One-time pad

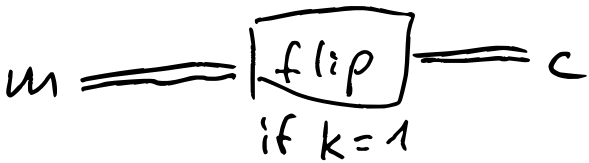
Classically:

Alice wants to send bit m to Bob with "perfect secrecy"

Secret key: $k \in \{0,1\}$

Message $m \in \{0,1\}$

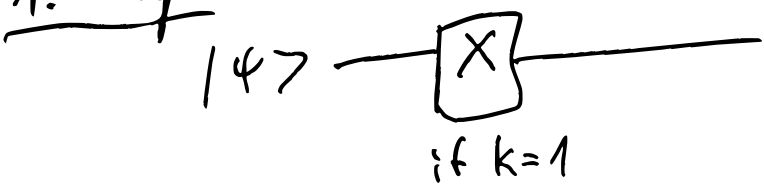
Alice sends: $c = m \oplus k$



Quantumly:

Message: qubit

1. try



Secure?

if $k=0$ if $k=1$

$$|0\rangle \rightsquigarrow \{ |0\rangle @ \tfrac{1}{2}, \; |1\rangle @ \tfrac{1}{2} \}$$

$$|1\rangle \rightsquigarrow \{ |1\rangle @ \tfrac{1}{2}, \; |0\rangle @ \tfrac{1}{2} \}$$

$$|+\rangle \rightsquigarrow \{ |+\rangle @ \tfrac{1}{2}, \; |+\rangle @ \tfrac{1}{2} \}$$

$$= \{ |+\rangle @ 1 \}$$

$$|-\rangle \rightsquigarrow \{ |-\rangle @ \tfrac{1}{2}, \; -|-\rangle @ \tfrac{1}{2} \}$$

$$\approx \{ |-\rangle @ 1 \}$$

$\Rightarrow$ Adv can perfectly distinguish enc of $|+\rangle$ and $|-\rangle$.

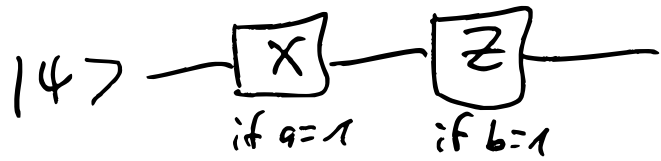
$\Rightarrow$ insecure

$$|+\rangle = \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle$$
$$\xrightarrow{X} \tfrac{1}{\sqrt{2}}|1\rangle + \tfrac{1}{\sqrt{2}}|0\rangle$$
$$= |+\rangle$$

Quantum OTP

Message : $|\psi\rangle \in \mathbb{C}^2$

Key : $a, b \in \{0,1\}$



Secure?

Def: For any $|\psi\rangle, |\psi'\rangle$, the output of this circuit is phys. ind.

> Caveat: This def. does not per se guarantee anything if msg is entangled with something else

Thm: Secure

Proof:

Say $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1$

$E = \{ |\psi\rangle @ \frac{1}{4}, X|\psi\rangle @ \frac{1}{4}, Z|\psi\rangle @ \frac{1}{4}, ZX|\psi\rangle @ \frac{1}{4} \}$

↑ distr. of output

$$E = \{ |\psi\rangle\langle\psi|\frac{1}{4},\ X|\psi\rangle\langle\psi|X\frac{1}{4},\ Z|\psi\rangle\langle\psi|Z\frac{1}{4},\ ZX|\psi\rangle\langle\psi|XZ\frac{1}{4} \}$$

$$\rho = \frac{1}{4}\Big(|\psi\rangle\langle\psi| + X|\psi\rangle\langle\psi|X + Z|\psi\rangle\langle\psi|Z + ZX|\psi\rangle\langle\psi|XZ \Big)$$

$$= \frac{1}{4}\left(A + ZAZ \right) \text{ with}$$

$$A := |\psi\rangle\langle\psi| + X|\psi\rangle\langle\psi|X$$

$$|\psi\rangle\langle\psi| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}(\bar\alpha\ \bar\beta) = \begin{pmatrix}|\alpha|^2 & \alpha\bar\beta\\ \bar\alpha\beta & |\beta|^2\end{pmatrix}$$

$$X|\psi\rangle\langle\psi|X = \begin{pmatrix}|\beta|^2 & \bar\alpha\beta\\ \alpha\bar\beta & |\alpha|^2\end{pmatrix}$$

$$A = \begin{pmatrix}1 & \alpha\bar\beta + \bar\alpha\beta\\ \alpha\bar\beta + \bar\alpha\beta & 1\end{pmatrix} \qquad ZAZ = \begin{pmatrix}1 & -\alpha\bar\beta - \bar\alpha\beta\\ -\alpha\bar\beta - \bar\alpha\beta & 1\end{pmatrix}$$

$$A + ZAZ = \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} \qquad \rho = \frac{1}{2}\mathbb{I}$$

$X = \begin{pmatrix}1 & \\ & -1\end{pmatrix}$, $X^+ = X$

$Z = \begin{pmatrix}1 & \\ & -1\end{pmatrix}$, $Z^+ = Z$

Output for $|\psi'\rangle$: also $\varrho = \frac{1}{2} I$

$\Rightarrow$ Enc $|\psi\rangle$, $|\psi'\rangle$

are phys. indist.

$\Rightarrow$ QOTP secure

(perfect secrecy) ∎

Thm/Def: ϱ is a density op. iff

- ϱ Hermitian ($\varrho^+ = \varrho$)
- $\varrho \geq 0$ (all eigenvalues ≥ 0)
- $\mathrm{tr}\,\varrho = 1$

→ If we have distribs with total prob ≤ 1, this becomes "$\mathrm{tr}\,\varrho \leq 1$"

Throwing away stuff (partial trace)

Motivation 1:

Have $f : \{0,1\}^n \to \{0,1\}^m$

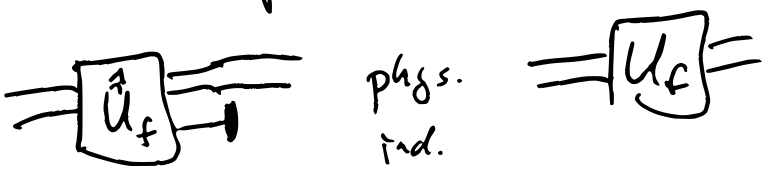
Want: $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$

Attempt 1: $\hat{U}_f : |x, y\rangle \to |x, y \oplus f(x), \text{stuff}\rangle$

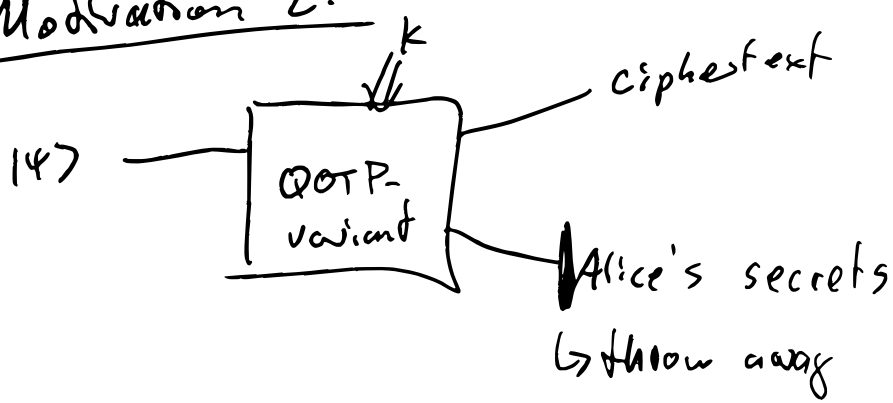
Attempt 2:

$\tilde{U}_f : |x, y\rangle \to |x, y \oplus f(x), 0\rangle$

Want to prove:



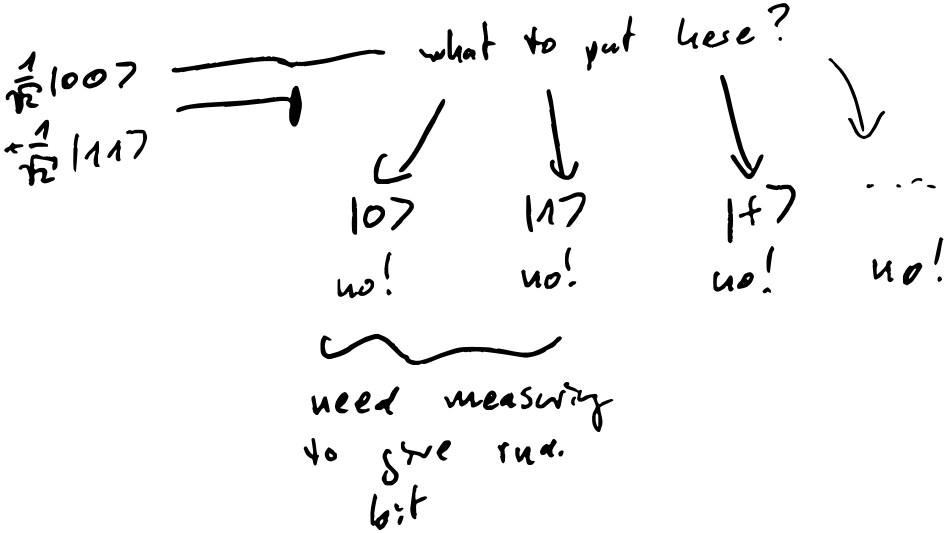
Motivation 2:



How to mathematically describe:

Say we describe it as a function $\mathbb{C}^{2^n \cdot 2^m} \longrightarrow \mathbb{C}^{2^n}$.

This does not work!



$\Rightarrow$ Need density op. to describe $\longrightarrow$

Want:

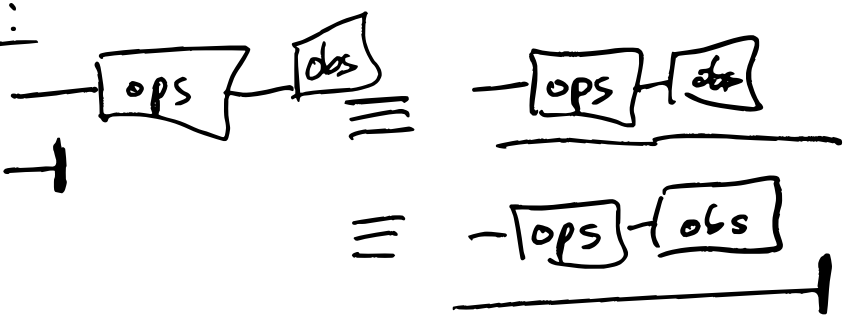
- some op that maps density ops on AB $(\mathbb{C}^{NM \times NM})$

  $\longrightarrow$

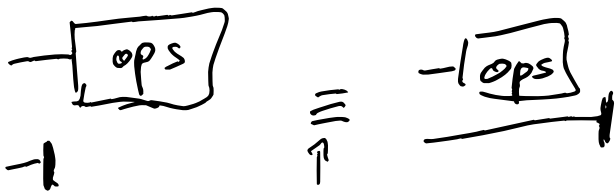
  density ops on A $(\mathbb{C}^{N \times M})$

- model "throwing away"

i.e.:



i.e:



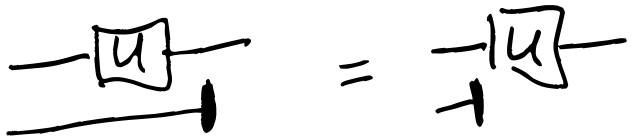
same density op

Answer: $\mathrm{tr}_B S$ defined by:

- $\sigma \otimes \tau \xrightarrow{\mathrm{tr}_B} \sigma \cdot \mathrm{tr}\,\tau$
- tr_B linear

---

tr_B "models throwing away"..



i.e.: $\mathrm{tr}_B (U \otimes I) \rho (U^\dagger \otimes I) = U \, \mathrm{tr}_B \rho \, U^\dagger$

and similar for measurements etc.