Fundamental Finite Key Limits for Information Reconciliation in Quantum Key Distribution

arXiv:1401.5194

Marco Tomamichel [1] Jesús Martínez-Mateo [2] Christoph Pacher [3]
David Elkouss [4]

[1]Centre for Quantum Technologies, National University of Singapore
School of Physics, The University of Sydney

[2]Universidad Politécnica de Madrid

[3]Safety & Security Department, AIT Austrian Institute of Technology

[4]Universidad Complutense de Madrid

Outline

Outline

Quantum Key Distribution (QKD)

- Cryptographic primitive for key agreement
- Two honest parties: Alice and Bob; dishonest party (eavesdropper): Eve.
- Achievement: Alice and Bob create an information-theoretic secure (composable) key.

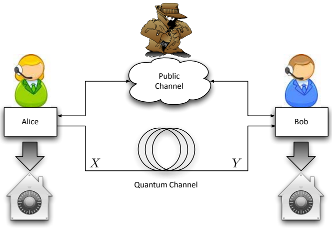
Quantum Key Distribution (QKD)

- Cryptographic primitive for key agreement
- Two honest parties: Alice and Bob; dishonest party (eavesdropper): Eve.
- Achievement: Alice and Bob create an information-theoretic secure (composable) key.

Information-theoretic security (informally)

The success probability of any (active or passive) attack is upper bounded by a (tiny) constant, regardless of the (quantum) computing resources used by the attacker.

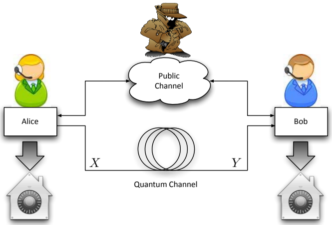
QKD protocol steps



Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

QKD protocol steps

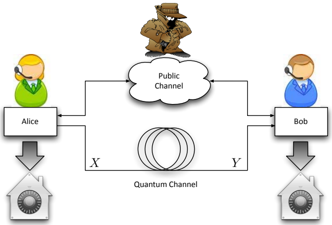


Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

1. quantum phase (A prepares N quantum systems, transmits, and B measures)

QKD protocol steps

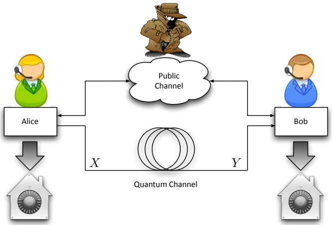


Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

1. quantum phase (A prepares N quantum systems, transmits, and B measures)
2. parameter estimation (A and B estimate correlation between X and Y)

QKD protocol steps

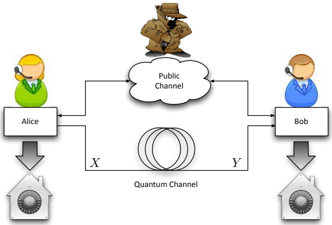


Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

1. quantum phase (A prepares N quantum systems, transmits, and B measures)
2. parameter estimation (A and B estimate correlation between X and Y)
3. sifting (A and B remove uncorrelated systems, produce raw keys of length n),

QKD protocol steps

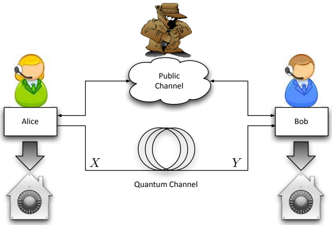


Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

1. quantum phase (A prepares N quantum systems, transmits, and B measures)
2. parameter estimation (A and B estimate correlation between X and Y)
3. sifting (A and B remove uncorrelated systems, produce raw keys of length n),
4. **information reconciliation** (exchanging messages on the classical channel Bob estimates Alice's raw key),

QKD protocol steps

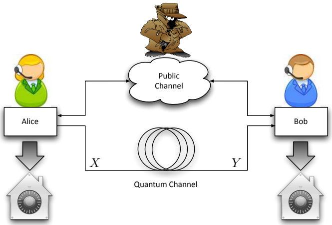


Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

1. quantum phase (A prepares N quantum systems, transmits, and B measures)
2. parameter estimation (A and B estimate correlation between X and Y)
3. sifting (A and B remove uncorrelated systems, produce raw keys of length n),
4. **information reconciliation** (exchanging messages on the classical channel Bob estimates Alice's raw key),
5. privacy amplification

QKD protocol steps



Prerequisites:

- Authentic classical channel (Eve can listen)
- Quantum channel (Eve introduces noise while listening)

1. quantum phase (A prepares N quantum systems, transmits, and B measures)
2. parameter estimation (A and B estimate correlation between X and Y)
3. sifting (A and B remove uncorrelated systems, produce raw keys of length n),
4. **information reconciliation** (exchanging messages on the classical channel Bob estimates Alice's raw key),
5. privacy amplification (ensures secrecy).

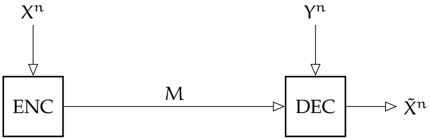
Outline

One Way Information Reconciliation

- Alice and Bob hold raw keys X^n, Y^n distributed according to $(P_{XY})^{\times n}$.

One Way Information Reconciliation

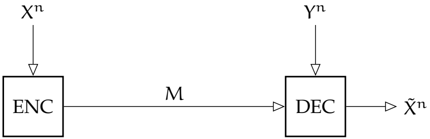
- Alice and Bob hold raw keys X^n, Y^n distributed according to $(P_{XY})^{\times n}$.



- Alice first computes a compressed version $M \in \mathcal{M}$ of her raw key X^n, and sends it to Bob (leakage to Eve).

One Way Information Reconciliation

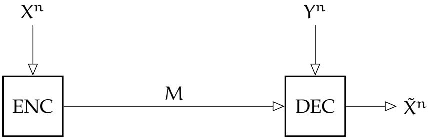
- Alice and Bob hold raw keys X^n, Y^n distributed according to $(P_{XY})^{\times n}$.



- Alice first computes a compressed version $M \in \mathcal{M}$ of her raw key X^n, and sends it to Bob (leakage to Eve).
- Bob uses M together with his own raw key Y^n to construct an estimate $\tilde{X}^n$ of X^n.

One Way Information Reconciliation

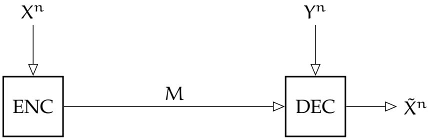
- Alice and Bob hold raw keys X^n, Y^n distributed according to $(P_{XY})^{\times n}$.



- Alice first computes a compressed version $M \in \mathcal{M}$ of her raw key X^n, and sends it to Bob (leakage to Eve).
- Bob uses M together with his own raw key Y^n to construct an estimate $\tilde{X}^n$ of X^n.
- One Way IR = Source Coding with Side Information

One Way Information Reconciliation

- Alice and Bob hold raw keys X^n, Y^n distributed according to $(P_{XY})^{\times n}$.



- Alice first computes a compressed version $M \in \mathcal{M}$ of her raw key X^n, and sends it to Bob (leakage to Eve).
- Bob uses M together with his own raw key Y^n to construct an estimate $\tilde{X}^n$ of X^n.
- One Way IR = Source Coding with Side Information
- Asymptotic limit it is sufficient to send $nH(X|Y)$ bits

Outline

Motivation for finite-length studies in QKD

- The secret key length ℓ of a QKD protocol is reduced by leak_{IR}, the amount of information leaked to an eavesdropper during IR.

Motivation for finite-length studies in QKD

- The secret key length ℓ of a QKD protocol is reduced by leak$_{IR}$, the amount of information leaked to an eavesdropper during IR.
- Since leak$_{IR}$ is hard to determine, the length of the IR messages $\log|\mathcal{M}|$ is often used as a bound

$$\text{leak}_{IR} \leq \log|\mathcal{M}|.$$

Motivation for finite-length studies in QKD

- The secret key length ℓ of a QKD protocol is reduced by leak_{IR}, the amount of information leaked to an eavesdropper during IR.
- Since leak_{IR} is hard to determine, the length of the IR messages $\log |\mathcal{M}|$ is often used as a bound

$$\text{leak}_{IR} \leq \log |\mathcal{M}|.$$

- Motivated by the asymptotic limit, the amount of information that is required to perform one-way IR is usually written as

$$\log |\mathcal{M}| = \xi \cdot nH(X|Y)_P,$$

where $\xi > 1$ is the reconciliation (in)efficiency.

Motivation for finite-length studies in QKD

- The secret key length ℓ of a QKD protocol is reduced by leak_{IR}, the amount of information leaked to an eavesdropper during IR.
- Since leak_{IR} is hard to determine, the length of the IR messages $\log|\mathcal{M}|$ is often used as a bound

$$\text{leak}_{IR} \leq \log|\mathcal{M}|.$$

- Motivated by the asymptotic limit, the amount of information that is required to perform one-way IR is usually written as

$$\log|\mathcal{M}| = \xi \cdot nH(X|Y)_P,$$

  where $\xi > 1$ is the reconciliation (in)efficiency.
- In the literature on QKD it is often assumed that $\xi \in [1.05, 1.20]$ for all scenarios.

Motivation for finite-length studies in QKD

- The secret key length ℓ of a QKD protocol is reduced by leak_{IR}, the amount of information leaked to an eavesdropper during IR.
- Since leak_{IR} is hard to determine, the length of the IR messages $\log|\mathcal{M}|$ is often used as a bound

$$\text{leak}_{IR} \leq \log|\mathcal{M}|.$$

- Motivated by the asymptotic limit, the amount of information that is required to perform one-way IR is usually written as

$$\log|\mathcal{M}| = \xi \cdot nH(X|Y)_P,$$

  where $\xi > 1$ is the reconciliation (in)efficiency.
- In the literature on QKD it is often assumed that $\xi \in [1.05, 1.20]$ for all scenarios.
- However, this choice should depend on the distribution P_{XY}, the frame length n, and the frame error rate ε.

Motivation for finite-length studies in QKD

- The secret key length ℓ of a QKD protocol is reduced by leak_{IR}, the amount of information leaked to an eavesdropper during IR.
- Since leak_{IR} is hard to determine, the length of the IR messages $\log|\mathcal{M}|$ is often used as a bound

$$\text{leak}_{IR} \leq \log|\mathcal{M}|.$$

- Motivated by the asymptotic limit, the amount of information that is required to perform one-way IR is usually written as

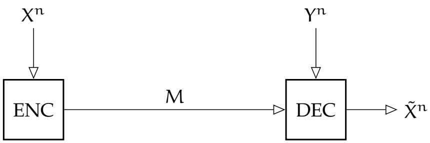
$$\log|\mathcal{M}| = \xi \cdot nH(X|Y)_P,$$

  where $\xi > 1$ is the reconciliation (in)efficiency.
- In the literature on QKD it is often assumed that $\xi \in [1.05, 1.20]$ for all scenarios.
- However, this choice should depend on the distribution P_{XY}, the frame length n, and the frame error rate ε.
- What are the fundamental / practical limits of $\log|\mathcal{M}|$ as a function of P_{XY}, n, and ε?

Outline

State of the art of $\log|\mathcal{M}|$

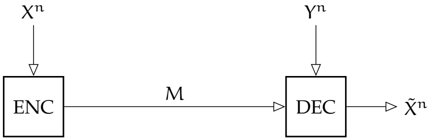
IR / Source coding with side information



Bounds on the asymptotic expansion up to second order (Hayashi 2008 and Tan and Kosut 2012)

State of the art of $\log|\mathcal{M}|$

IR / Source coding with side information

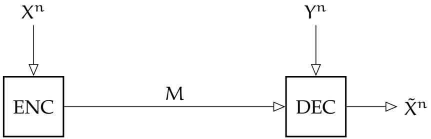


Bounds on the asymptotic expansion up to second order (Hayashi 2008 and Tan and Kosut 2012)

This work

State of the art of log $|\mathcal{M}|$

IR / Source coding with side information



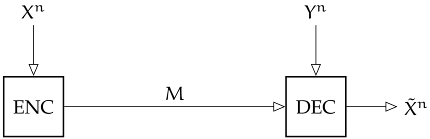
Bounds on the asymptotic expansion up to second order (Hayashi 2008 and Tan and Kosut 2012)

This work

1. For an arbitrary $(P_{XY})^{\times n}$ we provide the asymptotic expansion up to third order for the converse bound

State of the art of log $|\mathcal{M}|$

IR / Source coding with side information



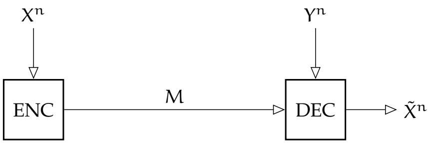
Bounds on the asymptotic expansion up to second order (Hayashi 2008 and Tan and Kosut 2012)

This work

1. For an arbitrary $(P_{XY})^{\times n}$ we provide the asymptotic expansion up to third order for the converse bound
2. For a special case we provide a non-asymptotic converse bound

State of the art of log $|\mathcal{M}|$

IR / Source coding with side information



Bounds on the asymptotic expansion up to second order (Hayashi 2008 and Tan and Kosut 2012)

This work

1. For an arbitrary $(P_{XY})^{\times n}$ we provide the asymptotic expansion up to third order for the converse bound
2. For a special case we provide a non-asymptotic converse bound
3. We compare these bounds to implementations of one-way IR using low-density parity-check codes.

Fundamental Limits For Information Reconciliation

Definition

An IR protocol is ε-correct on P_{XY} if

$$Pr[X^n \neq \tilde{X}^n] \leq \varepsilon.$$

Fundamental Limits For Information Reconciliation

Definition

An IR protocol is ε-correct on P_{XY} if

$$Pr[X^n \neq \tilde{X}^n] \leq \varepsilon.$$

Theorem (Converse bound (Normal approximation))

Let $0 < \varepsilon < 1$. Then, for large n, any ε-correct IR protocol on P_{XY} satisfies

$$\log|\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,,$$

Fundamental Limits For Information Reconciliation

Definition

An IR protocol is ε-correct on P_{XY} if

$$Pr[X^n \neq \tilde{X}^n] \leq \varepsilon.$$

Theorem (Converse bound (Normal approximation))

Let $0 < \varepsilon < 1$. Then, for large n, any ε-correct IR protocol on P_{XY} satisfies

$$\log|\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,,$$

where $H(X|Y) := \mathrm{Exp}\left[\log \frac{P_Y}{P_{XY}}\right]$ is the conditional entropy, $V(X|Y) := \mathrm{Var}\left[\log \frac{P_Y}{P_{XY}}\right]$ is the conditional entropy variance, and Φ is the cumulative standard normal distribution.

Special Case: Quantum Bit Error Rate Q

P^Q_{XY} results from measurements on a channel with (independent) qber Q:

$$P^Q_X(0) = P^Q_X(1) = P^Q_Y(0) = P^Q_Y(1) = 1/2,$$
$$P^Q_{XY}(0,0) = P^Q_{XY}(1,1) = (1-Q)/2,$$
$$P^Q_{XY}(0,1) = P^Q_{XY}(1,0) = Q/2.$$

Special Case: Quantum Bit Error Rate Q

P^Q_{XY} results from measurements on a channel with (independent) qber Q:

$$P^Q_X(0) = P^Q_X(1) = P^Q_Y(0) = P^Q_Y(1) = 1/2,$$
$$P^Q_{XY}(0,0) = P^Q_{XY}(1,1) = (1-Q)/2,$$
$$P^Q_{XY}(0,1) = P^Q_{XY}(1,0) = Q/2.$$

Definition

An IR protocol is (ε, Q)-correct if it is ε-correct on P^Q_{XY}.

Special Case: Quantum Bit Error Rate Q

P^Q_{XY} results from measurements on a channel with (independent) qber Q:

$$P^Q_X(0) = P^Q_X(1) = P^Q_Y(0) = P^Q_Y(1) = 1/2,$$
$$P^Q_{XY}(0,0) = P^Q_{XY}(1,1) = (1-Q)/2,$$
$$P^Q_{XY}(0,1) = P^Q_{XY}(1,0) = Q/2.$$

Definition

An IR protocol is (ε, Q)-correct if it is ε-correct on P^Q_{XY}.

Theorem (Non-asymptotic converse bound for (ε, Q)-correct prot.)

$$\log|\mathcal{M}| \geq nh(Q) + \left(n(1-Q) - F^{-1}\left(\varepsilon\left(1 + 1/\sqrt{n}\right); n, 1-Q\right) - 1\right) \log\frac{1-Q}{Q} - \frac{1}{2}\log n - \log\frac{1}{\varepsilon}.$$

where $F^{-1}(\,\cdot\,; n, p)$ is the inverse of the CDF of the binomial distribution.

Special Case: Quantum Bit Error Rate Q

Theorem (Converse bound (Normal approximation))

$$\log |\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,.$$

Special Case: Quantum Bit Error Rate Q

Theorem (Converse bound (Normal approximation))

$$\log|\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,.$$

Corollary (Converse bound for (ε, Q)-correct protocol)

Let $0 < \varepsilon < 1$ and let $0 < Q < \frac{1}{2}$. Then, for large n, any (ε, Q)-correct IR protocol satisfies

$$\log|\mathcal{M}| \geq \xi(n,\varepsilon;Q)\cdot nh(Q) - \frac{1}{2}\log n - O(1), \qquad \textit{where}$$

Special Case: Quantum Bit Error Rate Q

Theorem (Converse bound (Normal approximation))

$$\log|\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,.$$

Corollary (Converse bound for (ε, Q)-correct protocol)

Let $0 < \varepsilon < 1$ and let $0 < Q < \frac{1}{2}$. Then, for large n, any (ε, Q)-correct IR protocol satisfies

$$\log|\mathcal{M}| \geq \xi(n,\varepsilon;Q)\cdot nh(Q) - \frac{1}{2}\log n - O(1), \qquad \text{where}$$

$$\xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}}\frac{\sqrt{v(Q)}}{h(Q)}\Phi^{-1}(1-\varepsilon),$$

Special Case: Quantum Bit Error Rate Q

Theorem (Converse bound (Normal approximation))

$$\log|\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,.$$

Corollary (Converse bound for (ε, Q)-correct protocol)

Let $0 < \varepsilon < 1$ and let $0 < Q < \frac{1}{2}$. Then, for large n, any (ε, Q)-correct IR protocol satisfies

$$\log|\mathcal{M}| \geq \xi(n,\varepsilon;Q)\cdot nh(Q) - \frac{1}{2}\log n - O(1), \qquad \textit{where}$$

$$\xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}}\frac{\sqrt{v(Q)}}{h(Q)}\Phi^{-1}(1-\varepsilon),$$

$h(x) := -x\log x - (1-x)\log(1-x)$ *and* $v(x) := x(1-x)\log^2(x/(1-x))$.

Special Case: Quantum Bit Error Rate Q

Theorem (Converse bound (Normal approximation))

$$\log|\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,.$$

Corollary (Converse bound for (ε, Q)-correct protocol)

Let $0 < \varepsilon < 1$ and let $0 < Q < \frac{1}{2}$. Then, for large n, any (ε, Q)-correct IR protocol satisfies

$$\log|\mathcal{M}| \geq \xi(n,\varepsilon;Q)\cdot nh(Q) - \frac{1}{2}\log n - O(1), \qquad \textit{where}$$

$$\xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}}\,\frac{\sqrt{v(Q)}}{h(Q)}\Phi^{-1}(1-\varepsilon),$$

$h(x) := -x\log x - (1-x)\log(1-x)$ *and* $v(x) := x(1-x)\log^2\left(x/(1-x)\right)$.

Numerically, this simple bound matches the non-asymptotic bound very well.

Efficiency $\xi(n, \varepsilon; Q)$

- The efficiency of IR is the value multiplying the asymptotic limit

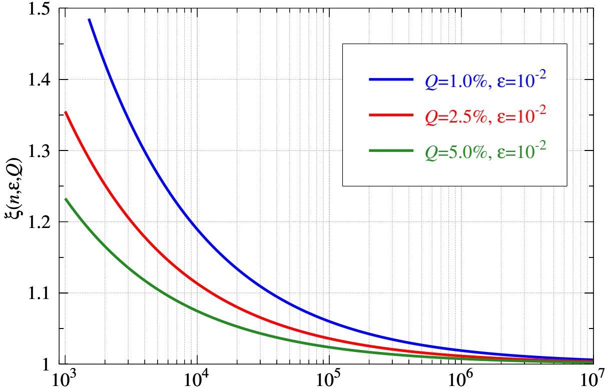
Efficiency $\xi(n, \varepsilon; Q)$

- The efficiency of IR is the value multiplying the asymptotic limit
- We obtain a forbidden region by plotting $\xi(n, \varepsilon; Q)$

Efficiency $\xi(n, \varepsilon; Q)$

- The efficiency of IR is the value multiplying the asymptotic limit
- We obtain a forbidden region by plotting $\xi(n, \varepsilon; Q)$

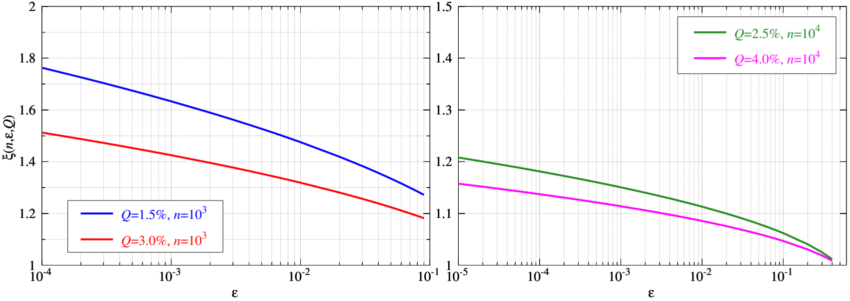
ξ as a function of the blocksize *n*



Efficiency $\xi(n, \varepsilon; Q)$

- The efficiency of IR is the value multiplying the asymptotic limit
- We obtain a forbidden region by plotting $\xi(n, \varepsilon; Q)$

ξ as a function of the frame error rate ε



But what about realistic IR codes?

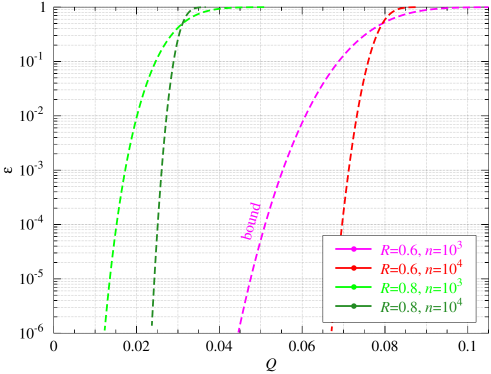
Theoretical Bound

$$\frac{\log|\mathcal{M}|}{nh(Q)} \approx \xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}}\frac{\sqrt{v(Q)}}{h(Q)}\Phi^{-1}(1-\varepsilon)$$

But what about realistic IR codes?

Theoretical Bound

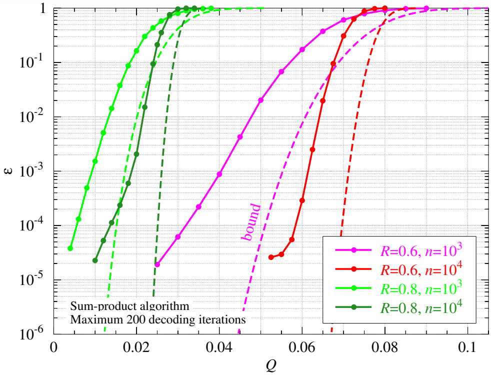
$$\frac{\log|\mathcal{M}|}{nh(Q)} \approx \xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}}\frac{\sqrt{v(Q)}}{h(Q)}\Phi^{-1}(1-\varepsilon)$$



But what about realistic IR codes?

Theoretical Bound

$$\frac{\log|\mathcal{M}|}{nh(Q)} \approx \xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}} \frac{\sqrt{v(Q)}}{h(Q)} \Phi^{-1}(1-\varepsilon)$$



But what about realistic IR codes?

Conjecture for LDPC codes

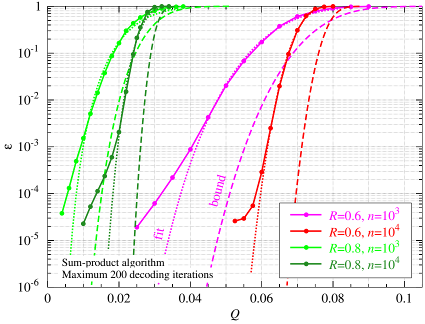
$$\frac{\log|\mathcal{M}|}{nh(Q)} =: \hat{\xi}(n,\varepsilon;Q) \approx \xi_1 + \xi_2 \cdot \frac{1}{\sqrt{n}} \frac{\sqrt{v(Q)}}{h(Q)} \Phi^{-1}(1-\varepsilon)$$

But what about realistic IR codes?

Conjecture for LDPC codes

$$\frac{\log|\mathcal{M}|}{nh(Q)} =: \hat{\xi}(n,\varepsilon;Q) \approx \xi_1 + \xi_2 \cdot \frac{1}{\sqrt{n}} \frac{\sqrt{v(Q)}}{h(Q)} \Phi^{-1}(1-\varepsilon)$$

Simulations of LDPC codes and fits

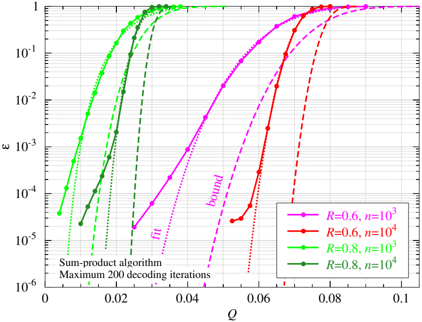


But what about realistic IR codes?

Conjecture for LDPC codes

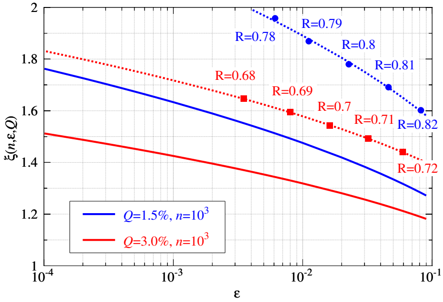
$$\frac{\log|\mathcal{M}|}{nh(Q)} =: \hat{\xi}(n,\varepsilon;Q) \approx \xi_1 + \xi_2 \cdot \frac{1}{\sqrt{n}} \frac{\sqrt{v(Q)}}{h(Q)} \Phi^{-1}(1-\varepsilon)$$

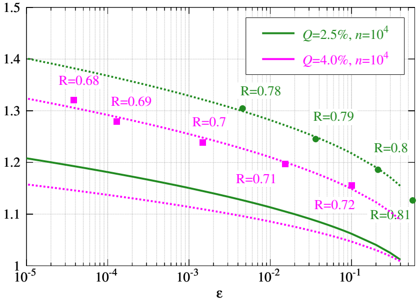
Simulations of LDPC codes and fits



n	$\log\lvert\mathcal{M}\rvert$	ξ_1	ξ_2
10^3	$4 \cdot 10^2$	1.11	1.39
10^3	$3 \cdot 10^2$	1.12	1.45
10^3	$2 \cdot 10^2$	1.13	1.69
10^4	$4 \cdot 10^3$	1.07	1.41
10^4	$3 \cdot 10^3$	1.08	1.44
10^4	$2 \cdot 10^3$	1.11	1.89

But what about realistic IR codes?





n	Q	ξ_1	ξ_2
10^3	0.015	1.16	1.52
10^3	0.030	1.16	1.31

n	Q	ξ_1	ξ_2
10^4	0.025	1.14	1.26
10^4	0.040	1.07	1.58

Outline

Conclusions / Open Questions

Conclusions

- Fundamental limits for information reconciliation in the finite key regime
- Commonly used approximation $\log|\mathcal{M}| \approx 1.1nh(Q)$ is often too optimistic for one-way IR
- Numerical simulations for LDPC codes $\rightarrow$ approximation that can be used for the design of QKD systems

Conclusions / Open Questions

Conclusions

- Fundamental limits for information reconciliation in the finite key regime
- Commonly used approximation $\log|\mathcal{M}| \approx 1.1nh(Q)$ is often too optimistic for one-way IR
- Numerical simulations for LDPC codes $\rightarrow$ approximation that can be used for the design of QKD systems

Open Questions

- Behaviour for different code families
- Joint consideration of fundamental limits for finite-length reconciliation and privacy amplification

Conclusions / Open Questions

Conclusions

- Fundamental limits for information reconciliation in the finite key regime
- Commonly used approximation $\log |\mathcal{M}| \approx 1.1 n h(Q)$ is often too optimistic for one-way IR
- Numerical simulations for LDPC codes $\rightarrow$ approximation that can be used for the design of QKD systems

Open Questions

- Behaviour for different code families
- Joint consideration of fundamental limits for finite-length reconciliation and privacy amplification

THANK YOU!