Randomness amplification against no-signaling adversaries using two devices

F.G.S.L Brandao[1], R. Ramanathan[2]
A. Grudka[3], K. [4], M. [5],P. [6] Horodeccy,
H. Wojewódka [5]

[1]Department of Computer Science, University College London
[2]National Quantum Information Centre in Gdańsku, Sopot
[3]Department of Physics, Adam Mickiewicz University, Poznań
[4]Institute of Informatics, University of Gdańsk, Gdańsk
[5]Institute of Theoretical Physics and Astrophysic, University of Gdańsk, Gdańsk
[6]Department of Physics and Applied Math, Technical University of Gdańsk, Gdańsk

[arXiv:1506.00509]

Qcrypt 2015
Hitotsubashi University Tokyo

Outline

- Scenario of device independent randomness amplification
- State of the art
- Setup of our protocol
- The result
- Main new ingredients of our techniques
- Bell inequality from contextuality
- Chernoff-like bound for SV sources
- Open problems

The weak sources of randomness and amplification

Santha-Vasirani ($\epsilon - SV$) source: sequence E,T_1 …. T_n satisfying

$$\frac{1}{2} - \epsilon \leq P(t_i \,|t_{i-1}, t_{i-2} \ldots t_1, e) \leq \frac{1}{2} + \epsilon$$

Scenario:

Honest parties have access to SV and additional devices

Task: generate fully random bits

Type of security: independent of device the proof of security bases solely on the statistics of the outcomes of the devices

Assumption: the honest parties do not signal to adversary and vice versa and do not signal to each other

Remark1: The honest parties does not need to know quantum mechanics

Remark2: Quantum mechanics is only used by the honest provider to build good devices

Remark3: Adversary may be supra-quantum

SV based Randomness Amplification state of the art

1984 [Santha & Vasirani]: Randomness Amplification (RA) is impossible using single weak source

2012: [Colbeck & Renner:] RA is possible using SV and quantum devices
2 parties, 2 devices , too many settings , not full range of epsilon, no tolerance of noise

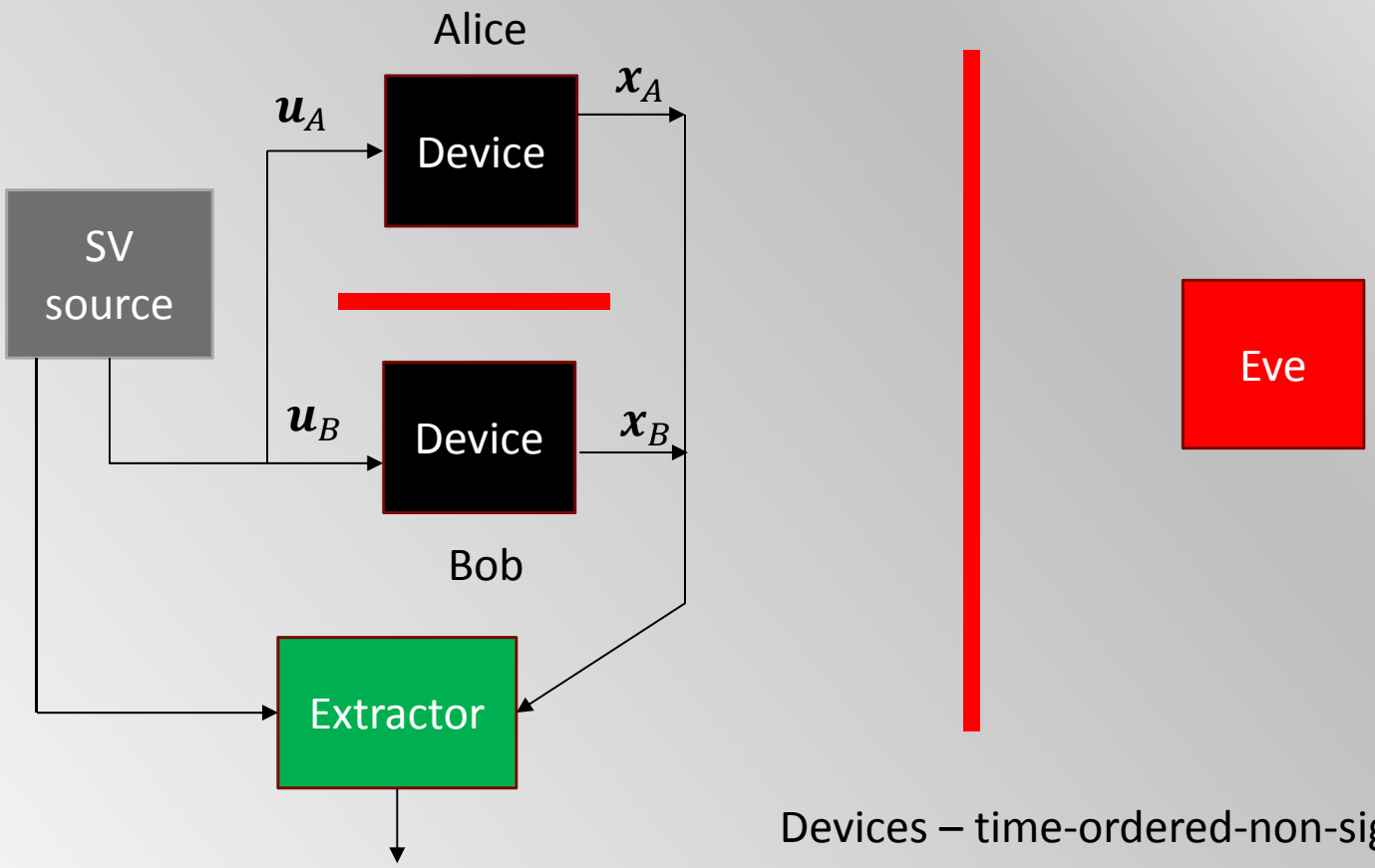
2013: [Gallego et al.]: RA is possible for full range of epsilon
5 parties, infinit number of devices, no tolerance of noise, unknown hash function

2014: [Grudka et al., Mironowicz et al., Augusiak et al.] further related results and partial improvements

2015: [Brandao et al.] control of noise, explicit extractors, zero rate
4-parties, 8 devices

Setup of the protocol

$$P(x_A x_B | u_A, u_B)$$



Devices – time-ordered-non-signaling

Extractor- deterministic function

The results: achievement of our protocol

2 parties + 2 devices + SV source + explicit extractor

$\Rightarrow$

1) Fully random secure bits for $\epsilon < \frac{\sqrt{2}-1}{2} \approx 0.2$
   - non-zero rate
   - noise tolerance

2) Fully random secure bit for $\epsilon \in (0, \frac{1}{2})$
   - single bit of output
   - noise tolerance

Depending on the choice of extractor [R.Raz 2005] or [E. Chattopadhyay and D. Zuckerman 20015]

2 parties + 2 devices + SV source + non-explicit extractor

$\Rightarrow$

Fully random secure bit for $\epsilon \in (0, \frac{1}{2})$
- non-zero rate
- noise tolerance

[arXiv:1506.00509]

Possible questions and answers

Basic idea: violation of Bell inequality => devices are to some extent random. They can be strongly or weakly random

Question: Do we follow recent result for 4 parties and 8 devices to make it 2 parties and 2 devices ?
Answer: No, (hard to take this way)

Question: What is the a difference ?
Answer:

1) Weak Bell inequality is sufficient
2) The Bell inequality is directly from contextuality
3) Ingredient: Chernoff-like property of SV source

Strong and weak Bell inequalities

Box - single-use device

Def. Bell inequality is strong if

every box which violates it maximally, for **every input and output** forms a 1-bit SV source itself

$$\exists f \quad \exists \gamma < \frac{1}{2} \quad \forall u \quad \forall\, P(x|u) \sim B \;:\; \frac{1}{2} - \gamma \leq P(f(x)|u) \leq \frac{1}{2} + \gamma$$

Hash function — For every input — If P violates B maximally — We have SV source with $\epsilon = \gamma$

[Papers by Gallego et al. An Brandao et. Al. use Bell inequalities implying strong randomness]

Def. Bell inequality is weak if

single input and single otuput has an upper bound on the probability of its occurence for every box maximally violating B

$$\exists (u^*, x^*), \qquad \exists \gamma < \frac{1}{2} \quad \forall P(x|u) \sim B \qquad 0 \leq P(x = x^* | u = u^*) \leq \frac{1}{2} + \gamma$$

Single input output pair — Upper bound

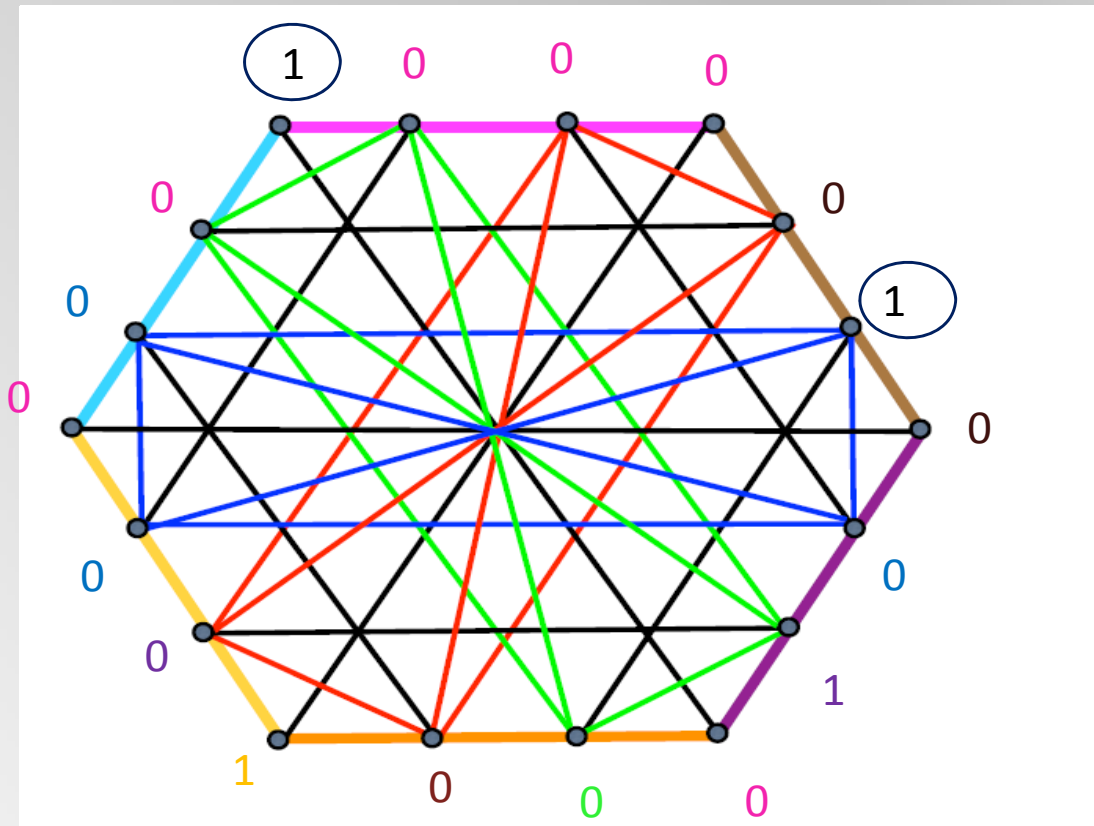
Towards weak Bell inquality via non-determinizm based on contextuality

Can the set of projectors be predetermined to set a pair deterministically to occur with probability 1 ? No ! Proof by contradiction

Vertex - projector

Clique of size 4 vN measurement (9 of them)

Orthogonal Projectors - connected by edge



Error:
Red clique has no 1 assigned only zeros.

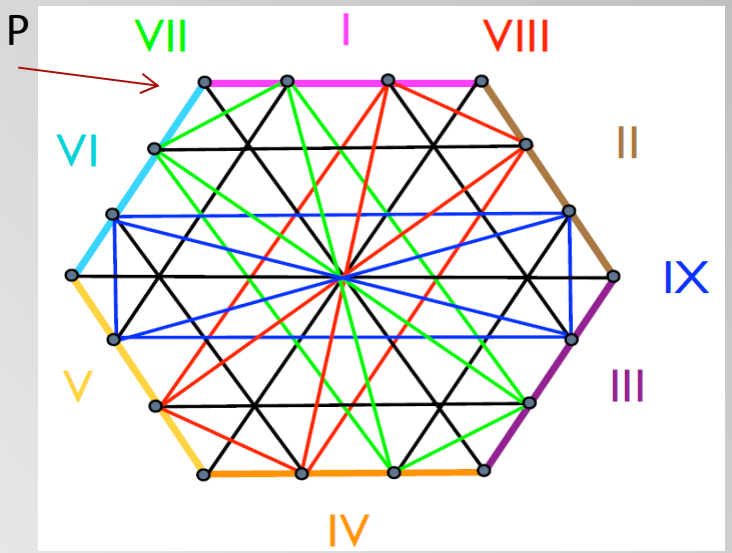
Conclusion:
The two projectors can not be both predetermined with probability 1

[Kochen and Specker 1967]

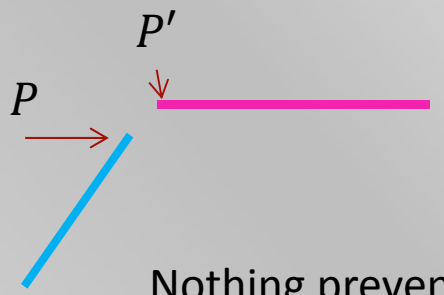
[A. Cabello 2008]

[see in this context Claudes and Svocil 2009]

From Contextuality to Bell inequality and why



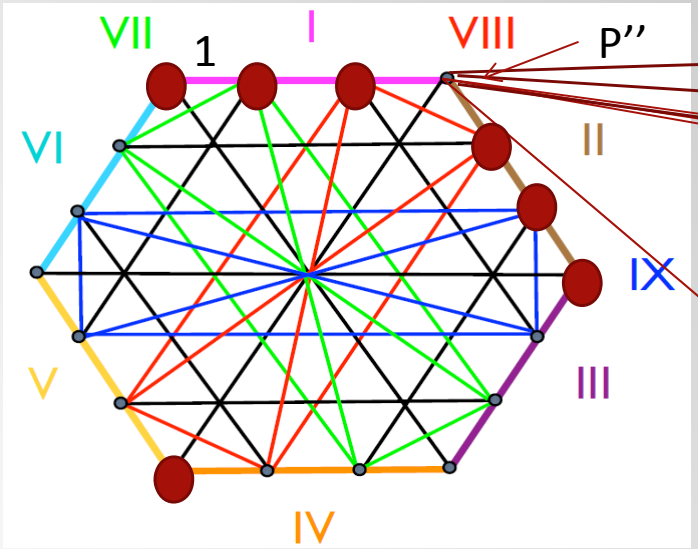
Single-party box
does not imply randomness

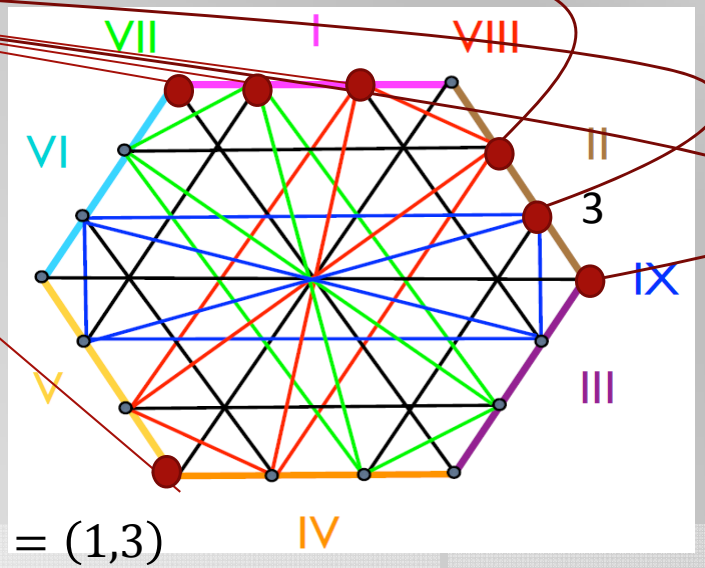


$P \neq P'$

Nothing prevents from cheating

Alice





Bob

(2,9,16) Bell inquality W $u^* = (pink, brawn), x^* = (1,3)$

The protocol

1) Alice and Bob check the value of a Bell inequality W and abort if it is too low — ACC_1

2) Alice and Bob check how many times (u*,x*) appears and abort if too low — ACC_2

3) If both tests pass, they apply 2-extractor to the bits from SV source and the outcomes of the devices

Measure of how random is the outcome „s”

$$d_c = \sum_{s,e} \max_w \sum_z \left| p(s,z,e|w,\mathrm{ACC}) - \frac{1}{|S|} p(z,e|w,\mathrm{ACC}) \right|$$

real distribution

Ideal distribution

$$ACC = ACC_1 \cap ACC_2$$

Security: either d_c is small, or ACC is small

SV satisfies Generalized Chernoff bound

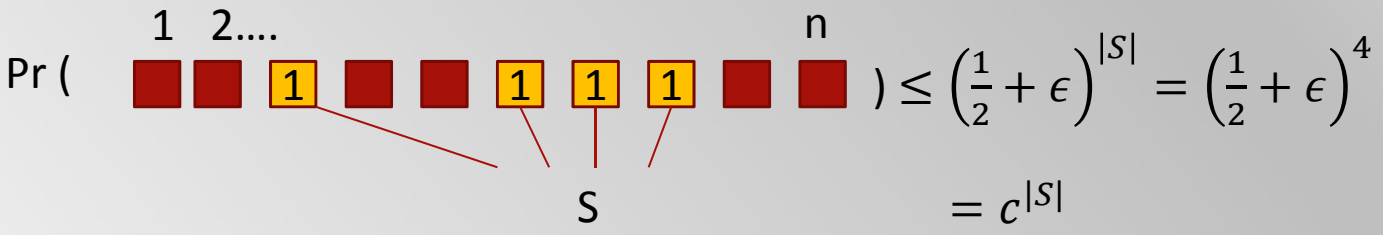
$X_1 \dots X_n$

$If\ \exists\ c\ \forall S \subset \{1, \dots, n\} \qquad \Pr[X_i = 1\ for\ all\ i \in S] \leq c^{|S|}$

Then $\Pr[\sum_i X_i = 1 \geq c_1 n] \leq e^{-nD(c|c_1)}$

Relative entropy „distance"

Example: SV source satisfies the above assumptions:



$$) \leq \left(\frac{1}{2} + \epsilon\right)^{|S|} = \left(\frac{1}{2} + \epsilon\right)^{4}$$

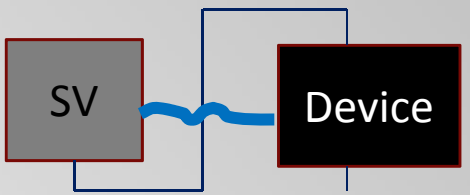
$$= c^{|S|}$$

Conclusion: linear number of (x^*, u^*) wil appear w.h.p.

[A. Panconesi and A. Srinivasa 1997] R. Impagliazzo and V. Kabane 2010

Open problems

- What if device is correlated with SV source ? (we assume it is not; work in progress) [H. Wojewódka et al.]



- The smallest dimension and/or settings ? [Idea in progress]
- Hmin ? – not with this method
- Optimality of the rates ?
- De Finetti approach ? rate is zero, but extractors are explicit [bipartite analogue]

Thanks for Your attention!

Idea of verification

- Verification:

- test the Bell value, (upper bound)

- test the number of the pairs (u*, x*) (lower bound)

Warning: Are u*,x* measured on good Bell value boxes ?

Solution: pigeonhole principle