Device Independent Randomness Extraction for Arbitrarily Weak Min-Entropy Source

Jan Bouda, Marcin Pawłowski, Matej Pivoluska, Martin Plesch

6.6.2014

Outline

- Motivation and Related Work.
- Ingredients.
- Our Protocol.

Importance of Randomness

Randomness is useful in:

- Gambling.
- Simulation and Computation.
- Cryptography.

Importance of Randomness

Randomness is useful in:

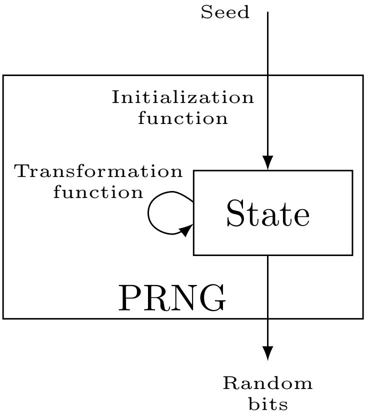
- Gambling.
- Simulation and Computation.
- Cryptography.

Impact of imperfect randomness can be devastating:

- Attacks on RSA [Lenstra et. al. (2012)]
- Attacks on QKD[Bouda et. al. (2012), Huber and Pawłowski (2013)]

Randomness Production + Testing

- **Pseudorandomness**
- Classical Hardware
- Quantum Hardware



Randomness Production + Testing

- Pseudorandomness
- **Classical Hardware**
- Quantum Hardware

Randomness Production + Testing

- Pseudorandomness
- Classical Hardware
- **Quantum Hardware**

Randomness Production + Testing

- Pseudorandomness
- Classical Hardware
- Quantum Hardware

- Statistical tests vs. Unpredictability
- Official certification

Random Number Generator Certificate

Operator: Entraction Solutions AB **URL:** www.entraction.com

This is to certify that iTech Labs has evaluated the Random Number Generator (RNG) used by Entraction Solutions AB and found that the RNG complies with the relevant standards.*

The RNG uses a widely recognized algorithm to generate random numbers. The numbers generated by this RNG have passed Marsaglia's "diehard" tests for statistical randomness.

iTech Labs has also evaluated the shuffling for 52 card decks and 32 card decks. Each shuffling test was conducted on samples ranging from 1,000 to 100,000 deals for a total of over one million deals.

iTech Labs has found that the card sequences are unpredictable, non-repeatable and uniformly distributed.

The certified code for the RNG has been fingerprinted.

Click here to view the Original iTech Labs Certificate.

Signed:

Ian Manning
Principal Consultant
iTech Labs Australia

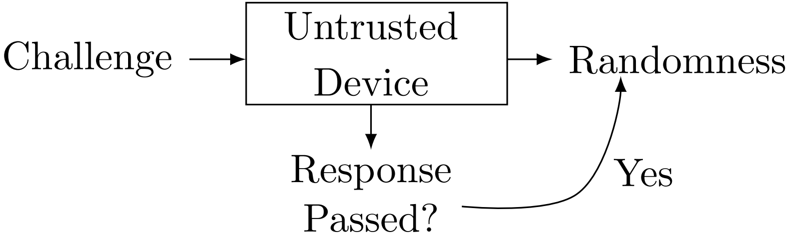
20 February 2010

* The RNG was tested according to relevant Isle of Man Gambling Supervision Commission, Alderney Gambling Control Commission (AGCC), UK Gambling Commission and Malta Lotteries & Gaming Authority standards. The software provider or operator of the gaming site may not necessarily be licensed in the gaming regulatory jurisdiction whose technical standards have been applied in the testing process. Before making enquiries with the gaming commission, check whether the gaming commission's logo is present on the gaming site's home page or undertake independent enquiries with the operator of the website.

Disclaimer.
While it is not possible to test all possible scenarios in a laboratory environment, iTech Labs has conducted a level of testing appropriate for a component test of this type.

iTech Labs Australia ACN 108 249 761 www.itechlabs.com.au
Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia. Tel. +61 3 9561 9955
iTech Labs is an IEC/ISO 17025 accredited testing laboratory

Device Independent Approach



- Challenges have to be random.
- Similarity to randomness extraction.

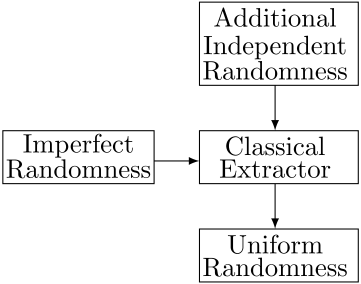
Randomness Extraction

- Randomness extraction is a procedure to transform imperfect randomness into (close to) perfect randomness.

Randomness Extraction

- Randomness extraction is a procedure to transform imperfect randomness into (close to) perfect randomness.

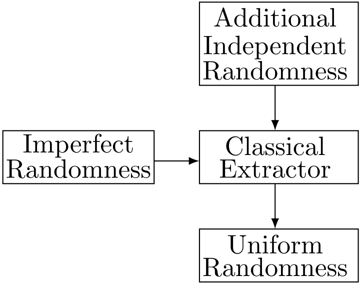
Classical Extraction



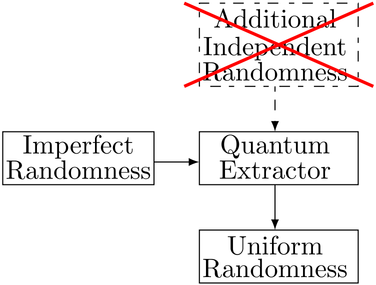
Randomness Extraction

- Randomness extraction is a procedure to transform imperfect randomness into (close to) perfect randomness.

Classical Extraction



Quantum Extraction



Related work

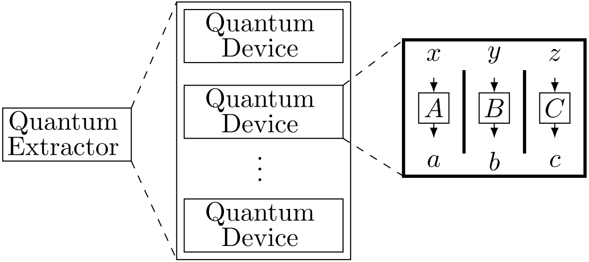
Santha-Vazirani sources

- Colbeck and Renner (2012).
- Gallego et. al. (2013).
- Brandão et. al. (2013).

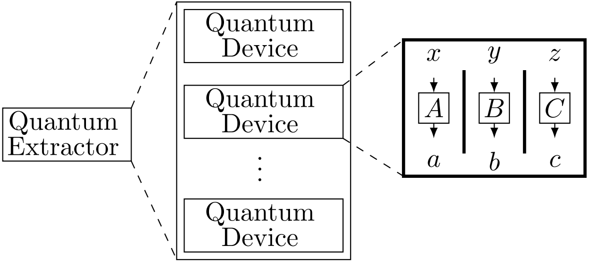
Min-Entropy sources

- Chung, Shi, Wu (2014).
- This presentation.

Quantum Device - GHZ test



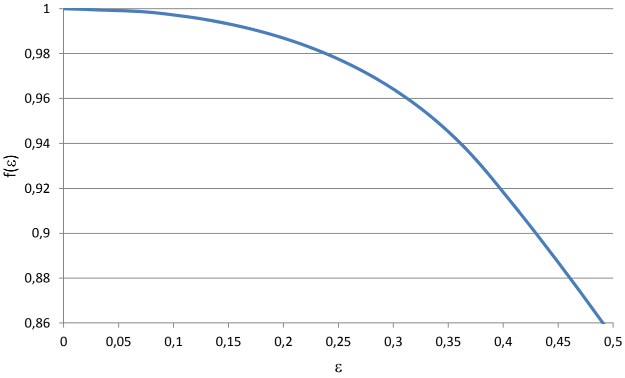
Quantum Device - GHZ test



- Input $xyz \in \{111, 001, 010, 100\}$.
- Test if $a \oplus b \oplus c = x \cdot y \cdot z$.
- Classical strategies succeed with probability at most 3/4.
- Quantum strategy succeeds with probability 1 and produces perfect random bits.

GHZ devices - rigidity (MP bound)

- Let inputs into D_i be uniform.
- If D_i wins GHZ game with probability $p > f(\epsilon)$ then bias of a_m is at most ϵ.
- Function $f(\epsilon)$ obtained by SDP.



Weak Source of Randomness - Definition

Source of randomness $\{X_i\}_{i\in\mathbb{N}}$ is (n,k) *block source* if

- X_i is random variable with n bit output.
- It holds that

$$\forall x_1,\ldots,x_{i-1}\in\{0,1\}^n, \forall e\in\mathcal{I}(E),$$
$$H_\infty(X_i|X_{i-1}=x_{i-1},\ldots,X_1=x_1,E=e)\geq k.$$

- H_∞ is min-entropy.

Weak Source of Randomness - Definition

Source of randomness $\{X_i\}_{i\in\mathbb{N}}$ is (n,k) *block source* if

- X_i is random variable with n bit output.
- It holds that

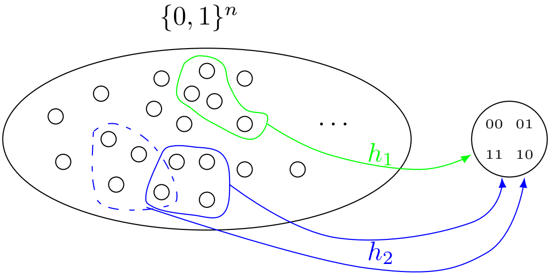
$$\forall x_1,\ldots,x_{i-1}\in\{0,1\}^n, \forall e\in\mathcal{I}(E),$$
$$H_\infty(X_i|X_{i-1}=x_{i-1},\ldots,X_1=x_1,E=e)\geq k.$$

- H_∞ is min-entropy.

Notes:

- Classically cannot be extracted.
- For $n=1$ Santha–Vazirani (SV) source is recovered.
- For $n>1$ cannot be transformed into SV source – existing protocols do not work.

Set of Hashing Functions

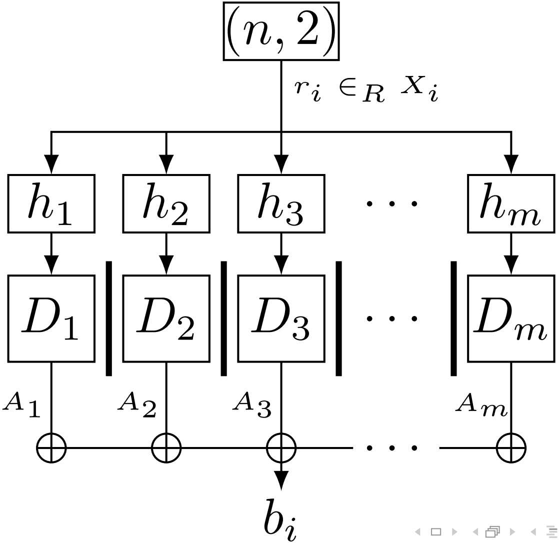


- Let $h_i : \{0,1\}^n \mapsto \{0,1\}^2$.
- Let $H = \{h_i\}_{i=1}^m$.
- For each subset S of $\{0,1\}^n$ of size 4 there exists h_i, such that $h_i(S) = \{00, 01, 10, 11\}$.
- There is a construction of H with size polynomial in n.

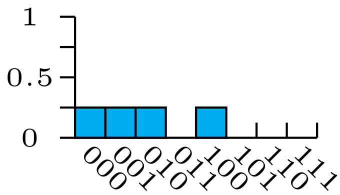
One Round of Protocol

1. We obtain the (weakly) random n bit string r_i from an $(n, 2)$ block source.
2. Into each device D_i we input the 3 bit string – inputs X_i, Y_i and Z_i derived from $h_i(r_i)$ – and obtain the outputs A_i, B_i and C_i.
3. We verify whether for each device D_i the condition $Z_i \oplus Y_i \oplus Z_i = A_i \cdot B_i \cdot C_i$ holds. If this is not true, we abort the protocol.
4. We define the output bit of the protocol as $b_i = \bigoplus_{j=1}^{m} A_j$.

Protocol – Scheme

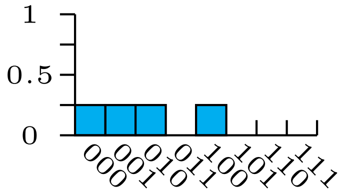


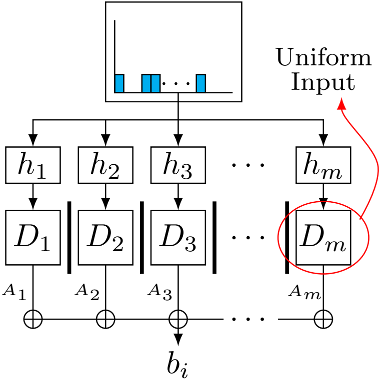
Single Round Analysis - The Flat Sources



- $(n, 2)$ flat source – 4 elements of $\{0,1\}^n$ with probability $\frac{1}{4}$, others with probability 0.

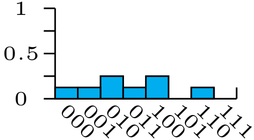
Single Round Analysis - The Flat Sources



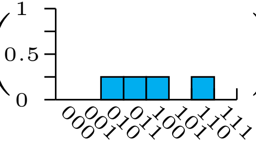
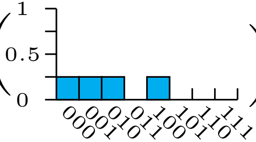


- $(n, 2)$ flat source – 4 elements of $\{0, 1\}^n$ with probability $\frac{1}{4}$, others with probability 0.

Single Round Analysis - The Non-Flat Sources

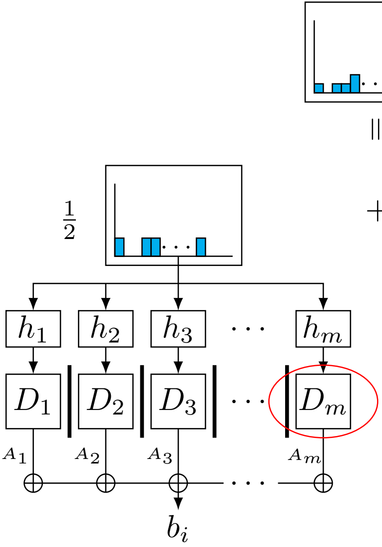


$$=$$

$\frac{1}{2}\Big($  $\Big) + \frac{1}{2}\Big($  $\Big)$

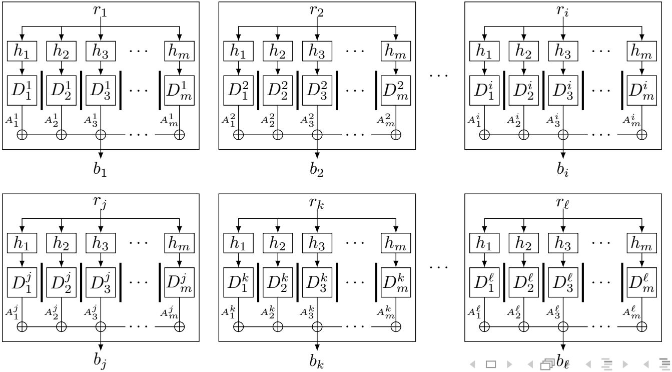
- Any $(n, 2)$ distribution d can be expressed as a convex combination of at most $N = 2^n$ $(n, 2)$ flat distributions d_i.

Single Round Analysis - The Non-Flat Sources II



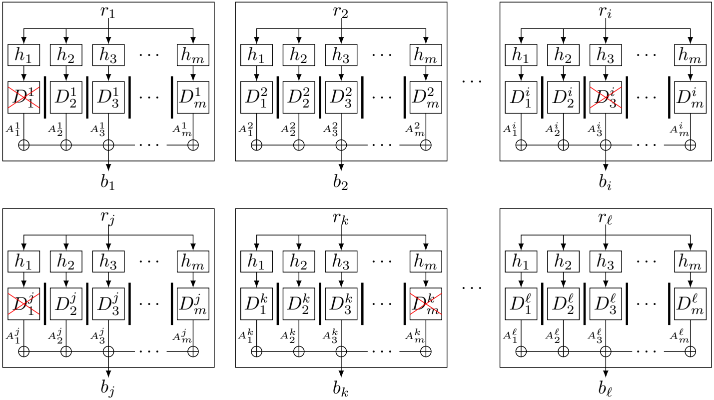
Multiple Rounds

- Repeat the protocol ℓ times. Output $b = \bigoplus_{j=1}^{l} b_j$.
- If b has bias greater than ϵ, each of b_i has bias at least ϵ.
- To achieve bias ϵ adversary has to risk ℓ times - success $f(\epsilon)^\ell$.
- For target parameters ϵ, δ set $\ell > \log \delta / \log f(\epsilon)$



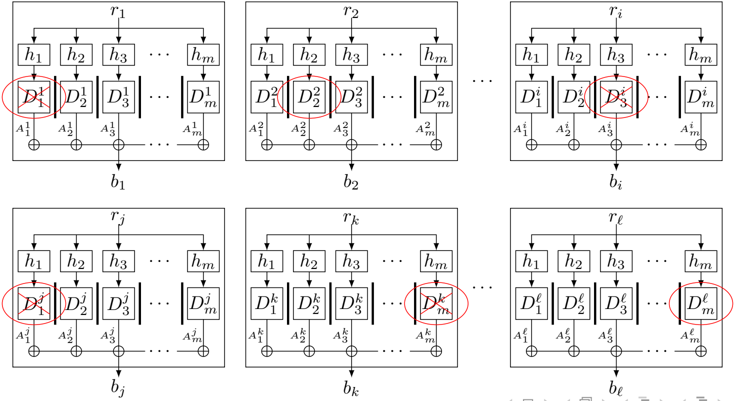
Robustness - Imperfect Honest Devices

- Let us allow $\mu = \frac{1-f(\epsilon)}{2m}$ fraction of all the $m\ell$ devices to fail the test.
- Then honest but faulty devices with failure probability $\mu/2$ pass the protocol with high probability.



Malicious Devices

- Adversary needs to cheat for devices with uniform input.
- By increasing number of rounds we can make sure that (a lot) less errors are allowed than the number of devices adversary needs to cheat.



Conclusion

- Protocol uses arbitrary block source.
- Protocol produces single bit biased at most ϵ with probability $1 - \delta$ for arbitrary ϵ, δ.
- Number of devices used scales polynomially with the length of the block.

Conclusion

- Protocol uses arbitrary block source.
- Protocol produces single bit biased at most ϵ with probability $1 - \delta$ for arbitrary ϵ, δ.
- Number of devices used scales polynomially with the length of the block.

THANK YOU!