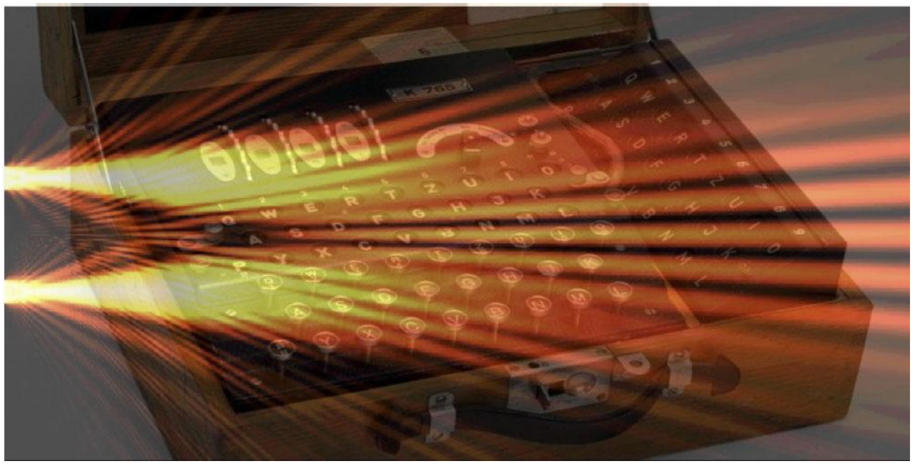
Quantum data locking and the locking capacity of a quantum channel

Guha, Hayden, Krovi, Lloyd, Lupo, Shapiro, Takeoka, Wilde, Winter



Summary

- Notions of Security
- Quantum Data Locking
- Locking Capacity
- Trading Security for Rate
- Locked Key Distribution

$p_A^x \qquad \rho_A^x$

$$\rho_A = \sum_x p_A^x \rho_A^x$$

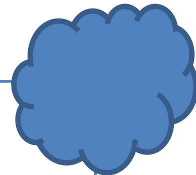
ρ_B

ρ_E

$$\rho_{AE} \sim \rho_A \rho_E$$

$$\left\| \rho_{AE} - \rho_A \rho_E \right\|_1 \leq \varepsilon$$

p_A^x ρ_A^x



ρ_B

ρ_E

$$\rho_A = \sum_x p_A^x \rho_A^x$$

$$\rho_{AE} \sim \rho_A \rho_E$$

$$\left\| \rho_{AE} - \rho_A \rho_E \right\|_1 \leq \varepsilon$$

M

p_E

$$p_{AE} \sim p_A p_E$$

$$\sup_M \left\| p_{AE} - p_A p_E \right\|_1 \leq \varepsilon$$

Pre-measurement security (Holevo inf.)

$$S\left(\rho_{AE} \| \rho_A \rho_E\right) = I\left(A,E\right)_{\rho_{AE}} = \chi\left(\left\{p^x, \rho_E^x\right\}\right)$$

After-measurement security (accessible inf.)

$$\sup_M S\left(p_{AE} \| p_A p_E\right) = I_{acc}\left(\left\{p^x, \rho_E^x\right\}\right) = I\left(A,E\right)_{p_{AE}}$$

Quantum Discord $\quad D = I - I_{acc} \geq 0$

Ollivier and Zurek PRL **88**, 017901 (2001)
Henderson and Vedral JPA **34**, 6899 (2001)

Total proportionality

If Eve acquires **n** bits, her information about the message should **not** increase by more than **n** bits.

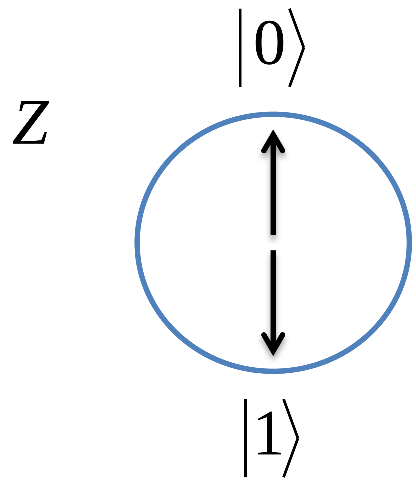
$$I(A,EK) \le I(A,E) + H(K)$$

- ✓ Classical mutual information
- ✓ Holevo information
- ✗ PR-box
- ✗ Accessible information

DiVincenzo et al. PRL **92**, 067902 (2004)

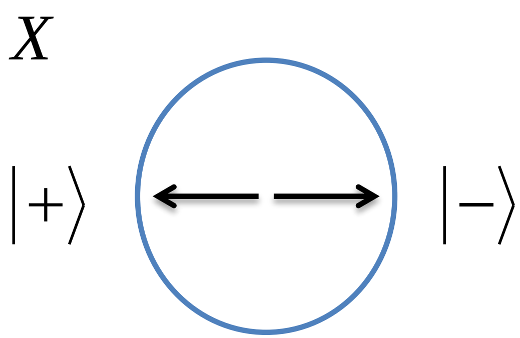
Principle of Information Causality
Pawłowski et al. Nature **461**, 1101 (2009)

Quantum Data Locking



Alice and Bob secretly agree on one of two conjugate bases

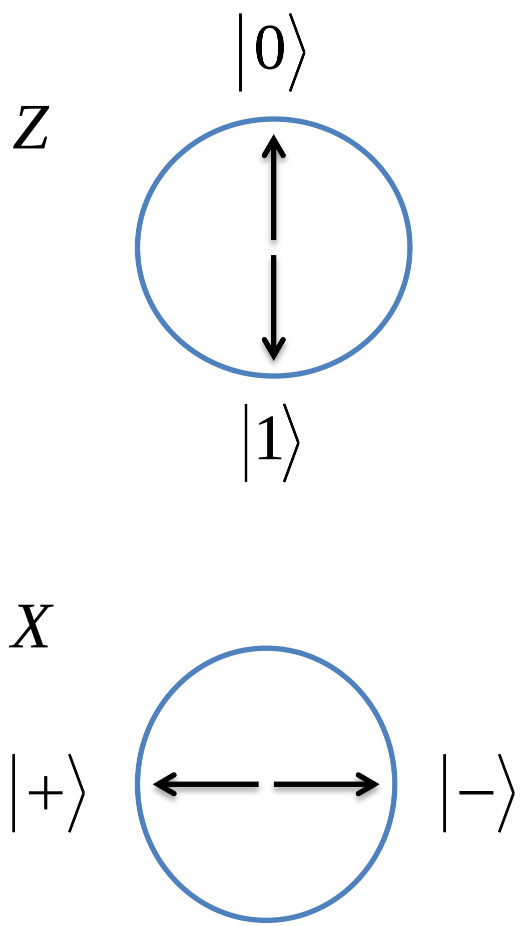
1 bit of secrecy



Alice sends to Bob **n** bits of classical inf using the chosen basis

DiVincenzo et al. PRL **92**, 067902 (2004)

Quantum Data Locking



$$I_{acc}(A,E) \leq n - \min_{POVM} H(Q|b)$$

Entropic uncertainty relations:

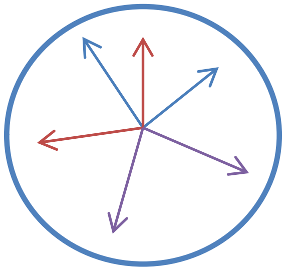
$$H(Q|b) = \frac{H(Q|X) + H(Q|Z)}{2} \geq \frac{n}{2}$$

Maassen and Uffink PRL 60, 1103 (1988)

$$I_{acc}(A,E) \leq \frac{n}{2}$$

DiVincenzo et al. PRL **92**, 067902 (2004)

Strong Data Locking



K unitaries U_k acting on n qubits

K bases $\quad |j_k\rangle = U_k |j\rangle \quad k = 1, 2, \ldots K$

$$I_{acc}(A, E) \leq n - \min_{POVM} H(Q|b)$$

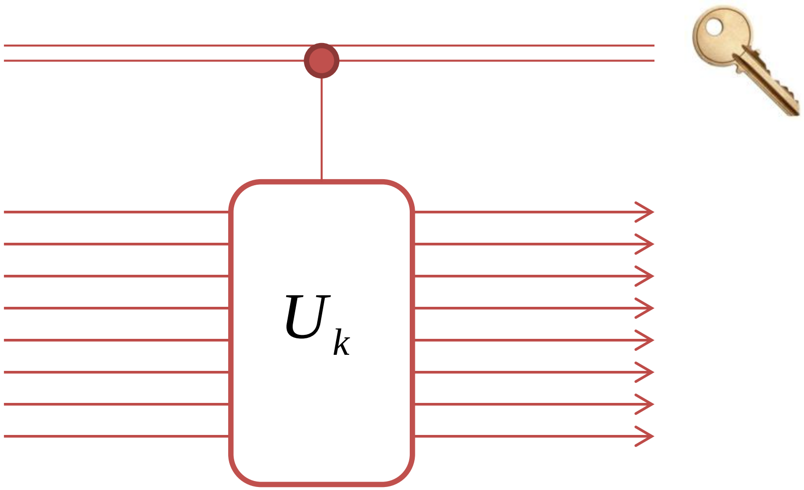
Strong ent. unc. relations $\quad H(Q|b) = \frac{1}{K}\sum_k H(Q|b_k) \geq (1-\varepsilon)n$

$$I_{acc}(A, E) \leq \varepsilon n$$

$\varepsilon \approx K^{-a}$

$a = 1/4$

Strong Data Locking



Haar-distributed random unitaries:

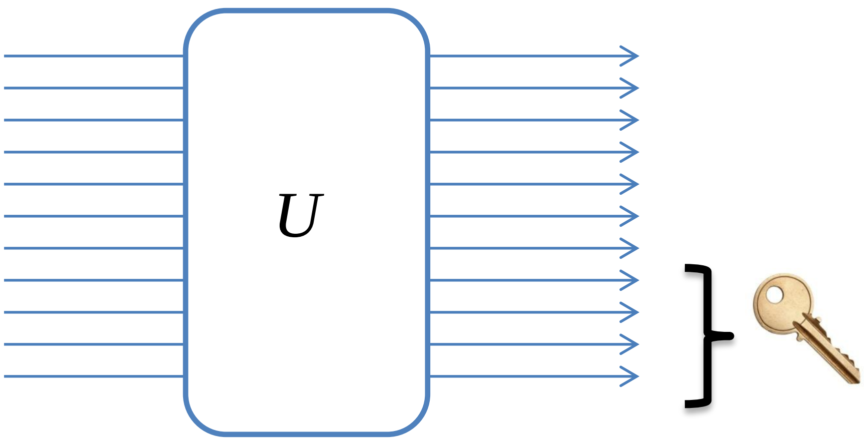
Hayden et al. CMP **250**, 371 (2004)

Pseudo-random unitaries:

Lupo, Wilde, Lloyd PRA **90**, 022326 (2014)

Explicit and efficient constructions:

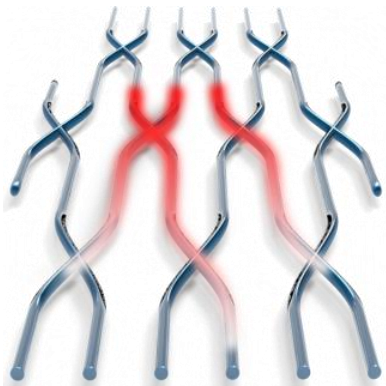
Fawzi et al. J. ACM **60**, 44 (2013)

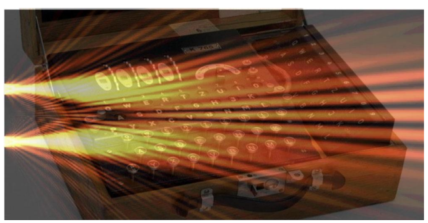


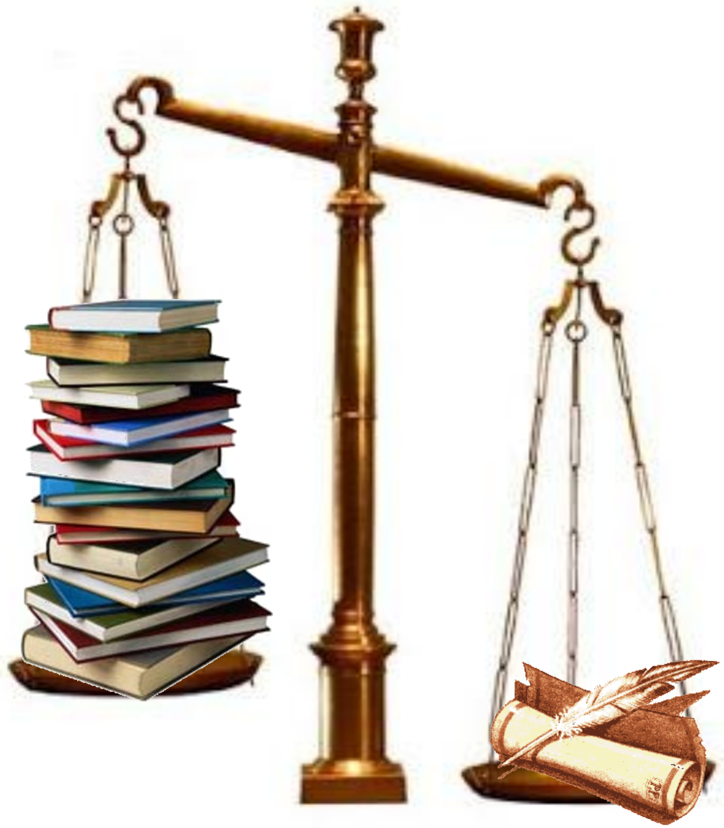
1 unitary
+ limited access to a subset of qubits

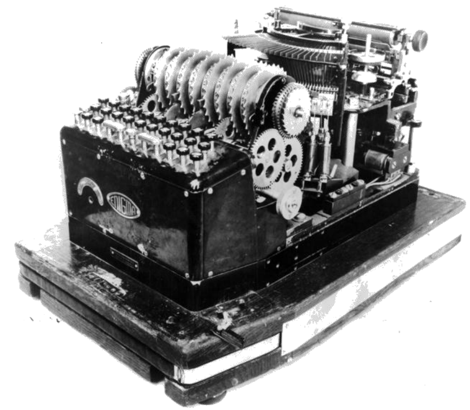
Dupuis et al. P Royal S A **469**, 2159 (2013)

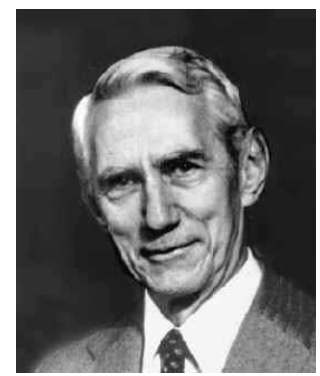
Quantum Enigma Machines





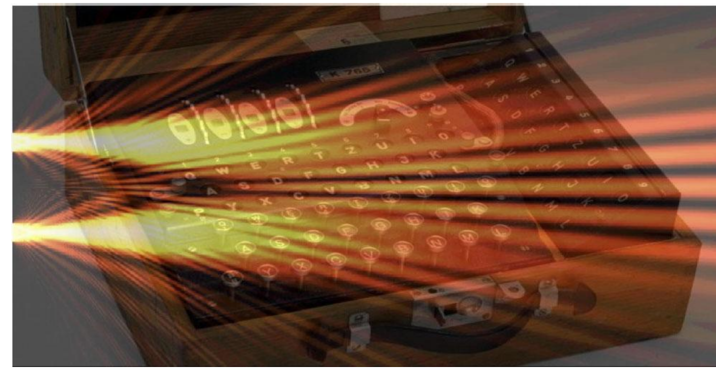






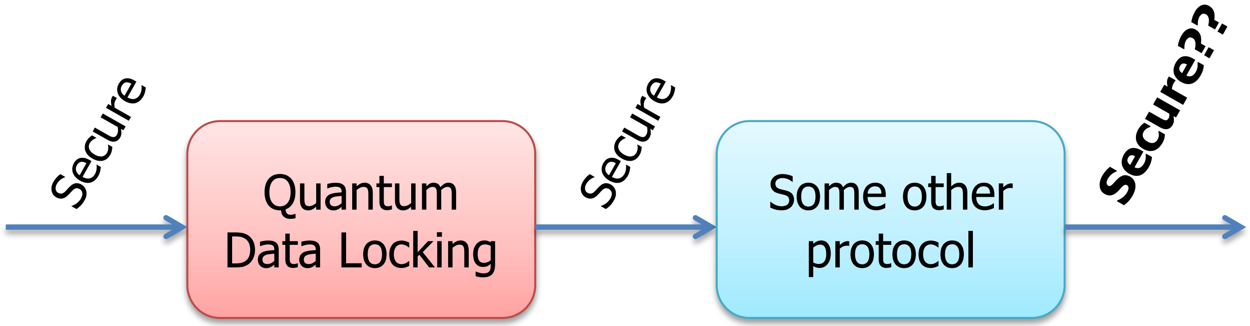
Lloyd, arXiv:1307.0380

Quantum Enigma Machines



- ✓ Composability (total proportionality)
- ✓ Noisy channels

Composability



Composable security:
The output of the protocol is still secure if used as input of another protocol

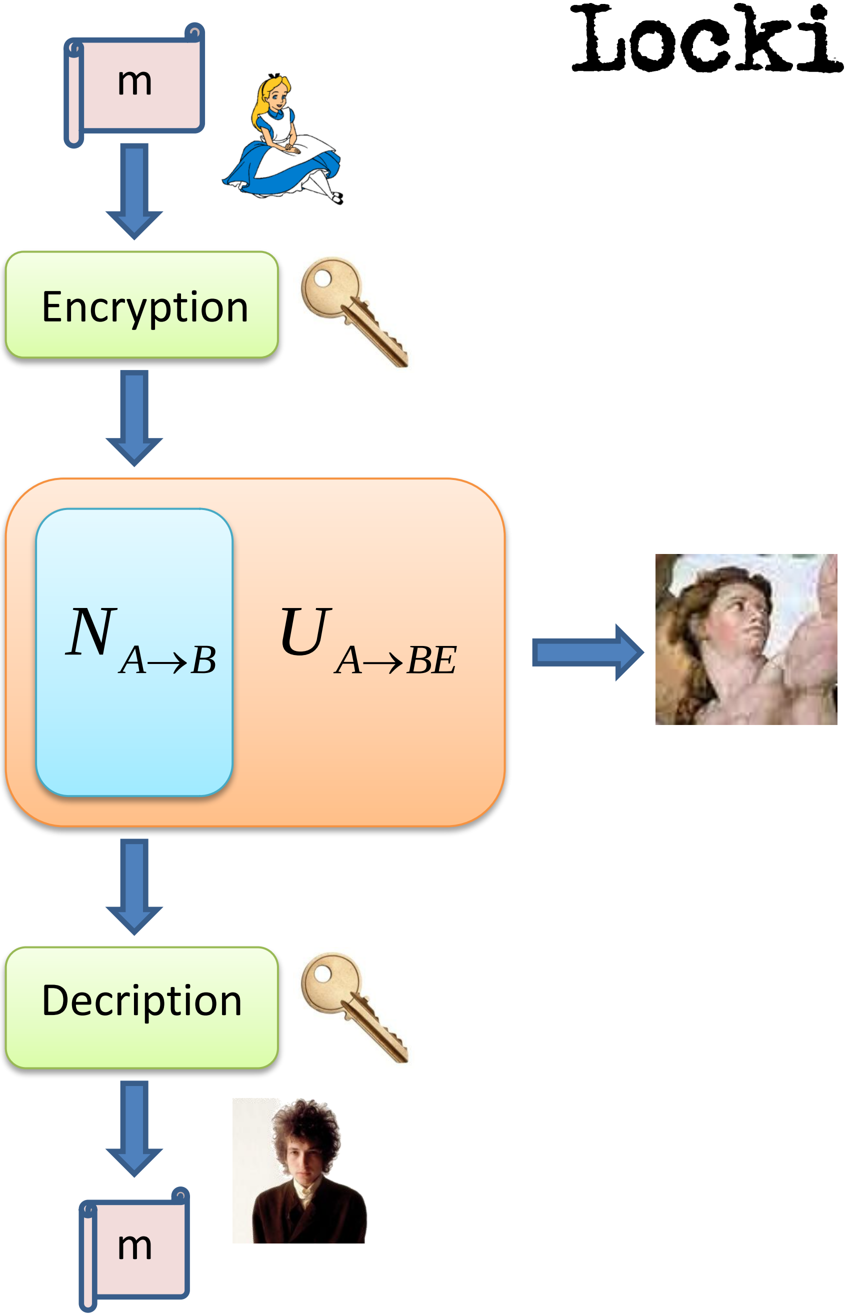
Examples:
1) key distributed by QDL is used for one-time pad
2) classical post-processing in QKD

Accessible information criterion **is not composable** in general

Koenig et al. PRL **98** 140502 (2007)

Physical assumption:
Eve's quantum memory storage time is finite.
(and Alice and Bob know it!)

Locking noisy channels



All communication systems suffer from **physical-layer noise**

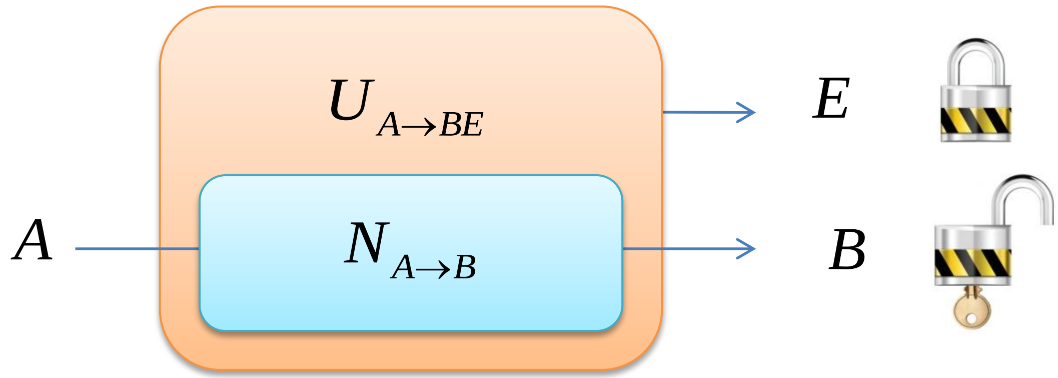
Error correction should be applied to achieve reliable (enigmatized) communication

Noisy channel can always be complemented to a **unitary transformation**

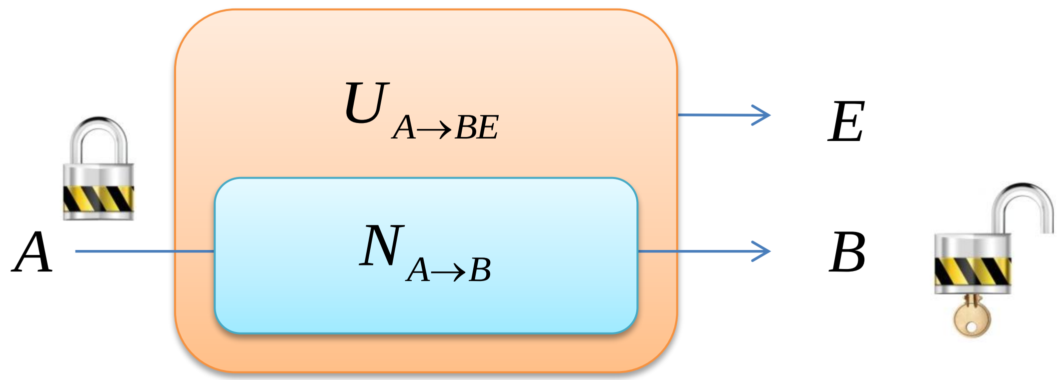
Eve has access to the **complement** of Bob output.

Weak and Strong Locking

Weak Locking Capacity L_W



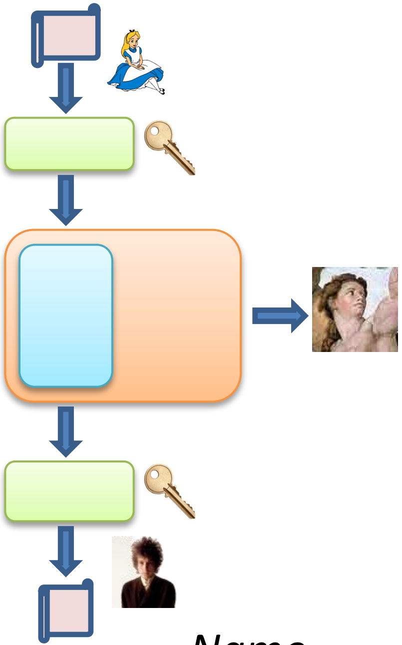
Strong Locking Capacity L_S



With the assistence of a (short) pre-shared secret key. # secret bits grows less than linearly in # of channel uses.

Guha et al. PRX **4**, 011016 (2014)

Locking noisy channels



The price of error correction is to reduce the communication rate

The capacity of the channel is the max communication rate (*with zero error for asymptotically long messages*)

Name	*Symbol*	*Requirements*
Classical capacity	C	Reliable communication from Alice to Bob. No secrecy.
Weak Locking capacity	L_W	Reliable comm. from A to B. Accessible inf. secrecy.
Private capacity	P	Reliable communication from A to B. Holevo inf. secrecy.

$$P \leq L_W \leq C$$

Guha et al. PRX **4**, 011016 (2014)

Locking vs Private Capacity

$$L_W \leq \sup \tfrac{1}{n}\left[\chi(A,B) - I_{acc}(A,E)\right]$$

$$\begin{aligned} L_W &\leq \sup \tfrac{1}{n}\left[\chi(A,B) - I_{acc}(A,E)\right] \\ &\leq \sup \tfrac{1}{n}\left[\chi(A,B) - \chi(A,E)\right] + \sup \tfrac{1}{n}\left[\chi(A,E) - I_{acc}(A,E)\right] \\ &= P + \sup \tfrac{1}{n} D \end{aligned}$$

$$L_W - P \leq \sup \tfrac{1}{n} D$$

Quantum discord is an upper bound to the gain provided by QDL.

Guha et al. PRX **4**, 011016 (2014)

- Is this upper bound achievable?
- Is there a nonzero gap between L_W and P ?

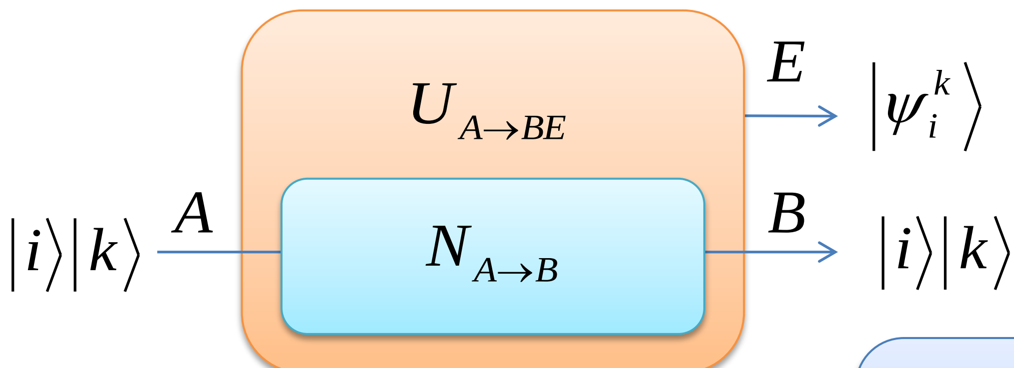
Locking vs Private Capacity

Upper bound achievable (and single-letter)
for Hadamard channels (complementary to ent breaking)

$$L_W = \sup \chi(A,B) - I_{acc}(A,E)$$

Winter, arXiv:1403.6361

Example:



$$X|\psi_i^0\rangle = \lambda_i|\psi_i^0\rangle$$

$$Z|\psi_i^1\rangle = \lambda_i|\psi_i^1\rangle$$

$$\dim A = \dim B = 2d$$

$$\dim E = d$$

$$P = 1$$

$$L_W = 1 + \tfrac{1}{2}\log d$$

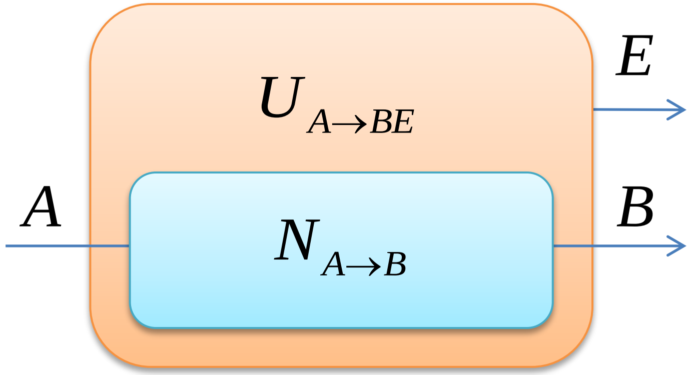
Locking vs Private Capacity

There exist channel with zero private capacity having arbitrary high locking capacity

Winter, arXiv:1403.6361

Example:

$$|\psi_i^k\rangle|\psi_i^k\rangle$$



$$|\psi_i^k\rangle \quad (E)$$

$$|\psi_i^k\rangle \quad (B)$$

$$X|\psi_i^0\rangle = \lambda_i|\psi_i^0\rangle$$

$$Z|\psi_i^1\rangle = \lambda_i|\psi_i^1\rangle$$

$$\dim A = 2d$$

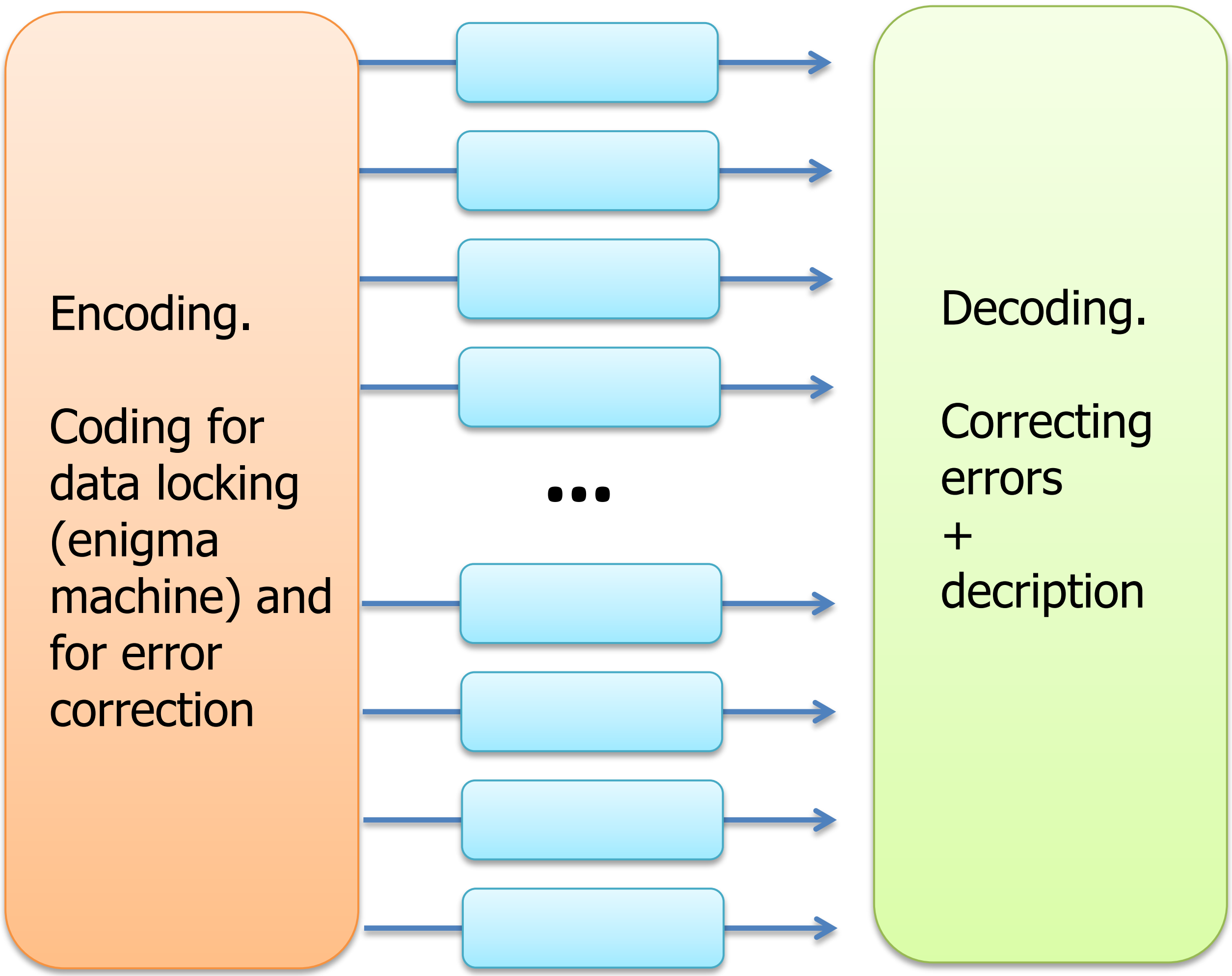
$$\dim B = \dim E = d$$

$$P = 0$$

$$L_W \geq \tfrac{1}{2}\log d$$

Proof strategy includes: bound the min-entropy using the entropic uncertainty relations, + use min-entropy extractor

Random coding

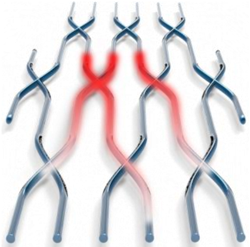


Information locked in qudits

Random coding for memoryless qudit channels

Memoryless qudit channel

Lupo, Lloyd, arXiv: 1406.4418

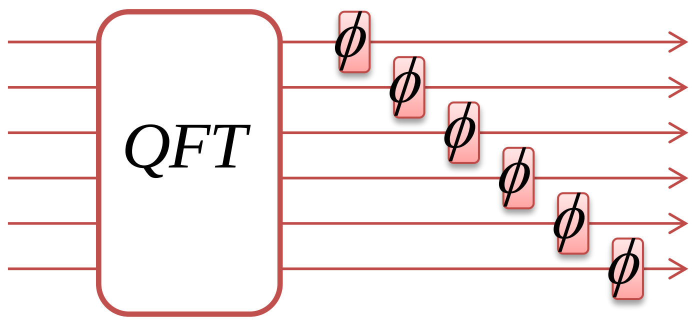


Linear Optics

Analogous to **d**-dimensional QKD with K different bases

$$|j_k\rangle = U_k |j\rangle$$

1 photon over d modes (unary encoding)



$$U_k = \sum_{\omega} e^{i\phi_k(\omega)} |\omega\rangle\langle\omega|$$

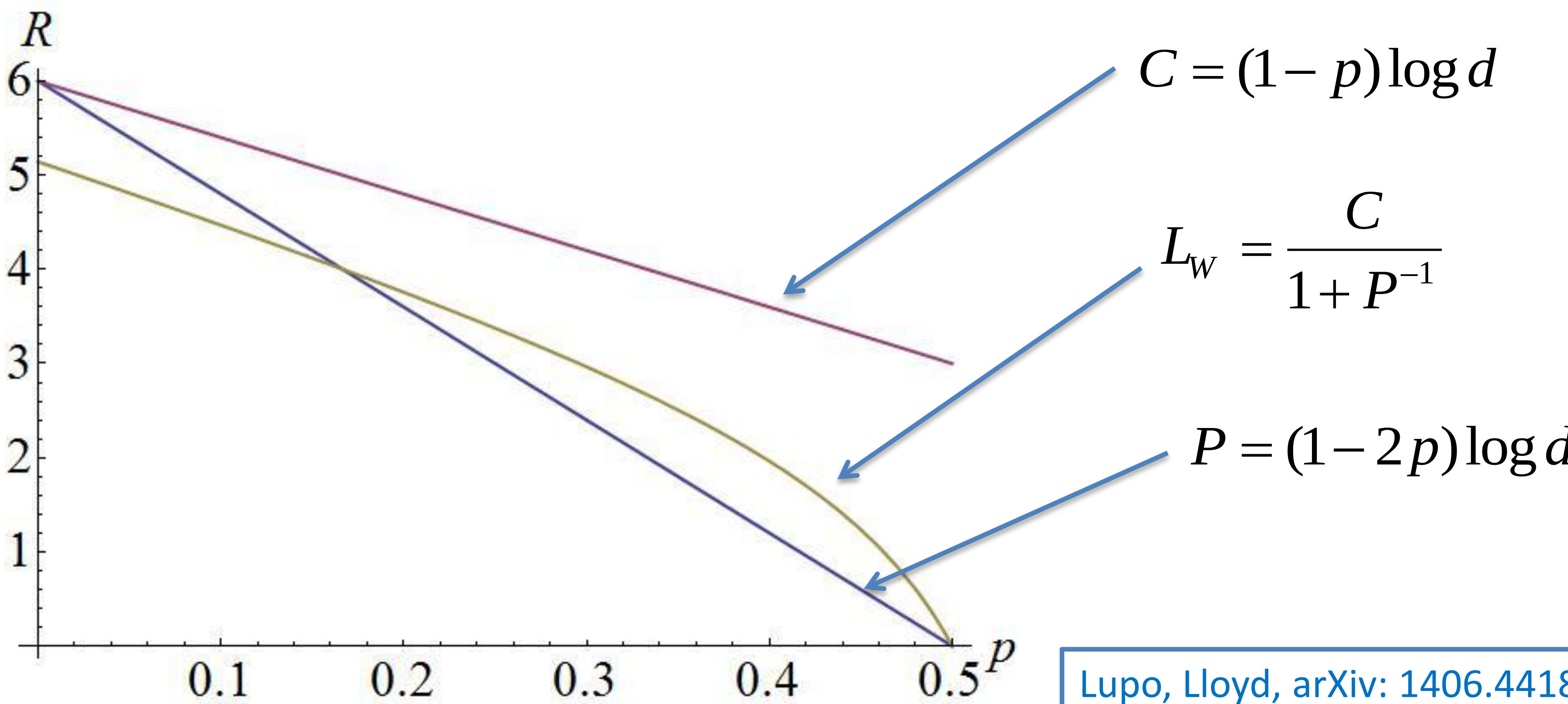
$$|\omega\rangle = \frac{1}{\sqrt{N}} \sum_j e^{i 2\pi j \omega / N}$$

Lupo, Lloyd, arXiv: 1406.4418

Locked communication

Qudit erasure channel with p<1/2.
(It models unary encoding with linear loss less than 50%).

- Use channel to produce a secret key (at the private capacity rate).
- Use the key to lock the message.



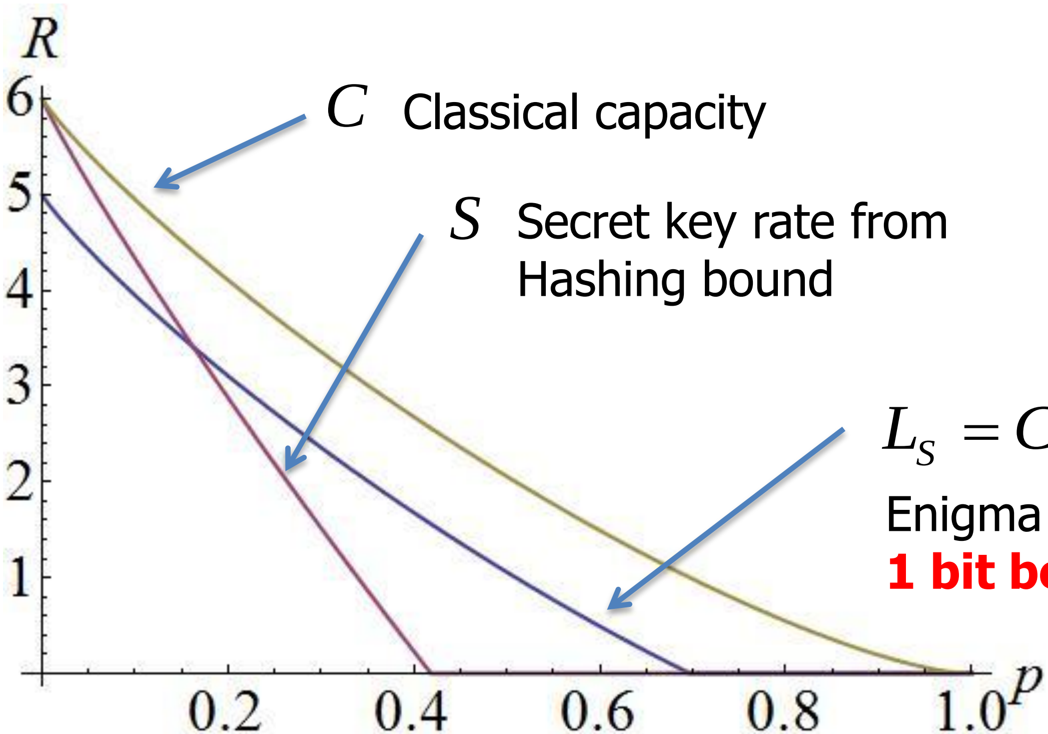
Lupo, Lloyd, arXiv: 1406.4418

Locked key generation

Qudit depolarizing channel.

- Start with a small secret key.
- Use the key to “data lock” the message.
- Wait for Eve’s quantum memory to decohere, then recycle part of the key and start again

An assumption about the coherence time of Eve’s quantum memory is required to guarantee security



$L_S = C - 1$

Enigma secret key generation rate

1 bit below the classical capacity!

Lupo, Lloyd, arXiv: 1406.4418

Conclusion

Large Gap between Security Criteria

Trading Security for Rate

High Gain in QKD
(under assumption on
Eve's Technology!)