Weak approximate unitary designs and applications to quantum encryption

Cécilia Lancien and **Christian Majenz**

Quantum Information Seminar@Perimeter Institute for Theoretical Physics

Remotely delivered from Copenhagen, Denmark

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

QuSoft
Research Center for Quantum Software

CWI
Centrum Wiskunde & Informatica

Results — overview

- We show that **very small approximate unitary t-designs** exist when the approximation error is measured in certain **non-stabilized norms**.
- This extends the line of work started by Hayden, Leung, Shor and Winter (CMP 04)
- Our proofs rely on a technical result by Aubrun (CMP 09)
- As an **application**, we exhibit a probabilistic construction of a **quantum encryption scheme** that is non-malleable against adversaries with no (or limited) quantum side information.

Introduction

The Haar measure

The Haar measure

- Natural ‘uniform’ probability measure on compact groups

The Haar measure

- Natural 'uniform' probability measure on compact groups
- Can be pushed forward to homogeneous spaces

The Haar measure

- Natural ‘uniform’ probability measure on compact groups
- Can be pushed forward to homogeneous spaces
- Quantum information: Unitary group, projective space (=set of pure states)

The Haar measure in quantum information

The Haar measure in quantum information

Countless applications…

The Haar measure in quantum information

Countless applications…

- Entanglement theory

The Haar measure in quantum information

Countless applications…

- Entanglement theory
- Coding theorems (noiseless, slepian-wolf, channel coding)

The Haar measure in quantum information

Countless applications…

- Entanglement theory
- Coding theorems (noiseless, slepian-wolf, channel coding)
- Existence proofs using probabilistic method, randomized constructions

The Haar measure in quantum information

Countless applications…

- Entanglement theory
- Coding theorems (noiseless, slepian-wolf, channel coding)
- **Existence proofs using probabilistic method, randomized constructions**

Designs

Designs

Definition: A t-design for a homogeneous space H is a finite subset $D \subset H$ that reproduces Haar expectation values of polynomials* on of degree t.

Designs

Definition: A t-design for a homogeneous space H is a finite subset $D \subset H$ that reproduces Haar expectation values of polynomials* on of degree t.

First example: Spherical designs

Designs

Definition: A t-design for a homogeneous space H is a finite subset $D \subset H$ that reproduces Haar expectation values of polynomials* on of degree t.

First example: Spherical designs

In quantum info: state designs, unitary desigs

Designs

Definition: A t-design for a homogeneous space H is a finite subset $D \subset H$ that reproduces Haar expectation values of polynomials* on of degree t.

First example: Spherical designs

In quantum info: state designs, unitary desigs

Other: Grassmannian designs

Designs

Definition: A t-design for a homogeneous space H is a finite subset $D \subset H$ that reproduces Haar expectation values of polynomials* on of degree t.

First example: Spherical designs

In quantum info: state designs, **unitary desigs**

Other: Grassmannian designs

Twirling channels

Twirling channels

Basic property of the Haar measure:

$$\mathop{\mathbb{E}}_{U \sim \mathrm{Haar}_d} \left[U X U^\dagger \right] = \frac{\mathrm{Tr}[X]}{d} \mathbb{I}$$

Twirling channels

Basic property of the Haar measure:

$$\mathop{\mathbb{E}}_{U\sim \mathrm{Haar}_d}\left[UXU^\dagger\right] = \frac{\mathrm{Tr}[X]}{d}\mathbb{I}$$

Haar measure implements depolarizing channel $T^{(1)}$

Twirling channels

Basic property of the Haar measure:

$$\mathop{\mathbb{E}}_{U\sim\mathrm{Haar}_d}\left[UXU^\dagger\right] = \frac{\mathrm{Tr}[X]}{d}\mathbb{I}$$

Haar measure implements depolarizing channel $T^{(1)}$

Twirling channels:

$$T^{(t)}(X) = \mathop{\mathbb{E}}_{U\sim\mathrm{Haar}_d}\left[U^{\otimes t}X\left(U^{\otimes t}\right)^\dagger\right]$$

Twirling channels

Basic property of the Haar measure:

$$\mathop{\mathbb{E}}_{U\sim\mathrm{Haar}_d}\left[UXU^\dagger\right] = \frac{\mathrm{Tr}[X]}{d}\mathbb{I}$$

Haar measure implements depolarizing channel $T^{(1)}$

Twirling channels:

$$T^{(t)}(X) = \mathop{\mathbb{E}}_{U\sim\mathrm{Haar}_d}\left[U^{\otimes t}X\left(U^{\otimes t}\right)^\dagger\right]$$

$$T^{(1,1)}(X) = \mathop{\mathbb{E}}_{U\sim\mathrm{Haar}_d}\left[\left(U\otimes\bar{U}\right)X\left(U^\dagger\otimes U^T\right)\right]$$

Approximate unitary designs

$D \subset H$ is a unitary t-design $\Leftrightarrow$ $$T^{(t)} = T^{(t)}_D := \frac{1}{|D|} \sum_{U \in D} U^{\otimes t}(\,\cdot\,)\left(U^{\otimes t}\right)^\dagger$$

Approximate unitary designs

$D \subset H$ is a unitary t-design $\quad \Leftrightarrow \quad T^{(t)} = T_D^{(t)} := \frac{1}{|D|} \sum_{U \in D} U^{\otimes t}(\,\cdot\,)\left(U^{\otimes t}\right)^{\dagger}$

Natural definition of approximate unitary t-designs:

$D \subset H$ is an ε-approximate unitary t-design $\quad \Leftrightarrow \quad \left\| T^{(t)} - T_D^{(t)} \right\| \leq \varepsilon$

Approximate unitary designs

$D \subset H$ is a unitary t-design $\Leftrightarrow$ $T^{(t)} = T_D^{(t)} := \frac{1}{|D|} \sum_{U \in D} U^{\otimes t} (\cdot) \left(U^{\otimes t} \right)^{\dagger}$

Natural definition of approximate unitary t-designs:

$D \subset H$ is an ε-approximate unitary t-design $\Leftrightarrow$ $\left\| T^{(t)} - T_D^{(t)} \right\| \leq \varepsilon$

What norm should we use?

Approximate unitary designs

$D \subset H$ is a unitary t-design $\Leftrightarrow$ $T^{(t)} = T^{(t)}_D := \frac{1}{|D|} \sum_{U \in D} U^{\otimes t}(\,\cdot\,)\left(U^{\otimes t}\right)^\dagger$

Natural definition of approximate unitary t-designs:

$D \subset H$ is an ε-approximate unitary t-design $\Leftrightarrow$ $\left\| T^{(t)} - T^{(t)}_D \right\| \leq \varepsilon$

What norm should we use?

In quantum information theory:
$\|\cdot\|_\diamond$ most natural

Approximate unitary designs

$D \subset H$ is a unitary t-design $\quad\Leftrightarrow\quad$ $T^{(t)} = T_D^{(t)} := \frac{1}{|D|} \sum_{U \in D} U^{\otimes t}(\,\cdot\,)\left(U^{\otimes t}\right)^{\dagger}$

Natural definition of approximate unitary t-designs:

$D \subset H$ is an ε-approximate unitary t-design $\quad\Leftrightarrow\quad$ $\left\| T^{(t)} - T_D^{(t)} \right\|_{\diamond} \leq \varepsilon$

Approximate unitary designs

$D \subset H$ is a unitary t-design $\Leftrightarrow$ $T^{(t)} = T_D^{(t)} := \frac{1}{|D|} \sum_{U \in D} U^{\otimes t} (\,\cdot\,) \left(U^{\otimes t}\right)^{\dagger}$

Natural definition of approximate unitary t-designs:

$D \subset H$ is an ε-approximate unitary t-design $\Leftrightarrow$ $\left\| T^{(t)} - T_D^{(t)} \right\|_{\diamond} \leq \varepsilon$

Plenty of constructions: Random quantum circuits (BHH 16), random quantum circuits with a lot of structure (HMMHEGR 20, also CLLW 15, NHMW 17 for 2-designs)

$t = 1$: Quantum one-time pad

$t = 1$: Quantum one-time pad

Pauli Group

Standard example of a 1-design:

$$D_1 = \left\{ X^i Z^j \,|\, i, j \in \{0,1\} \right\} = \mathscr{P}_1 / \{1, -1, i, -i\}$$

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$D_1 = \left\{ X^i Z^j \,|\, i, j \in \{0,1\} \right\} = \mathscr{P}_1 \big/ \{1, -1, i, -i\}$

$D_n = D_1^{\otimes n}$

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$$D_1 = \left\{X^i Z^j \,|\, i, j \in \{0,1\}\right\} = \mathscr{P}_1 \Big/ \{1, -1, i, -i\}$$

$$D_n = D_1^{\otimes n}$$

# of elements: 2^{2n}

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$$D_1 = \left\{X^i Z^j \,|\, i, j \in \{0,1\}\right\} = \mathscr{P}_1 \big/ \{1, -1, i, -i\}$$

$$D_n = D_1^{\otimes n}$$

\# of elements: 2^{2n}

Maximally entangled state

D_n has minimal size: $T_{D_n}^{(1)} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|) = \mathbb{1},$

$$|D_n| \geq \mathrm{rk}\left(T_{D_n}^{(1)} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|)\right) = 2^{2n}$$

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$D_1 = \left\{X^i Z^j \,|\, i, j \in \{0,1\}\right\} = \mathscr{P}_1 \big/ \{1, -1, i, -i\}$

$D_n = D_1^{\otimes n}$

# of elements: 2^{2n}

D_n has minimal size: $T^{(1)}_{D_n} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|) = \mathbb{1}$,

$|D_n| \geq \mathrm{rk}\left(T^{(1)}_{D_n} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|)\right) = 2^{2n}$

Similar for ε-approximate case

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$$D_1 = \left\{X^i Z^j \,|\, i, j \in \{0,1\}\right\} = \mathscr{P}_1 \big/ \{1, -1, i, -i\}$$

$$D_n = D_1^{\otimes n}$$

\# of elements: 2^{2n}

D_n has minimal size: $T_{D_n}^{(1)} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|) = \mathbb{I}$,

$$|D_n| \geq \mathrm{rk}\left(T_{D_n}^{(1)} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|)\right) = 2^{2n}$$

Similar for ε-approximate case

What if we are only interested in isolated systems?

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$$D_1 = \left\{X^i Z^j \,|\, i, j \in \{0,1\}\right\} = \mathscr{P}_1 \big/ \{1, -1, i, -i\}$$

$$D_n = D_1^{\otimes n}$$

\# of elements: 2^{2n}

D_n has minimal size: $T_{D_n}^{(1)} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|) = \mathbb{1}$,

$$|D_n| \geq \mathrm{rk}\left(T_{D_n}^{(1)} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|)\right) = 2^{2n}$$

Similar for ε-approximate case

What if we are only interested in isolated systems?

Note: $\mathrm{rk}\left(T_{D_n}^{(1)}(|\psi\rangle\langle\psi|)\right) \leq 2^n$

$t = 1$: Quantum one-time pad

Standard example of a 1-design:

$$D_1 = \left\{X^i Z^j \,|\, i,j \in \{0,1\}\right\} = \mathscr{P}_1 \Big/ \{1,-1,i,-i\}$$

$$D_n = D_1^{\otimes n}$$

\# of elements: 2^{2n}

D_n has minimal size: $T^{(1)}_{D_n} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|) = \mathbb{1}$,

$$|D_n| \geq \mathrm{rk}\left(T^{(1)}_{D_n} \otimes \mathrm{id}(|\phi^+\rangle\langle\phi^+|)\right) = 2^{2n}$$

Similar for ε-approximate case

What if we are only interested in isolated systems?

Note: $\mathrm{rk}\left(T^{(1)}_{D_n}(|\psi\rangle\langle\psi|)\right) \leq 2^n$

Naively, 2^n elements could be enough!

ε-randomizing channels

No side information: 1-to-1-norm $\|\Phi\|_{1\to 1} = \sup_X \frac{\|\Phi(X)\|_1}{\|X\|_1}$

ε-randomizing channels

No side information: 1-to-1-norm $\|\Phi\|_{1\to 1} = \sup_X \frac{\|\Phi(X)\|_1}{\|X\|_1}$

More generally, $\|\Phi\|_{p\to q} = \sup_X \frac{\|\Phi(X)\|_q}{\|X\|_p}$

ε-randomizing channels

No side information: 1-to-1-norm $\|\Phi\|_{1\to 1} = \sup_X \dfrac{\|\Phi(X)\|_1}{\|X\|_1}$

More generally, $\|\Phi\|_{p\to q} = \sup_X \dfrac{\|\Phi(X)\|_q}{\|X\|_p}$

Does there exist $D \subset U(2^n)$ with roughly 2^n elements such that

$$\left\| \, T^{(1)} - T_D^{(1)} \, \right\|_{1\to 1} \leq \varepsilon \ ?$$

ε-randomizing channels

No side information: 1-to-1-norm $\|\Phi\|_{1\to 1} = \sup_X \frac{\|\Phi(X)\|_1}{\|X\|_1}$

More generally, $\|\Phi\|_{p\to q} = \sup_X \frac{\|\Phi(X)\|_q}{\|X\|_p}$

Does there exist $D \subset U(2^n)$ with roughly 2^n elements such that

$$\left\| \, T^{(1)} - T_D^{(1)} \, \right\|_{1\to 1} \leq \varepsilon \text{ ?}$$

Hayden, Leung, Shor, Winter 04: Yes!

$\exists D : |D| \leq \mathcal{O}(n 2^n \varepsilon^{-2})$ s.t.

$$2^n \left\| \, T^{(1)} - T_D^{(1)} \, \right\|_{1\to\infty} \leq \varepsilon.$$

ε-randomizing channels

No side information: 1-to-1-norm $\|\Phi\|_{1\to 1} = \sup_X \frac{\|\Phi(X)\|_1}{\|X\|_1}$

More generally, $\|\Phi\|_{p\to q} = \sup_X \frac{\|\Phi(X)\|_q}{\|X\|_p}$

Does there exist $D \subset U(2^n)$ with roughly 2^n elements such that

$$\left\| T^{(1)} - T_D^{(1)} \right\|_{1\to 1} \leq \varepsilon \text{ ?}$$

Hayden, Leung, Shor, Winter 04: Yes!

$\exists D : |D| \leq \mathcal{O}(n 2^n \varepsilon^{-2})$ s.t.

$$\left\| T^{(1)} - T_D^{(1)} \right\|_{1\to 1} \leq 2^n \left\| T^{(1)} - T_D^{(1)} \right\|_{1\to\infty} \leq \varepsilon.$$

ε-randomizing channels

No side information: 1-to-1-norm $\|\Phi\|_{1\to 1} = \sup_X \frac{\|\Phi(X)\|_1}{\|X\|_1}$

More generally, $\|\Phi\|_{p\to q} = \sup_X \frac{\|\Phi(X)\|_q}{\|X\|_p}$

Does there exist $D \subset U(2^n)$ with roughly 2^n elements such that

$$\left\| T^{(1)} - T_D^{(1)} \right\|_{1\to 1} \leq \varepsilon\ ?$$

Hayden, Leung, Shor, Winter 04: Yes!

$\exists D : |D| \leq \mathcal{O}(n 2^n \varepsilon^{-2})$ s.t.

$$\left\| T^{(1)} - T_D^{(1)} \right\|_{1\to 1} \leq 2^n \left\| T^{(1)} - T_D^{(1)} \right\|_{1\to\infty} \leq \varepsilon.$$

Independent Haar-random unitaries work whp.!

Subsampling

Subsampling

Ok, independently Haar-random unitaries work. Simpler constructions?

Subsampling

Ok, independently Haar-random unitaries work. Simpler constructions?

Yes, independent samples from a (full) 1-design (Aubrun 09).

Subsampling

Ok, independently Haar-random unitaries work. Simpler constructions?

Yes, independent samples from a (full) 1-design (Aubrun 09).

“Subsampling” (ABW 09)

Subsampling

Ok, independently Haar-random unitaries work. Simpler constructions?

Yes, independent samples from a (full) 1-design (Aubrun 09).

“Subsampling” (ABW 09)

For D with $|D| = \Omega(n^6 2^n \varepsilon^{-2})$ independently random 1-design elements,

$$2^n \left\| T^{(1)} - T_D^{(1)} \right\|_{1\to\infty} \leq \varepsilon$$

with constant probability.

Results

Weak approximate unitary designs

D's from last 2 slides: *Weak approximate 1-designs.*

Weak approximate unitary designs

D's from last 2 slides: *Weak approximate 1-designs.*

Definition:

An n qubit weak ε-approximate unitary t-design is a finite subset $D \subset U(2^n)$ such that

$$\left\| T^{(t)} - T_D^{(t)} \right\|_{1\to 1} \le \varepsilon$$

Weak approximate unitary designs

D's from last 2 slides: *Weak approximate 1-designs.*

Definition:
An n qubit weak ε-approximate unitary t-design is a finite subset $D \subset U(2^n)$ such that

$$\left\| T^{(t)} - T_D^{(t)} \right\|_{1\to 1} \leq \varepsilon$$

For $t = 2$: Variants for $T^{(1,1)}$ and T^{ch}:

$$T^{ch}(\Phi)(X) = \mathop{\mathbb{E}}_{U\sim \mathrm{Haar}_d} \left[U^\dagger \Phi(UXU^\dagger)U\right]$$

Weak approximate unitary designs

D's from last 2 slides: *Weak approximate 1-designs.*

Definition:
An n qubit weak ε-approximate unitary t-design is a finite subset $D \subset U(2^n)$ such that

$$\left\| T^{(t)} - T_D^{(t)} \right\|_{1\to 1} \leq \varepsilon$$

For $t = 2$: Variants for $T^{(1,1)}$ and T^{ch}:

$$T^{ch}(\Phi)(X) = \mathop{\mathbb{E}}_{U\sim \mathrm{Haar}_d} \left[U^\dagger \Phi(UXU^\dagger)U\right]$$

T^{ch} is a "super-duper-operator" 😉. Define $\| \cdot \|_{\diamond\to\diamond}$

Weak approximate unitary designs

D's from last 2 slides: *Weak approximate 1-designs.*

$\boxed{\begin{array}{l}\text{Definition:} \\ \text{An } n \text{ qubit weak } \varepsilon\text{-approximate unitary } t\text{-design is a finite} \\ \text{subset } D \subset U(2^n) \text{ such that} \\ \qquad\qquad \left\| T^{(t)} - T^{(t)}_D \right\|_{1\to 1} \leq \varepsilon \end{array}}$

For $t = 2$: Variants for $T^{(1,1)}$ and T^{ch}:

$$T^{ch}(\Phi)(X) = \mathop{\mathbb{E}}_{U\sim \mathrm{Haar}_d} \left[U^\dagger \Phi(UXU^\dagger)U\right]$$

T^{ch} is a "super-duper-operator" 😉. Define $\| \cdot \|_{\diamond\to\diamond}$

Can we generalize the result by Aubrun?

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Lemma 5. *Let* $U_1, \dots, U_N \in \mathcal{U}(d)$ *be* deterministic *unitary operators and let* (ε_i) *be a sequence of independent Bernoulli random variables. Then*

$$\mathbf{E}_\varepsilon \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^N \varepsilon_i U_i \rho U_i^\dagger \right\|_\infty \leqslant C (\log d)^{5/2} \sqrt{\log N} \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^N U_i \rho U_i^\dagger \right\|_\infty^{1/2}$$

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Lemma 5. *Let* $U_1, \ldots, U_N \in \mathcal{U}(d)$ *be* deterministic *unitary operators and let* (ε_i) *be a sequence of independent Bernoulli random variables. Then*

$$N^{-1}\,\mathbf{E}_\varepsilon \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left\|\sum_{i=1}^N \varepsilon_i U_i \rho U_i^\dagger\right\|_\infty \leqslant C(\log d)^{5/2}\sqrt{\log N} \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left(\left\|\sum_{i=1}^N U_i \rho U_i^\dagger\right\|_\infty^{1/2} N^{-1/2}\right) N^{-1/2}$$

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Lemma 5. *Let $U_1, \ldots, U_N \in \mathcal{U}(d)$ be* deterministic *unitary operators and let (ε_i) be a sequence of independent Bernoulli random variables. Then*

Banach space geometry!

$$N^{-1}\, \mathbf{E}_\varepsilon \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^N \varepsilon_i U_i \rho U_i^\dagger \right\|_\infty \leqslant C (\log d)^{5/2} \sqrt{\log N} \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left(\left\| \sum_{i=1}^N U_i \rho U_i^\dagger \right\|_\infty^{1/2} N^{-1/2} \right) N^{-1/2}$$

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Proof sketch of subsampling weak 1-design given this Lemma:

Lemma 5. *Let* $U_1, \ldots, U_N \in \mathcal{U}(d)$ *be* deterministic *unitary operators and let* (ε_i) *be a sequence of independent Bernoulli random variables. Then*

$$N^{-1}\ \mathbf{E}_\varepsilon \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^N \varepsilon_i U_i \rho U_i^\dagger \right\|_\infty \leqslant C (\log d)^{5/2} \sqrt{\log N} \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left(\left\| \sum_{i=1}^N U_i \rho U_i^\dagger \right\|_\infty^{1/2} N^{-1/2} \right) N^{-1/2}$$

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Proof sketch of subsampling weak 1-design given this Lemma:

Lemma 5. *Let* $U_1, \ldots, U_N \in \mathcal{U}(d)$ *be* deterministic *unitary operators and let* (ε_i) *be a sequence of independent Bernoulli random variables. Then*

$$N^{-1}\, \mathbf{E}_\varepsilon \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^N \varepsilon_i U_i \rho U_i^\dagger \right\|_\infty \leqslant C (\log d)^{5/2} \sqrt{\log N} \sup_{\rho \in \mathcal{D}(\mathbf{C}^d)} \left(\left\| \sum_{i=1}^N U_i \rho U_i^\dagger \right\|_\infty^{1/2} N^{-1/2} \right) N^{-1/2}$$

Massage weak 1-design error into this form

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Proof sketch of subsampling weak 1-design given this Lemma:

Lemma 5. *Let* $U_1, \ldots, U_N \in \mathcal{U}(d)$ *be* deterministic *unitary operators and let* (ε_i) *be a sequence of independent Bernoulli random variables. Then*

$$N^{-1}\, \mathbf{E}_\varepsilon \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^N \varepsilon_i U_i \rho U_i^\dagger \right\|_\infty \leqslant C(\log d)^{5/2}\sqrt{\log N} \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left(\left\| \sum_{i=1}^N U_i\rho U_i^\dagger \right\|_\infty^{1/2} N^{-1/2} \right) N^{-1/2}$$

Massage weak 1-design error into this form

Bound this by weak 1-design error + $\|T^{(1)}(\rho)\|_\infty$

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Proof sketch of subsampling weak 1-design given this Lemma:

Lemma 5. *Let $U_1, \dots, U_N \in \mathcal{U}(d)$ be* deterministic *unitary operators and let (ε_i) be a sequence of independent Bernoulli random variables. Then*

$$N^{-1}\,\mathbf{E}_\varepsilon \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left\| \sum_{i=1}^{N} \varepsilon_i U_i \rho U_i^\dagger \right\|_\infty \leqslant C(\log d)^{5/2}\sqrt{\log N} \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left(\left\| \sum_{i=1}^{N} U_i \rho U_i^\dagger \right\|_\infty^{1/2} N^{-1/2} \right) N^{-1/2}$$

Massage weak 1-design error into this form

Bound this by weak 1-design error + $\|T^{(1)}(\rho)\|_\infty$

Conclude that weak 1-design error is bounded if $N \geq \mathrm{polylog}(d) d^2 \|T^{(1)}(\rho)\|_\infty$

Let's look inside (Aubrun 09)….

Key lemma in Aubrun 09:

Proof sketch of subsampling weak 1-design given this Lemma:

Lemma 5. *Let $U_1, \dots, U_N \in \mathcal{U}(d)$ be* deterministic *unitary operators and let (ε_i) be a sequence of independent Bernoulli random variables. Then*

$$N^{-1}\,\mathbf{E}_\varepsilon \sup_{\rho\in\mathcal{D}(\mathbf{C}^d)} \left\|\sum_{i=1}^N \varepsilon_i U_i\rho U_i^\dagger\right\|_\infty \leqslant C(\log d)^{5/2}\sqrt{\log N}\sup_{\rho\in\mathcal{D}(\mathbf{C}^d)}\left(\left\|\sum_{i=1}^N U_i\rho U_i^\dagger\right\|_\infty^{1/2} N^{-1/2}\right) N^{-1/2}$$

Massage weak 1-design error into this form

Bound this by weak 1-design error + $\|T^{(1)}(\rho)\|_\infty$

Conclude that weak 1-design error is bounded if $N \geq \mathrm{polylog}(d) d^2 \|T^{(1)}(\rho)\|_\infty$

Observation: Yields interesting bound whenever subsampling from a design approximating a channel with small $1 \to \infty$ norm!!!

Abstracting the technique of (Aubrun 09)

Lemma (relatively straightforward from (Aubrun 09)):

Let $\hat{D} \subset U(d)$ be such that

$$\left\| T_{\hat{D}}^{(1)} \right\|_{1\to\infty} \leq \delta.$$

Then the subsampling design D fulfils

$$d \left\| T_{D}^{(1)} - T_{\hat{D}}^{(1)} \right\|_{1\to\infty} \leq \varepsilon$$

provided that $|D| \geq \mathrm{polylog}(d)\dfrac{\delta d^2}{\varepsilon^2}$

Abstracting the technique of (Aubrun 09)

Lemma (relatively straightforward from (Aubrun 09)):
Let $\hat{D} \subset U(d)$ be such that

$$\left\| T^{(1)}_{\hat{D}} \right\|_{1\to\infty} \leq \delta.$$

Then the subsampling design D fulfils

$$d \left\| T^{(1)}_{D} - T^{(1)}_{\hat{D}} \right\|_{1\to\infty} \leq \varepsilon$$

provided that $|D| \geq \mathrm{polylog}(d)\dfrac{\delta d^2}{\varepsilon^2}$

Can apply this to t-design setting! Take full t-design $\tilde{D} \subset U(d)$, set

$$\hat{D} = \{U^{\otimes t} \,|\, U \in \tilde{D}\} \subset U(d^t)$$

Abstracting the technique of (Aubrun 09)

Lemma (relatively straightforward from (Aubrun 09)):
Let $\hat{D} \subset U(d)$ be such that

$$\left\| T^{(1)}_{\hat{D}} \right\|_{1 \to \infty} \leq \delta.$$

Then the subsampling design D fulfils

$$d \left\| T^{(1)}_{D} - T^{(1)}_{\hat{D}} \right\|_{1 \to \infty} \leq \varepsilon$$

provided that $|D| \geq \mathrm{polylog}(d) \dfrac{\delta d^2}{\varepsilon^2}$

Can apply this to t-design setting! Take full t-design $\tilde{D} \subset U(d)$, set

$$\hat{D} = \{ U^{\otimes t} \,|\, U \in \tilde{D} \} \subset U(d^t)$$

$\Rightarrow$ need bound on $\left\| T^{(t)} \right\|_{1 \to \infty}$.

Abstracting the technique of (Aubrun 09)

$\boxed{\begin{array}{l}\text{Lemma (relatively straightforward from (Aubrun 09)):} \\ \text{Let } \hat{D} \subset U(d) \text{ be such that} \\ \qquad \left\| T^{(1)}_{\hat{D}} \right\|_{1\to\infty} \leq \delta. \\ \text{Then the subsampling design } D \text{ fulfils} \\ \qquad d \left\| T^{(1)}_{D} - T^{(1)}_{\hat{D}} \right\|_{1\to\infty} \leq \varepsilon \\ \text{provided that } |D| \geq \mathrm{polylog}(d)\dfrac{\delta d^2}{\varepsilon^2}\end{array}}$

Can apply this to t-design setting! Take full t-design $\tilde{D} \subset U(d)$, set

$$\hat{D} = \{U^{\otimes t} \,|\, U \in \tilde{D}\} \subset U(d^t)$$

$\Rightarrow$ need bound on $\left\| T^{(t)} \right\|_{1\to\infty}$.

Representation theory!!!

Representation theory of $U(d)$

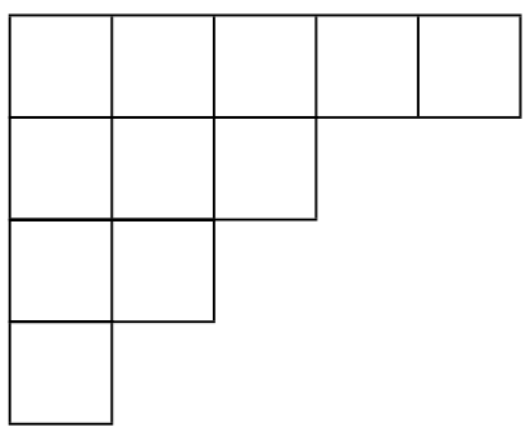
$U(d) \to U(d^t)$, $U \mapsto U^{\otimes t}$ is a representation of $U(d)$

Representation theory of $U(d)$

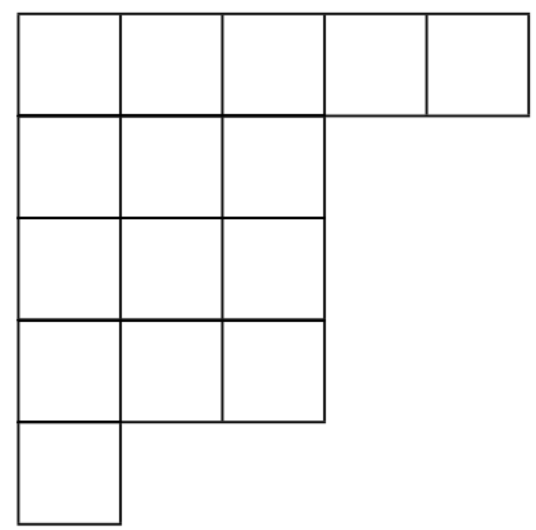
$U(d) \to U(d^t)$, $U \mapsto U^{\otimes t}$ is a representation of $U(d)$

Irreducible representations of $U(d)$: $V_{\lambda,d}$ labeled by *Young diagrams*

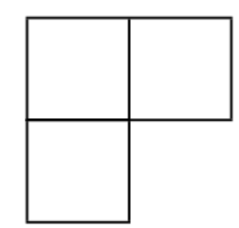
Examples:



$\lambda = (5,3,2,1) \vdash 11$



$\lambda = (5,3^3,1) \vdash 15$



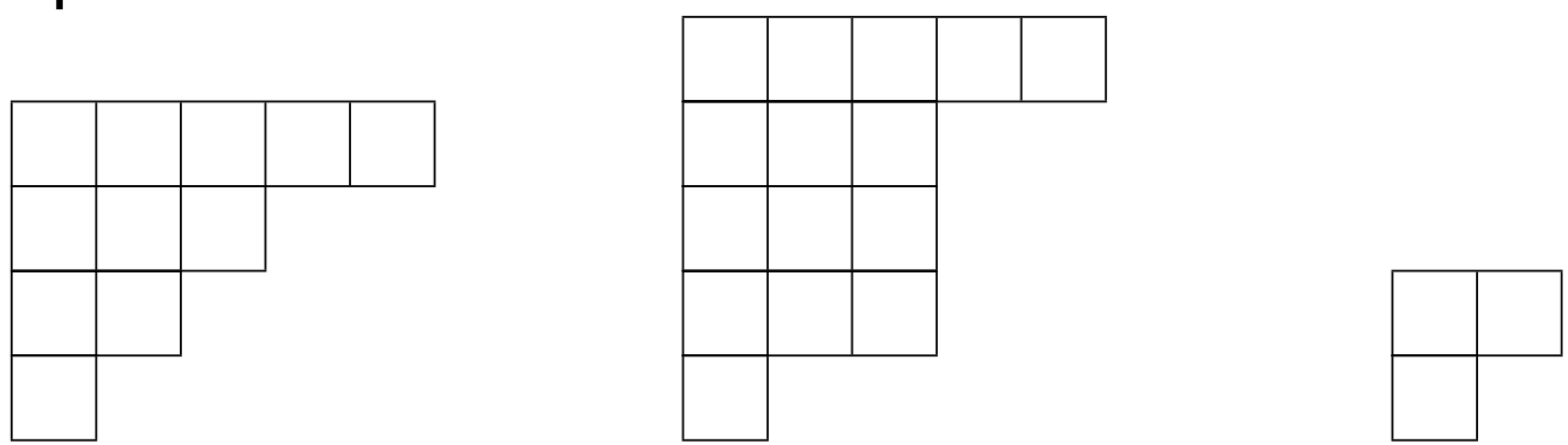
$\lambda = (2,1) \vdash 3$

Representation theory of $U(d)$

$U(d) \to U(d^t)$, $U \mapsto U^{\otimes t}$ is a representation of $U(d)$

Irreducible representations of $U(d)$: $V_{\lambda,d}$ labeled by *Young diagrams*

Examples:



$\lambda = (5,3,2,1) \vdash 11 \quad \lambda = (5,3^3,1) \vdash 15 \quad \lambda = (2,1) \vdash 3$

Dimension of $V_{\lambda,d}$: combinatorial formula in λ and d

Analyzing $T^{(t)}$

Decompose $\left(\mathbb{C}^d\right)^{\otimes t}$ into irreps of $U(d)$:

$$\left(\mathbb{C}^d\right)^{\otimes t} \cong \bigoplus_{\lambda \vdash_d t} V_{\lambda,d} \otimes \mathbb{C}^{m_\lambda}$$

Young diagrams with t boxes
(and at most d rows)

Analyzing $T^{(t)}$

Decompose $\left(\mathbb{C}^d\right)^{\otimes t}$ into irreps of $U(d)$:

$$\left(\mathbb{C}^d\right)^{\otimes t} \cong \bigoplus_{\lambda \vdash_d t} V_{\lambda,d} \otimes \mathbb{C}^{m_\lambda}$$

Schur's Lemma implies

$$T^{(t)}(X) = \bigoplus_{\lambda \vdash_d t} \tau_{V_{\lambda,d}} \otimes \mathrm{Tr}_{V_{\lambda,d}}\left[P_\lambda X\right]$$

Maximally mixed state

Analyzing $T^{(t)}$

Decompose $\left(\mathbb{C}^d\right)^{\otimes t}$ into irreps of $U(d)$:

$$\left(\mathbb{C}^d\right)^{\otimes t} \cong \bigoplus_{\lambda \vdash_d t} V_{\lambda,d} \otimes \mathbb{C}^{m_\lambda}$$

Schur's Lemma implies

$$T^{(t)}(X) = \bigoplus_{\lambda \vdash_d t} \tau_{V_{\lambda,d}} \otimes \mathrm{Tr}_{V_{\lambda,d}}\left[P_\lambda X\right]$$

$$\Rightarrow \qquad \|T^{(t)}(X)\|_\infty \leq \max_{\lambda \vdash_d t} \|\tau_{V_{\lambda,d}}\|_\infty \|X\|_1 \leq \max_{\lambda \vdash_d t} (\dim V_{\lambda,d})^{-1} \|X\|_1$$

Analyzing $T^{(t)}$

Decompose $\left(\mathbb{C}^d\right)^{\otimes t}$ into irreps of $U(d)$:

$$\left(\mathbb{C}^d\right)^{\otimes t} \cong \bigoplus_{\lambda \vdash_d t} V_{\lambda,d} \otimes \mathbb{C}^{m_\lambda}$$

Schur's Lemma implies

$$T^{(t)}(X) = \bigoplus_{\lambda \vdash_d t} \tau_{V_{\lambda,d}} \otimes \mathrm{Tr}_{V_{\lambda,d}}\left[P_\lambda X\right]$$

$\Rightarrow$ $$\|T^{(t)}(X)\|_\infty \leq \max_{\lambda \vdash_d t} \|\tau_{V_{\lambda,d}}\|_\infty \|X\|_1 \leq \max_{\lambda \vdash_d t} (\dim V_{\lambda,d})^{-1} \|X\|_1$$

$\Rightarrow$ $$\|T^{(t)}\|_{1\to\infty} \leq \max_{\lambda \vdash_d t} (\dim V_{\lambda,d})^{-1}$$

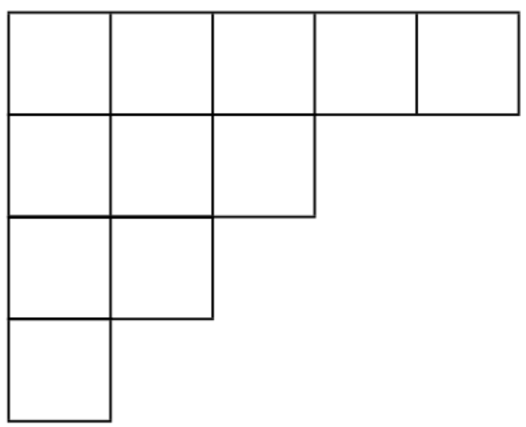
Analyzing $T^{(t)}$

Analyzing $T^{(t)}$

Weyl dimension formula: $\dim V_{\lambda,d} = \displaystyle\prod_{\substack{i,j\in\{1,\ldots,d\}\\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$

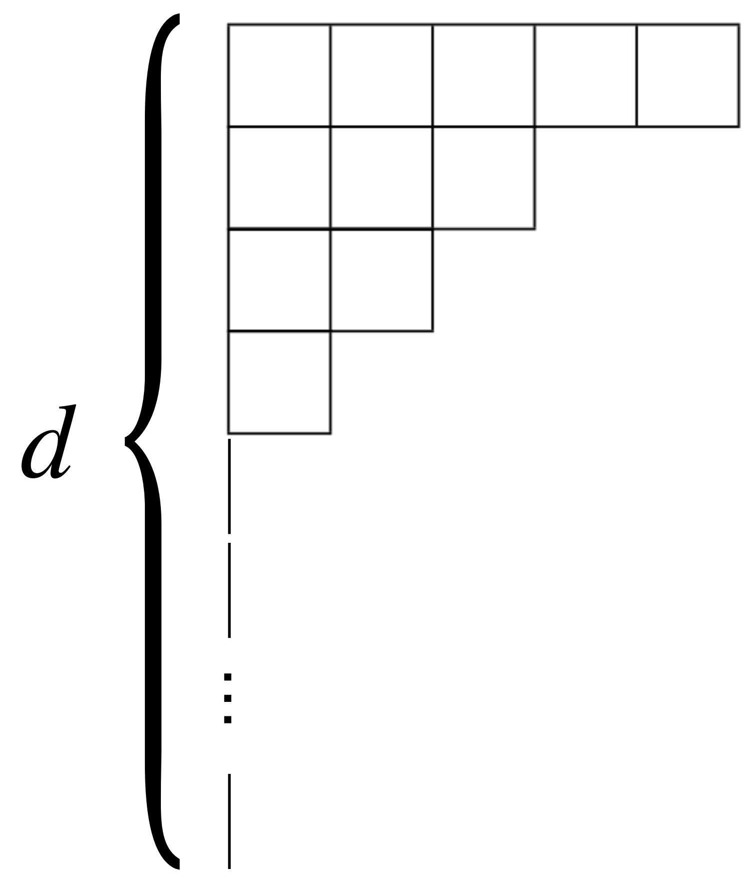
Analyzing $T^{(t)}$

Weyl dimension formula: $\dim V_{\lambda,d} = \prod_{\substack{i,j \in \{1,\ldots,d\} \\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$



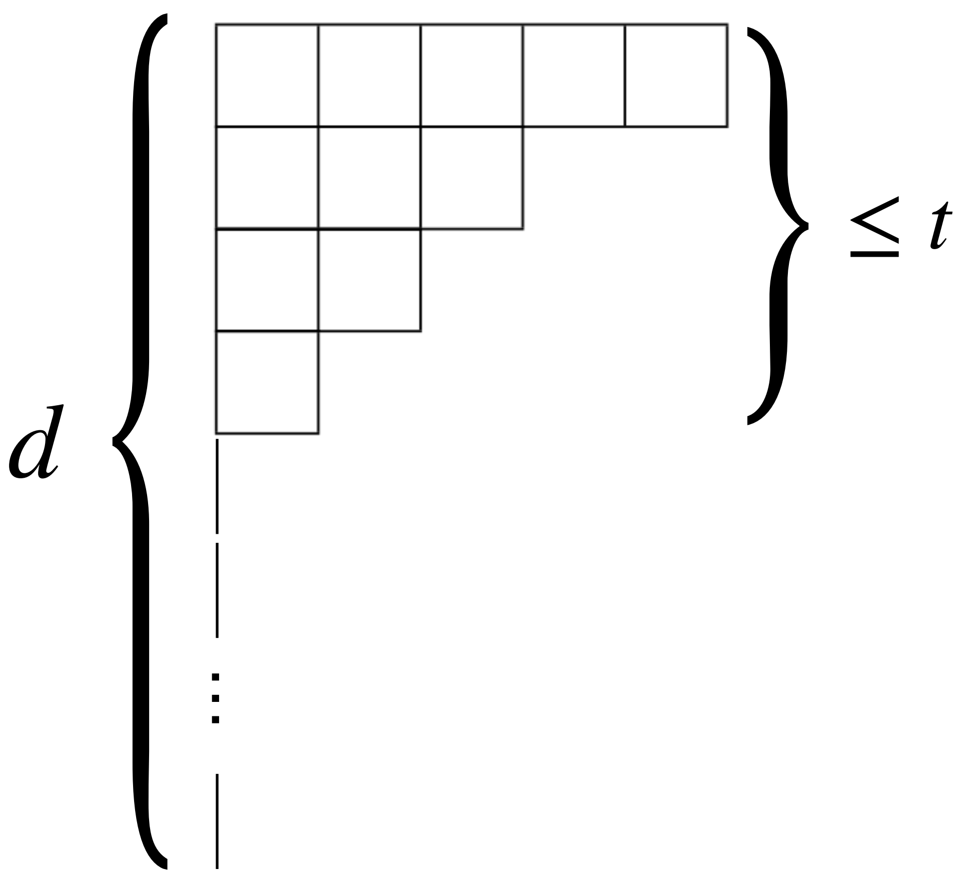
Analyzing $T^{(t)}$

Weyl dimension formula: $\dim V_{\lambda,d} = \prod_{\substack{i,j \in \{1,\ldots,d\} \\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$



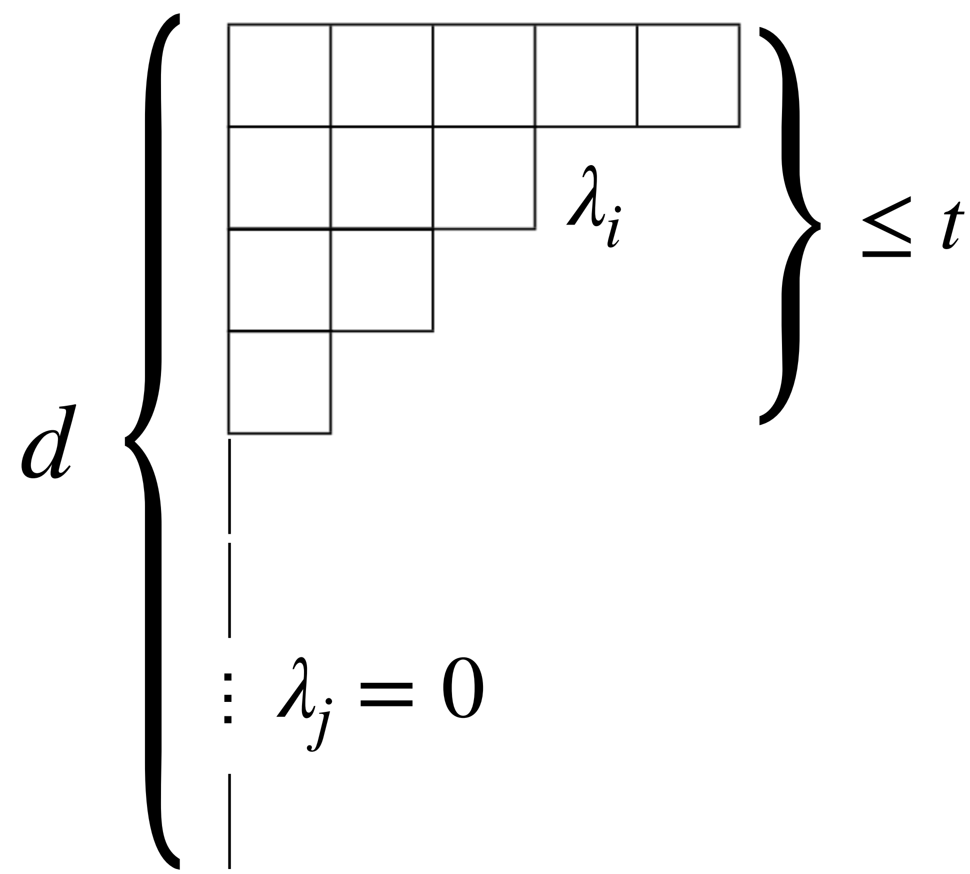
Analyzing $T^{(t)}$

Weyl dimension formula: $\dim V_{\lambda,d} = \prod_{\substack{i,j \in \{1,\ldots,d\} \\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$



Analyzing $T^{(t)}$

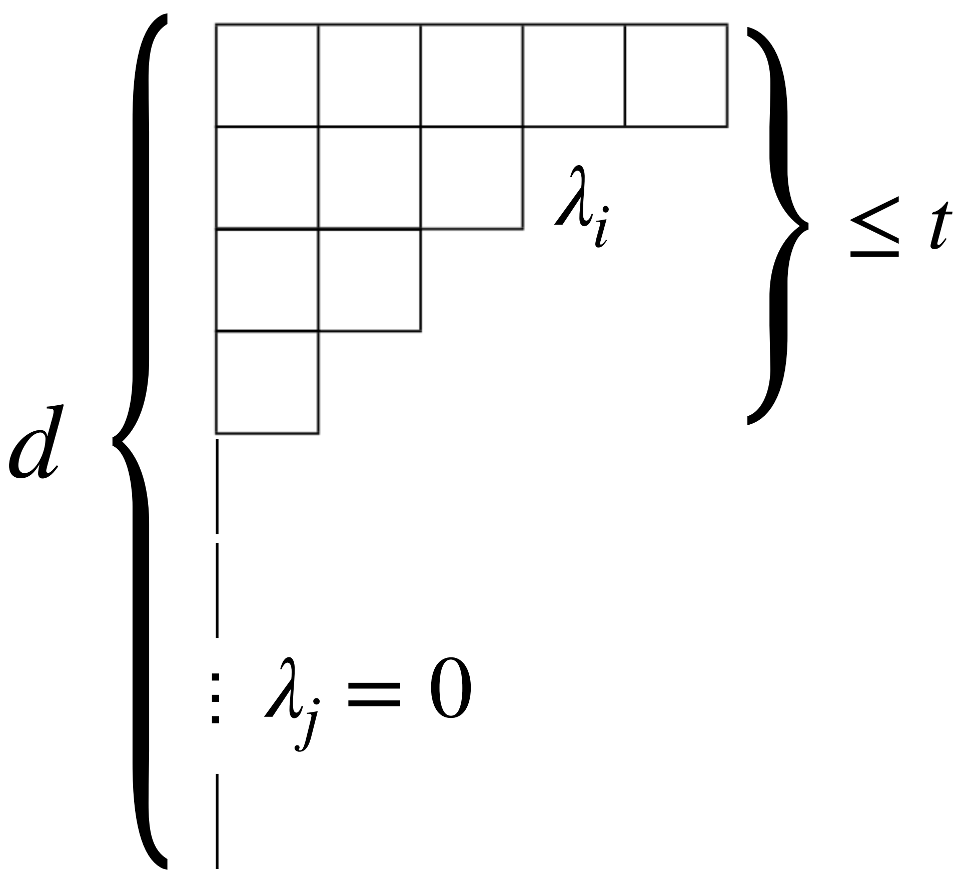
Weyl dimension formula: $\dim V_{\lambda,d} = \prod_{\substack{i,j \in \{1,\ldots,d\} \\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$



Analyzing $T^{(t)}$

Weyl dimension formula: $\dim V_{\lambda,d} = \prod_{\substack{i,j \in \{1,\ldots,d\} \\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$

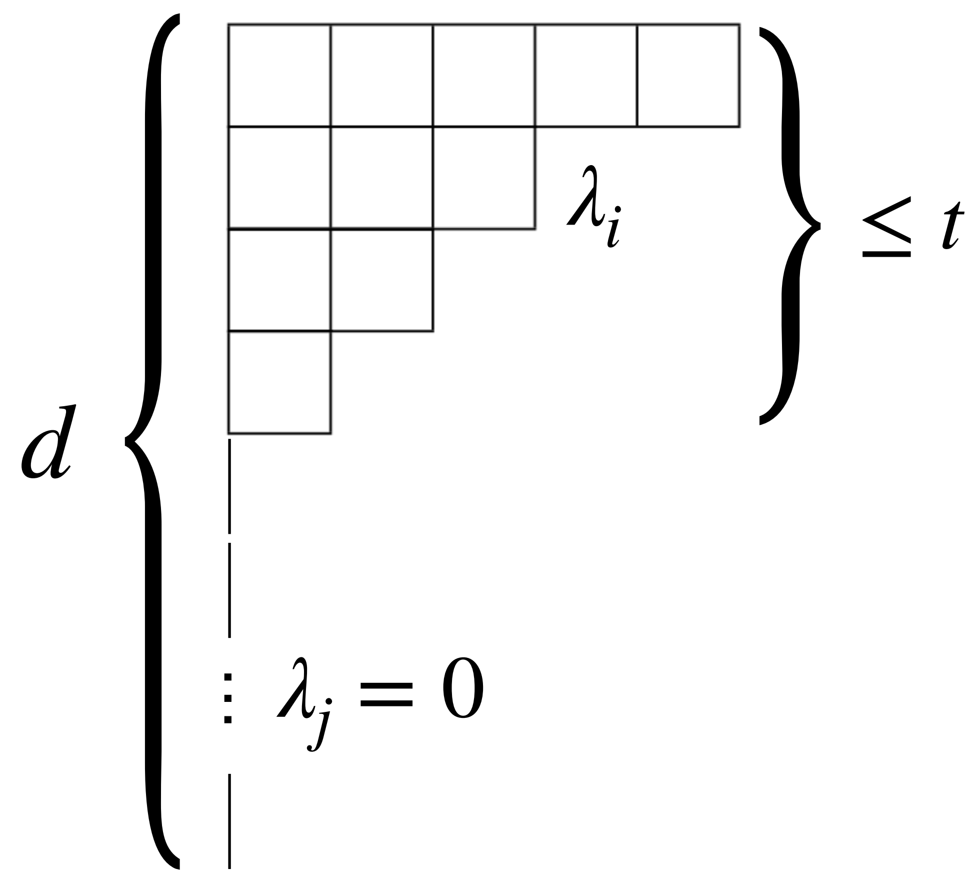
"Telescopic" product



Analyzing $T^{(t)}$

Weyl dimension formula: $\dim V_{\lambda,d} = \prod_{\substack{i,j \in \{1,\ldots,d\} \\ i<j}} \frac{\lambda_i - \lambda_j + j - i}{j - i}$

"Telescopic" product



$\Rightarrow \dim V_{\lambda,d} \geq \left(\frac{d}{2t}\right)^t$ for $\lambda \vdash t$

Main result

Theorem (Lancien, CM):

Let $\hat{D} \subset U(d)$ be a unitary t-design. Then the subsampling design D fulfils

$$d^t \left\| T_D^{(t)} - T^{(t)} \right\|_{1\to\infty} \leq \varepsilon$$

provided that $|D| \geq \mathrm{poly}(\log d, t)\varepsilon^{-2}(td)^t$

Variant for $T^{(1,1)}$

Theorem (Lancien, CM):
Let $\hat{D} \subset U(d)$ be a unitary 2-design. Then the subsampling design D fulfils

$$\left\| T_D^{(1,1)} - T^{(1,1)} \right\|_{1\to1} \le \varepsilon$$

provided that $|D| \ge \mathrm{poly}(\log d)\varepsilon^{-2} d^2$

Variant for $T^{(1,1)}$

Theorem (Lancien, CM):
Let $\hat{D} \subset U(d)$ be a unitary 2-design. Then the subsampling design D fulfils

$$\left\| T_D^{(1,1)} - T^{(1,1)} \right\|_{1 \to 1} \leq \varepsilon$$

provided that $|D| \geq \mathrm{poly}(\log d)\varepsilon^{-2}d^2$

Non-trivial because $\|T^{(1,1)}\|_{1\to\infty} = 1$ (invariance of $|\phi^+\rangle$)

Variant for $T^{(1,1)}$

Theorem (Lancien, CM):
Let $\hat{D} \subset U(d)$ be a unitary 2-design. Then the subsampling design D fulfils

$$\left\| T_D^{(1,1)} - T^{(1,1)} \right\|_{1\to 1} \leq \varepsilon$$

provided that $|D| \geq \mathrm{poly}(\log d)\varepsilon^{-2}d^2$

Non-trivial because $\|T^{(1,1)}\|_{1\to\infty} = 1$ (invariance of $|\phi^+\rangle$)

Variant for $T^{(1,1)}$

Theorem (Lancien, CM):
Let $\hat{D} \subset U(d)$ be a unitary 2-design. Then the subsampling design D fulfils

$$\left\| T_D^{(1,1)} - T^{(1,1)} \right\|_{1\to 1} \leq \varepsilon$$

provided that $|D| \geq \mathrm{poly}(\log d)\varepsilon^{-2}d^2$

Non-trivial because $\|T^{(1,1)}\|_{1\to\infty} = 1$ (invariance of $|\phi^+\rangle$)

$|\phi^+\rangle\langle\phi^+|$, invariant

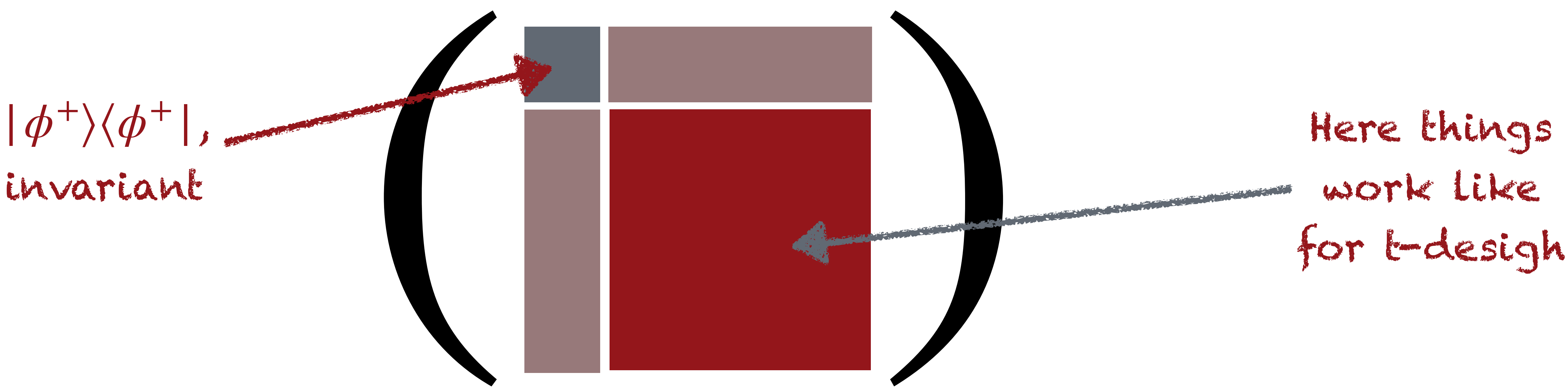
Variant for $T^{(1,1)}$

Theorem (Lancien, CM):
Let $\hat{D} \subset U(d)$ be a unitary 2-design. Then the subsampling design D fulfils

$$\left\| T_D^{(1,1)} - T^{(1,1)} \right\|_{1\to 1} \leq \varepsilon$$

provided that $|D| \geq \mathrm{poly}(\log d)\varepsilon^{-2}d^2$

Non-trivial because $\|T^{(1,1)}\|_{1\to\infty} = 1$ (invariance of $|\phi^+\rangle$)



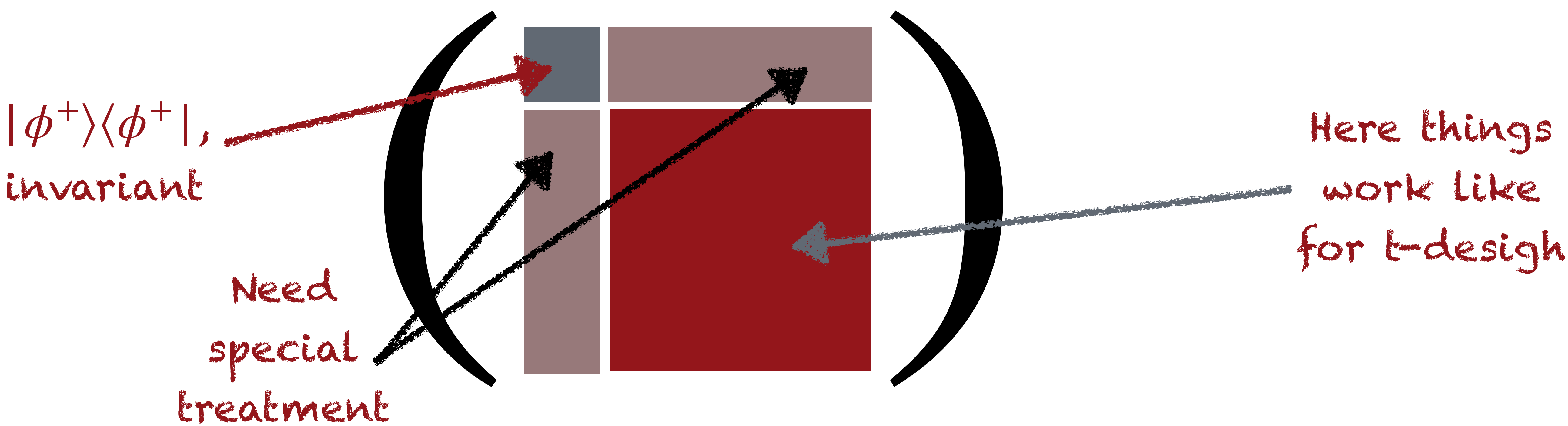
Variant for $T^{(1,1)}$

Theorem (Lancien, CM):
Let $\hat{D} \subset U(d)$ be a unitary 2-design. Then the subsampling design D fulfils

$$\left\| T_D^{(1,1)} - T^{(1,1)} \right\|_{1\to 1} \leq \varepsilon$$

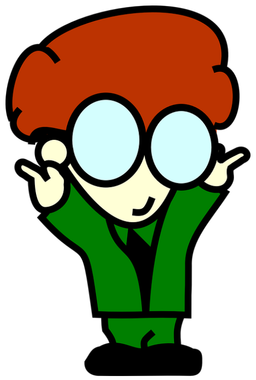
provided that $|D| \geq \mathrm{poly}(\log d)\varepsilon^{-2}d^2$

Non-trivial because $\|T^{(1,1)}\|_{1\to\infty} = 1$ (invariance of $|\phi^+\rangle$)

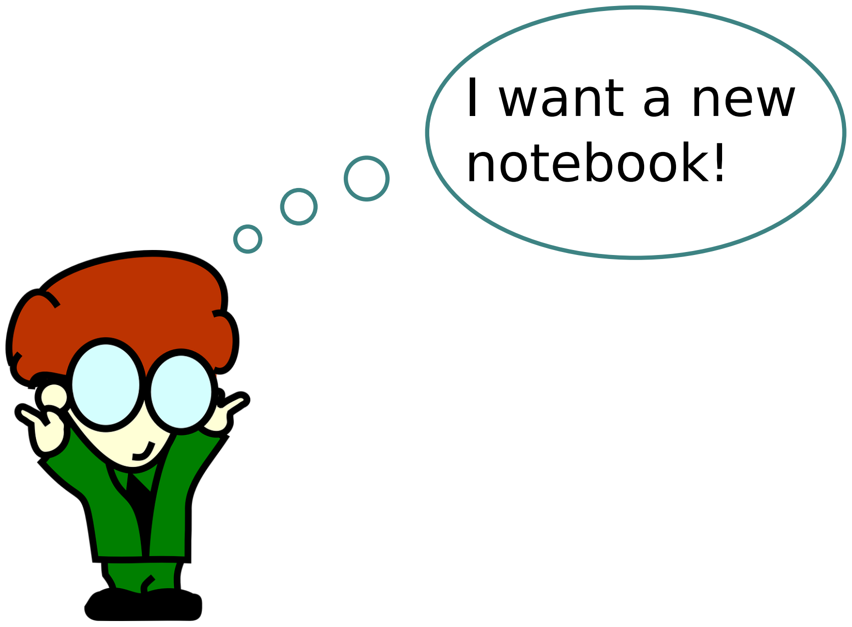


Application: Non-malleable encryption

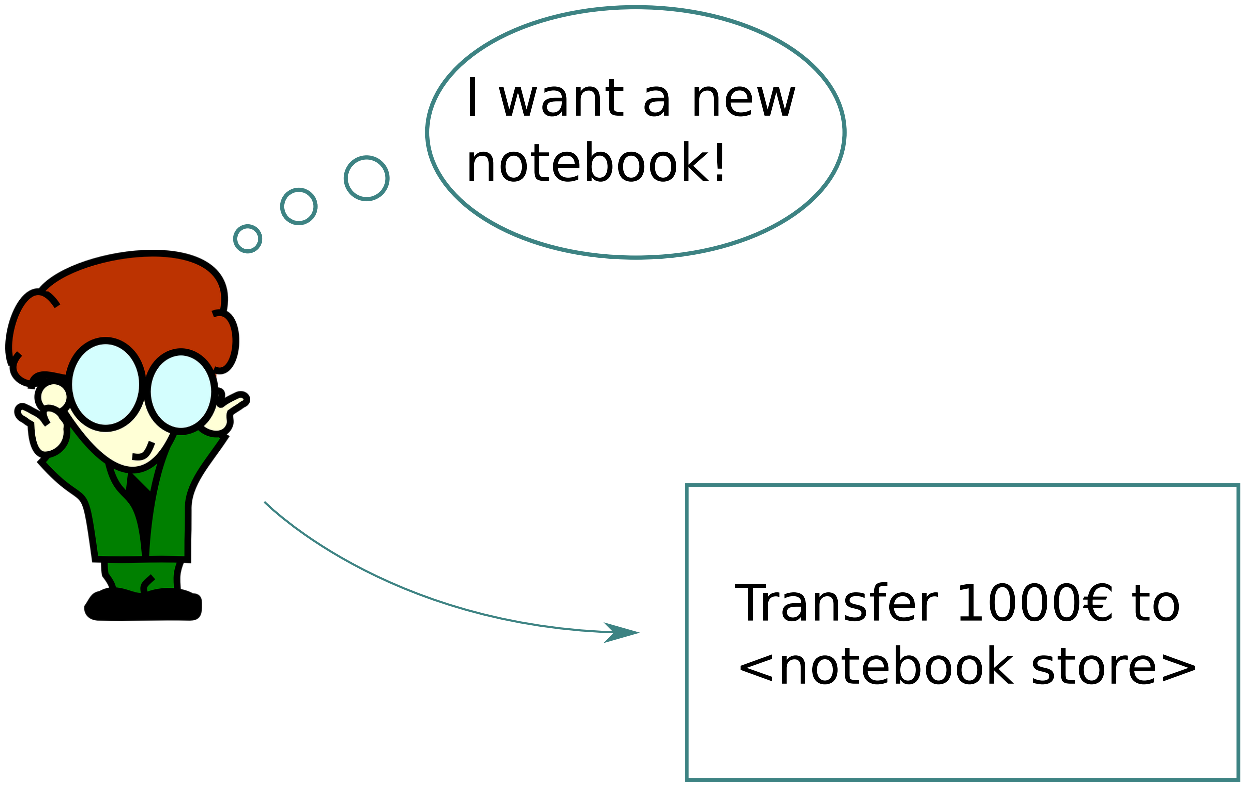
Non-malleability



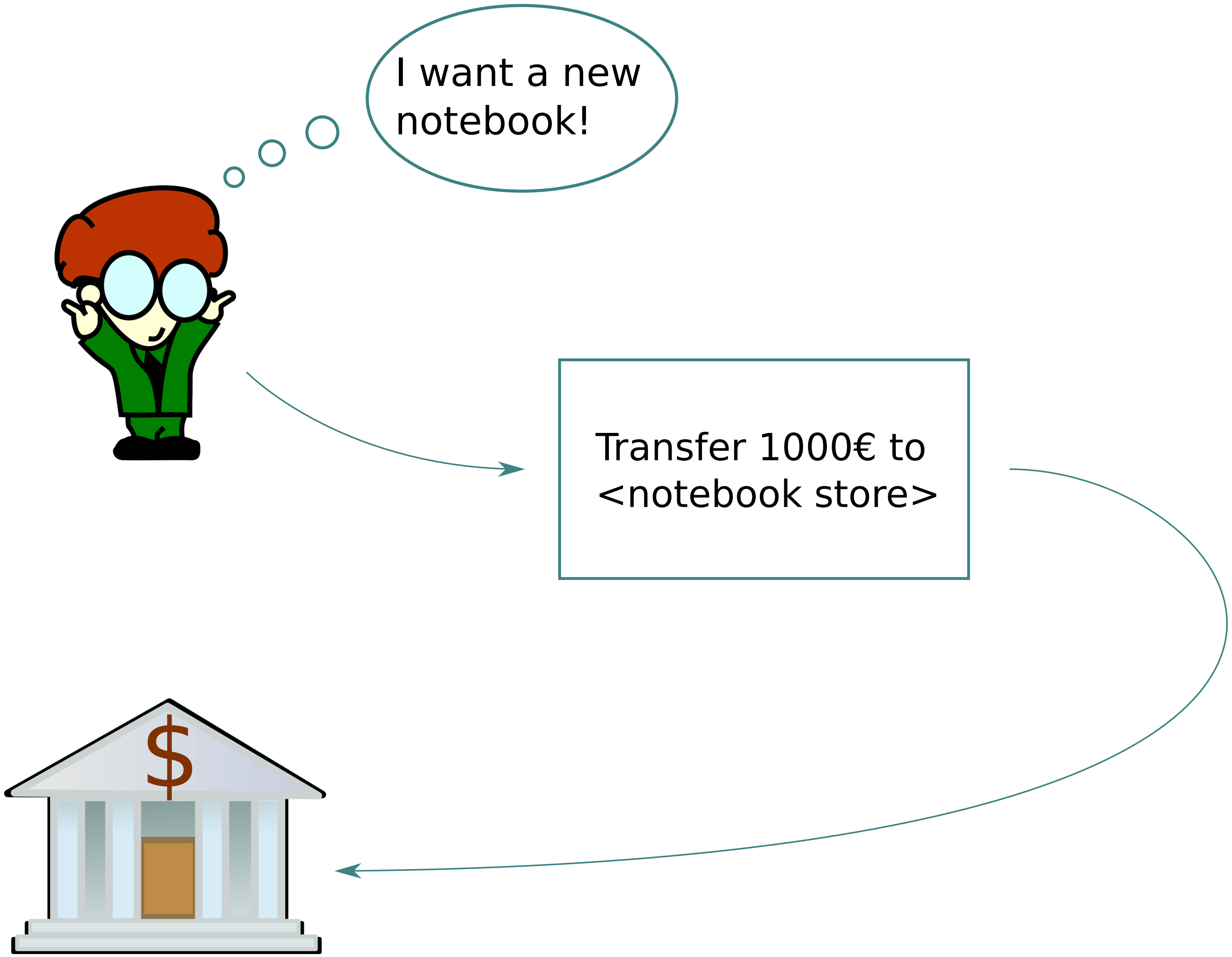
Non-malleability



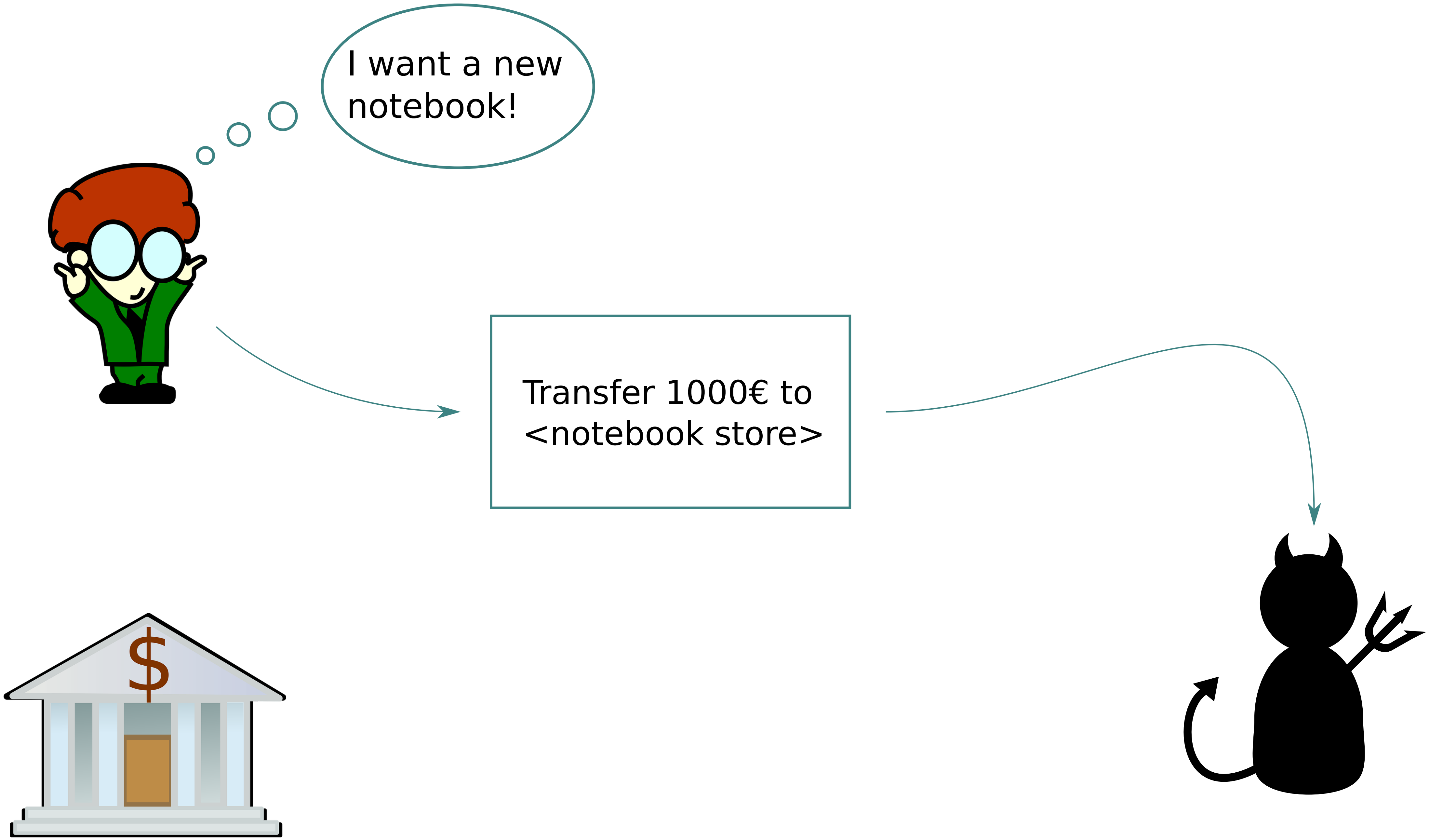
Non-malleability



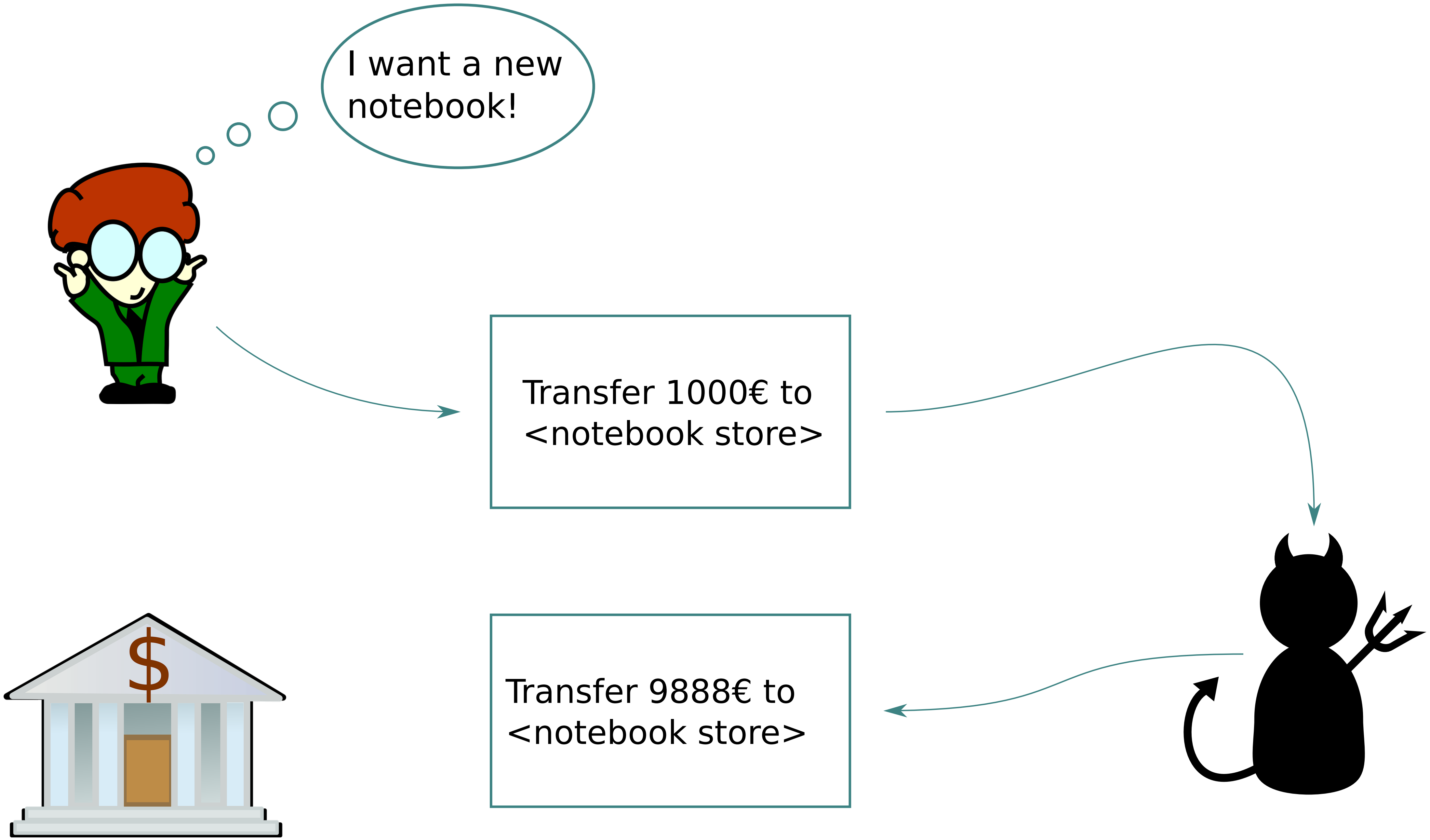
Non-malleability



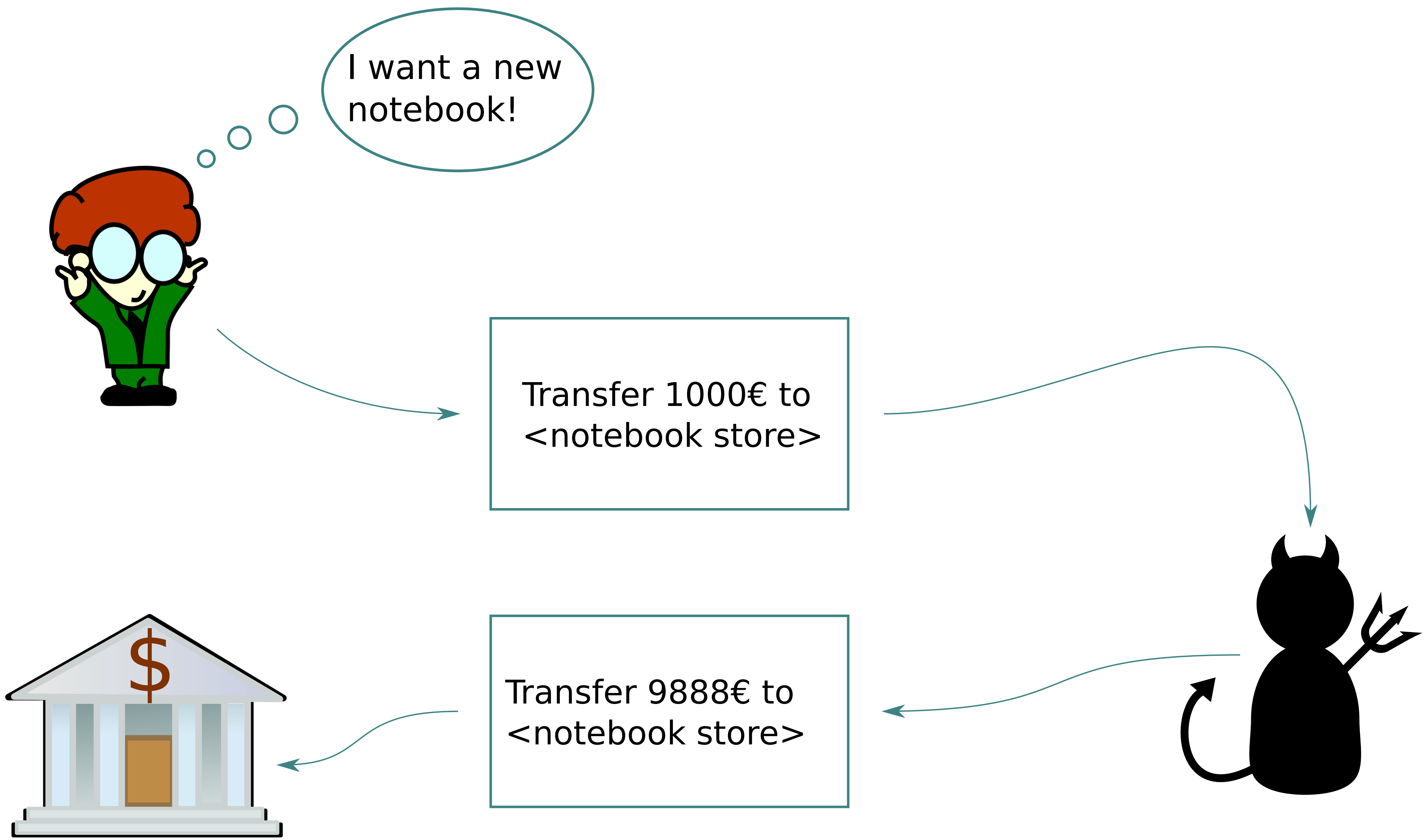
Non-malleability



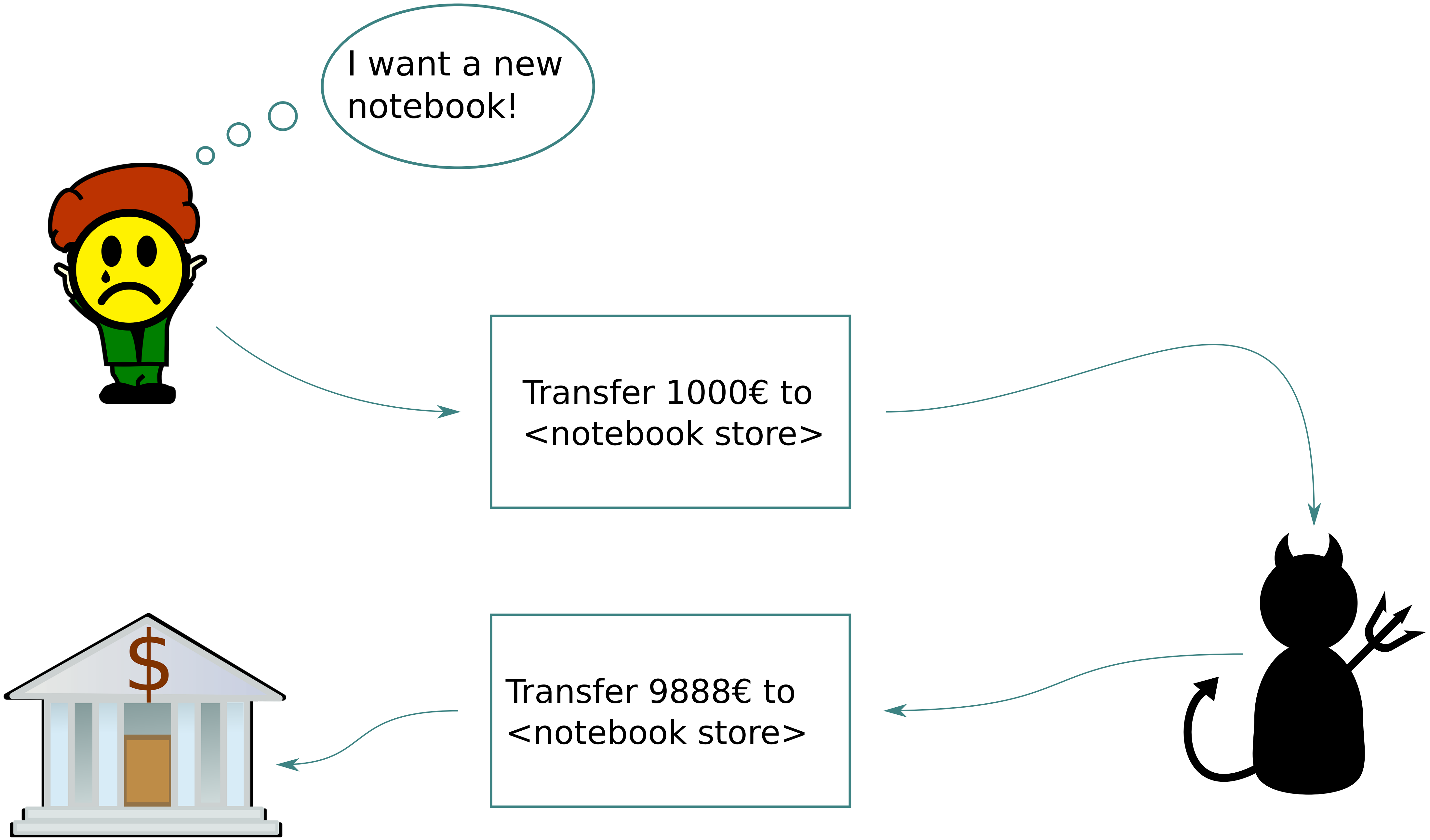
Non-malleability



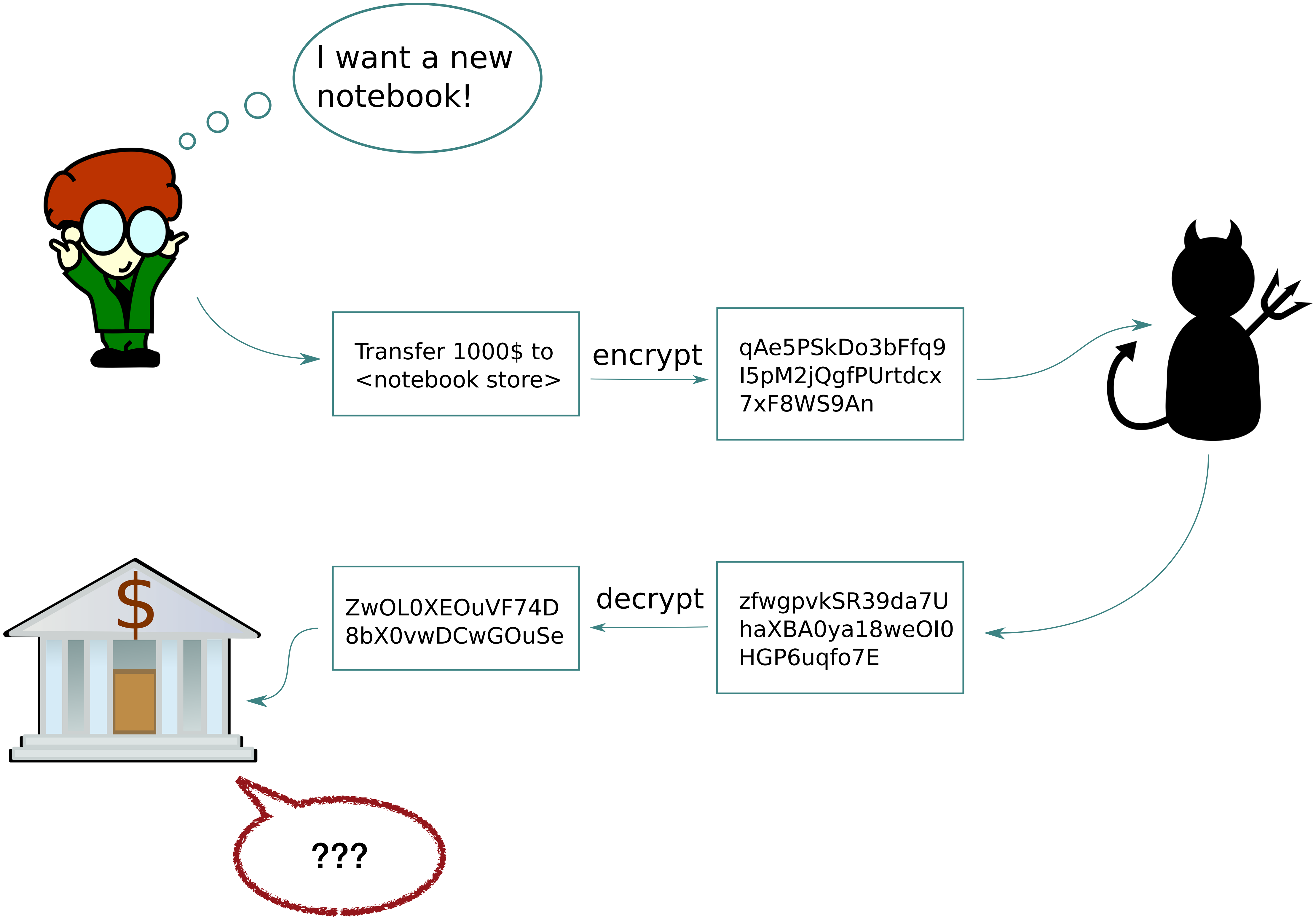
Non-malleability



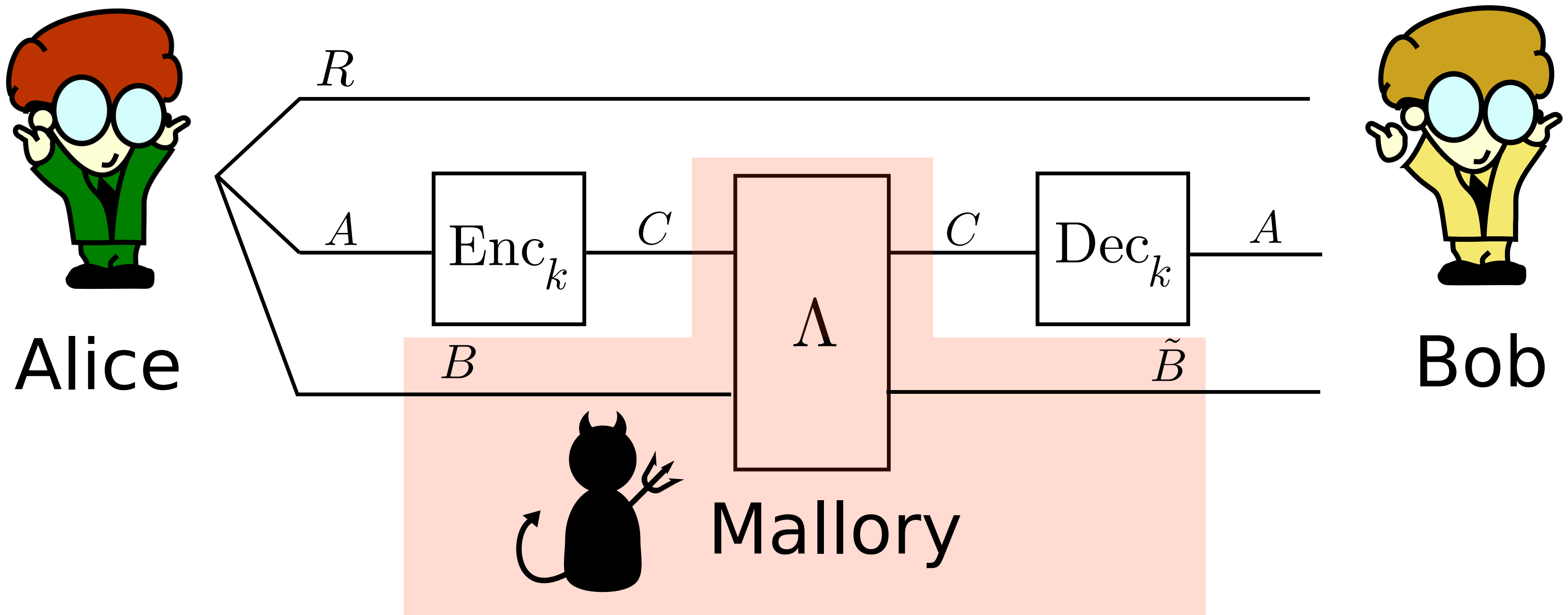
Non-malleability



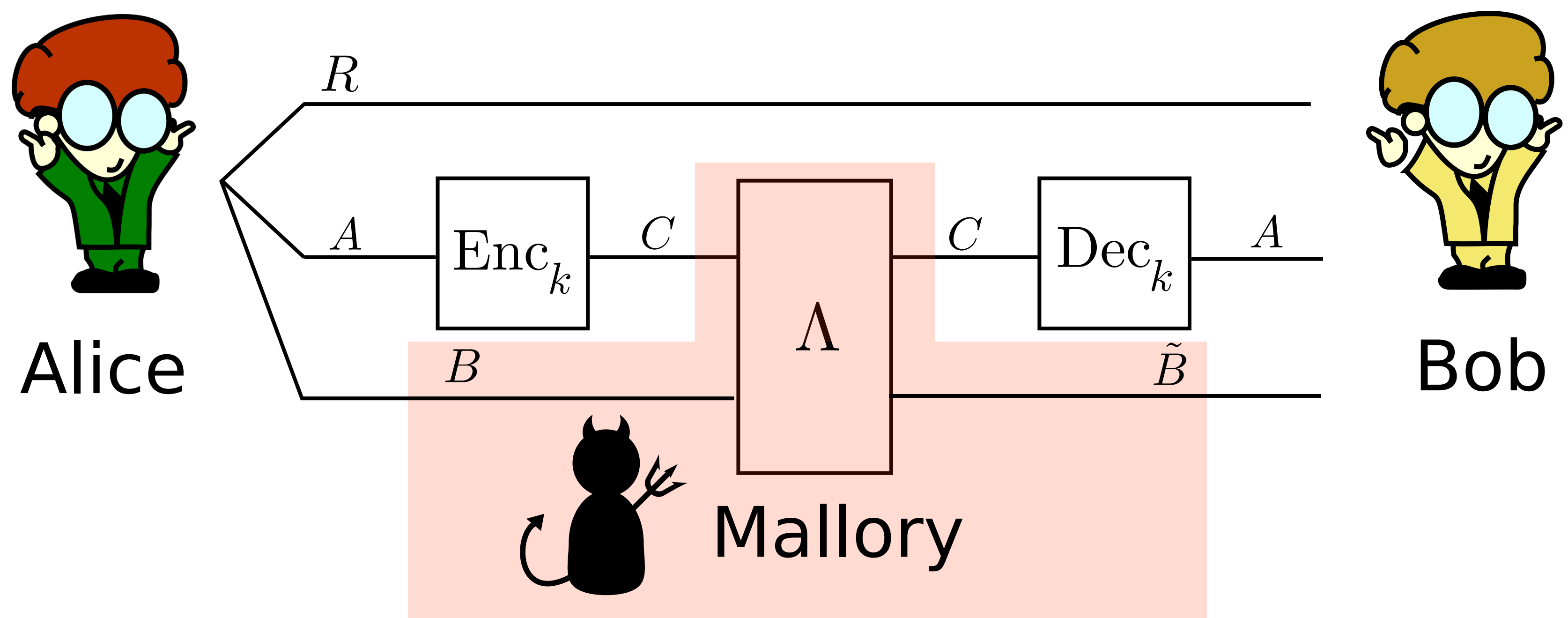
Non-malleability



Non-malleability

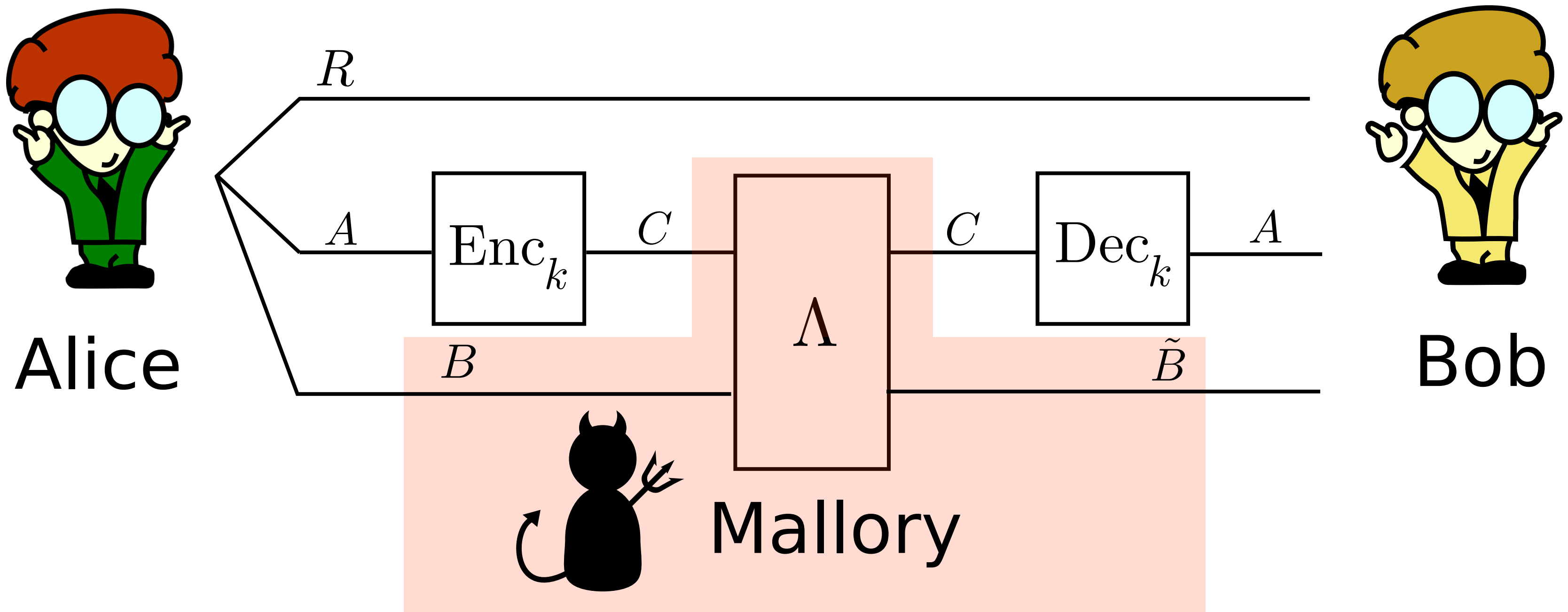


Non-malleability



Encryption with 2-design works (ABW 09; AM 17). Key length: $\sim 4n$ bits for n qubit encryption (shorter keys and larger ciphertexts are also possible, BCGST04)

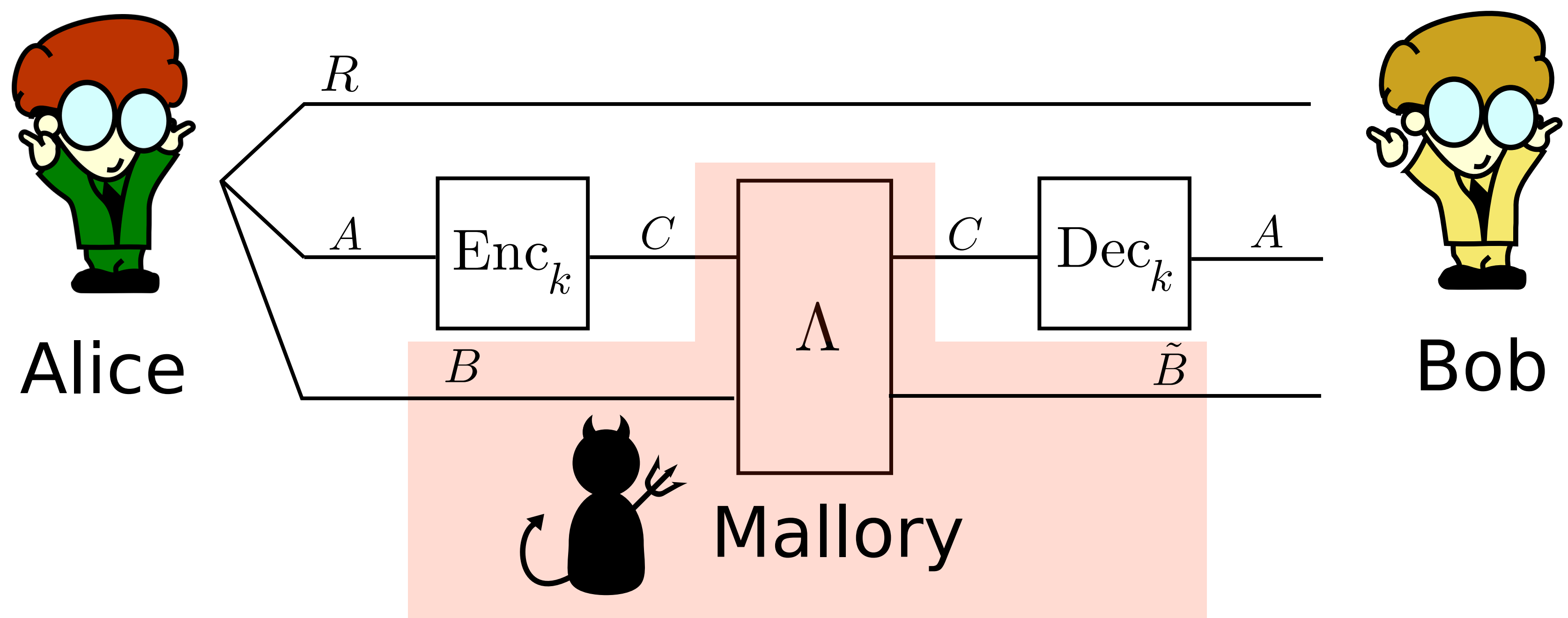
Non-malleability



Encryption with 2-design works (ABW 09; AM 17). Key length: $\sim 4n$ bits for n qubit encryption (shorter keys and larger ciphertexts are also possible, BCGST04)

Weak designs: randomized construction of unitary encryption scheme nm against adversaries with $\leq s$ bits of quantum memory, key length $\sim 2(n+s)$

Non-malleability



Encryption with 2-design works (ABW 09; AM 17). Key length: $\sim 4n$ bits for n qubit encryption (shorter keys and larger ciphertexts are also possible, BCGST04)

Weak designs: randomized construction of unitary encryption scheme nm against adversaries with $\leq s$ bits of quantum memory, key length $\sim 2(n+s)$

Full confidentiality 'for free'.

Summary, open questions

Summary:

- We use a technique of Aubrun to give a randomized construction of t-designs in weak norms
- For $t = 2$, our techniques can be used to construct weak designs for the $U \otimes \bar{U}$ and channel twirls
- As an application, we give a randomized construction of a quantum encryption scheme that achieves non-malleability against adversaries without quantum side information with short keys

Open questions:

- For the $U \otimes \bar{U}$ twirl, we only obtain a result for the $1 \to 1$ norm. Can it be strengthened to $d\|\cdot\|_{1\to\infty}$?