Thesis Oral

On the Communication Complexity of Classical Correlation Distillation and Quantum Entanglement Distillation

Ke Yang

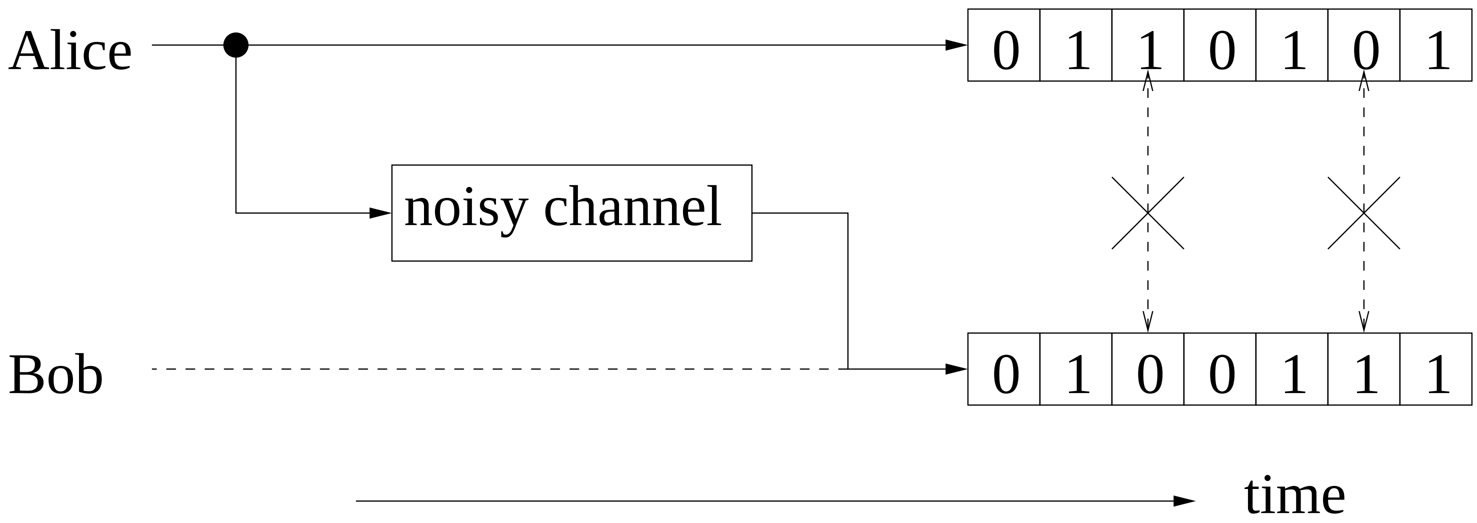
Thesis Committee
Steven Rudich (chair)
Avrim Blum
Robert Griffiths
Andris Ambainis (IAS)

On Repairing Corrupted Correlation

Recurring Theme in Information Theory

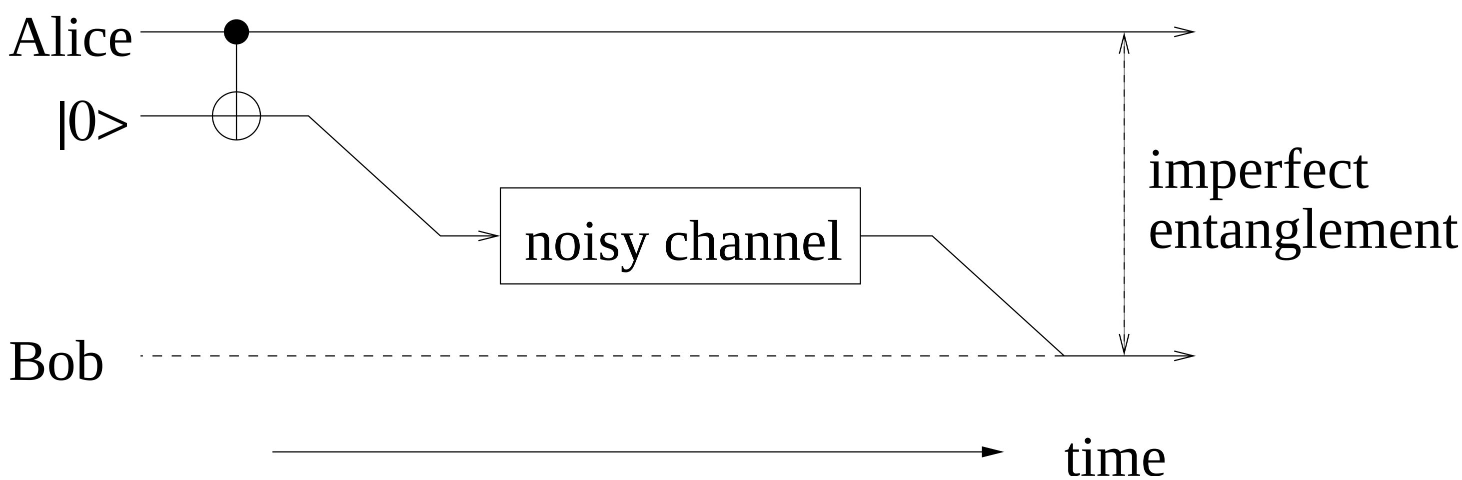
- Correlation Corruption
  Alice and Bob share imperfectly correlated information
- Correlation Recovery
  Alice and Bob take action to recover perfect correlation

Classical Noisy Channel



- Alice sends bits to Bob
- Correlation corruption by the noisy channel

Quantum Noisy Channel



- Alice sends qubits to Bob
- Entanglement corruption by the noisy channel

"Correlation" Overloading

- classical::correlation = correlation
- quantum::correlation = entanglement

Strategies for Correlation Recovery

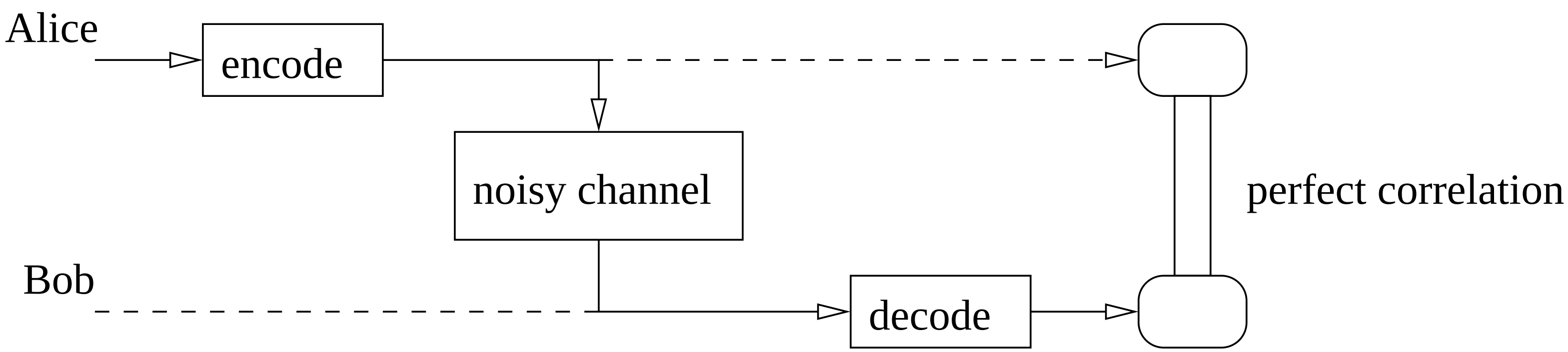
- **Preventive Strategy**

  Adding redundancy before the corruption

- **Reparative Strategy**

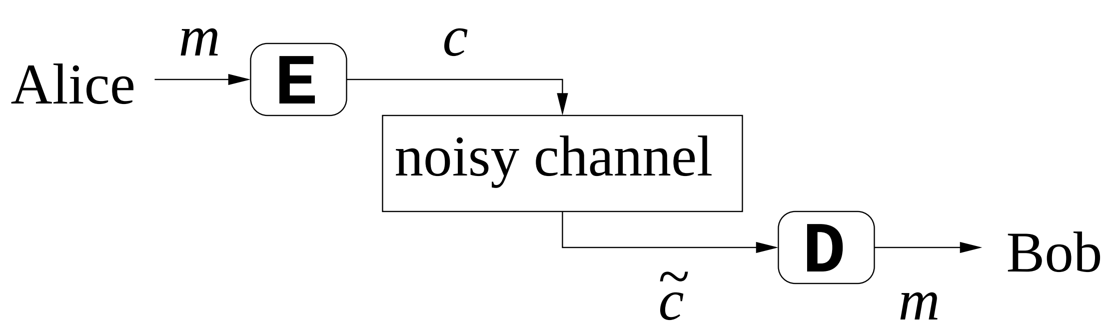
  Recovering correlation only after corruption

Preventive Strategy



- Information encoded before the corruption
- Error Correcting Codes (ECCs)
- Quantum Error Correcting Codes (QECCs)

Error Correcting Codes



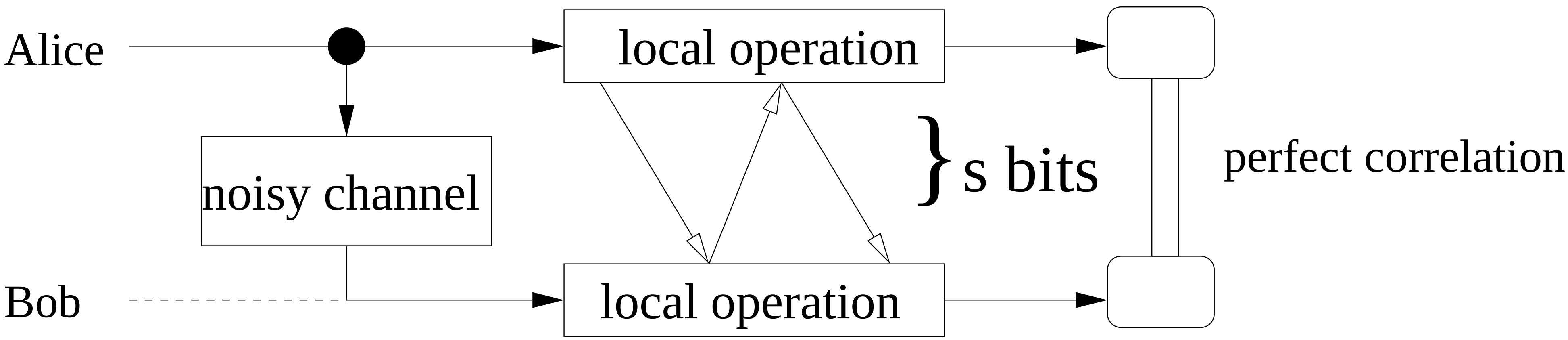
- (n, k, d)-ECC: $\{0,1\}^k \mapsto \{0,1\}^n$, such that

$$\mathrm{DIST}(E(m_1), E(m_2)) \geq d$$

- Code Overhead: $(n - k)$ bits
- Noise Tolerance: $\leq (d - 1)/2$ bit flips

(encoding/decoding complexity not our focus)

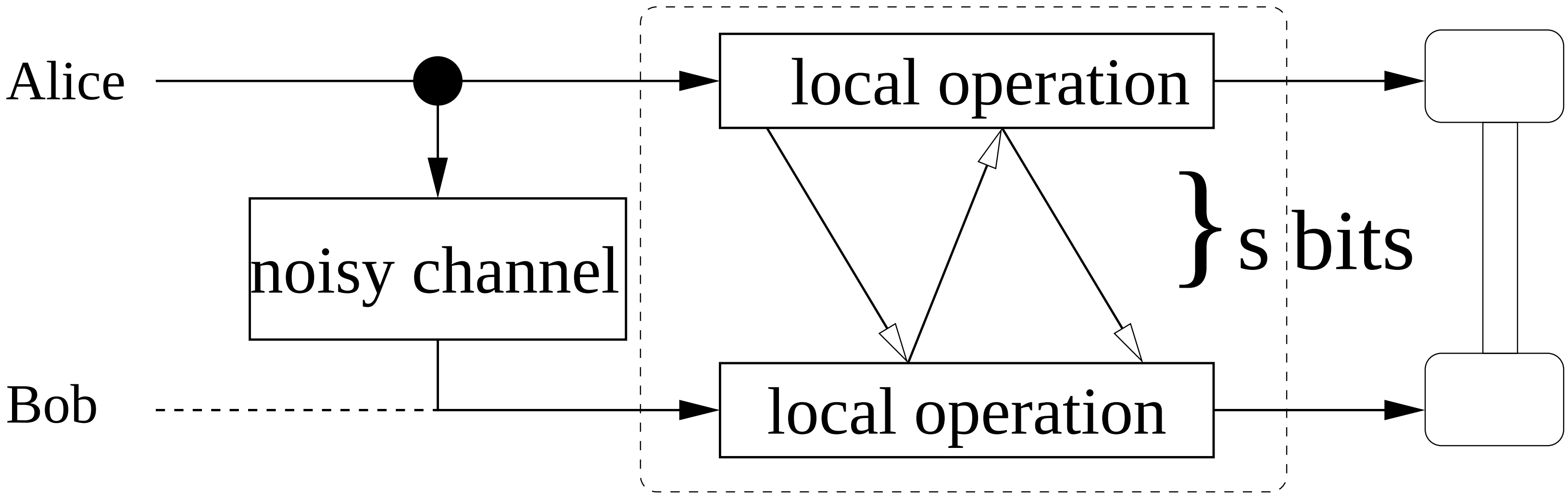
Reparative Strategy



- Correlation repaired after the corruption
- Alice and Bob exchange s bits to recover the correlation
  - ASSUMPTION: noiseless classical communication
  - GOAL: minimize s

    (computational complexity not our focus)

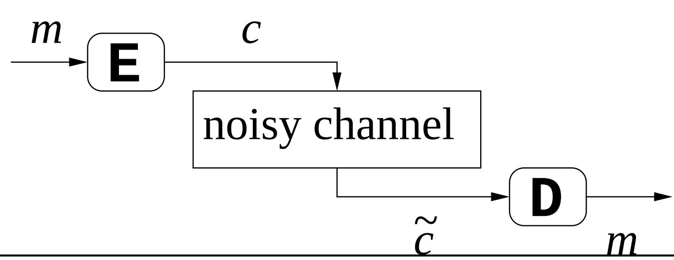
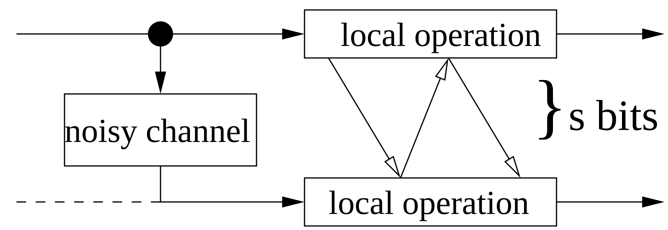
Correlation Distillation



- Classical Correlation Distillation Protocol (CDP)
- Quantum Entanglement Distillation Protocol (EDP)

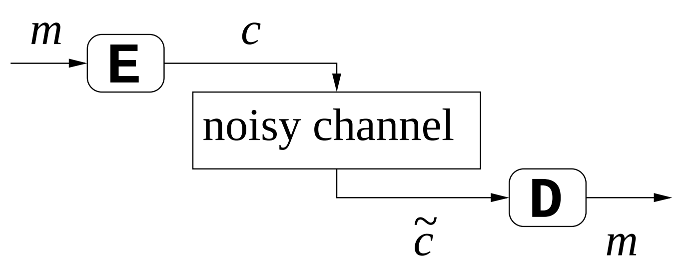
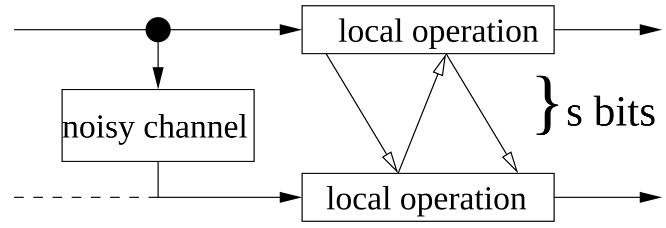
Information Transmission

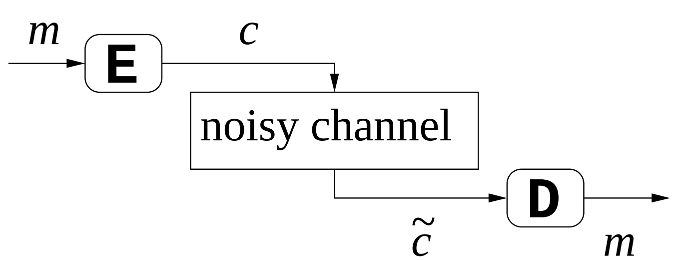
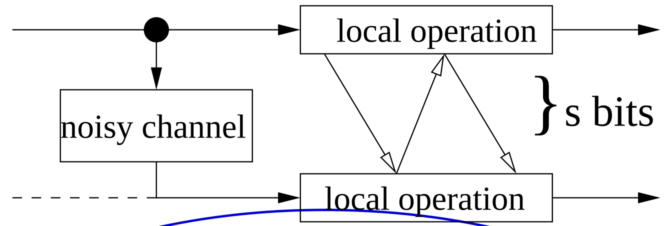
Alice wishes to transmit m to Bob, noiselessly

<table>
<tr><th>preventive</th><th>reparative</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>1. Encoding: $c = E(m)$
2. Transmission: $c \to \tilde{c}$
3. Decoding: $m = D(\tilde{c})$

Overhead $= |c| - |m|$</td><td>1. Transmission: $m \to \tilde{m}$
2. Distillation:
$(m, \tilde{m}) \xrightarrow{\mathcal{P}} (m, m)$

Overhead $= s$</td></tr>
</table>

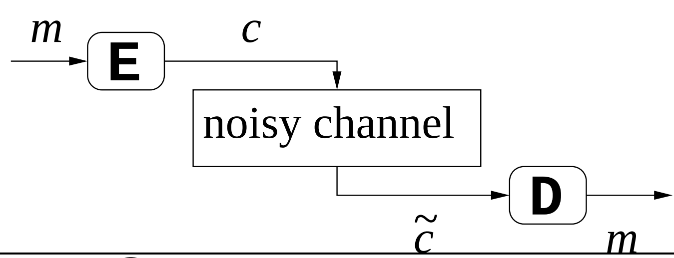
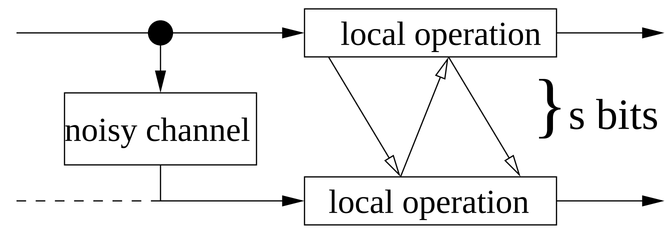
	preventive  	**reparative** 
classical	Error Correcting Code	Correlation Distillation Protocol
quantum	Quantum Error Correcting Code	Entanglement Distillation Protocol
overhead	$\|c\| - \|m\|$	s
status	well−studied, well−understood	less studied, fewer results

	preventive  	**reparative** 
classical	Error Correcting Code	Correlation Distillation Protocol
quantum	Quantum Error Correcting Code	Entanglement Distillation Protocol
overhead	$\|c\| - \|m\|$	s
status	well−studied, well−understood	less studied, fewer results

My thesis

why?

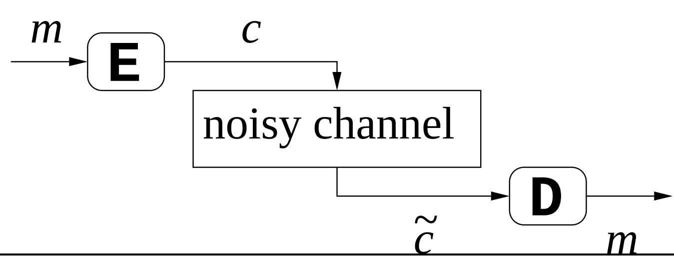
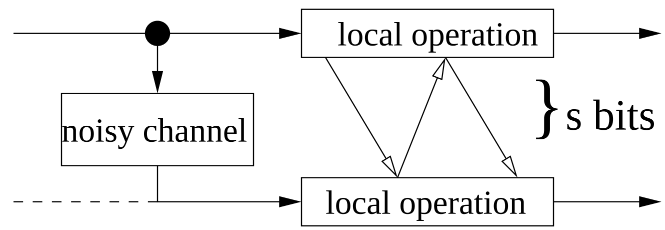
Error Correction is Great!

preventive	reparative
	
☺ non-interactive	interactive

"An ounce of prevention is worth a pound of cure."

(FYI: 1 pound = 16 ounces)

"An Ounce of Prevention is Worth a Pound of Cure."

preventive	reparative
	
Overhead $= \|c\| - \|m\|$	Overhead $= s$

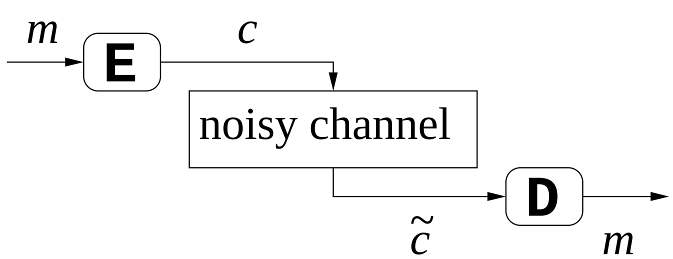
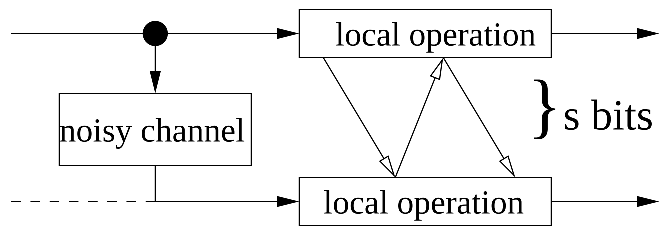
same level of corruption, $16\times$ more efficient?

Not Necessarily

Correlation distillation is ...

1. as efficient as error correction
2. applicable to a wider range of applications

Information Transmission

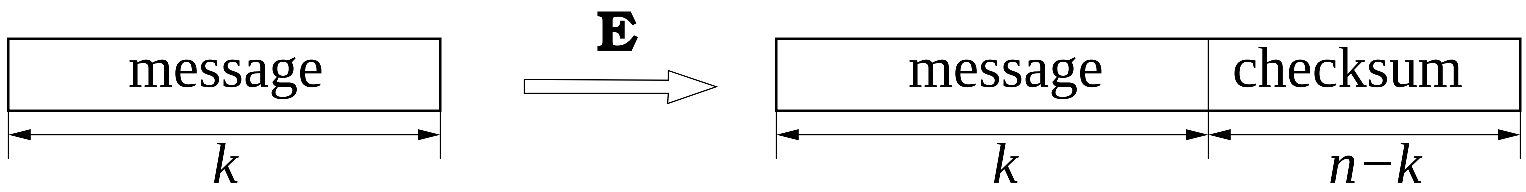
preventive	reparative
	
Overhead $= \lvert c\rvert - \lvert m\rvert$	Overhead $= s$

THM (n, k, d)-linear ECC $\Rightarrow$ CDP of overhead $s = (n - k)$

THM (n, k, d)-stabilizer QECC $\Rightarrow$ EDP of overhead $s = (n - k)$

Proof

THM (n, k, d)-linear ECC $\Rightarrow$ $(n-k)$-bit CDP



PROOF

1. Alice sends the $(n-k)$-bit check-sum
2. Bob decodes

"An ounce of prevention is worth a ~~pound~~ of cure."

an ounce

Correlation Distillation Beats ECCs

THM Correlation distillation is provably more powerful than ECCs

$\exists$ noisy channel, s.t.

- No ECC can achieve a non-trivial rate.
- But Correlation Distillation Protocols can

Entanglement Distillation Beats QECCs

[Bennett, Di Vincenzo, Smolin, Wootters 1996]
Entanglement Distillation is provably more powerful than QECCs

$\exists$ noisy channel, s.t.

- No QECC can work
- But Entanglement Distillation Protocols can

~~"An ounce of prevention is worth a pound of cure."~~

"In a corrupted world, prevention is useless, yet there is cure."

Correlation Distillation has More Applications

Assumptions made by error correction —

Preventive encoding must precede the noise

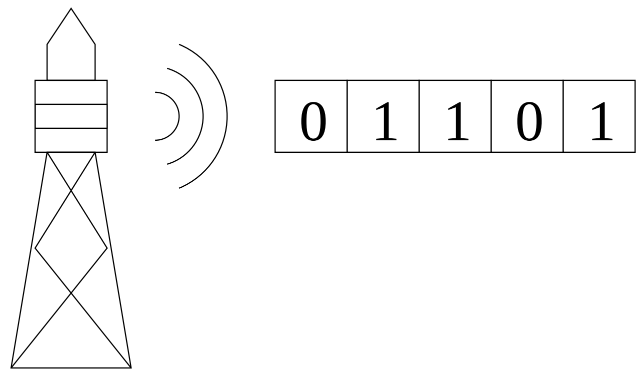
“What if encoding is impossible?”

Noise model identical independent noise, known noise rate

“What if the noise model is different?”

Have to guess an upper bound on noise rate

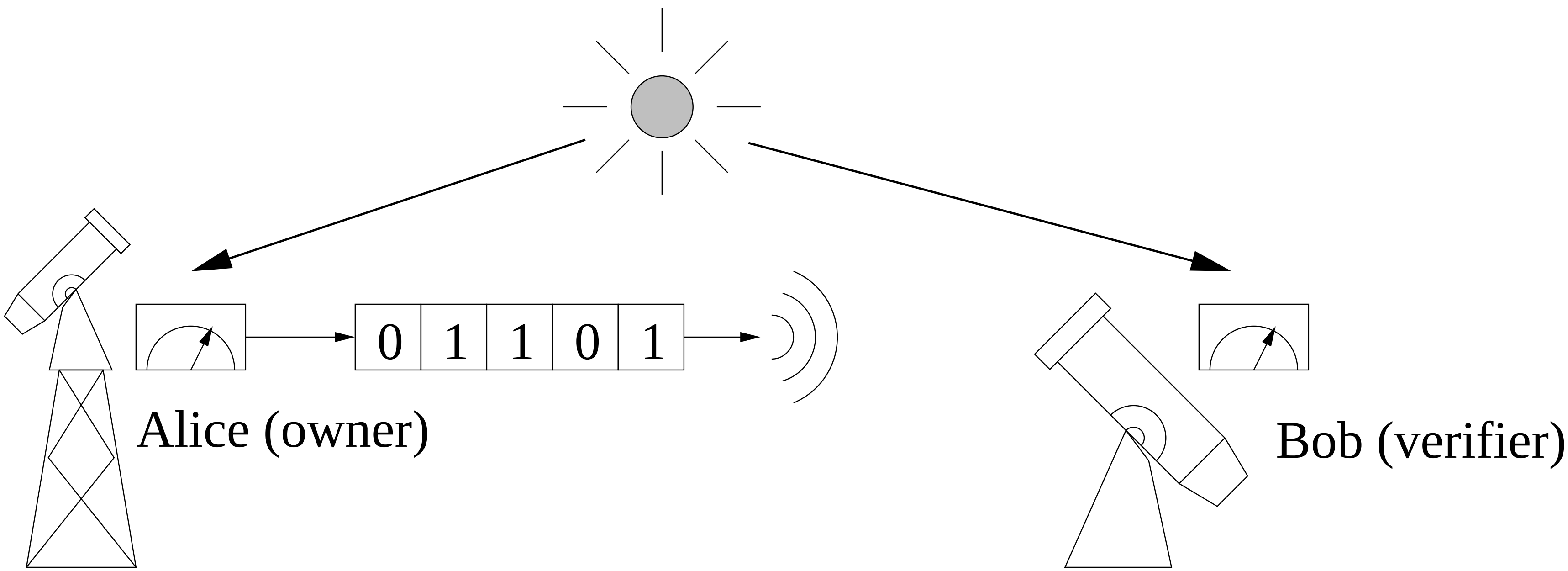
Random Beacon



A real-time, verifiable random source

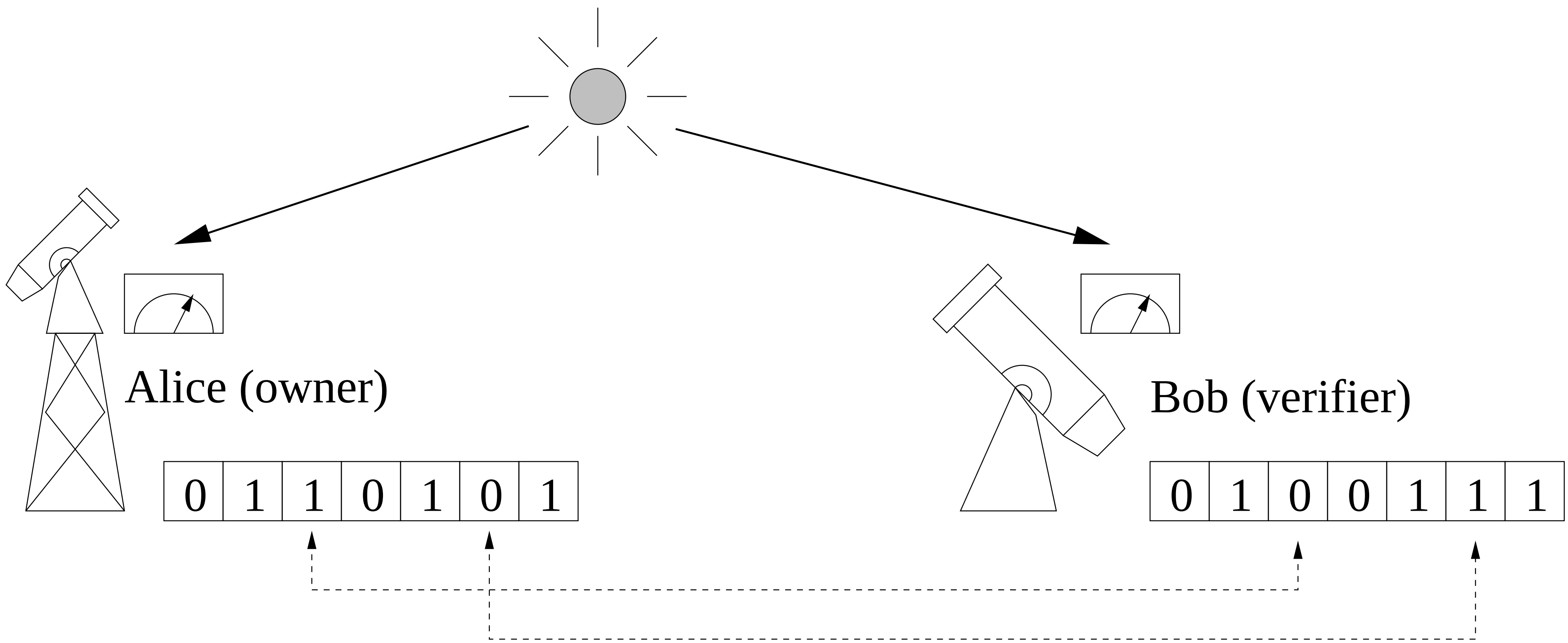
- verifiable lottery
- information-theoretically secure cryptography — key-exchange, encryption... (assuming bounded storage)

How to Build a Random Beacon



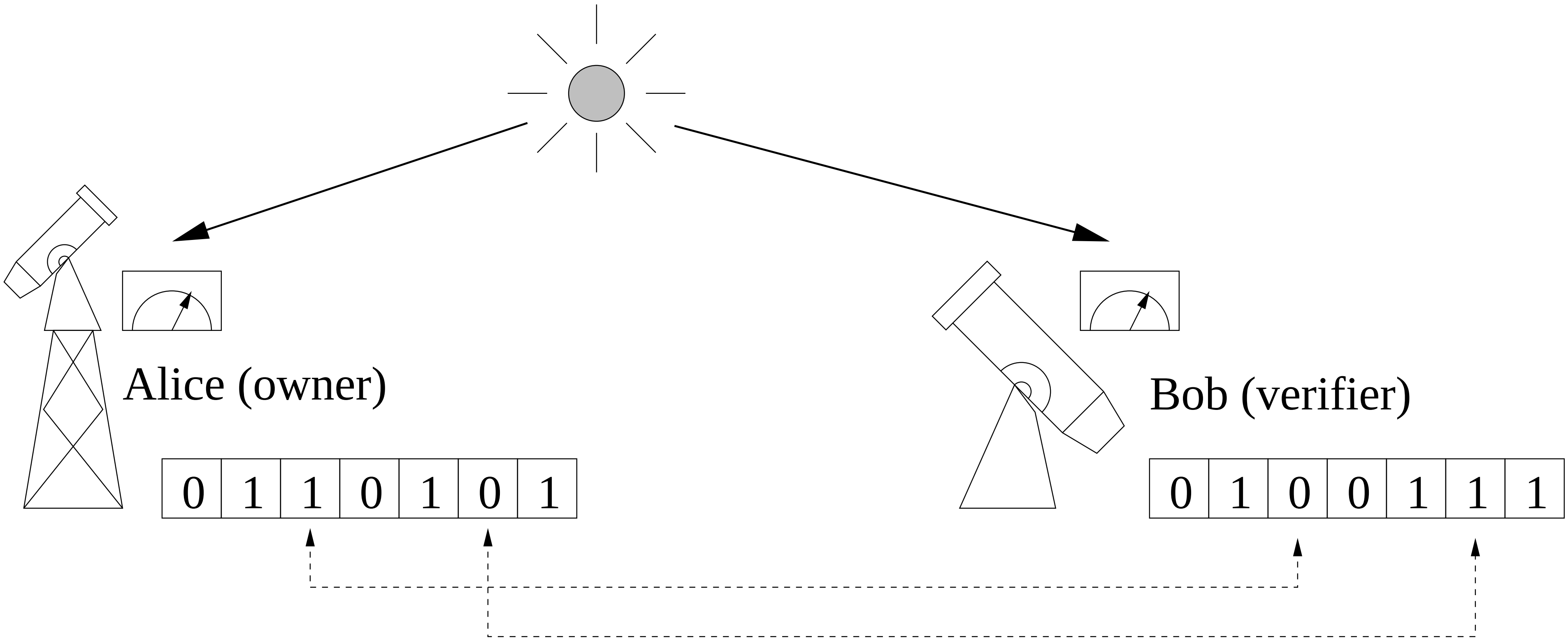
- Point a telescope to a pulsar
- Measure the signal, convert to random bits
- Real-time verifiable: (almost) everyone can see the pulsar

Noisy Measurement



Measurement errors — corrupted correlation

Correlation Recovery for Random Beacons

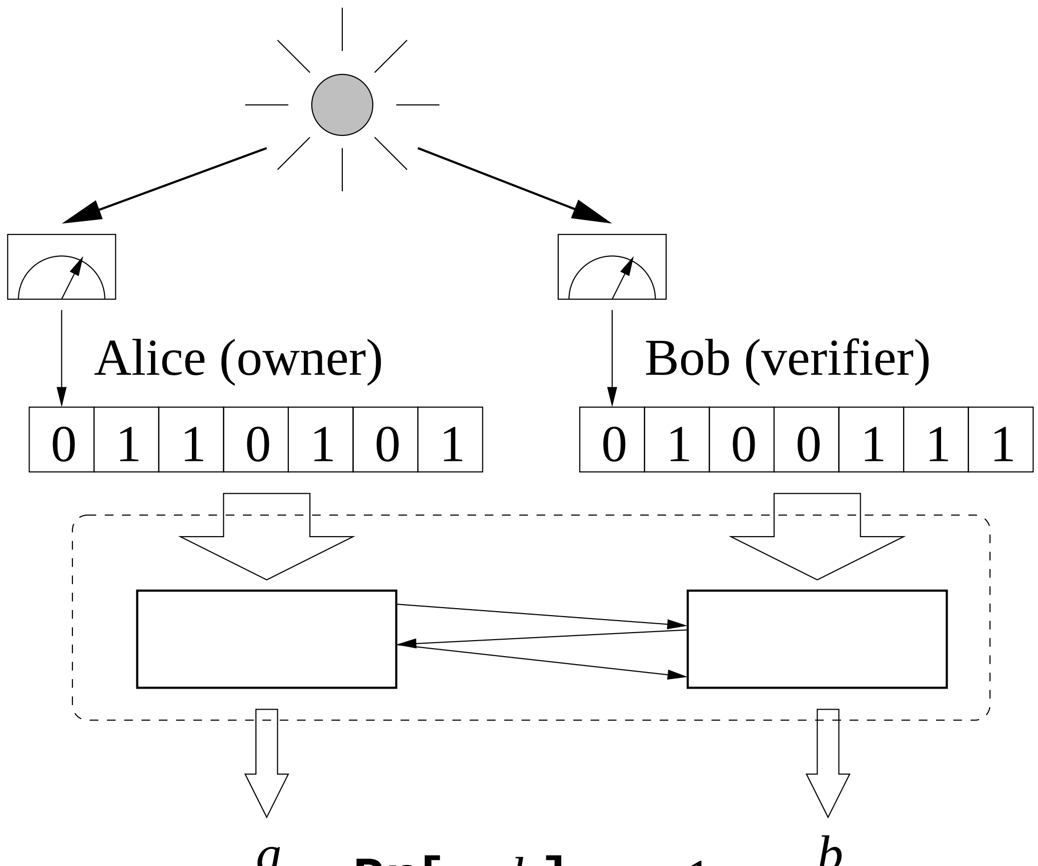


GOAL = to achieve (almost) perfect correlation

Error Correction on a Pulsar ?!

- Both Alice and Bob have corrupted information
- Preventive strategy doesn't work
- Okay to produce "fresh" random bits

Correlation Distillation for Random Beacon



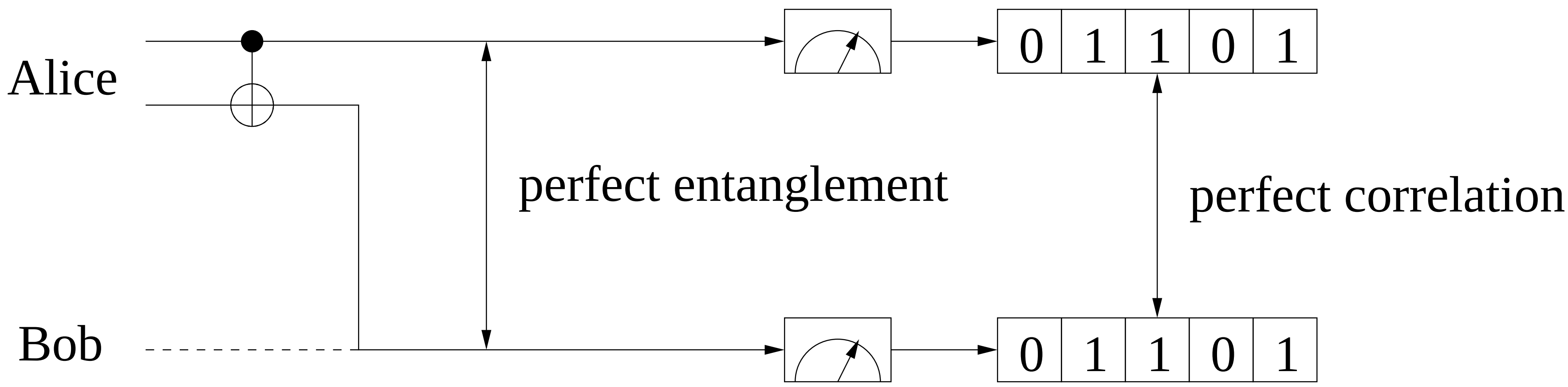
$\Pr[a=b] \longrightarrow 1$

Random Beacon: error correction doesn't apply

Storing EPR Pairs

- EPR pairs are useful quantum objects, but hard to store
- Constantly decaying — varying noise rate
- QECC has to guess an upper bound of noise rate

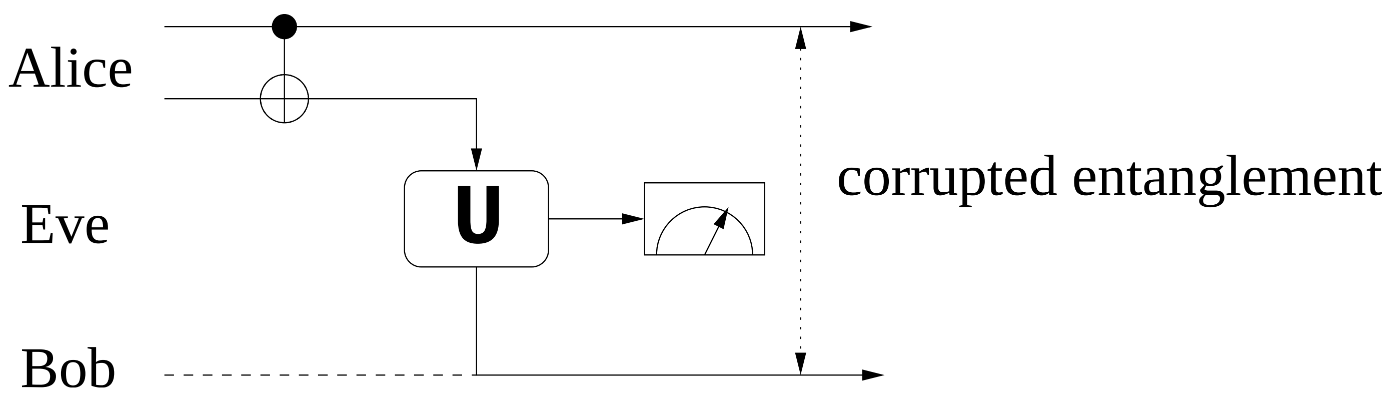
Quantum Key Distribution (Ideal)



[Bennett-Brassard 84, Bennett 92] (modified)

- Alice sends random qubits to Bob and keeps a copy herself
- (Ideally) perfectly entangled qubits
- Both measure $\Rightarrow$ (Ideally) perfectly correlated bits

Quantum Key Distribution (Real life)



- Eve intercepts some qubits and distorts them
- corrupted entanglement $\Rightarrow$ corrupted correlation

Error Correction for Eve?

QECC assumes identical independent noise

but...

Eve is adversarial

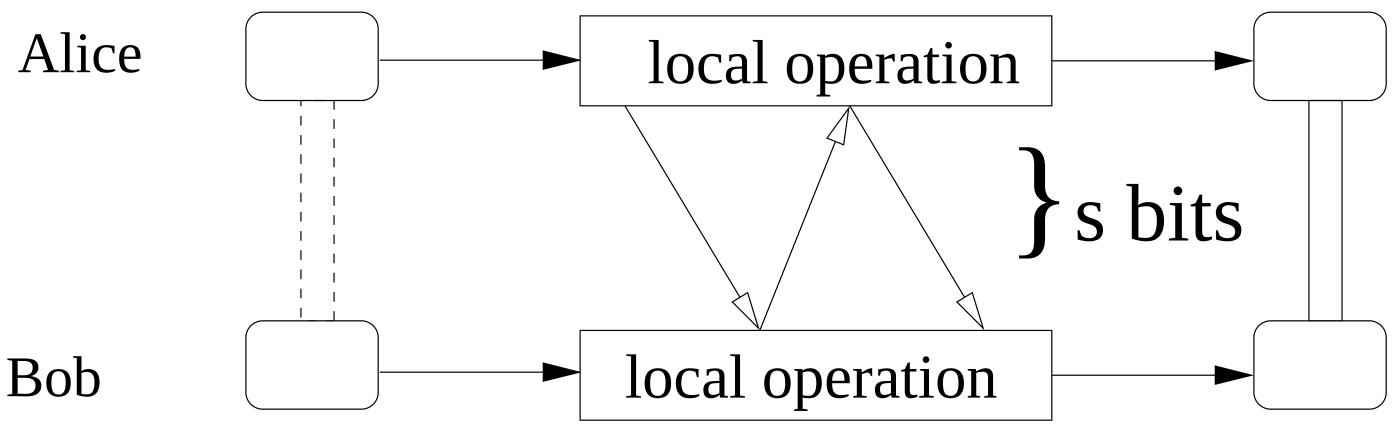
Quantum Key Distribution: error correction uses a different model

Why Reparative?

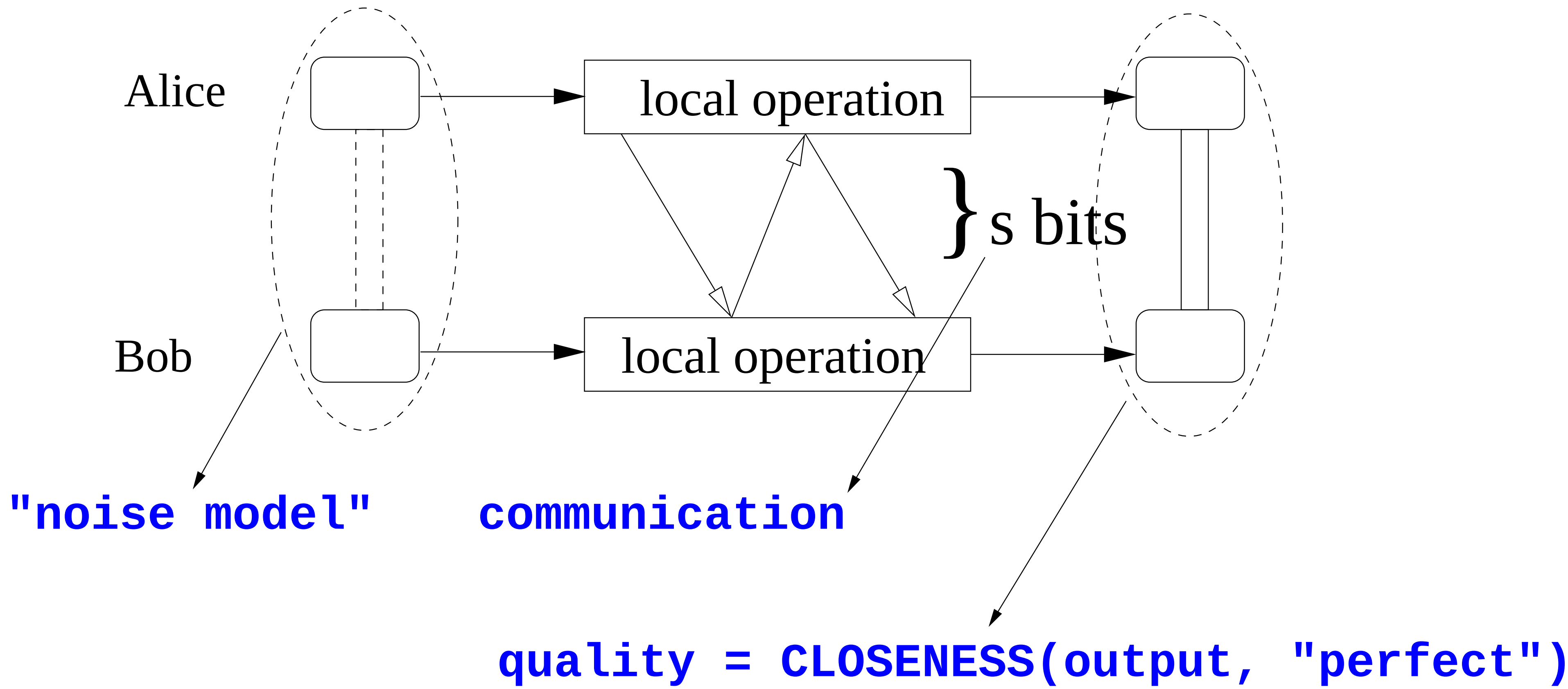
Scenario	Reason
Information Transmission	Correlation distillation is as efficient as error correction (and can be more useful)
Random Beacon	ECCs don't apply (can't error correct a pulsar)
Storing EPR pairs	QECCs are inefficient (varying noise rate)
Quantum Key Distribution	QECCs don't apply (different noise models)

What's known?

Quantifying Distillation Protocols



Fix Noise Model, Study Communication vs. Quality



communication

quality

noise model	0	1	many	
bounded corruption				classical
binary symmetric				
binary erasure				
tensor product				
bounded corruption				quantum
bounded measurement				
depolarization				
entanglement				
fidelity				

Type	noise model	communication: 0	communication: 1	communication: many
classical	bounded corruption			L
classical	binary symmetric	😐 U	☺ L	L
classical	binary erasure	☺ U		L
classical	tensor product	☺ U		
quantum	bounded corruption	☺ U		L
quantum	bounded measurement	☺ U		L
quantum	depolarization	☺ U		L
quantum	entanglement	😐 U	😐 U	😐 U
quantum	fidelity	☺ L U	☺ L U	☺ L U

- **L** = lower bound
- **U** = upper bound
- ☺ = my orignal result
- 😐 = independent result

Related Publications

[Ambainis, Smith, Yang 2002] "Extracting Quantum Entanglement (General Entanglement Purification Protocols)", *IEEE Conference on Computational Complexity 2002*.

[Yang 2004] "On the (Im)possibility of Non-interactive Correlation Distillation", *Latin American Theoretical INformatics (LATIN 2004)*.

[Ambainis, Yang 2004] "Towards the Classical Communication Complexity of Entanglement Distillation Protocols with Incomplete Information", *IEEE Conference of Computational Complexity (CCC 2004)*.

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result

communication

noise model	0	1	many	
bounded corruption			L	classical
binary symmetric	😐 U	☺ L	L	classical
binary erasure	☺ U		L	classical
tensor product	☺ U			classical
bounded corruption	☺ U		L	quantum
bounded measurement	☺ U		L	quantum
depolarization	☺ U		L	quantum
entanglement	😐 U	😐 U	😐 U	quantum
fidelity	☺ L U	☺ L U	☺ L U	quantum

linear ECC => perfect CDP

stablizer QECC => perfect EDP

- **L** = lower bound
- **U** = upper bound
- ☺ = my orignal result
- 😐 = independent result

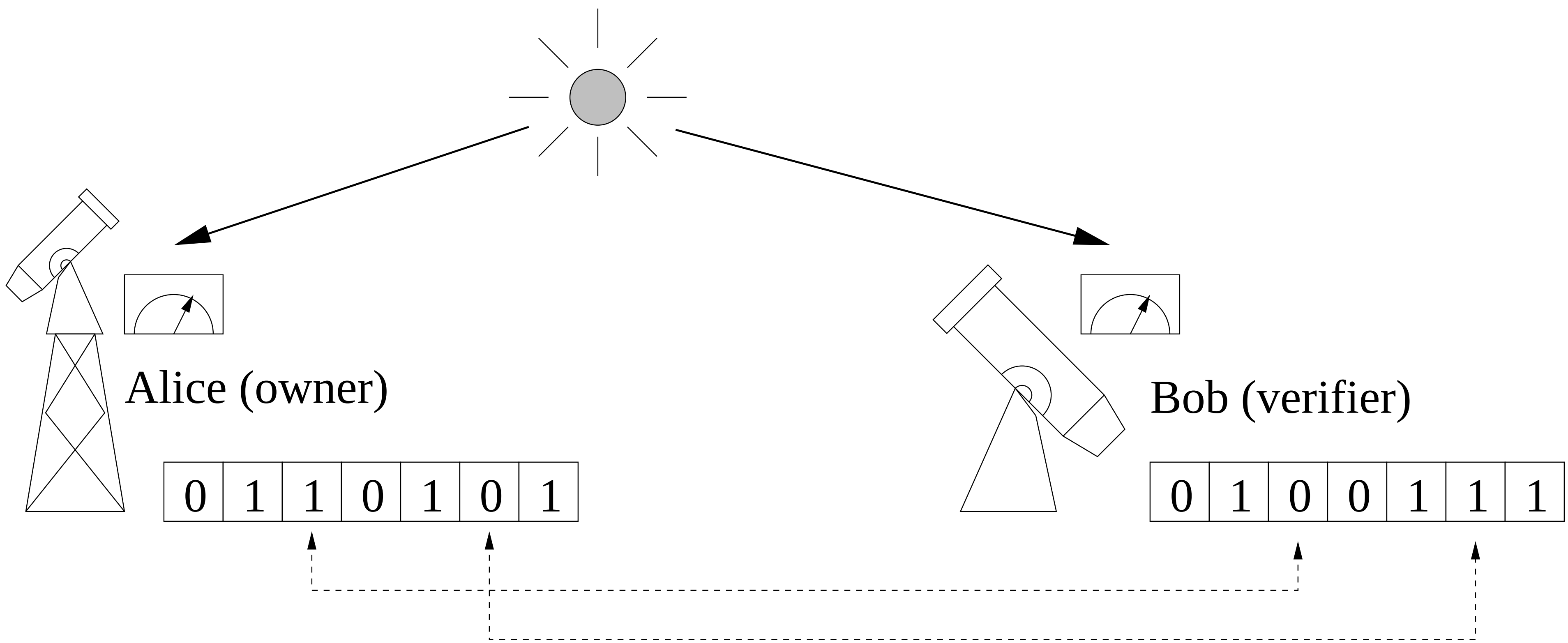
	noise model	communication: 0	1	many
classical	bounded corruption			L
	binary symmetric	😐 U	☺ L	L
	binary erasure	☺ U		L
	tensor product	☺ U		
quantum	bounded corruption	☺ U		L
	bounded measurement	☺ U		L
	depolarization	☺ U		L
	entanglement	😐 U	😐 U	😐 U
	fidelity	☺ L U	☺ L U	☺ L U

non−interactive correlation distillation

Non-interactive Correlation Distillation

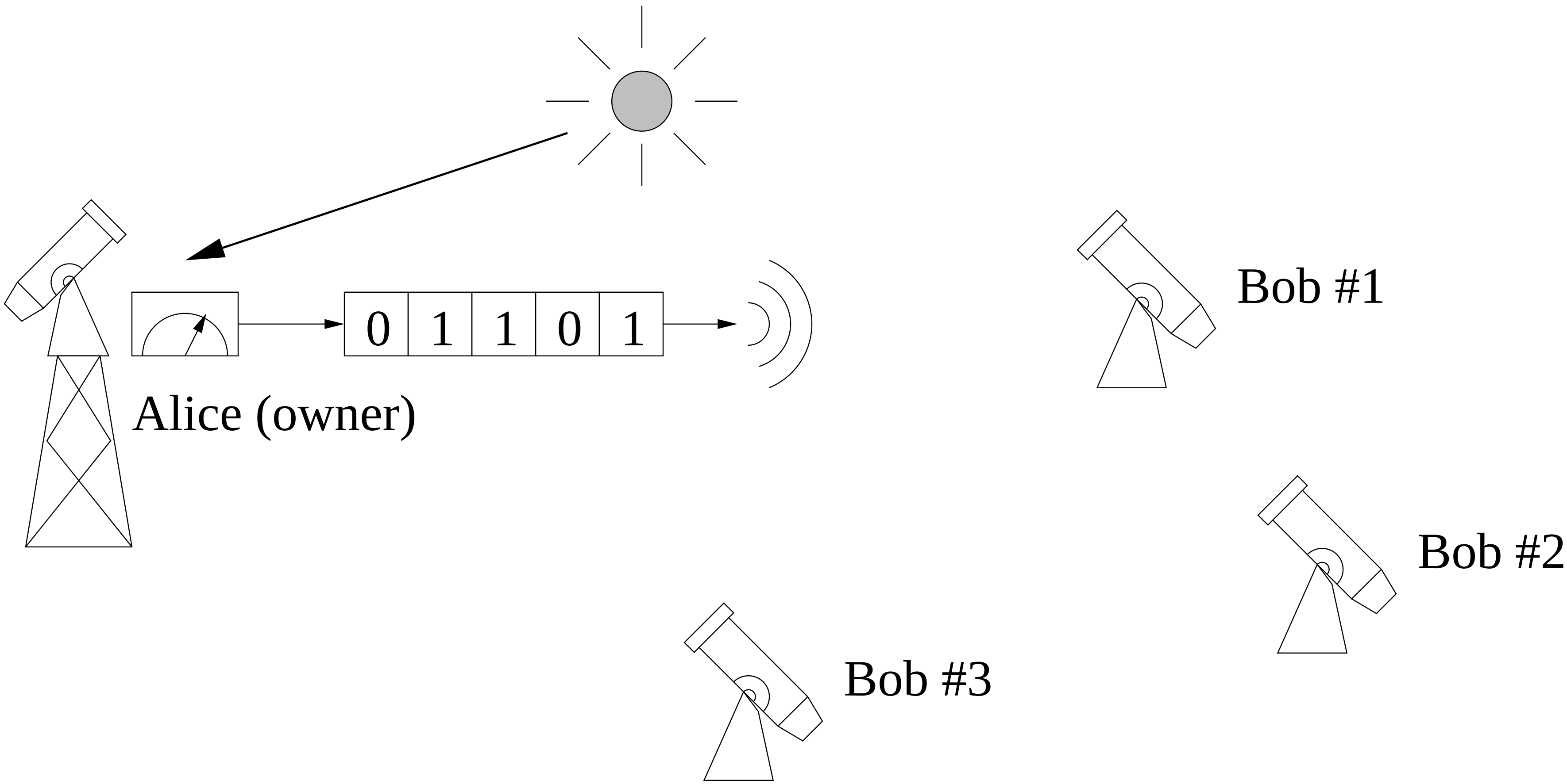
Alice and Bob distill correlation without communicating

Correlation Recovery for Random Beacons

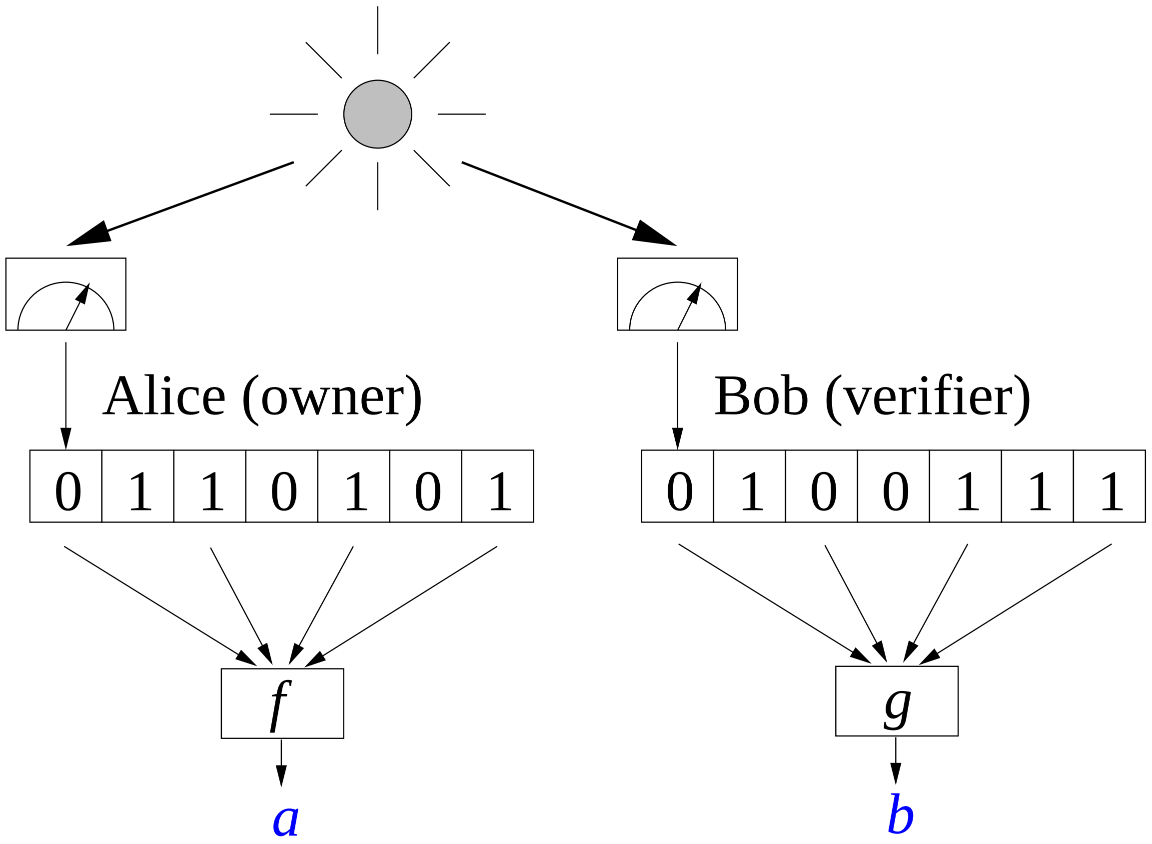


GOAL = to achieve (almost) perfect correlation

One Alice, Many Bobs



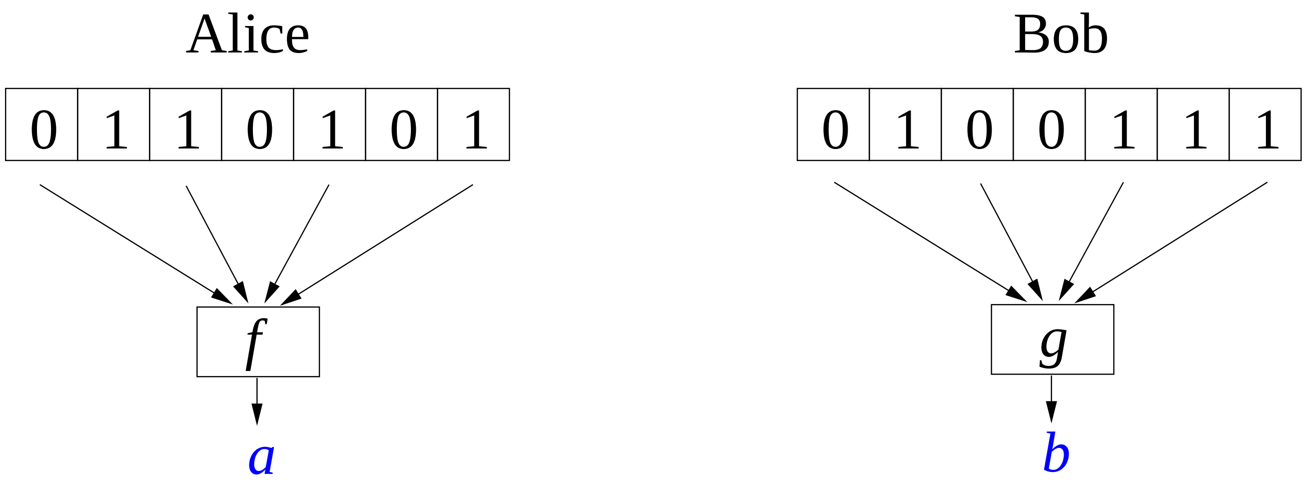
Non-Interactive Correlation Distillation for Random Beacon



Both a and b unbiased

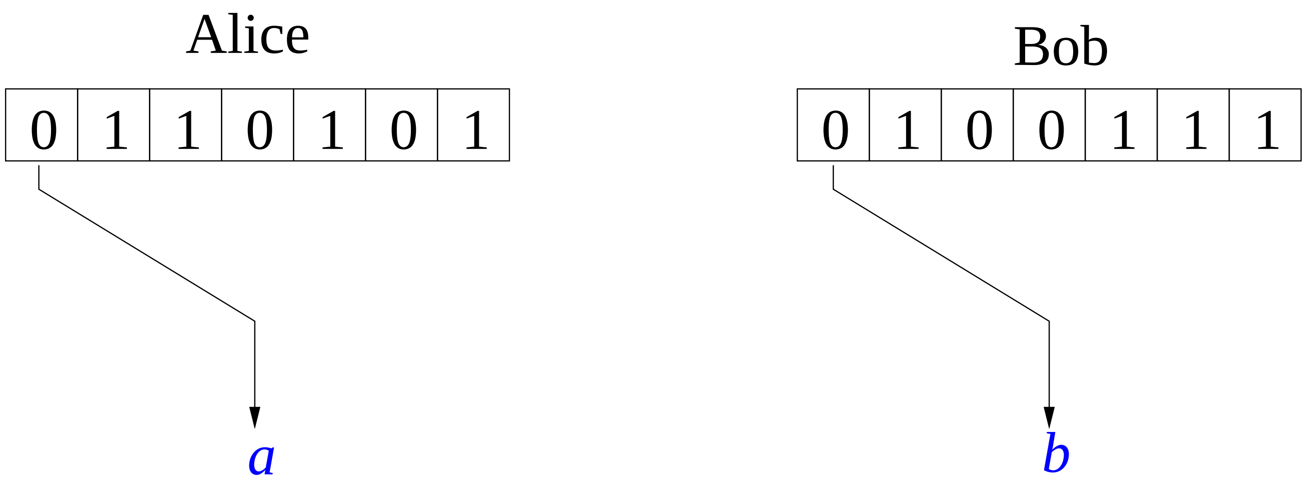
$\Pr[a = b] \longrightarrow 1$

Correlation Extraction, Mathematically



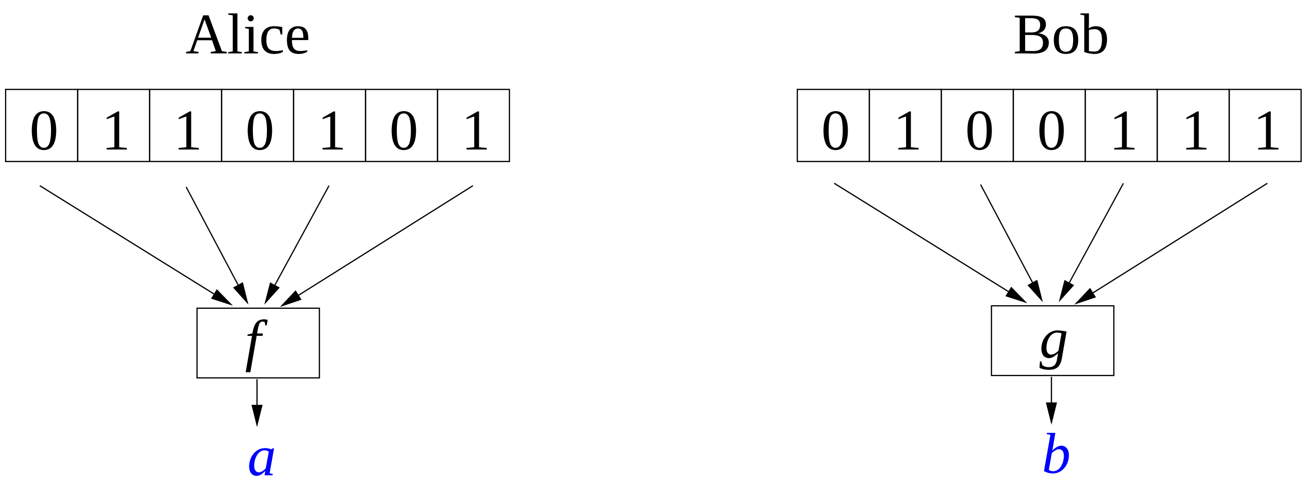
- Alice $x_1, x_2, ..., x_n$, Bob $y_1, y_2, ..., y_n$, s.t. $\Pr[x_k = y_k] = 1 - p$
- Alice $a = f(x_1, x_2, .., x_n)$; Bob $b = g(y_1, y_2, ..., y_n)$
- Unbiased bits $\Pr[a = 0] = 1/2$, $\Pr[b = 0] = 1/2$
- Maximize $\Pr[a = b]$

Naïve Strategy



- Both output the first bit
- $\Pr[a = b] = 1 - p$

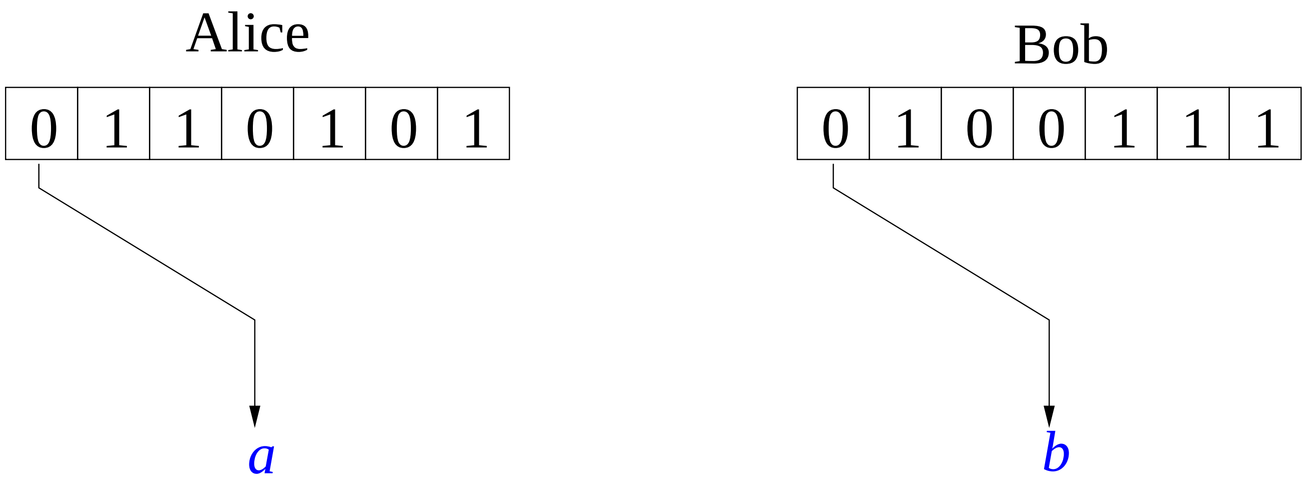
Can We do Better?



- Alice $x_1, x_2, ..., x_7$, Bob $y_1, y_2, ..., y_7$, $\Pr[x_k = y_k] = 0.9$
- Can $\Pr[a = b] \geq 0.91$?

(mutual information = 3.72)

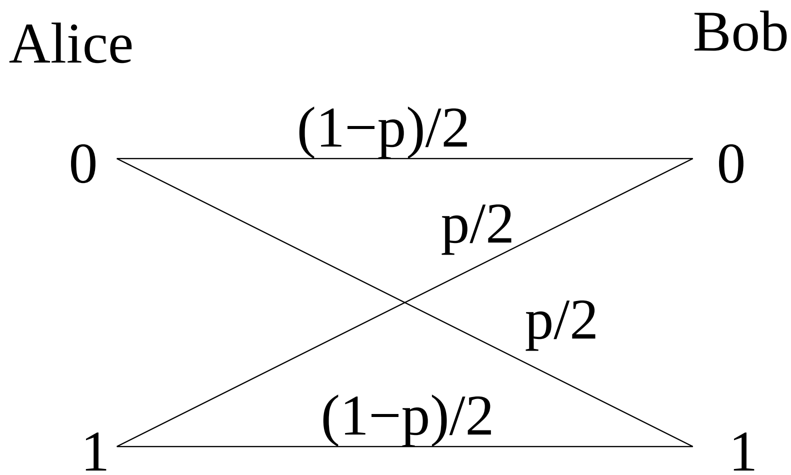
No



[Alon, Maurer, Wigderson], [Mossel, O'Donnell], [Yang 2004]

- The naïve strategy is optimal
- All optimal strategies are naïve

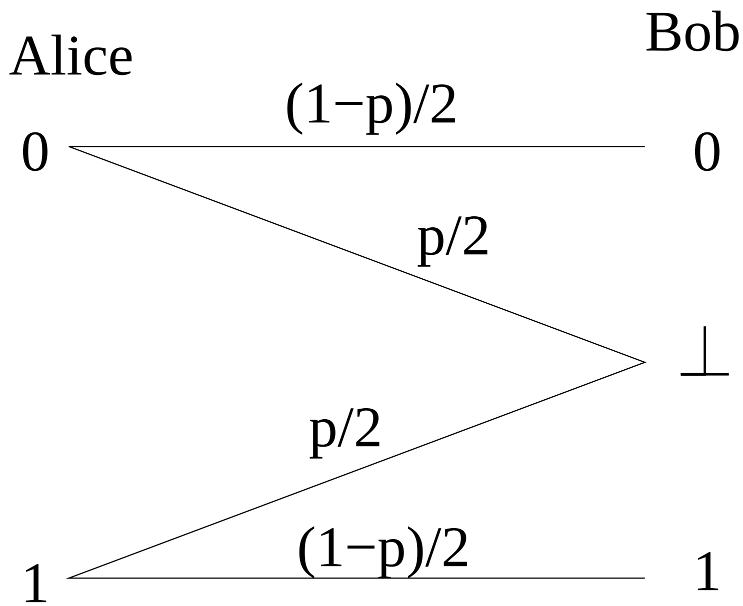
Binary Symmetric Model



[Yang 2004] generalization to Tensor Product Model

(large alphabet, more general noise)

Binary Erasure Model



[Yang 2004] The naïve strategy is asymptotically optimal

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result

communication

noise model	0	1	many	
bounded corruption			L	classical
binary symmetric	😐 U	☺ L	L	classical
binary erasure	☺ U		L	classical
tensor product	☺ U			classical
bounded corruption	☺ U		L	quantum
bounded measurement	☺ U		L	quantum
depolarization	☺ U		L	quantum
entanglement	😐 U	😐 U	😐 U	quantum
fidelity	☺ L U	☺ L U	☺ L U	quantum

non−interactive correlation distillation

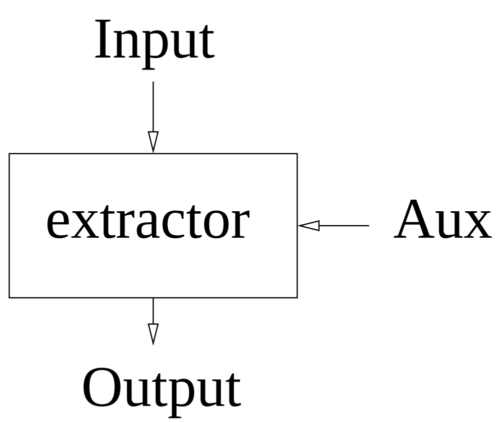
noise model		communication: 0	1	many
bounded corruption	classical			L
binary symmetric	classical	😐 U	☺ L	L
binary erasure	classical	☺ U		L
tensor product	classical	☺ U		
bounded corruption	quantum	☺ U		L
bounded measurement	quantum	☺ U		L
depolarization	quantum	☺ U		L
entanglement	quantum	😐 U	😐 U	😐 U
fidelity	quantum	☺ L U	☺ L U	☺ L U

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result

impossibility for general EPR extraction

Motivation: classical randomness extraction

Randomness Extractors



Input: random source

Aux: uniform random bits

Output: near−uniform random bits

produce near-uniform random bits from arbitrary random sources

Facts About Extractors

Very useful, works with very general input

- input = arbitrary random source.
- |output| $\longleftarrow$ min-entropy(input)
- |auxiliary input| = $\Theta(\log(|\text{input}|))$
- [Ta-Shma, Umans, Zuckerman 2001] Near-optimal constructions exist

“General Entanglement Distillation?”

classical	**quantum**
uniform bits randomness in purest form	EPR pairs entanglement in purest form
extractor low-quality randomness $\Downarrow$ high-quality randomness	entanglement distillation low-quality entanglement $\Downarrow$ high-quality entanglement
input arbitrary random bits	input arbitrary entangled state?

No

THM General entanglement distillation is impossible
(no protocol extracts EPR pairs from arbitrary entangled states)

Proof Sketch

classical unique distribution of max entropy

quantum infinitely many maximally entangled states

The 4 Bell states:

$$\begin{aligned}
\Phi^+ &= \frac{1}{\sqrt{2}}\left(|0\rangle^A|0\rangle^B + |1\rangle^A|1\rangle^B\right) \\
\Phi^- &= \frac{1}{\sqrt{2}}\left(|0\rangle^A|0\rangle^B - |1\rangle^A|1\rangle^B\right) \\
\Psi^+ &= \frac{1}{\sqrt{2}}\left(|0\rangle^A|1\rangle^B + |1\rangle^A|0\rangle^B\right) \\
\Psi^- &= \frac{1}{\sqrt{2}}\left(|0\rangle^A|1\rangle^B - |1\rangle^A|0\rangle^B\right)
\end{aligned}$$

Proof Sketch, cont'd

Suppose there exists such a protocol $\mathcal{P}$, s.t.,

$$\mathcal{P}(\Phi^+) \rightarrow \Phi^+,\ \mathcal{P}(\Phi^-) \rightarrow \Phi^+,\ \mathcal{P}(\Psi^+) \rightarrow \Phi^+,\ \mathcal{P}(\Psi^-) \rightarrow \Phi^+$$

Let ρ be a mixed state:

$$\rho = \frac{1}{4}\left(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\right)$$

We should also have:

$$\mathcal{P}(\rho) \rightarrow \Phi^+$$

Change of Basis

$$\rho = \frac{1}{4}\left(|\Phi^{+}\rangle\langle\Phi^{+}| + |\Phi^{-}\rangle\langle\Phi^{-}| + |\Psi^{+}\rangle\langle\Psi^{+}| + |\Psi^{-}\rangle\langle\Psi^{-}|\right)$$

By changing of basis:

$$\rho = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$$

ρ is disentangled $\Rightarrow$ impossible to produce EPR pairs $\Rightarrow\Leftarrow$

	noise model	communication: 0	1	many
classical	bounded corruption			L
classical	binary symmetric	😐 U	☺ L	L
classical	binary erasure	☺ U		L
classical	tensor product	☺ U		
quantum	bounded corruption	☺ U		L
quantum	bounded measurement	☺ U		L
quantum	depolarization	☺ U		L
quantum	entanglement	😐 U	😐 U	😐 U
quantum	fidelity	☺ L U	☺ L U	☺ L U

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result

impossibility for general EPR extraction

Why General Entanglement Extraction Fails?

- No protocol can do well on average
- Useful protocol only if input is “close” to some state

The Fidelity Noise Model

[Ambainis, Smith, Yang 2002]

$$\text{fidelity(input, ``perfect'')} \geq 1 - \epsilon$$

[Lo, Chau 1999], [Shor, Preskill 2000]
used it in proof of security of [BB84] key distribution protocol

communication

noise model	0	1	many	
bounded corruption			L	classical
binary symmetric	😐 U	☺ L	L	classical
binary erasure	☺ U		L	classical
tensor product	☺ U			classical
bounded corruption	☺ U		L	quantum
bounded measurement	☺ U		L	quantum
depolarization	☺ U		L	quantum
entanglement	😐 U	😐 U	😐 U	quantum
fidelity	☺ L U	☺ L U	☺ L U	quantum

matching lower/upper bounds

L = lower bound

U = upper bound

☺ = my orignal result

😐 = independent result

Lower Bound: a Construction

[Ambainis, Smith, Yang 2002]

$\forall\, n, s,\ \exists\ s$-bit protocol, on n qubit pairs of fidelity $1-\epsilon$, either:

- fails with probability ϵ (nothing is output), or
- outputs $(n-s)$ pairs of qubits of fidelity $1-\frac{2^{-s}}{(1-\epsilon)}$

(output fidelity = output quality)

+ Can increase the fidelity as close to 1 as possible, sacrificing logarithmic number of qubit pairs and using logarithmic bit of communication

− Fails with probability ϵ.

Failure is Unavoidable

[Ambainis, Smith, Yang 2002]
$\exists$ n qubit pairs in state ρ of fidelity $1-\epsilon$, s.t. any protocol taking ρ as input and outputting m qubit pairs, has average fidelity at most $1-\frac{1-2^{-m}}{1-2^{-n}}\epsilon \approx 1-\epsilon$.

Cannot increase the overall fidelity

Optimality of Our Construction

[Ambainis, Smith, Yang 2002]

$\forall\, n, s,\ \exists\ s$-bit protocol, on n qubit pairs of fidelity $1 - \epsilon$, either:

- fails with probability ϵ (nothing is output), or
- outputs $(n - s)$ pairs of qubits of fidelity $1 - \frac{2^{-s}}{(1-\epsilon)}$

Optimal...

- Failure Probability — Must fail with probability ϵ in order to achieve close-to-one "lucky fidelity"
- Yield — $(n - s)$ qubit pairs, asymptotically optimal

More Optimality

[Ambainis, Smith, Yang 2002]

$\forall\, n, s,\ \exists\ s$-bit protocol, on n qubit pairs of fidelity $1-\epsilon$, either:

- fails with probability ϵ (nothing is output), or
- outputs $(n-s)$ pairs of qubits of fidelity $1-\frac{2^{-s}}{(1-\epsilon)}$

[Ambainis, Yang 2004] ♡

Communication complexity optimal up to an additive constant

A Bit More Technically...

Analysis of general two-party protocols prior to [Ambainis, Yang 2004]

[Nielsen 1999] "Simulation-based Reduction"

- For pure state input, Alice can "simulate" Bob's actions
- Arbitrary protocol $\rightarrow$ single-message protocol

(Alice measures; Alice sends message to Bob; Bob measures)

Simulation-based Reduction

"reducing any protocol to a single-message protocols"

- Does not work for protocols with mixed states as input
- [Bennett, Di Vincenzo, Smolin, Wootters 1996]
  Two-way protocols more powerful than one-way protocols
- Reduction doesn't work!
- Other techniques do not seem to work with mixed states either (e.g [Hayden, Winter 2002])

Our Contribution

[Ambainis, Yang 2004]

Novel technique for mixed states and two-way protocols

- Keep track of the local density matrices of Alice and Bob
- Communication causes a density matrix to “split”
- Maintain an invariant with communication history

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result

communication

noise model	**0**	**1**	**many**	
bounded corruption			L	**classical**
binary symmetric	😐 U	☺ L	L	
binary erasure	☺ U		L	
tensor product	☺ U			
bounded corruption	☺ U		L	**quantum**
bounded measurement	☺ U		L	
depolarization	☺ U		L	
entanglement	😐 U	😐 U	😐 U	
fidelity	☺ L U	☺ L U	☺ L U	

matching lower/upper bounds

communication

noise model	0	1	many	
bounded corruption			L	classical
binary symmetric	😐 U	☺ L	L	classical
binary erasure	☺ U		L	classical
tensor product	☺ U			classical
bounded corruption	☺ U		L	quantum
bounded measurement	☺ U		L	quantum
depolarization	☺ U		L	quantum
entanglement	😐 U	😐 U	😐 U	quantum
fidelity	☺ L U	☺ L U	☺ L U	quantum

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result

One−bit protocol provably better than non−interactive protocols

non−interactive entanglement distillation

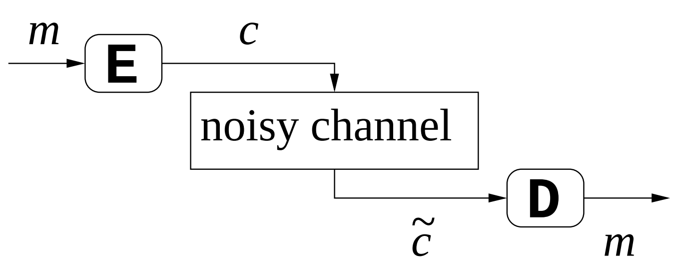
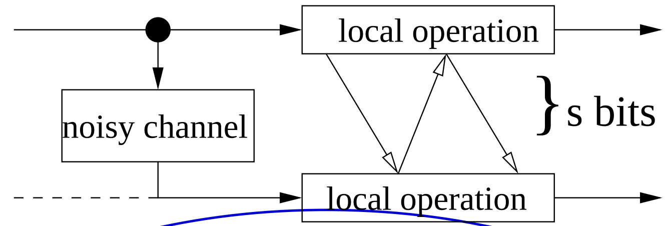
Summary

- Reparative: Correlation/Entanglement Distillation Protocols
- CDP/EDPs as efficient and ECC/QECC, maybe more
- Wider applications
- Results:
  - Impossibility of NICD/NIED
  - Impossibility of general EPR extraction
  - Optimal protocl for fidelity model
  - One-bit protocol for binary symmetric model

Thanks!

Questions?

What's next?

	preventive 	**reparative** 
classical	Error Correcting Code	Correlation Distillation Protocol
quantum	Quantum Error Correcting Code	Entanglement Distillation Protocol
overhead	$\|c\| - \|m\|$	s
status	well−studied, well−understood	less studied, fewer results

My thesis

L	=	lower bound
U	=	upper bound
☺	=	my orignal result
😐	=	independent result

		communication		
	noise model	**0**	**1**	**many**
classical	bounded corruption			L
	binary symmetric	😐 U	☺ L	L
	binary erasure	☺ U		L
	tensor product	☺ U		
quantum	bounded corruption	☺ U		L
	bounded measurement	☺ U		L
	depolarization	☺ U		L
	entanglement	😐 U	😐 U	😐 U
	fidelity	☺ L U	☺ L U	☺ L U

	noise model	communication: 0	1	many
classical	bounded corruption			L
classical	binary symmetric	😐 U	☺ L	L
classical	binary erasure	☺ U		L
classical	tensor product	☺ U		
quantum	bounded corruption	☺ U		L
quantum	bounded measurement	☺ U		L
quantum	depolarization	☺ U		L
quantum	entanglement	😐 U	😐 U	😐 U
quantum	fidelity	☺ L U	☺ L U	☺ L U

L = lower bound
U = upper bound
☺ = my orignal result
😐 = independent result
empty = unknown result

optimality?

communication−qualiity tradeoff?

Big Questions

- Optimality of constructions

  "Linear ECC $\Rightarrow$ CDP, Stabilizer QECC $\Rightarrow$ EDP, are they optimal?"

- More Trade-off on interactive correlation distillation

  "What's the optimal quality Alice and Bob can get with s bits of communication?"

- Unified results

  "Are there noise models more general than, say, the fidelity model?"

  "Can we merge the results to make the table smaller?"

More Immediate Questions: one-bit Protocols

- Can we upper bound the quality of one-bit CDP/EDPs?
- Is the protocol with the binary symmetric model optimal?

Time-line

[2003/3 — 2004/3] Continue research

[2004/4 — 2004/9] Write thesis