□ SQRNG Protocol

– a semi-quantum user (Alice) interacts with an untrusted quantum server (Eve) to generate random numbers securely.

* semi-quantum user : restricted to operations in a single, publicly known basis $\{|0\rangle, |1\rangle\}$ or to ignoring the quantum signal & reflecting it undisturbed.

Single round of SQRNG protocol assuming honest server:

1) The server prepares the state $|+\rangle$ and sends it to Alice.
2) Alice chooses randomly to `Reflect` the signal or to `Measure-Resend`, (recording the measurement result).
3) Upon receiving Alice's qubit, the server makes an X basis measurement and reports the outcome over a classical channel (this channel need not be authenticated).
   - If Alice chose `Reflect`, she should expect the message from the server to be "+" and any other response will be considered noise and will be later factored into our security analysis.
   - If Alice chose `Measure-Resend`, she will have a classical measurement outcome $a \in \{0, 1\}$. Ideally, the server's message will be either "+" or "−" randomly in this event.

Repeated N times ⟹ raw random string of size $n \leq N$

hashing ⟸

Seed Randomness for Alice's Choices

$\binom{N}{m}$: # of ways to choose m elements from N

$\log_2 \binom{N}{m}$: # of seed random bits required to randomly select m rounds from N.

$\frac{1}{N} \log_2 \binom{N}{m}$: avg. # of extra bits of randomness required per qubit.

m is chosen to be arbitrarily small compared to N.

$$N \to \infty \implies \binom{N}{m} = \frac{N!}{(N-m)!\,m!} \to 1 \implies \frac{1}{N} \log_2 \binom{N}{m} \to 0$$

$\therefore$ The seed randomness required for Alice to execute the protocol is not considered for the analysis.

□ Purified SQRNG

1) Eve prepares a large N qubit state (N: # of protocol rounds) possibly entangled with her private ancilla.

2) Alice on receipt of the N qubits, will choose a subset Θ. For each $i = 1, 2, \cdots, N$

$\Theta_i = 0 \Rightarrow$ Alice will Reflect i^{th} qubit

$\Theta_i = 1 \Rightarrow$ Alice will apply CNOT with

control register: i^{th} qubit sent from the server

target register: $|0\rangle$ state in a private register.

- Measure Resent step.

Alice will later measure her private register in the Z basis, which will in effect simulate the case where Alice measures the qubits immediately.

$$CNOT(x, y) = CNOT(x, x \oplus y)$$

$$\therefore CNOT(x, 0) = (x, x) \quad \& \quad CNOT(x, 1) = (x, \bar{x})$$

where $x \in \{0, 1\}$.

$\Rightarrow$ Alice uses a CNOT operation to defer the measurement of qubits

- Principle of Deferred Measurement

3) The entire N qubits return to Eve, who performs a quantum instrument mapping the N qubits & her private ancilla to a classical N bit message space modelled as a quantum ancilla register and an updated ancilla from which Eve will attempt to learn as much as possible about Alice's measurement results or Alice's private register which she will measure subsequently.

□ e-QRNG Protocol

1) A quantum source, Eve, prepares an entangled state $|\tau\rangle_{ACE} \in \mathcal{H}_A \otimes \mathcal{H}_C \otimes \mathcal{H}_E$. The A and C registers are each of dimension 2^N for user specified N (as before, N is the number of rounds used by the protocol). The A system is sent to Alice while the C register is sent to the trusted server (who may also be Alice). Eve keeps the E register private.
2) Alice, on receipt of the state, has two choices for each round (i.e., each of the N qubits), as in the SQRNG protocol. We call these two choices here `Measure-Resend` and `Reflect` to keep the notation consistent with the SQRNG case, however the operations are different in the e-QRNG case. If Alice chooses `Reflect`, she will measure that qubit in the X basis, and *abort the entire protocol* if she observes $|-\rangle$. That is, to simulate a true "reflection" in the semi-quantum case, A will only continue with the protocol if she measures and observes $|+\rangle$. We say Alice *accepts* the state if she observes $|+\rangle$. Alternatively, if Alice chooses `Measure-Resend`, she will measure that particular qubit in the Z basis.

3) The trusted server, on receipt of the C system, simply measures all N qubits in the X basis, and *publicly reports the outcome*. Note that in the e-QRNG case, the server is honest in this measurement and, in fact, this C register measurement may even be done by Alice. Note that this may be done before, in parallel to, or after Alice's operations in step 2.

* The protocol completely aborts if Alice observes $|->$ on a Reflect test case because $|+\rangle$ will simulate a Reflect in the SQRNG case, whereas an observation of $|->$ will produce a quantum state that cannot exist in the SQRNG case (shown in the proof of Theorem 1).

⇒ e-QRNG protocol is highly inefficient due to the high probability of aborting, however this protocol is just to prove security of actual SQRNG protocol.

Theorem 1: shows how an attack on the SQRNG protocol translates into an attack on e-QRNG.

(i) $\mathcal{E}$: an attack against the SQRNG protocol

θ : represents Alice's choices of operations in the SQRNG protocol

$ct_0(\theta)$: how many qubits Alice chose to Reflect instead of Measure-Resend.

$|\Psi(\mathcal{E},\theta)\rangle$: quantum state in the purified SQRNG model.

$|Z(\mathcal{E},\theta)\rangle$: quantum state in the e-QRNG model

The prob. that Alice does not abort is,

$$P_a = P\{\text{Alice gets } |+\rangle \text{ for all } 0\text{'s in } \theta\}$$

$$= \underbrace{\frac{1}{2} \times \frac{1}{2} \times \cdots \times \frac{1}{2}}_{ct_0(\theta)} = \frac{1}{2^{ct_0(\theta)}}$$

(ii) If Alice does not abort, then the quantum state in e-QRNG is exactly the same as in the purified SQRNG.

$$|\tau(\varepsilon,\theta)\rangle = |\psi(\varepsilon,\theta)\rangle$$

⇒ The security of purified SQRNG is guaranteed as long as e-QRNG is secure.

(iii) If the SQRNG protocol is attacked using a collective attack (the initial state in e-QRNG is a product state instead of entagled) then the final constructed state $|\tau\rangle$ is also a product state after applying the attack, ie., $|\tau\rangle = |\tau_0\rangle^{\otimes N}$.

The probability of obtaining $|-\rangle$ on any individual signal in e-QRNG is exactly $1/2$.
ie., when Alice measures in the X basis, she has a 50% chance of obtaining $|-\rangle$.

Proof.

Purified SQRNG

a general attack consists of Eve first preparing an arbitrary quantum state $|\psi_0\rangle_{AE}$ (initial state in purified SQRNG).

A: Alice's qubits, E: Eve's private ancilla.

$$|\psi_0\rangle = \sum_{a \in \{0,1\}^{2N}} \alpha_a |a\rangle |E_a\rangle$$

$|E_a\rangle$: arbitrary normalized states in Eve's private ancilla.

$|a\rangle$: N qubit basis states

The A portion is sent to Alice.

Now, Alice decides whether to Measure-Resend or Reflect for each qubit, based on her choice vector Θ:

$\Theta_i = 1 \rightarrow$ apply CNOT gate to an ancilla

$\Theta_i = 0 \rightarrow$ Do nothing (Reflect) i.e., I

Alice's initial ancilla is set to $|0 \cdots 0\rangle_A$.

toffoli$(x, y, z) = (x, y, z \oplus xy)$

toffoli$(x, y, 0) = (x, y, xy) = (x, y, x \wedge y)$

Here, $x = \Theta_i$

$\Theta_i = 1$ then $a_i \wedge \Theta_i = a_i \Rightarrow$ qubit a_i is copied to the ancilla

$\Theta_i = 0$ then $a_i \wedge \Theta_i = 0 \Rightarrow$ ancilla qubit remains 0

The result of this action on $|\psi_0\rangle$ is:

$$|0\cdots0\rangle_A \otimes |\psi_0\rangle \rightarrow |\psi_0'\rangle = \sum_{a\in\{0,1\}^N} \alpha_a |a \wedge \theta\rangle_A \otimes |a\rangle_T \otimes |E_a\rangle_E$$

$\theta_i = 1$: corresp. qubit a_i is copied into Alice's ancilla via CNOT

$\theta_i = 0$: ancilla remains 0 at i

$|a\rangle_T$: the transit qubit returning to Eve

After Alice's operations, the T register returns to Eve $\Rightarrow$ Eve now apply a general quantum operation U (quantum instrument) on the transit qubits register T and her ancilla E, instead of measuring in the X basis, that copy preserving coherence & entanglement.

this is equivalent to applying an isometry U mapping Eve's ancilla and the Transit register into a quantum ancilla for Eve and a Hilbert space spanned by all possible classical messages that could have been sent.

After applying the isometry U to the returning system and Eve's ancilla from her initial state preparation, she measures the message Hilbert space. The measurement outcome determines the message transcript she sends to Alice while the post measured system represents her quantum ancilla in the event she had sent that message using the quantum instrument attack.

$$U|a, E_a\rangle = \sum_{m \in \{+1,-1\}^N} |m, F_{a,m}\rangle_{ME}$$

M register is Eve's classical message.

Applying U to the state $|\psi_0'\rangle$ yields:

$$|\psi\rangle = \sum_{a \in \{0,1\}^N} \alpha_a |a \wedge \theta\rangle \otimes \sum_{m \in \{+,-\}^N} |m, F_{a,m}\rangle_{cl,E}$$

Eve then measures M to determine the classical message she sends to Alice.

Let's decompose the sum over $a \in \{0,1\}^N$ in $|\psi\rangle$ into 2 parts:

- part where $\theta_i = 0$ (these qubits are reflected by Alice)
- part where $\theta_i = 1$ (these qubits are Measured-Resent by Alice)

Let a_0 be the part of 'a' corresp. to indices where $\theta_i = 0$

a_1 be the part of 'a' corresp. indices where $\theta_i = 1$

$\therefore$ $a = \overline{\Pi}_\theta(a_0, a_1)$ where

$\overline{\Pi}_\theta$: permutation function that rearranges a_0 and a_1 into the original ordering of 'a'.

Here, the length of a_0 = # of 0s in θ

$$|a_0| = ct_0(\theta) \quad \& \quad |a_1| = ct_1(\theta)$$

$$|\Psi\rangle = \sum_{a \in \{0,1\}^N} \alpha_a |a \wedge \Theta\rangle \otimes \sum_{m \in \{+1,-1\}^N} |m, F_{a,m}\rangle_{cl,E}$$

$$= \sum_{a_0, a_1} \alpha_{\pi_\theta(a_0,a_1)} \left|\pi_\theta(0 \cdots 0, a_1)\right\rangle \otimes \sum_{m \in \{+1,-1\}^N} \left|m, F_{\pi_\theta(a_0,a_1),m}\right\rangle_{cl,E} \quad \text{— eq. 5}$$

where $a_0 \in \{0,1\}^{ct_0(\theta)}$ and $a_1 \in \{0,1\}^{ct_1(\theta)}$.

e-QRNG protocol

Assume Eve prepares the initial state:

$$|\tau\rangle_{ACE} = U\left(\sum_{a\in\{0,1\}^{2N}} \alpha_a |a\rangle_A \otimes |E_a\rangle_E\right)$$

$$= \sum_{a\in\{0,1\}^{2N}} \alpha_a |a\rangle_A \otimes \sum_{m\in\{+,-\}^N} |m, F_{a,m}\rangle_{CE}$$

The A and C registers are sent to Alice and the trusted server respectively (as discussed, the trusted server may in fact be Alice in the e-QRNG protocol case).

$$|\tau\rangle = \sum_{a_0,a_1} \alpha_{\pi_\theta(a_0,a_1)} |\pi_\theta(a_0,a_1)\rangle \otimes \sum_m |m, F_{\pi_\theta(a_0,a_1)}\rangle$$

$$|+^2\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

$$= \frac{1}{\sqrt{4}}(|00\rangle+|01\rangle+|10\rangle+|11\rangle) = \frac{1}{\sqrt{2^2}} \sum_{a_0\in\{0,1\}^2} |a_0\rangle$$

$$\therefore |+^m\rangle = \frac{1}{\sqrt{2^m}} \sum_{a_0\in\{0,1\}^m} |a_0\rangle$$

$$\therefore \sum_{a_0\in\{0,1\}^m} |a_0\rangle = \sqrt{2^m}\, |+^m\rangle$$

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$
$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$
$$\Big\} \quad |i\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + (-1)^i |-\rangle\right)$$

$$\therefore |a_0\rangle = |i_1 i_2 \cdots i_m\rangle \quad \text{where} \quad m = ct_0(\theta)$$

$$= |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_m\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle + (-1)^{i_1} |-\rangle\right) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|+\rangle + (-1)^{i_m} |-\rangle\right)$$

$$= \frac{1}{\sqrt{2^m}} |+^m\rangle + b$$

Changing the basis to $\{|+\rangle, |-\rangle\}$ for those qubits of A where $\theta_i = 0$.

$$|\tau\rangle = \frac{1}{\sqrt{2^m}} \sum_{a_0, a_1} \alpha_{\pi_\theta(a_0,a_1)} |\pi_\theta(+^m, a_1)\rangle \otimes \sum_m |m, F_{\pi_\theta(a_0,a_i)}\rangle + |\mu\rangle_{AE}$$

$$\cong \frac{1}{\sqrt{2^{ct_0(\theta)}}} |\psi\rangle + |\mu\rangle \quad ?$$

$m = ct_0(\theta)$: # of times 0 appears in θ (# of times Alice chose to Reflect instead of Measure resend).

where $|\mu\rangle_{AE}$: some state that has at least one $|-\rangle$ where $\theta_i = 0$ in Alice's register, which would lead to protocol aborting.

conditioned on Alice not aborting the e-QRNG protocol (i.e., accepting the state $|\tau\rangle$), the state collapses to $|\psi\rangle$, the same state that would have been produced if the SQRNG protocol had been run.

$\langle\psi|\psi\rangle = 1$ & $\langle\psi|M\rangle = 0$

$\therefore$

The probability of Alice not aborting (i.e., accepting) is exactly $= \frac{1}{\sqrt{2^{ct_0(\Theta)}}} > 0$

Finally, to prove claim (3), we note that if Equation 3 were produced by a collective attack, then Equation 4 would be a product state also and the probability of accepting will remain $\frac{1}{\sqrt{2^{ct_0(\Theta)}}}$ implying that the probability of accepting any particular signal is exactly $1/2$ completing the proof. $\square$

Theorem 1 implies that any attack against the SQRNG protocol (whose security we want to prove) can be translated to an attack against the e-QRNG protocol which: (1) produces the same quantum system for Alice and Eve conditioned on Alice accepting the e-QRNG state (thus any entropy computation will be identical and any observed statistics will also be identical in the accepting case); and (2) the probability of accepting is strictly positive and known. Note that, even though the e-QRNG protocol is highly inefficient, this is not relevant as we are only interested in bounding the quantum entropy of the e-QRNG protocol conditioned on a non-abort. This will translate directly to a bound on the entropy of the SQRNG protocol (which never aborts, unless Alice determines the noise is too high - a threshold which we can compute later). Thus, even though the e-QRNG protocol is highly inefficient, this does not matter as it is only a theoretical tool for the security proof and not an actual protocol to run in practice. Note, also, that there are many more attacks against the e-QRNG protocol, including attacks which would cause it to always abort; however analyzing those "denial of service" attacks are not relevant as they would never appear in the SQRNG protocol.

Secure Bit Rate Analysis

Our goal is to derive an asymptotic bit generation rate for the SQRNG protocol. Consider a run of the SQRNG protocol where Eve employed some (unknown) attack described by $\mathcal{E}$, and Θ was Alice's choice of operations resulting in state $|\psi_{SQRNG}\rangle$. From Theorem 1, there exists an equivalent quantum state $|\psi\rangle$ produced by the e-QRNG protocol. We will derive a bit generation rate for this e-QRNG state which will translate directly to a bit-generation rate for the SQRNG protocol. Since $\mathcal{E}$ and Θ were arbitrary, our method will work for any attack and choice of Θ for the SQRNG protocol thus proving the SQRNG protocol secure.

We first assume collective attacks for the SQRNG protocol (and thus, by condition (3) of Theorem 1 also for the e-QRNG protocol state); namely, the state $|\psi\rangle$ may be described as a product state $|\psi\rangle = |\mu\rangle^{\otimes N}$ with the probability of accepting any particular signal state $|\mu\rangle$ is $1/2$ (i.e., the probability of Alice observing a $|+\rangle$ in $|\mu\rangle$ is $1/2$) .

$$|\mu\rangle = \sum_{a\in\{0,1\}} \sum_{c\in\{+,-\}} |a\rangle_A \otimes |c\rangle_C \otimes |e_{a,c}\rangle_E$$

$$= \sum_{a,c\in\{0,1\}} |a,c\rangle_{AC} \otimes |e_{a,c}\rangle_E \qquad \text{— eq. 6}$$

where the $|e_{a,c}\rangle$ states are arbitrary (not necessarily normalized nor orthogonal) states in Eve's ancilla. Note that, when $c = 0$ in the summation we actually mean a state of $|+\rangle$ while $c = 1$ implies $|-\rangle$.

Now,

$$P(A=a \wedge C=c) = P_{a,c}^{AC} = \left(\langle a,c| \otimes \langle e_{a,c}|\right)\left(\sum_{a',c'\in\{0,1\}} |a',c'\rangle \otimes |e_{a',c'}\rangle\right)$$

$$= \langle e_{a,c} | e_{a,c} \rangle$$

$= \frac{1}{4}$ ideally because there are 4 possible measurement outcomes.

Consider,

$$P(C=+ \mid \text{accept}) = P_{+|acc}$$

$$|\mu\rangle = \sum_c \sum_{a\in\{0,1\}} \frac{1}{\sqrt{2}}\left(|+\rangle + (-1)^a|-\rangle\right)\otimes|c\rangle\otimes|e_{a,c}\rangle$$

$$= \frac{1}{\sqrt{2}}|+\rangle\otimes\sum_c|c\rangle\otimes\left(|e_{0,c}\rangle+|e_{1,c}\rangle\right) + \frac{1}{\sqrt{2}}|-\rangle\otimes\sum_c|c\rangle\otimes\sum_a(-1)^a|e_{a,c}\rangle$$

$$= \frac{1}{\sqrt{2}}|+\rangle\otimes\sum_c|c\rangle\otimes\left(|e_{0,c}\rangle+|e_{1,c}\rangle\right) +$$

$$\frac{1}{\sqrt{2}}|-\rangle\otimes\sum_c|c\rangle\otimes\left(|e_{0,c}\rangle-|e_{1,c}\rangle\right)$$

Theorem 1 $\Rightarrow$ Alice measuring $|+\rangle$ (accepting) happens coith probability $1/2$ for each signal state independently.

The measurement collapses $|\mu\rangle$ to the corresponding state with $|+\rangle_A$ & the state is now conditioned on Alice's measurement outcome being $|+\rangle$.

The conditional state collapses to:

$$|+\rangle_A\otimes\underbrace{\left[|0\rangle_c\otimes\left(|e_{0,0}\rangle+|e_{1,0}\rangle\right)+|1\rangle_c\otimes\left(|e_{0,1}\rangle+|e_{1,1}\rangle\right)\right]}_{|\mu'\rangle}$$

$$P_{+|acc} = \left[\langle 0| \otimes \left(\langle e_{0,0}| + \langle e_{1,0}|\right)\right] |M'\rangle = P\left(C = + \,|\, accept\right)$$

$$= \left(\langle e_{0,0}| + \langle e_{1,0}|\right)\left(|e_{0,0}\rangle + |e_{1,0}\rangle\right)$$

$$= \langle e_{0,0}|e_{0,0}\rangle + \langle e_{1,0}|e_{1,0}\rangle + 2\,\mathrm{Re}\,\langle e_{0,0}|e_{1,0}\rangle$$

Similarly,

$$P_{-|acc} = \langle e_{0,1}|e_{0,1}\rangle + \langle e_{1,1}|e_{1,1}\rangle + 2\,\mathrm{Re}\,\langle e_{0,1}|e_{1,1}\rangle$$

- $P_{+|acc}$ $(P_{-|acc})$ coincide directly with the probability the server sends the message $+$ $(-)$ conditioned on Alice choosing Reflect in the SQRNG case.

$$|M\rangle = \sum_{a\in\{0,1\}} \sum_{c\in\{+,-\}} |a\rangle_A \otimes |c\rangle_C \otimes |e_{a,c}\rangle_E$$

$$= \sum_{a,c\in\{0,1\}} |a,c\rangle_{AC} \otimes |e_{a,c}\rangle_E$$

Measuring in the Z basis collapses Alice's state to either $|0\rangle$ or $|1\rangle$.

If Alice measures 0, the post-measurement state collapses to: $|0\rangle \otimes \sum_c |c\rangle \otimes |e_{0,c}\rangle = \Pi_0 |M\rangle$ $\left[\Pi_i = |i\rangle\langle i|\right.$

If Alice measures 1, the post-measurement state collapses to: $|1\rangle \otimes \sum_c |c\rangle \otimes |e_{1,c}\rangle = \Pi_1 |M\rangle$

∴ The state after Alice's measurement in the Z basis is a probabilistic mixture of the states corresponding to measurement outcomes $a=0$ and $a=1$.

$$\rho^{(0)}_{ACE} = \left(|0\rangle \otimes \sum_c |c\rangle \otimes |e_{0,c}\rangle\right)\left(\langle 0| \otimes \sum_{c'} \langle c'| \otimes \langle e_{0,c'}|\right)$$

$$= |0\rangle\langle 0| \otimes \sum_{c,c'} |c\rangle\langle c'| \otimes |e_{0,c}\rangle\langle e_{0,c'}|$$

$$\mathrm{tr}\left(\tilde{\rho}^{(a)}_{ACE}\right) = \mathrm{tr}\left(|a\rangle\langle a|\right)\cdot \sum_c \mathrm{tr}\left(|c\rangle\langle c|\right)\cdot \mathrm{tr}\left(|e_{a,c}\rangle\langle e_{a,c}|\right)$$

$$= \sum_c \langle e_{a,c}|e_{a,c}\rangle = \sum_c P^{AC}_{a,c} = P(A=a)$$

$$\rho^{(a)}_{ACE} = \frac{\tilde{\rho}^{(a)}_{ACE}}{P(A=a)}$$

$$\rho_{ACE} = \sum_a P(A=a)\,\rho^{(a)}_{ACE}$$

$$= \sum_a P(A=a)\,\frac{|a\rangle\langle a| \otimes \sum_c |c\rangle\langle c| \otimes |e_{a,c}\rangle\langle e_{a,c}|}{P(A=a)}$$

$$= \sum_a |a\rangle\langle a| \otimes \sum_c |c\rangle\langle c| \otimes |e_{a,c}\rangle\langle e_{a,c}|$$

$$= \sum_a |a\rangle\langle a| \otimes \left(\sum_c |c, e_{a,c}\rangle\langle c, e_{a,c}|\right)$$

$$= \sum_a [a] \otimes \sum_c [c, e_{a,c}]$$

$$= [0]_A \otimes \left(\sum_c [c, e_{0,c}]\right) + [1]_A \otimes \left(\sum_c [c, e_{1,c}]\right)$$

— eq. 7

Changing the order of systems A & C,

$$\rho_{ACE} = \sum_c P(C=c)|c\rangle\langle c| \otimes \left[\sum_a \frac{P^{AC}_{a,c}}{P(C=c)} |a\rangle\langle a| \otimes |e_{a,c}\rangle\langle e_{a,c}| \right]$$

$$S\left(\sum_a \frac{P^{AC}_{a,c}}{P(C=c)} |a\rangle\langle a| \otimes |e_{a,c}\rangle\langle e_{a,c}|\right) = h\left(\frac{P^{AC}_{0,c}}{P(C=c)}\right)$$

$$S(ACE) = h(P(C=c)) + \sum_c P(C=c)\, h\left(\frac{P^{AC}_{0,c}}{P(C=c)}\right)$$

$$S(ACE) = h\left(P^{AC}_{0,0} + P^{AC}_{1,0}\right) + \sum_c \left(P^{AC}_{0,c} + P^{AC}_{1,c}\right) h\left(\frac{P^{AC}_{0,c}}{P^{AC}_{0,c} + P^{AC}_{1,c}}\right)$$

⑤ Joint entropy theorem

Suppose P_i are probabilities, $|i\rangle$ are orthogonal states for a system A, and ρ_i is any set of density operators for another system B. Then,

$$S\left(\sum_i P_i |i\rangle\langle i| \otimes \rho_i\right) = H(P_i) + \sum_i P_i S(\rho_i)$$

s.t $h(x) = -x \log x - (1-x)\log(1-x)$ is the Binary entropy function.

$$\rho_{CE} = tr_A(\rho_{ACE}) = \sum_a (I \otimes \langle a| \otimes I)\, \rho_{ACE}\, (I \otimes |a\rangle \otimes I)$$

$$\rho_{CE} = \sum_c P(C=c)\, |c\rangle\langle c| \otimes \left(\sum_a \frac{P^{AC}_{a,c}}{P(C=c)} \frac{|e_{a,c}\rangle\langle e_{a,c}|}{P^{AC}_{a,c}} \right)$$

$$\sum_a \frac{P^{AC}_{a,c}}{P(C=c)} \frac{|e_{a,c}\rangle\langle e_{a,c}|}{P^{AC}_{a,c}} = \rho^{(E)}$$

$$\boxed{\alpha = \langle e_{0,c} | e_{1,c}\rangle \qquad \alpha^* = \langle e_{1,c} | e_{0,c}\rangle}$$

$$\rho^{(E)}_{0,0} = \frac{1}{P(C=c)} \left(|\langle e_{0,c} | e_{0,c}\rangle|^2 + |\langle e_{0,c} | e_{1,c}\rangle|^2 \right) = \frac{(P^{AC}_{0,c})^2 + |\alpha|^2}{P^{AC}_{0,c} + P^{AC}_{1,c}}$$

$$\rho^{(E)}_{0,1} = \frac{1}{P(C=c)} \left(\langle e_{0,c} | e_{0,c}\rangle\langle e_{0,c} | e_{1,c}\rangle + \langle e_{0,c} | e_{1,c}\rangle\langle e_{1,c} | e_{1,c}\rangle \right)$$

$$= \frac{\langle e_{0,c} | e_{1,c}\rangle}{P(C=c)} \left(\langle e_{0,c} | e_{0,c}\rangle + \langle e_{1,c} | e_{1,c}\rangle \right) = \frac{\alpha (P^{AC}_{0,c} + P^{AC}_{1,c})}{P^{AC}_{0,c} + P^{AC}_{1,c}} = \alpha$$

$$\rho^{(E)}_{1,0} = \frac{1}{P(C=c)} \left(\langle e_{1,c} | e_{0,c}\rangle\langle e_{0,c} | e_{0,c}\rangle + \langle e_{1,c} | e_{1,c}\rangle\langle e_{1,c} | e_{0,c}\rangle \right)$$

$$= \frac{\langle e_{1,c} | e_{0,c}\rangle}{P(C=c)} \left(P(C=c) \right) = \alpha^*$$

$$\rho^{(E)}_{1,1} = \frac{1}{P(C=c)} \left(\langle e_{1,c} | e_{0,c}\rangle\langle e_{0,c} | e_{1,c}\rangle + \langle e_{1,c} | e_{1,c}\rangle\langle e_{1,c} | e_{1,c}\rangle \right)$$

$$= \frac{1}{P(C=c)} \left(|\alpha|^2 + (P^{AC}_{1,c})^2 \right) = \frac{|\alpha|^2 + P^{AC}_{1,c}}{P^{AC}_{0,c} + P^{AC}_{1,c}}$$

$$\sum_a \frac{P^{AC}_{a|c}}{P(C=c)} \frac{|e_{a|c}\rangle\langle e_{a|c}|}{P^{AC}_{a|c}} = \rho^{(E)} = \frac{1}{P^{AC}_{0,c} + P^{AC}_{1,c}} \begin{bmatrix} (P_{0,c})^2 + |\alpha|^2 & \alpha^* \\ \alpha & |\alpha|^2 + (P_{1,c})^2 \end{bmatrix}$$

$$H = \begin{bmatrix} a & d \\ d^* & b \end{bmatrix} \Rightarrow tr(H) = a+b = \lambda_1 + \lambda_2$$

$$\det(H) = ab - |d|^2 = \lambda_1 \lambda_2$$

$$|H - \lambda I| = 0 = \begin{vmatrix} a-\lambda & d \\ d^* & b-\lambda \end{vmatrix} = \lambda^2 - (a+b)\lambda + ab - |d|^2 = 0$$

$$\lambda = \frac{(a+b) \pm \sqrt{(a+b)^2 - 4(ab - |d|^2)}}{2}$$

$$= \frac{(a+b) \pm \sqrt{(a-b)^2 + 4|d|^2}}{2}$$

$$tr(\rho^{(E)}) = 1 \Longrightarrow 2|\alpha|^2 + (P^{AC}_{0|c})^2 + (P^{AC}_{1,c})^2 = P^{AC}_{0|c} + P^{AC}_{1|c}$$

in any basis

$$\lambda_\pm = \frac{1}{2}\left[1 \pm \sqrt{\frac{((P^{AC}_{0,c})^2 - (P^{AC}_{1|c})^2)^2}{(P^{AC}_{0|c} + P^{AC}_{1|c})^2} + 4\frac{|\alpha|^2}{(P^{AC}_{0|c} + P^{AC}_{1|c})^2}}\right]$$

$$= \frac{1}{2}\left[1 \pm \frac{\sqrt{((P^{AC}_{0|c} - P^{AC}_{1,c})(P^{AC}_{0|c} + P^{AC}_{1|c}))^2 - 4|\alpha|^2}}{P^{AC}_{0|c} + P^{AC}_{1|c}}\right]$$

* Seems to differ slightly from the paper. (eq. 9)

$$S(\rho^{(E)}) = h(\lambda_+) = h(\lambda'_c)$$

$$\rho_{CE} = \sum_c P(C=c)\,|c\rangle\langle c| \otimes \left(\sum_a \frac{P^{AC}_{a,c}}{P(C=c)} \frac{|e_{a,c}\rangle\langle e_{a,c}|}{P^{AC}_{a,c}} \right)$$

$$= \sum_c P(C=c)\,|c\rangle\langle c| \otimes \rho_c^{(E)}$$

$$S(\rho_{CE}) = h(P(C=0)) + \sum_c P(C=c)\, h(\lambda'_c)$$

$$= h\left(P^{AC}_{0,0} + P^{AC}_{1,0}\right) + \sum_c \left(P^{AC}_{0,c} + P^{AC}_{1,c}\right) h(\lambda'_c)$$

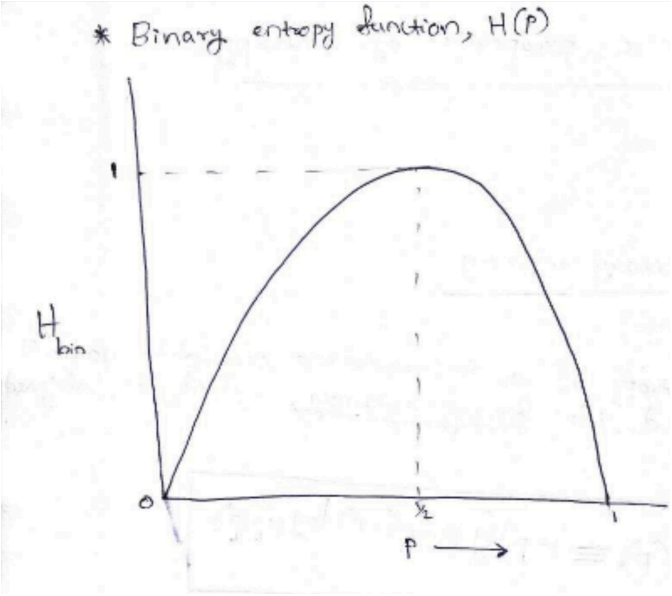
$$S(ACE) = h\left(P^{AC}_{0,0} + P^{AC}_{1,0}\right) + \sum_c \left(P^{AC}_{0,c} + P^{AC}_{1,c}\right) h\left(\frac{P^{AC}_{0,c}}{P^{AC}_{0,c} + P^{AC}_{1,c}}\right)$$

$$S(A|CE) = S(ACE) - S(CE)$$

$$= \left(P^{AC}_{0,0} + P^{AC}_{1,0}\right)\left[h\left(\frac{P^{AC}_{0,0}}{P^{AC}_{0,0} + P^{AC}_{1,0}}\right) - h(\lambda'_0) \right]$$

$$+ \left(P^{AC}_{0,1} + P^{AC}_{1,1}\right)\left[h\left(\frac{P^{AC}_{0,1}}{P^{AC}_{0,1} + P^{AC}_{1,1}}\right) - h(\lambda'_1) \right]$$

* Binary entropy function, $H(p)$



$$\lambda_c' = \frac{1}{2} + \Delta \quad \text{where } \Delta > 0$$

Δ increases as $\alpha = \langle e_{0,c} | e_{1,c} \rangle$ increases.

$\Rightarrow h(\lambda_c')$ decreases

$\Rightarrow S(CE)$ decreases

$\therefore S(A|CE) = S(ACE) - S(CE)$ min. when $S(CE)$ is max

ie., $\alpha = \langle e_{0,c} | e_{1,c} \rangle$ is min.

Thus,

$$|\alpha|^2 = (\mathrm{Re}(\alpha))^2 + (\mathrm{Im}(\alpha))^2 \geq (\mathrm{Re}(\alpha))^2 = \mathrm{Re}^2 \langle e_{0,c} | e_{1,c} \rangle$$

$$\Rightarrow \lambda_c' \geq \frac{1}{2}\left[1 + \frac{\sqrt{\left(P_{0,c}^{AC} - P_{1,c}^{AC}\right)\left(P_{0,c}^{AC} + P_{1,c}^{AC}\right)^2 - 4\,\mathrm{Re}^2 \langle e_{0,c} | e_{1,c} \rangle}}{P_{0,c}^{AC} + P_{1,c}^{AC}}\right] = \lambda_c$$

— eq. 9

* Eq. 9 seems to differ slightly from the paper, with the term $P_{0,c}^{AC} + P_{1,c}^{AC}$?

where, $P_{+|ac} = \langle e_{0,0} | e_{0,0} \rangle + \langle e_{1,0} | e_{1,0} \rangle + 2\,\mathrm{Re} \langle e_{0,0} | e_{1,0} \rangle$

$$S(A|CE) = S(ACE) - S(CE)$$

$$= \left(P_{0,0}^{AC} + P_{1,0}^{AC}\right)\left[h\left(\frac{P_{0,0}^{AC}}{P_{0,0}^{AC} + P_{1,0}^{AC}}\right) - h(\lambda_0')\right]$$

$$+ \left(P_{0,1}^{AC} + P_{1,1}^{AC}\right)\left[h\left(\frac{P_{0,1}^{AC}}{P_{0,1}^{AC} + P_{1,1}^{AC}}\right) - h(\lambda_1')\right]$$

$$\geq \left(P_{0,0}^{AC} + P_{1,0}^{AC}\right)\left[h\left(\frac{P_{0,0}^{AC}}{P_{0,0}^{AC} + P_{1,0}^{AC}}\right) - h(\lambda_0)\right]$$

$$+ \left(P_{0,1}^{AC} + P_{1,1}^{AC}\right)\left[h\left(\frac{P_{0,1}^{AC}}{P_{0,1}^{AC} + P_{1,1}^{AC}}\right) - h(\lambda_1)\right]$$

—— eq. 8

$\Rightarrow$ This enable us to compute the quantum entropy of the e-QRNG case conditioned on the protocol not aborting.

$\Rightarrow$ bound on the random bit generation rate.