Quantum Cyber Security
Lecture 8: Quantum Key Distribution II

Petros Wallden

University of Edinburgh

8th February 2024

This Lecture

- From **QBER** to **secure key distribution** (general expression and how to use it)
- **Simplifying assumptions** (physical restrictions, classical efficiency, adversary's limitations, composability)
- **Security proof** for the basic BB84 protocol
- **Classical post-processing** and its **cost**

- **General Expression:**

$$\boxed{R = \frac{Q}{2}\left(\xi H(A:B) - S(A:E) - \Delta(n,\epsilon)\right)}$$

- R is the secret **key-rate**: Expected secret bits per qubit sent.

From QBER to Secure Key Distribution

- **General Expression:**

$$\boxed{R = \frac{Q}{2}\left(\xi H(A:B) - S(A:E) - \Delta(n,\epsilon)\right)}$$

- R is the secret **key-rate**: Expected secret bits per qubit sent.
- Q is the prob that sent single-photons are detected (not lost)
- factor $\frac{1}{2}$ is due to the raw key that includes only the positions that Alice and Bob measured in same basis
- ξ is due to non-ideal classical post-processing (IR and PA)
- $\Delta(n,\epsilon)$ is a factor due to finite-size effects (measured value differing from expectation)

From QBER to Secure Key Distribution

- For simplicity we consider: **perfect detection**, **ideal post-processing** and **asymptotic limit**

$$Q = 1 \; ; \; \xi = 1 \; ; \; \Delta(n, \epsilon) = 0$$

From QBER to Secure Key Distribution

- For simplicity we consider: **perfect detection**, **ideal post-processing** and **asymptotic limit**

$$Q = 1 \; ; \; \xi = 1 \; ; \; \Delta(n, \epsilon) = 0$$

- Using details of BB84 protocol we get:

$$\boxed{R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - h(e_b) - h(e_p)\right)} \qquad (1)$$

where e_b and e_p are the average errors in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases and $h(p) := -p \log_2 p - (1-p) \log_2(1-p)$ is the binary entropy

From QBER to Secure Key Distribution

- For simplicity we consider: **perfect detection**, **ideal post-processing** and **asymptotic limit**

$$Q = 1\ ;\ \xi = 1\ ;\ \Delta(n, \epsilon) = 0$$

- Using details of BB84 protocol we get:

$$\boxed{R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - h(e_b) - h(e_p)\right)} \qquad (1)$$

where e_b and e_p are the average errors in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases and $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy

- If the errors in different bases equal and equal to the QBER ($e_b = e_p = D$) we finally get:

$$\boxed{R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - 2h(D)\right)} \qquad (2)$$

Examples: How to compute key rate (ideal case)

- Example 1: Given $e_b = 0.05, e_p = 0.1$ find the rate.

$$R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - h(0.05) - h(0.1)\right) = \frac{1}{2}\left(1 - 0.29 - 0.47\right) = 0.12$$

The protocol does not abort

Examples: How to compute key rate (ideal case)

- Example 1: Given $e_b = 0.05, e_p = 0.1$ find the rate.

  $$R_{\mathrm{BB84}} = \frac{1}{2}(1 - h(0.05) - h(0.1)) = \frac{1}{2}(1 - 0.29 - 0.47) = 0.12$$

  The protocol does not abort

- Example 2: Which is the largest QBER D (symmetric in two bases) that BB84 does not abort (error tolerance)?

  $$R_{\mathrm{BB84}} = \frac{1}{2}(1 - 2h(D)) = 0 \Rightarrow h(D) = 1/2 \Rightarrow D \approx 0.11$$

Examples: How to compute key rate (ideal case)

- Example 1: Given $e_b = 0.05, e_p = 0.1$ find the rate.

$$R_{\mathrm{BB84}} = \frac{1}{2}(1 - h(0.05) - h(0.1)) = \frac{1}{2}(1 - 0.29 - 0.47) = 0.12$$

  The protocol does not abort

- Example 2: Which is the largest QBER D (symmetric in two bases) that BB84 does not abort (error tolerance)?

$$R_{\mathrm{BB84}} = \frac{1}{2}(1 - 2h(D)) = 0 \Rightarrow h(D) = 1/2 \Rightarrow D \approx 0.11$$

- Example 3: Does intercept, measure Z & resend attack abort?

$$e_b = 0 \;;\; e_p = 0.5 \;; R_{\mathrm{BB84}} = \frac{1}{2}(1 - h(0.5)) = 0$$

Restrictions and Assumptions

- For the expressions above, certain assumptions were made
- The proof can be generalised (with adjusted parameters and simple protocol modifications)

Restrictions and Assumptions

- For the expressions above, certain assumptions were made
- The proof can be generalised (with adjusted parameters and simple protocol modifications)
- Physical Restrictions:
  - **Losses:** Detecting a single photon becomes less likely with the distance travelled. The rate decreases rapidly with distance (Q expresses the % of photons detected at a given distance)

Restrictions and Assumptions

- For the expressions above, certain assumptions were made
- The proof can be generalised (with adjusted parameters and simple protocol modifications)
- Physical Restrictions:
  - **Losses:** Detecting a single photon becomes less likely with the distance travelled. The rate decreases rapidly with distance (Q expresses the % of photons detected at a given distance)
  - **Dark counts and Errors:** A single-photon detector (rarely) detects photons when there aren't or make a mistake in identifying the correct polarisation. When very small incoming intensity this effect can dominate.

Restrictions and Assumptions

- For the expressions above, certain assumptions were made
- The proof can be generalised (with adjusted parameters and simple protocol modifications)
- Physical Restrictions:
  - **Losses:** Detecting a single photon becomes less likely with the distance travelled. The rate decreases rapidly with distance (Q expresses the % of photons detected at a given distance)
  - **Dark counts and Errors:** A single-photon detector (rarely) detects photons when there aren't or make a mistake in identifying the correct polarisation. When very small incoming intensity this effect can dominate.
  - **True single-photon source:** In practise sources frequently produce pairs of (identical) photons instead of single photons (this affects the security)

Restrictions and Assumptions

- For the expressions above, certain assumptions were made
- The proof can be generalised (with adjusted parameters and simple protocol modifications)
- Physical Restrictions:
  - **Losses:** Detecting a single photon becomes less likely with the distance travelled. The rate decreases rapidly with distance (Q expresses the % of photons detected at a given distance)
  - **Dark counts and Errors:** A single-photon detector (rarely) detects photons when there aren't or make a mistake in identifying the correct polarisation. When very small incoming intensity this effect can dominate.
  - **True single-photon source:** In practise sources frequently produce pairs of (identical) photons instead of single photons (this affects the security)
  - **Fully trusted quantum devices:** Assumptions on how the preparation and measuring devices behave and what information on their workings could leak (e.g. due to a hacking/side-channel attack)

Restrictions and Assumptions

- Finite-size effects: Bounds on the mutual information are computed based on expectations values of observables.

  Measured values differ from expectation values for finite size keys, but they converge (exponentially – cf Chernoff bounds) when the length of the string tends to infinity.

  Finite-size corrections are required for **practical QKD**

Restrictions and Assumptions

- Finite-size effects: Bounds on the mutual information are computed based on expectations values of observables.

  Measured values differ from expectation values for finite size keys, but they converge (exponentially – cf Chernoff bounds) when the length of the string tends to infinity.

  Finite-size corrections are required for **practical QKD**

- Cost of classical post-processing: Theoretical error-correction (IR) leaks information to make A', B' perfectly correlated, related with the conditional entropy $H(A|B)$

  Practical error-correction leaks more bits of information (cf ξ-coefficient)

Assumptions: Adversary's model

- Ability of adversary: (from weaker to stronger)
  - i.i.d. attacks: Interacts with sent each qubit separately, independently and identically
    Can reduce remarks regarding **strings of qubits** to the **expected effect on a single qubit**
    State Alice prepares: $|x\rangle_A \langle x| \otimes \rho_B^x$ where x represents the classical info Alice stores (which BB84 state was prepared).

Assumptions: Adversary's model

- Ability of adversary: (from weaker to stronger)
  - i.i.d. attacks: Interacts with sent each qubit separately, independently and identically
    Can reduce remarks regarding **strings of qubits** to the **expected effect on a single qubit**
    State Alice prepares: $|x\rangle_A \langle x| \otimes \rho_B^x$ where x represents the classical info Alice stores (which BB84 state was prepared).
    General action: $U_{BE}\left(\rho_B^x \otimes |0,0\rangle_E \langle 0,0|\right) = \sigma_{BE}^x$ and sending system B to Bob (wlog E is 2-qubit).
    $\sigma_E^x = \mathrm{Tr}_B(\sigma_{BE}^x)$ is Eve's system. She performs measurement to obtain the max info on classical variable x

Assumptions: Adversary's model

- Ability of adversary: (from weaker to stronger)
  - i.i.d. attacks: Interacts with sent each qubit separately, independently and identically
    Can reduce remarks regarding **strings of qubits** to the **expected effect on a single qubit**
    State Alice prepares: $|x\rangle_A \langle x| \otimes \rho_B^x$ where x represents the classical info Alice stores (which BB84 state was prepared).
    General action: $U_{BE}\left(\rho_B^x \otimes |0,0\rangle_E \langle 0,0|\right) = \sigma_{BE}^x$ and sending system B to Bob (wlog E is 2-qubit).
    $\sigma_E^x = \mathrm{Tr}_B(\sigma_{BE}^x)$ is Eve's system. She performs measurement to obtain the max info on classical variable x
  - Collective attacks: Uses **different private system** for each qubit, interacts with each qubit (non iid) and then measures conditionally on other previous actions

Assumptions: Adversary's model

- Ability of adversary: (from weaker to stronger)
  - i.i.d. attacks: Interacts with sent each qubit separately, independently and identically
    Can reduce remarks regarding **strings of qubits** to the **expected effect on a single qubit**
    State Alice prepares: $|x\rangle_A \langle x| \otimes \rho_B^x$ where x represents the classical info Alice stores (which BB84 state was prepared).
    General action: $U_{BE}\left(\rho_B^x \otimes |0,0\rangle_E \langle 0,0|\right) = \sigma_{BE}^x$ and sending system B to Bob (wlog E is 2-qubit).
    $\sigma_E^x = \mathrm{Tr}_B(\sigma_{BE}^x)$ is Eve's system. She performs measurement to obtain the max info on classical variable x
  - Collective attacks: Uses **different private system** for each qubit, interacts with each qubit (non iid) and then measures conditionally on other previous actions
  - Coherent Attacks: Uses private system(s), **interacts with all passing qubits**, stores everything and **measures all systems at the end** (possibly in entangled basis)

Assumptions: Composability

- Composability: In modern crypto, security is proven is such a way that essential **properties proven** are directly maintained **when composed with other protocols** (e.g. used as subroutine in a larger protocol)

  This is **essential for QKD** too (since it is used as part of larger protocols)

Assumptions: Composability

- Composability: In modern crypto, security is proven is such a way that essential **properties proven** are directly maintained **when composed with other protocols** (e.g. used as subroutine in a larger protocol)

  This is **essential for QKD** too (since it is used as part of larger protocols)

  Way to prove:

  - Define ideal properties that protocol would have
  - Any adversary has **bound probability of distinguishing** the real protocol from a simulated protocol that uses the ideal protocol
  - In quantum case, bounding this probability reduces in bounding the **trace-distance** of the real protocol from an ideal protocol

BB84: A basic security proof

- Disclaimer: Here we present **older proof** that is more intuitive. Modern proofs (that can be made composable) involve mapping the protocol to entanglement-based and reducing security to entanglement-distillation

BB84: A basic security proof

- Disclaimer: Here we present **older proof** that is more intuitive. Modern proofs (that can be made composable) involve mapping the protocol to entanglement-based and reducing security to entanglement-distillation
- Simplifying Assumptions:
  - Asymptotic limit ($N \to \infty$)
  - No losses ($Q = 1$)
  - trusted and ideal single-photon source and measuring devices
  - ideal classical post-processing ($\xi = 1$)

BB84: A basic security proof

- Disclaimer: Here we present **older proof** that is more intuitive. Modern proofs (that can be made composable) involve mapping the protocol to entanglement-based and reducing security to entanglement-distillation
- Simplifying Assumptions:
  - Asymptotic limit ($N \to \infty$)
  - No losses ($Q = 1$)
  - trusted and ideal single-photon source and measuring devices
  - ideal classical post-processing ($\xi = 1$)
- Adversarial Model: **i.i.d.** and **non-composable**

BB84: A basic security proof

- Disclaimer: Here we present **older proof** that is more intuitive. Modern proofs (that can be made composable) involve mapping the protocol to entanglement-based and reducing security to entanglement-distillation
- Simplifying Assumptions:
  - Asymptotic limit ($N \to \infty$)
  - No losses ($Q = 1$)
  - trusted and ideal single-photon source and measuring devices
  - ideal classical post-processing ($\xi = 1$)
- Adversarial Model: **i.i.d.** and **non-composable**
- Proof **can be generalised** for stronger adversaries and without the simplifying assumptions, adjusting parameters and with simple protocol modifications

BB84: A basic security proof

- i.i.d. case see effects on **single qubit** (rather than strings)
- Need to bound (subject to average errors e_b, e_p):

$$\boxed{R = \frac{1}{2}(H(A:B) - S(A:E))}$$

- See also alternative proof later

BB84: A basic security proof

- i.i.d. case see effects on **single qubit** (rather than strings)
- Need to bound (subject to average errors e_b, e_p):

$$\boxed{R = \frac{1}{2}(H(A:B) - S(A:E))}$$

- See also alternative proof later
- $H(A:B) = H(A) - H(A|B) = 1 - \frac{1}{2}(h(e_b) + h(e_p))$
  $H(A) = 1$ since A is chosen randomly
  $H(A) = -1/2\log_2\frac{1}{2} - 1/2\log_2\frac{1}{2} = 1$
  $H(A|B)$ when state is sent in the Z basis is
  $H(A|B) = -(1-e_b)\log_2(1-e_b) - e_b\log_2 e_b = h(e_b)$ and happens in half cases
  $H(A|B)$ when state is sent in the X basis is
  $H(A|B) = -(1-e_p)\log_2(1-e_p) - e_p\log_2 e_p = h(e_p)$ and happens in the other cases
- Overall: $H(A|B) = \frac{1}{2}(h(e_b) + h(e_p))$

BB84: A basic security proof

- Need to bound $S(A:E)$. Eve has the quantum state:

$$\sigma_E^x = \mathrm{Tr}_B \left(U_{BE} (\rho_B^x \otimes |0,0\rangle_E \langle 0,0|) \right)$$

Need to min the classical info about x that she can extract.

BB84: A basic security proof

- Need to bound $S(A:E)$. Eve has the quantum state:

$$\sigma_E^x = \mathrm{Tr}_B \left(U_{BE}(\rho_B^x \otimes |0,0\rangle_E \langle 0,0|) \right)$$

Need to min the classical info about x that she can extract. Accessible Information: Given ensemble $F := \{(p(x), \sigma^x)\}$, the (generalised) measurement $\{M\}$, and the random variable corresponding to the measurement's outcome Y_M:

$$I_{acc}(F) = \max_M H(X:Y_M)$$

- **Holevo bound:** Given ensemble $F := \{(p(x), \sigma^x)\}$, the accessible information is upper bounded by the Holevo quantity $\chi(F)$

$$I_{acc}(F) \leq \chi(F) := S(\sum_x p(x)\sigma^x) - \sum_x p(x)S(\sigma^x)$$

(i.e. the VN-entropy of the average state minus the average VN-entropy of the ensemble)

BB84: A basic security proof

- **Holevo bound:** Given ensemble $F := \{(p(x), \sigma^x)\}$, the accessible information is upper bounded by the Holevo quantity $\chi(F)$

$$I_{acc}(F) \leq \chi(F) := S(\sum_x p(x)\sigma^x) - \sum_x p(x) S(\sigma^x)$$

(i.e. the VN-entropy of the average state minus the average VN-entropy of the ensemble)

- It is easy to see that $S(\rho) \leq \log_2 d$, where d is the dimension of the density matrix ρ, i.e. the number of qubits.

- **Holevo bound:** Given ensemble $F := \{(p(x), \sigma^x)\}$, the accessible information is upper bounded by the Holevo quantity $\chi(F)$

$$I_{acc}(F) \leq \chi(F) := S(\sum_x p(x)\sigma^x) - \sum_x p(x)S(\sigma^x)$$

(i.e. the VN-entropy of the average state minus the average VN-entropy of the ensemble)

- It is easy to see that $S(\rho) \leq \log_2 d$, where d is the dimension of the density matrix ρ, i.e. the number of qubits.
- In our case Eve's register is $d = 2^2$ and thus:

$$I_{acc} \leq \chi(F) \leq 2$$

The **maximum classical information extractable from a single qubit** (irrespective of the number of classical states encoded) is **one bit**!

BB84: A basic security proof

- Let $\sigma_{BE} = |\psi\rangle_{BE} \langle\psi|$ be a **pure state** (global), then:

$$S(\sigma_B) := S(\mathrm{Tr}_E(\sigma_{BE})) = S(\sigma_E) := S(\mathrm{Tr}_B(\sigma_{BE}))$$

(See **Schmidt decomposition** for proof)

BB84: A basic security proof

- Let $\sigma_{BE} = |\psi\rangle_{BE}\langle\psi|$ be a **pure state** (global), then:

$$S(\sigma_B) := S(\mathrm{Tr}_E(\sigma_{BE})) = S(\sigma_E) := S(\mathrm{Tr}_B(\sigma_{BE}))$$

(See **Schmidt decomposition** for proof)

- In our case ($F = \{p(x), \sigma_E^x\}$) for the individual terms, σ_{BE}^x is pure so we can use the entropy of the B system, which for given x is give by the resp error:

$$S(A:E) \leq I_{acc}(F) \leq \chi(F) = S(\sigma_E) - \frac{1}{2}(h(e_b) + h(e_p))$$

Leading to

$$R \geq \frac{1}{2}(H(A:B) - \chi(F)) = \frac{1}{2}(1 - S(\sigma_E))$$

- It can also be shown that $S(\sum_x \frac{1}{4}\sigma_E^x) \leq h(e_b) + h(e_p)$
- Algebraically has 2 maximum value (if Bob's state is random and independent of the state of Alice)
- This leads to the final expression given by Eq. (1)

$$R_{BB84} \geq \frac{1}{2}(1 - h(e_b) - h(e_p))$$

- This becomes negative if e_p, e_b increase (has max value -1 when these become $1/2$)
- The overall $1/2$ factor in Eq. (1) can be removed if the states sent are mainly in one (preferred) basis. This is possible if there are sufficient states sent in the other basis to have good enough statistics (cf finite-size effects)

BB84: Another proof based on entropic uncertainty

- Consider tripartite system ABE. System A is either measured in Z or X basis to result to classical variable A^Z, A^X resp
- For simplicity systems A, B are assumed to be single qubits, then the following **inequality** holds for all global states ρ_{ABE}

$$\boxed{S(A^X|B) + S(A^Z|E) \geq 1} \qquad (3)$$

BB84: Another proof based on entropic uncertainty

- Consider tripartite system ABE. System A is either measured in Z or X basis to result to classical variable A^Z, A^X resp
- For simplicity systems A, B are assumed to be single qubits, then the following **inequality** holds for all global states ρ_{ABE}

$$\boxed{S(A^X|B) + S(A^Z|E) \geq 1} \tag{3}$$

- We have

$$H(A:B) - S(A:E) = S(A|E) - H(A|B) = S(A|E) - S(A|B)$$

which we can break to two terms depending the basis used:

$$\frac{1}{2}\Big(S(A^Z|E) - S(A^Z|B^Z) + S(A^X|E) - S(A^X|B^X)\Big)$$

BB84: Another proof based on entropic uncertainty

- From Eq. (3) we get:

$$I(A:B) - S(A:E) \geq \frac{1}{2}\Big((1 - S(A^X|B^X)) - S(A^Z|B^Z) +$$

$$+ (1 - S(A^Z|B^Z)) - S(A^X|B^X)\Big)$$

BB84: Another proof based on entropic uncertainty

- From Eq. (3) we get:

$$I(A:B) - S(A:E) \geq \frac{1}{2}\Big((1 - S(A^X|B^X)) - S(A^Z|B^Z) +$$

$$+ (1 - S(A^Z|B^Z)) - S(A^X|B^X)\Big)$$

- Noting that $S(A^Z|B^Z) = h(e_b)$; $S(A^X|B^X) = h(e_p)$

$$I(A:B) - S(A:E) \geq 1 - h(e_b) - h(e_p)$$

which then leads to the known expression Eq. (1)

Classical Post-Processing

- Once raw-key is obtained and QBER computed and threshold is achieved, we still need to classically process the resulted keys to ensure that they are **identical** between Alice and Bob and **completely secret** from Eve.

Classical Post-Processing

- Once raw-key is obtained and QBER computed and threshold is achieved, we still need to classically process the resulted keys to ensure that they are **identical** between Alice and Bob and **completely secret** from Eve.

- Information Reconciliation (IR): Exchange information (error-correcting codes) to make $A' = B'$

  The number of bits required is estimated from the mutual information $H(A : B)$ using the QBER. This **amount of information** is also **leaked to Eve**

Classical Post-Processing

- Once raw-key is obtained and QBER computed and threshold is achieved, we still need to classically process the resulted keys to ensure that they are **identical** between Alice and Bob and **completely secret** from Eve.

- Information Reconciliation (IR): Exchange information (error-correcting codes) to make $A' = B'$

  The number of bits required is estimated from the mutual information $H(A : B)$ using the QBER. This **amount of information** is also **leaked to Eve**

- Privacy Amplification (PA): Use family of **universal hash functions** to ensure that the final (smaller) key Alice and Bob share, is completely secret from Eve (i.e. amplify the privacy). Map strings to smaller strings s.t. entropy $H(A''|E'')$ of new strings $A'' = g(A')$; $E'' = g(E')$ is maximum

Information Reconciliation

Many methods exist. Old but mostly used: **CASCADE**
"Secret-key reconciliation by public discussion", by Brassard & Salvail, EUROCRYPT 1993

Information Reconciliation

Many methods exist. Old but mostly used: **CASCADE**
"Secret-key reconciliation by public discussion", by Brassard & Salvail, EUROCRYPT 1993

1. Alice and Bob **divide their strings to blocks** of k_1-size (fixed by amount of IR required given from QBER)

Information Reconciliation

Many methods exist. Old but mostly used: **CASCADE**
"Secret-key reconciliation by public discussion", by Brassard & Salvail, EUROCRYPT 1993

1. Alice and Bob **divide their strings to blocks** of k_1-size (fixed by amount of IR required given from QBER)
2. They **exchange the parities** of each block
   - If error, **Bob finds and corrects** it using **binary search**

Information Reconciliation

Many methods exist. Old but mostly used: **CASCADE**
"Secret-key reconciliation by public discussion", by Brassard & Salvail, EUROCRYPT 1993

1. Alice and Bob **divide their strings to blocks** of k_1-size (fixed by amount of IR required given from QBER)
2. They **exchange the parities** of each block
   - If error, **Bob finds and corrects** it using **binary search**
3. They **repeat** with different blocks and different block-sizes k_i
   - If error, Bob finds and corrects with binary search
   - Then **back to all previous blocks** that their parity changed and with binary search **find another error**

Information Reconciliation

Many methods exist. Old but mostly used: **CASCADE**
"Secret-key reconciliation by public discussion", by Brassard & Salvail, EUROCRYPT 1993

1. Alice and Bob **divide their strings to blocks** of k_1-size (fixed by amount of IR required given from QBER)
2. They **exchange the parities** of each block
   - If error, **Bob finds and corrects** it using **binary search**
3. They **repeat** with different blocks and different block-sizes k_i
   - If error, Bob finds and corrects with binary search
   - Then **back to all previous blocks** that their parity changed and with binary search **find another error**
4. Terminates after few rounds (once more than required bits are leaked) and **whp the strings are now identical**

Information Reconciliation

Many methods exist. Old but mostly used: **CASCADE**
"Secret-key reconciliation by public discussion", by Brassard & Salvail, EUROCRYPT 1993

1. Alice and Bob **divide their strings to blocks** of k_1-size (fixed by amount of IR required given from QBER)
2. They **exchange the parities** of each block
   - If error, **Bob finds and corrects** it using **binary search**
3. They **repeat** with different blocks and different block-sizes k_i
   - If error, Bob finds and corrects with binary search
   - Then **back to all previous blocks** that their parity changed and with binary search **find another error**
4. Terminates after few rounds (once more than required bits are leaked) and **whp the strings are now identical**

Due to non-ideal procedure, to ensure identical output **leaked bits are increased by a factor** ξ compared to ideal Shannon limit

Privacy Amplification

- Leftover hash lemma: if a secret bit-string A of length n has t bits leaked (at unknown positions), then you can produce a bit string of $m \leq n - t - 2\log_2(1/\epsilon)$ bits that is totally secret (almost optimal)

Privacy Amplification

- Leftover hash lemma: if a secret bit-string A of length n has t bits leaked (at unknown positions), then you can produce a bit string of $m \leq n - t - 2\log_2(1/\epsilon)$ bits that is totally secret (almost optimal)
- An estimate of t is obtained from the $H(E'|A')$ (taking into account info leaked both at the protocol and in the IR phase)

Privacy Amplification

- Leftover hash lemma: if a secret bit-string A of length n has t bits leaked (at unknown positions), then you can produce a bit string of $m \leq n - t - 2\log_2(1/\epsilon)$ bits that is totally secret (almost optimal)
- An estimate of t is obtained from the $H(E'|A')$ (taking into account info leaked both at the protocol and in the IR phase)
- 2-Universal hash family: Let a family of functions $g_i \in G$ with $i \in S$ (cardinality of family $|S|$), where $g_i : \{U \rightarrow [m] = \{0,1\}^m\}$:
  1. for fixed $A \in U$ if g_i is randomly chosen from the family, the $g_i(A)$ is uniformly distributed in $[m]$
  2. for any pair $A, E \in U$, if i is chosen randomly, $g_i(A), g_i(E)$ are independent variables

Privacy Amplification

- Leftover hash lemma: if a secret bit-string A of length n has t bits leaked (at unknown positions), then you can produce a bit string of $m \leq n - t - 2\log_2(1/\epsilon)$ bits that is totally secret (almost optimal)
- An estimate of t is obtained from the $H(E'|A')$ (taking into account info leaked both at the protocol and in the IR phase)
- 2-Universal hash family: Let a family of functions $g_i \in G$ with $i \in S$ (cardinality of family $|S|$), where $g_i : \{U \rightarrow [m] = \{0,1\}^m\}$:
  1. for fixed $A \in U$ if g_i is randomly chosen from the family, the $g_i(A)$ is uniformly distributed in $[m]$
  2. for any pair $A, E \in U$, if i is chosen randomly, $g_i(A), g_i(E)$ are independent variables
- Consider a string A with $(n-t)$-bits of randomness. If $m \leq (n-t)$ then using the 2-universal hash family G:

$$\delta[(g_i(A), i), (R, i)] \leq \epsilon$$

R uniformly random m-bit string, δ stat distance