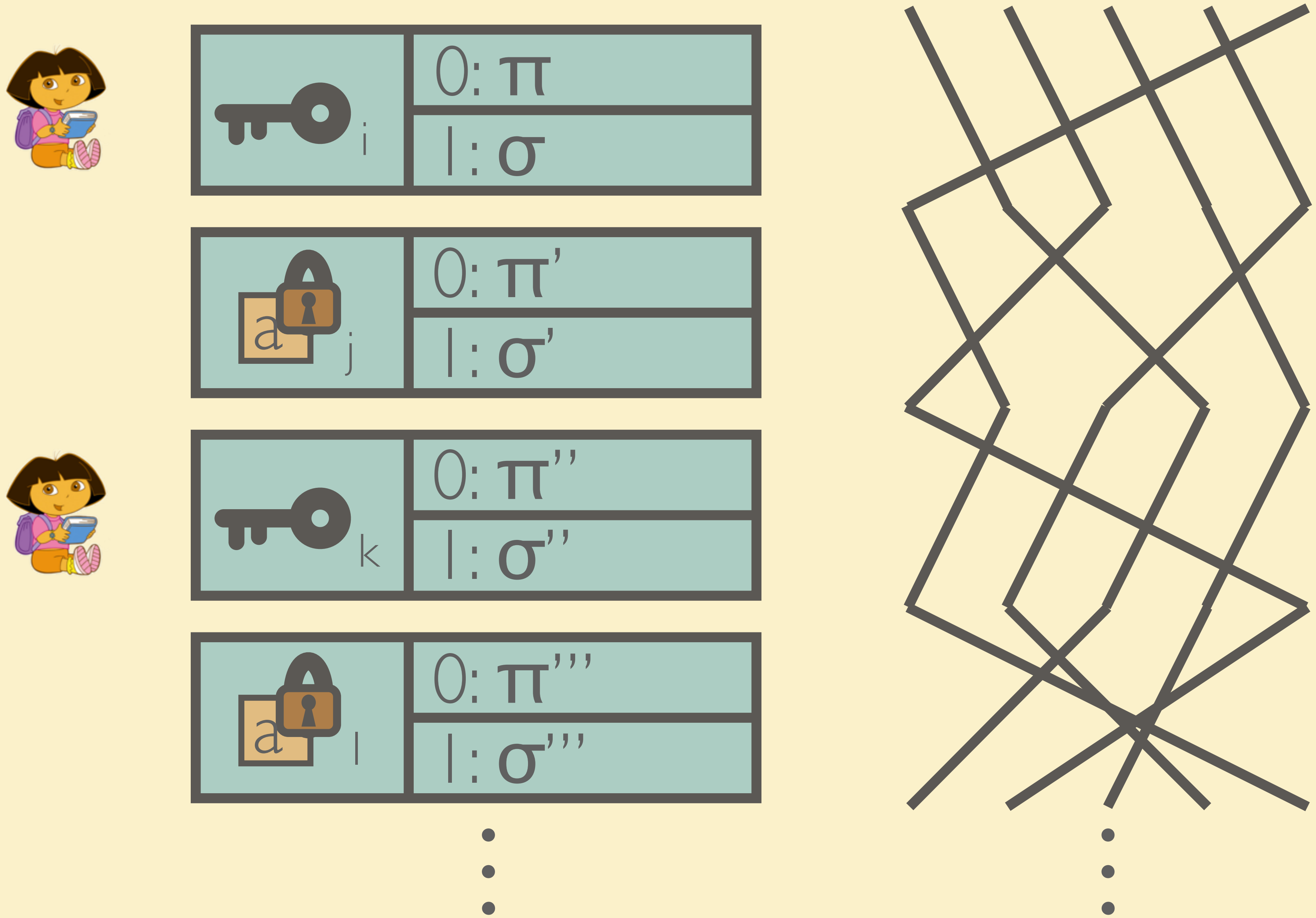
ERROR CORRECTION GADGET



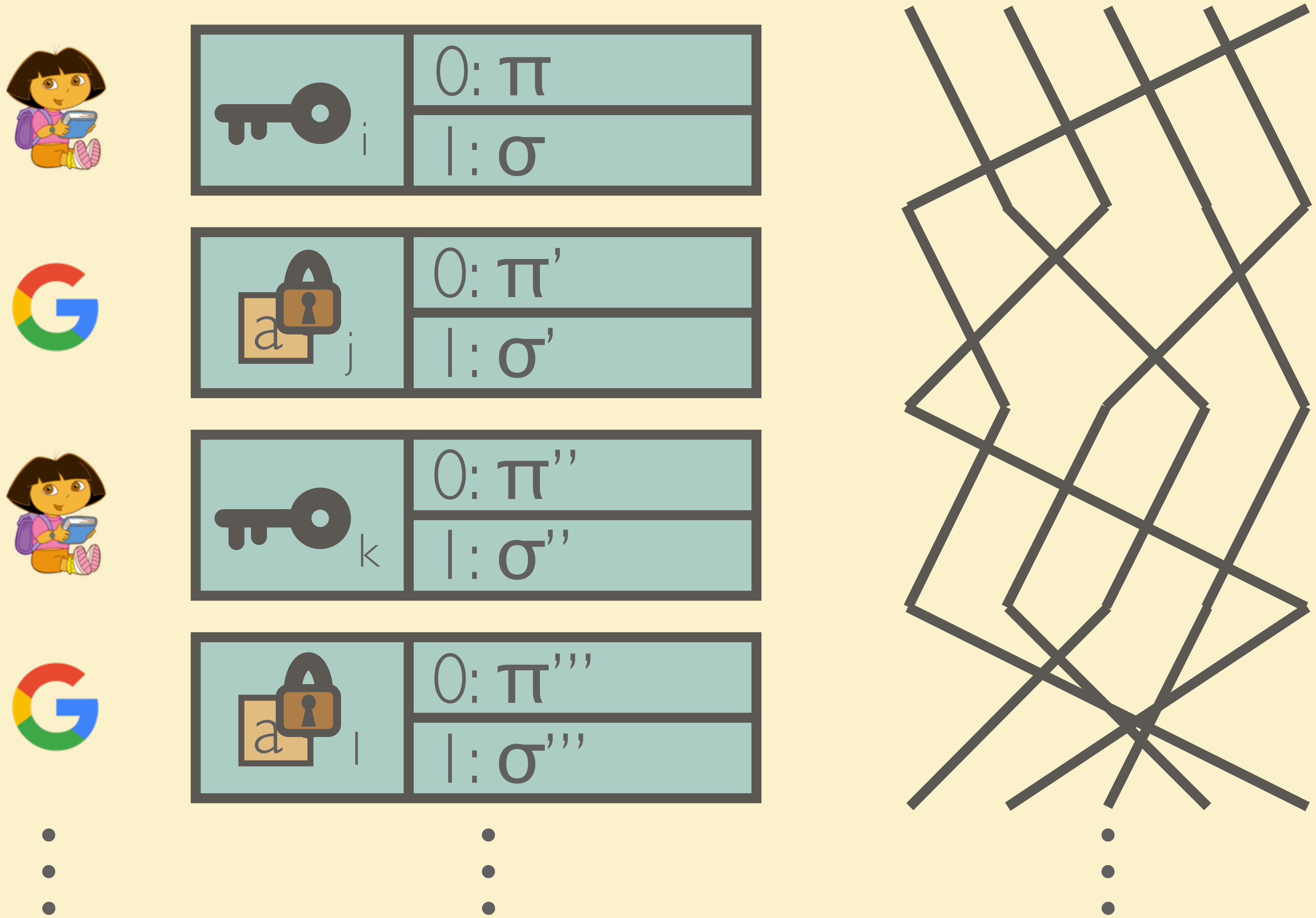
ERROR CORRECTION GADGET



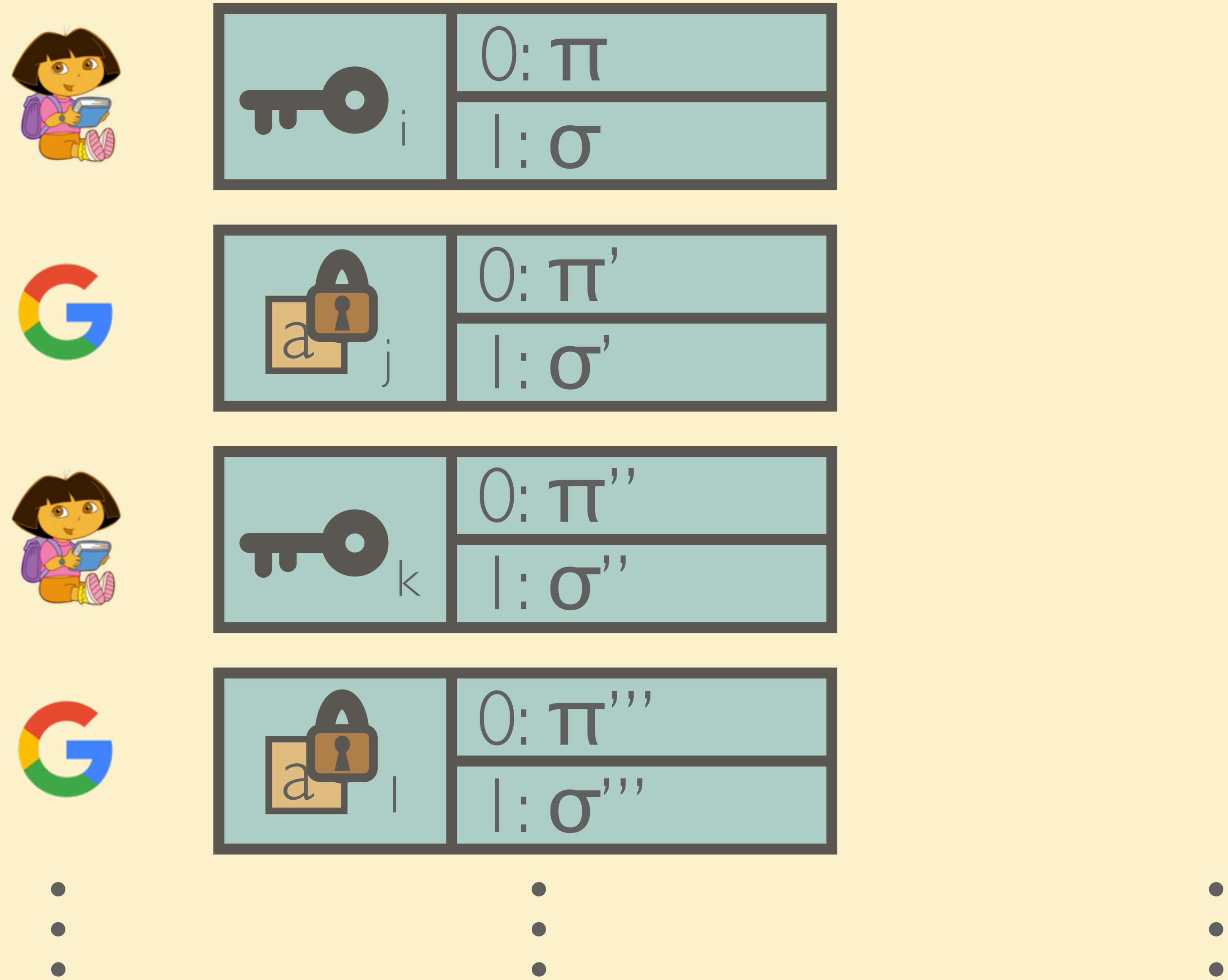
ERROR CORRECTION GADGET



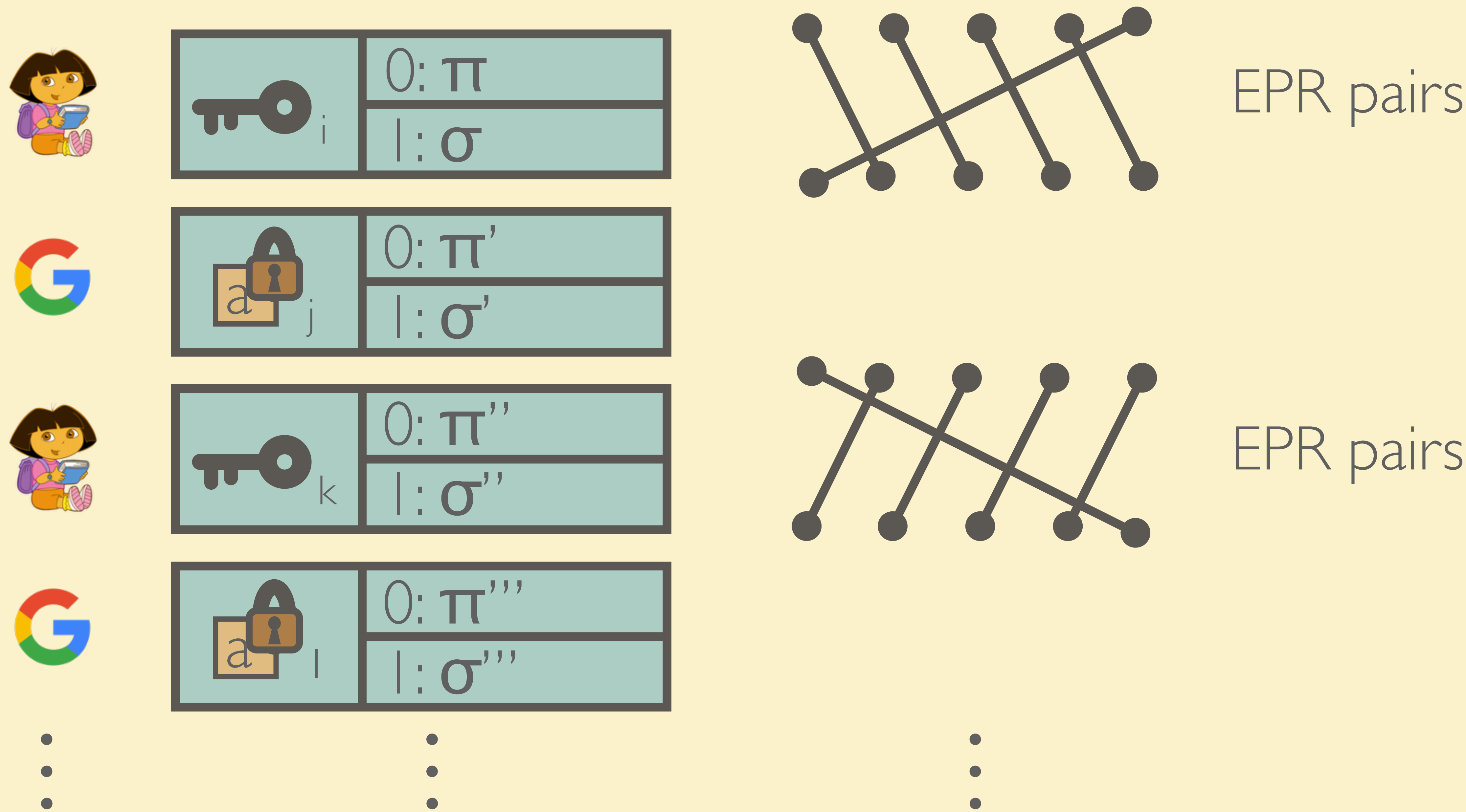
ERROR CORRECTION GADGET



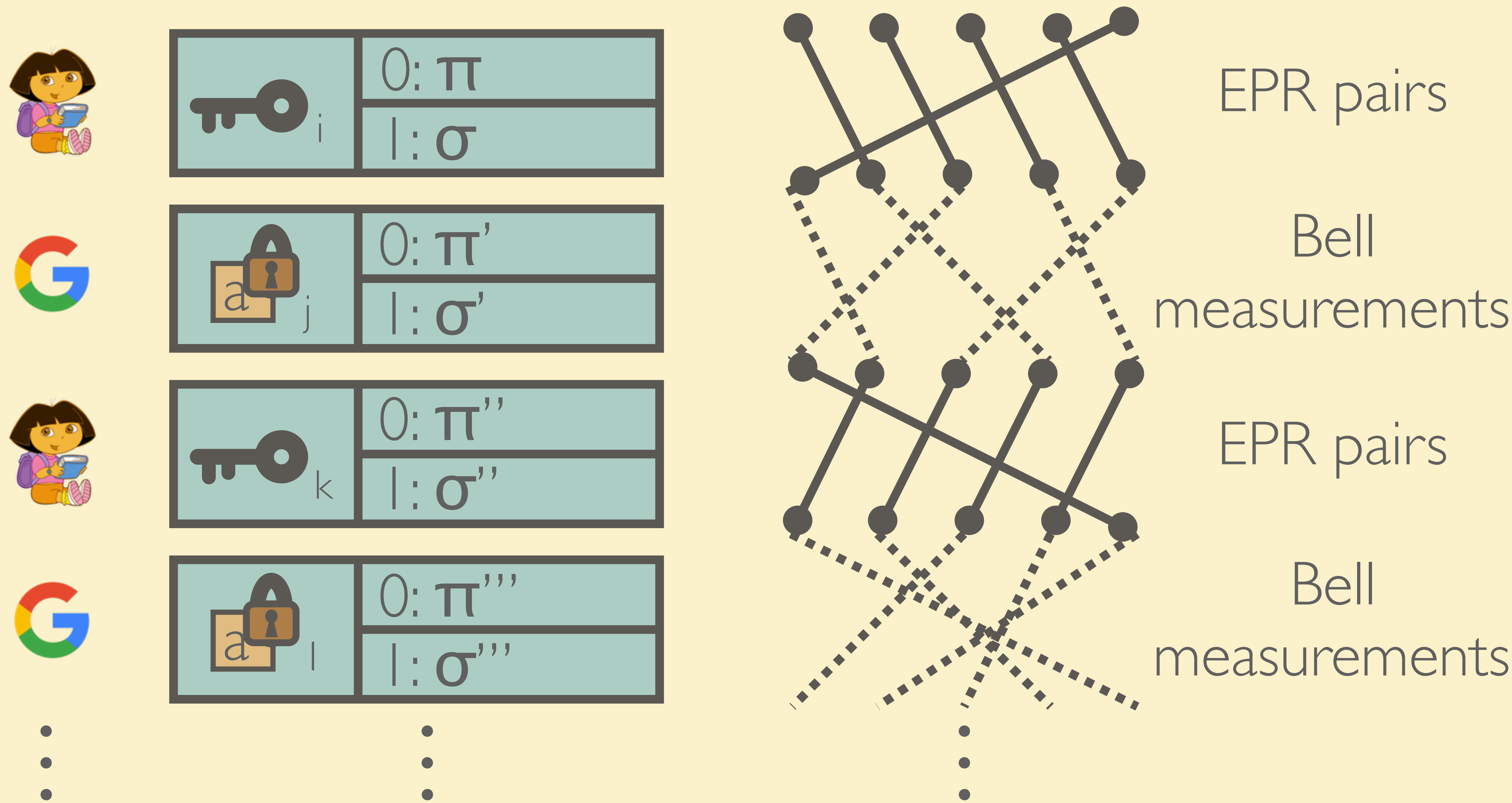
ERROR CORRECTION GADGET



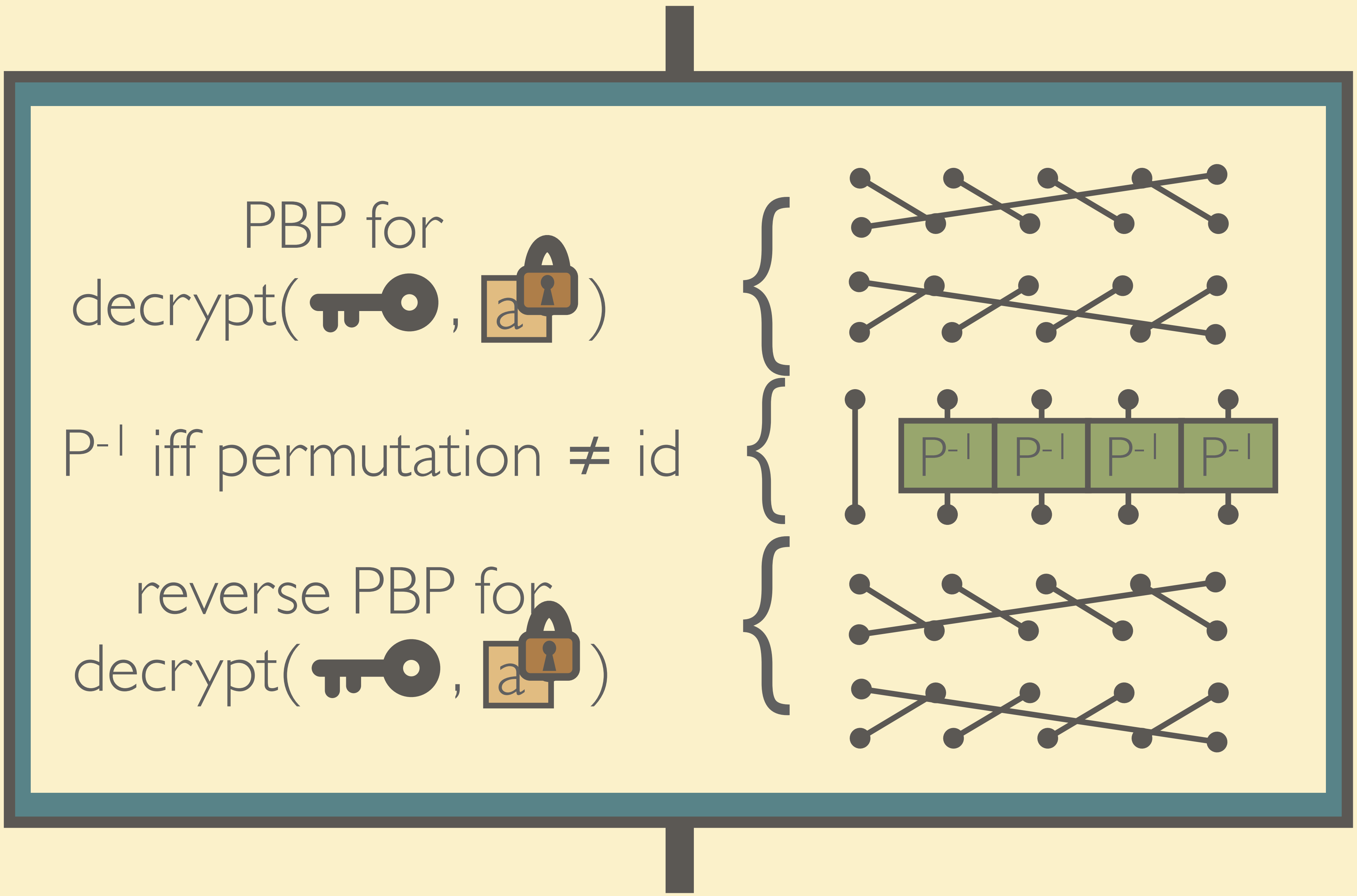
ERROR CORRECTION GADGET



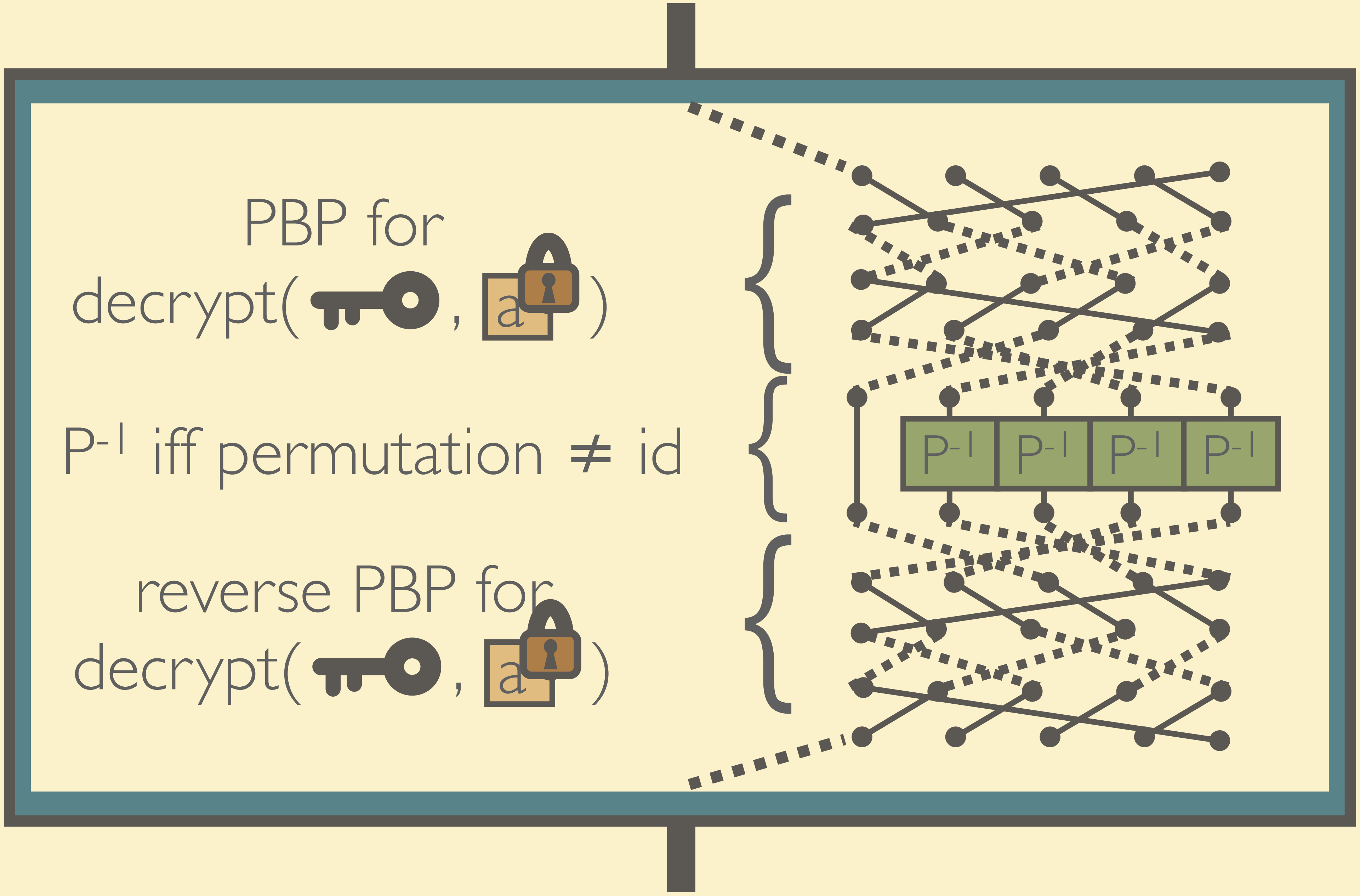
ERROR CORRECTION GADGET



ERROR CORRECTION GADGET



ERROR CORRECTION GADGET



NEW SCHEME: OVERVIEW

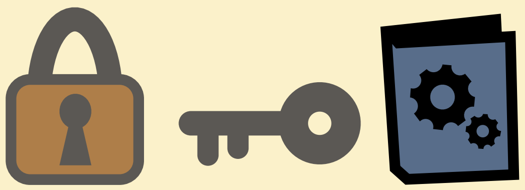
NEW SCHEME: OVERVIEW

KEY GENERATION

NEW SCHEME: OVERVIEW

KEY GENERATION

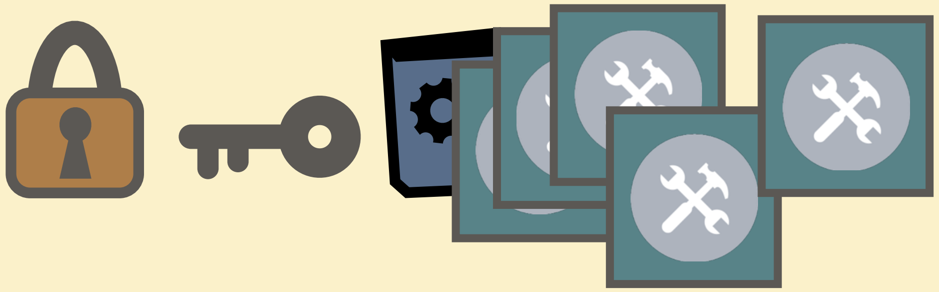
- classical keys



NEW SCHEME: OVERVIEW

KEY GENERATION

- classical keys
- gadgets

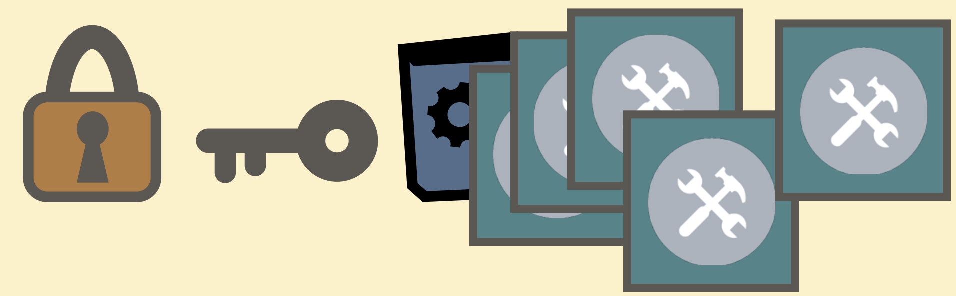


NEW SCHEME: OVERVIEW

KEY GENERATION

- classical keys
- gadgets

ENCRYPTION

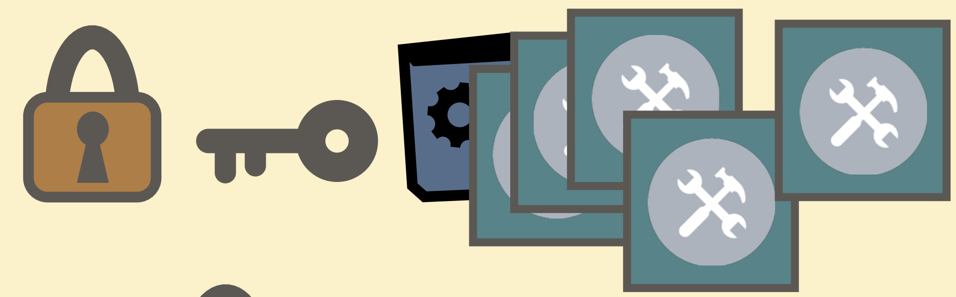


$|\psi\rangle$

NEW SCHEME: OVERVIEW

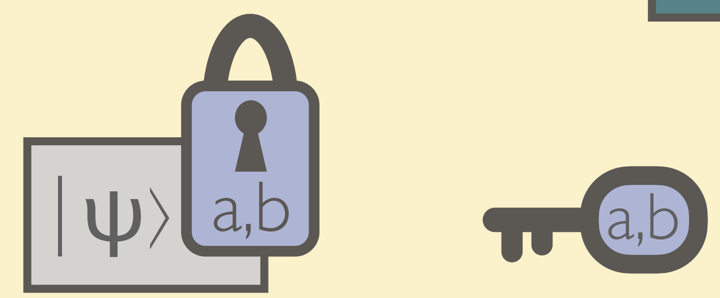
KEY GENERATION

- classical keys
- gadgets



ENCRYPTION

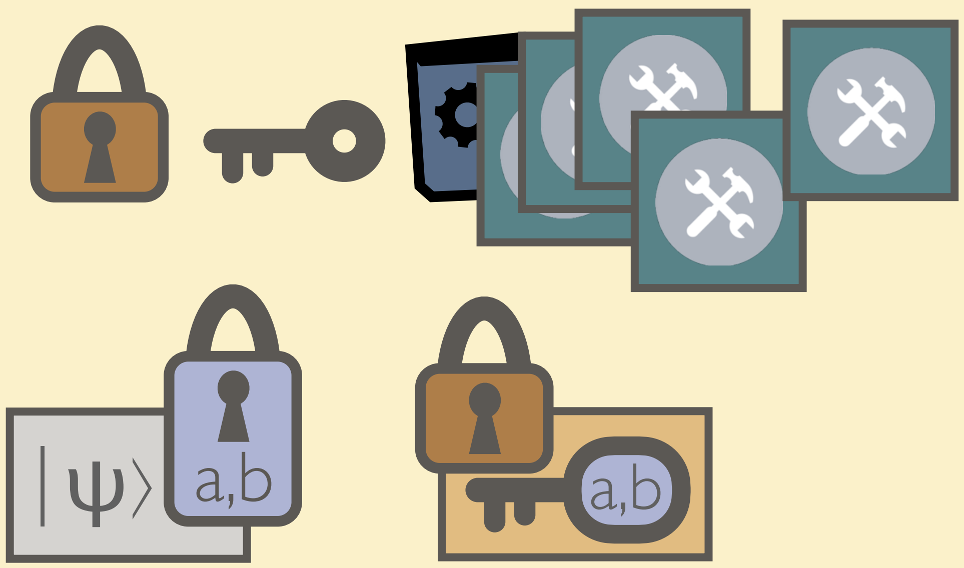
- apply quantum one-time pad



NEW SCHEME: OVERVIEW

KEY GENERATION
- classical keys
- gadgets

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



NEW SCHEME: OVERVIEW

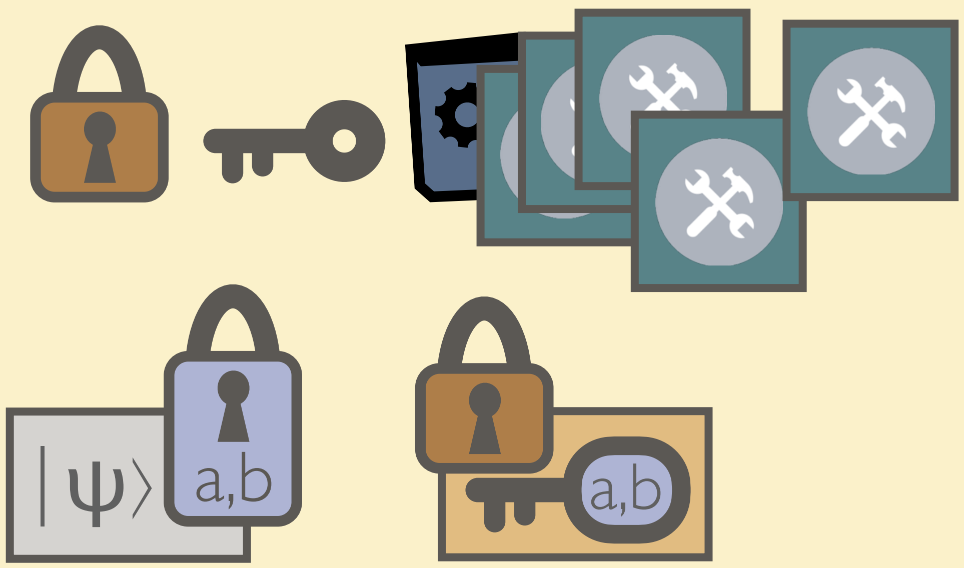
KEY GENERATION

- classical keys
- gadgets

ENCRYPTION

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

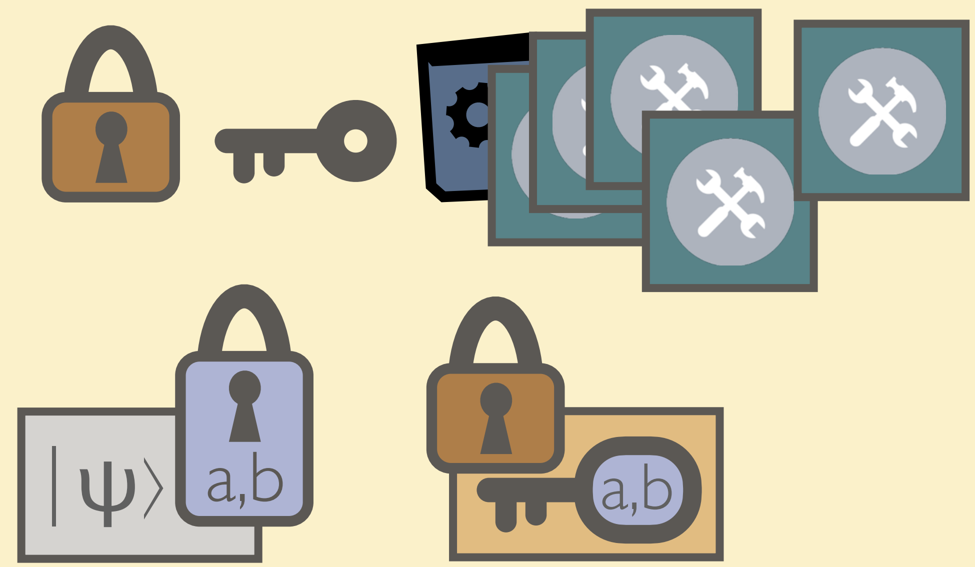
EVALUATION



NEW SCHEME: OVERVIEW

KEY GENERATION

- classical keys
- gadgets



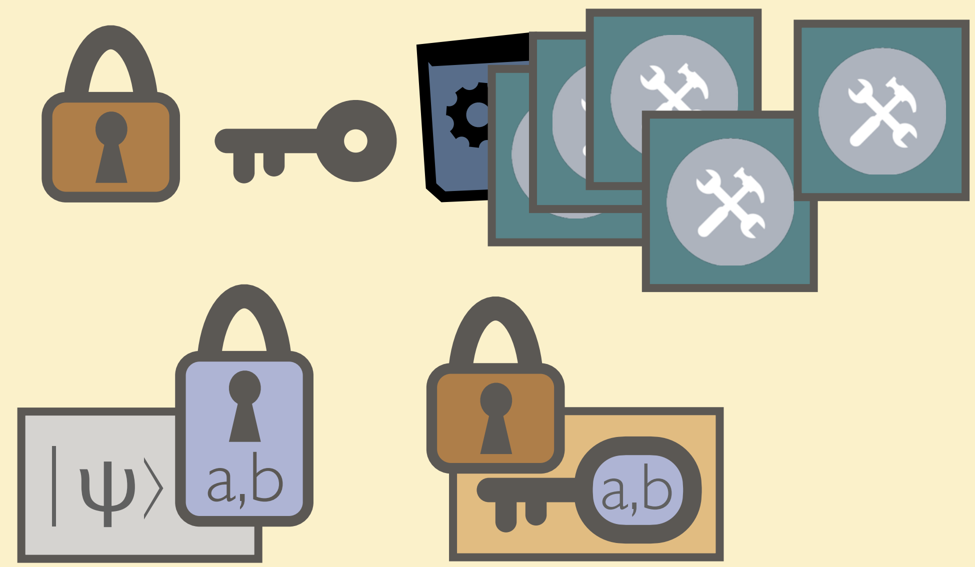
ENCRYPTION

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

EVALUATION

- after H / P / CNOT: classically update keys

NEW SCHEME: OVERVIEW



KEY GENERATION

- classical keys
- gadgets

ENCRYPTION

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

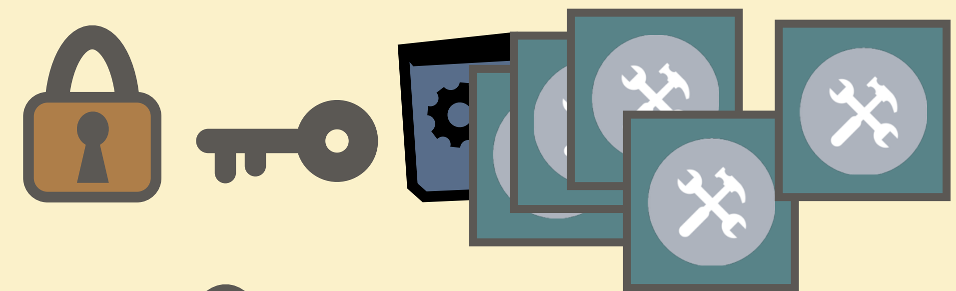
EVALUATION

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

NEW SCHEME: OVERVIEW

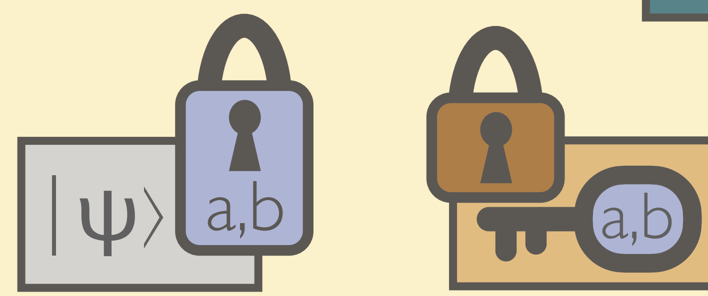
KEY GENERATION

- classical keys
- gadgets



ENCRYPTION

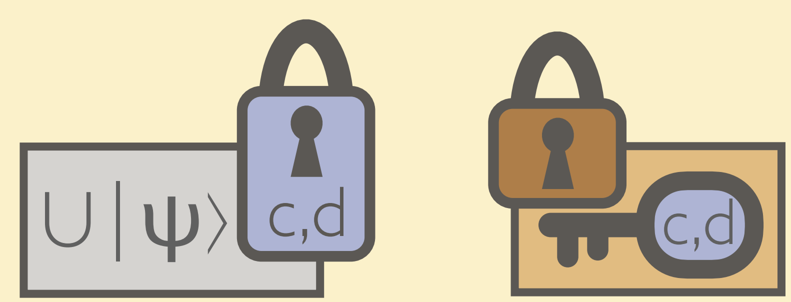
- apply quantum one-time pad
- classically encrypt pad keys



EVALUATION

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

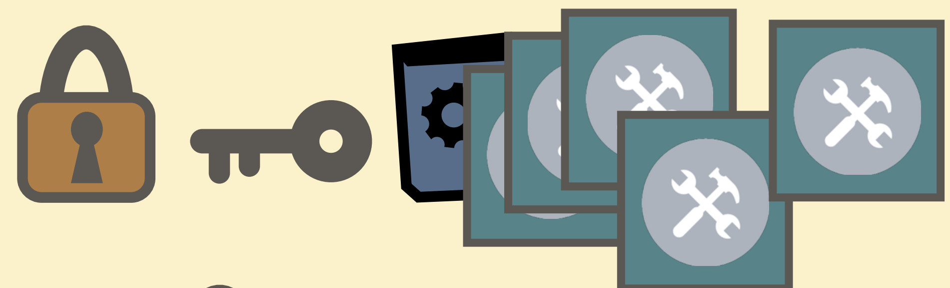
DECRYPTION



NEW SCHEME: OVERVIEW

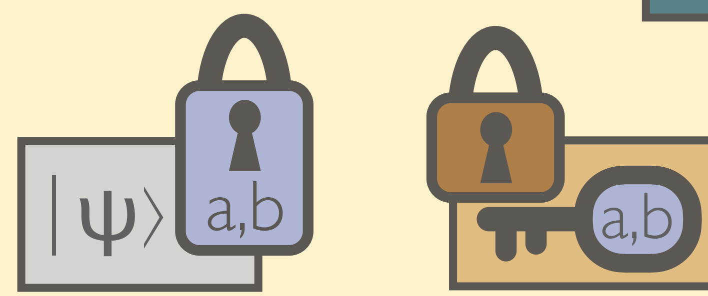
KEY GENERATION

- classical keys
- gadgets



ENCRYPTION

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



EVALUATION

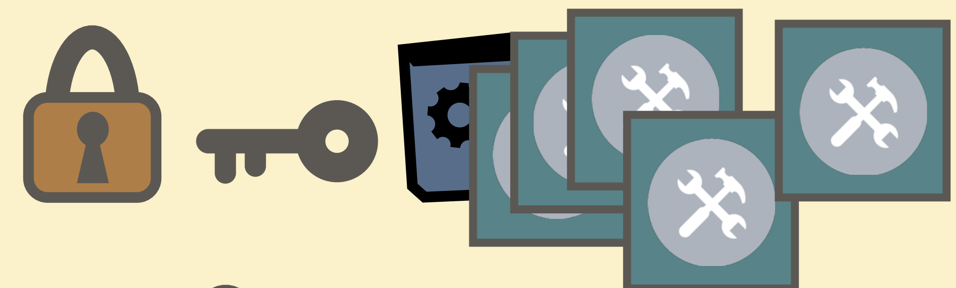
- after H / P / CNOT: classically update keys
- after T : use 

DECRYPTION

- classically decrypt pad keys

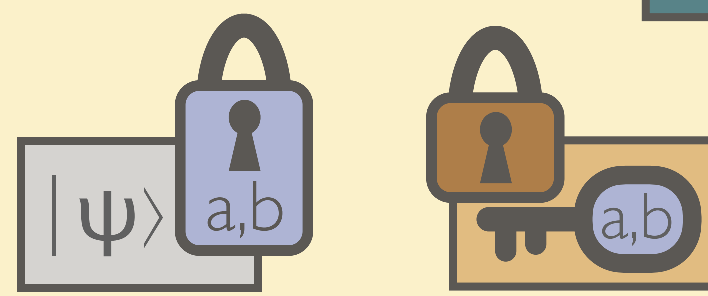
NEW SCHEME: OVERVIEW

KEY GENERATION



- classical keys
- gadgets

ENCRYPTION



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

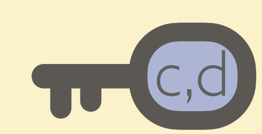
EVALUATION

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

DECRYPTION

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

$U|\psi\rangle$



FUTURE WORK

FUTURE WORK

- non-leveled QFHE?

FUTURE WORK

- non-leveled QFHE?
- verifiable delegated quantum computation

FUTURE WORK

- non-leveled QFHE?
- verifiable delegated quantum computation
- quantum obfuscation?

FUTURE WORK

- non-leveled QFHE?
- verifiable delegated quantum computation
- quantum obfuscation?
- …

THANK YOU!

QuSoft is hiring two principle investigators:
http://tinyurl.com/qusoft-job
Application deadline: 1 September 2016