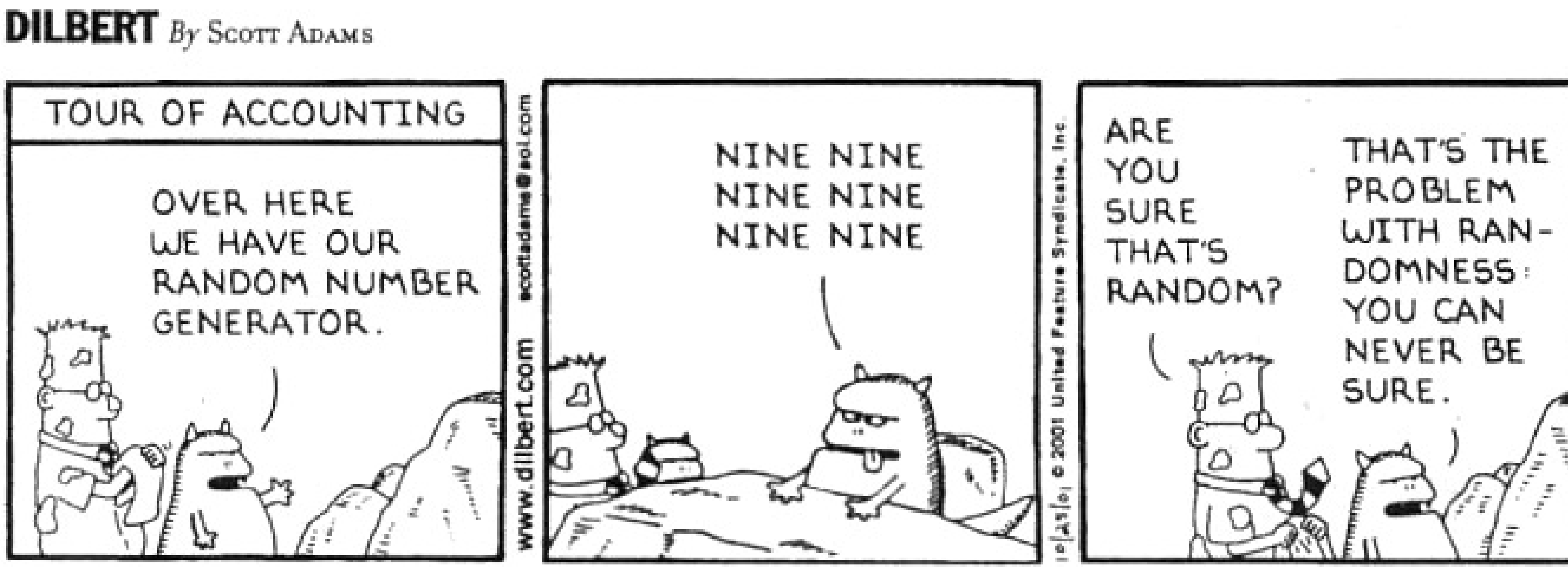
Certifiable Quantum Dice
(or, device-independent randomness generation)

Thomas Vidick,

MIT

Based on joint work with Umesh V. Vazirani,
U.C. Berkeley

arXiv:1111.6054


DILBERT By SCOTT ADAMS
TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RAN-DOMNESS: YOU CAN NEVER BE SURE.

Certifying randomness

Given a set of dice, how do you certify them?

Sample and check statistics.

What if the dice have memory?
Or if they are 2^{10000}-sided?

01101101000011...

Why certify randomness

- RSA, BB’84,…, crucially rely on *private* randomness

CNET › News › InSecurity Complex

Researchers find flaw in key generation with popular cryptography

by Elinor Mills | February 14, 2012 1:42 PM PST

Follow

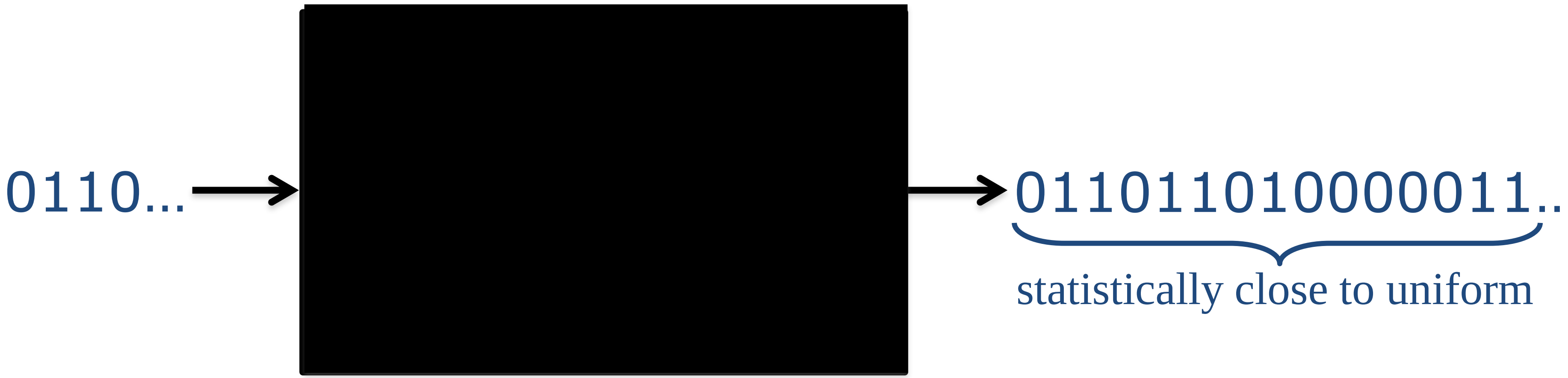
Small percentage of public keys in sample found online were not randomly generated as they should be, paper says.

A group of researchers has uncovered a flaw in the way public keys are generated using the RSA algorithm for encrypting sensitive online communications and transactions.

They found that a small fraction of public keys--27,000 out of a sample of about 7 million--had not been randomly generated as they should be. This means it would be possible for someone to figure out the secret prime numbers which were used to create the public key, according to The New York Times, which reported on the research today.

→ Crucial that random bits are unbiased and trusted

Goal: a *certifiable* source of randomness



1. You provide specifications for the inner workings of the device.

2. No guarantee that the specifications were followed.

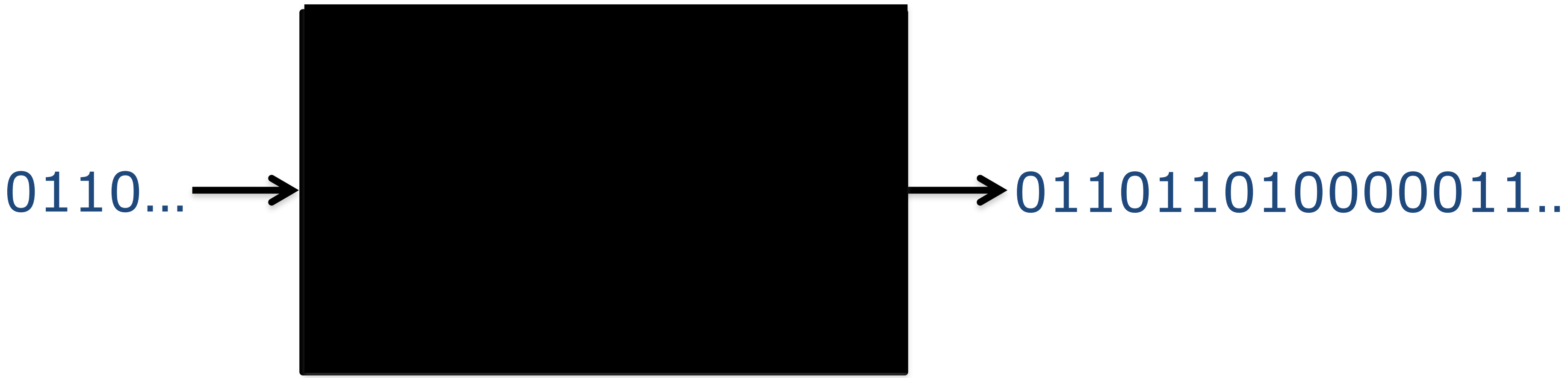
3. You use the box only once.

4. Provide test for output's randomness:

✓ if the box was manufactured according to specification, the output must pass the test with very high probability.

✓ if any box passes the test, its output is close to uniformly random.

Goal: a *certifiable* source of randomness



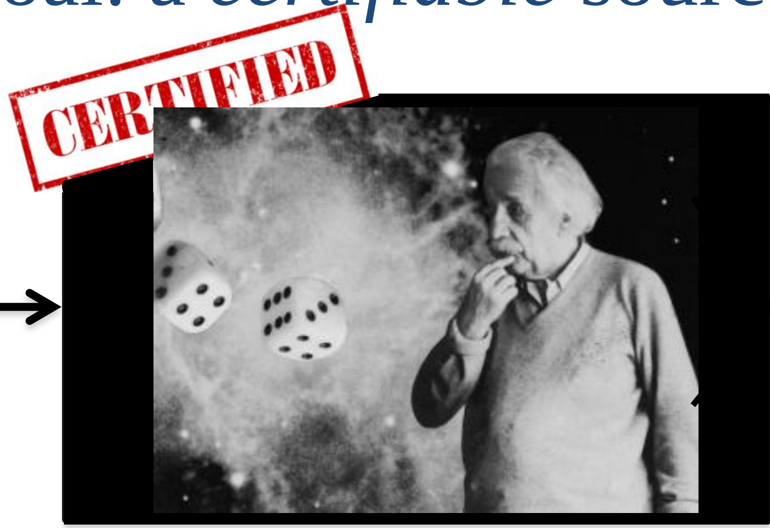
Two inevitable assumptions:

1. Test requires use of (a small amount of) initial randomness

2. Need *physical* assumption on device

   - Device could be pre-programmed to choose next output bit to deterministically maximize expected success

Goal: a *certifiable* source of randomness

0110… → 

→ 01101101000011…

Physical assumption:

The device is made of two non-communicating parts

- Randomness certification based on Bell inequality violation
- First suggested by Colbeck (Ph.D. thesis '09)
- [PAM+,Nature'10] gave rigorous analysis (+experimental results!)
  → Protocol uses $\sqrt{n}$ random bits, generates n near-uniform bits
- We give more efficient protocol
  + randomness *certified against quantum side information*

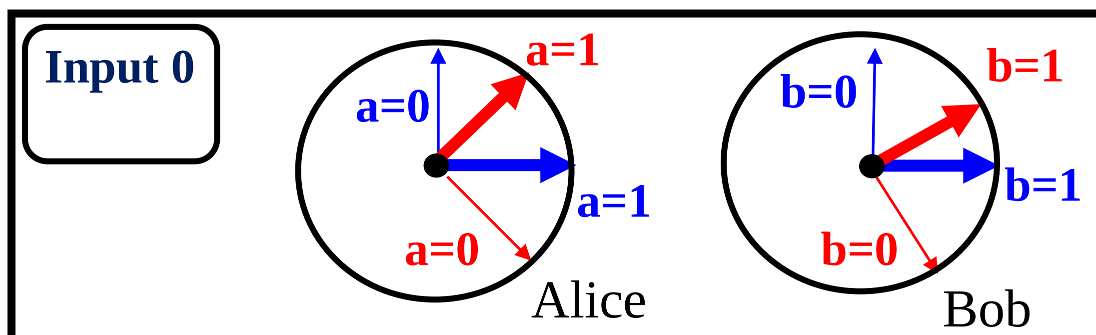
A randomness expansion protocol

n = target #random bits
ϵ = security parameter

(input x)
(output a)

(input y)
(output b)

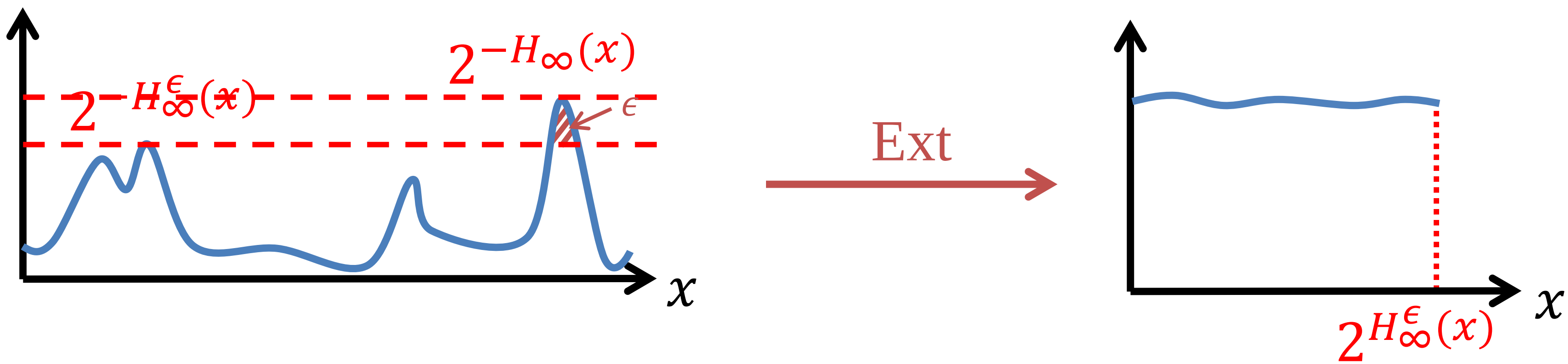
- Inputs divided into blocks of $O(\log n + \log(1/\epsilon))$ identical inputs
- [dummy blocks]: Most blocks use input (0,0)
- [check blocks]: polylog(n/ϵ) blocks use randomly chosen inputs
- Repeat poly(n/ϵ) times
- Test: (variant of chained ineq.)
  - dummy blocks: *all* outputs satisfy $a_i = b_i$
  - check blocks: correlations are within 5% of predictions of QM



An aside: measuring randomness

- Goal: generate bits ϵ-close to perfectly uniform

- Min-entropy $H_\infty(X) = -\log\big(\Pr(\textit{most likely event})\big)$



- *Smooth* min-entropy $H_\infty^\epsilon(X)$

$\rightarrow$ Number of bits of ϵ-*near-uniform* randomness that can be extracted

- *Quantum conditional* min-entropy [R'05]
  - $H_\infty(X|E) = -\log P_{guess}(X|E)$ [KRS'09] (X=classical, E=quantum)
  - $H_\infty^\epsilon(X|E)$: max. nb. of ϵ-*near-uniform* (to any adversary holding E) bits that can be extracted from X

Results

n = target #random bits
ϵ = security parameter

The certification theorem: Suppose that

1. The initial randomness is perfectly uniform
2. The devices did not communicate throughout
3. The experimenter's test passes
4. Quantum mechanics is correct

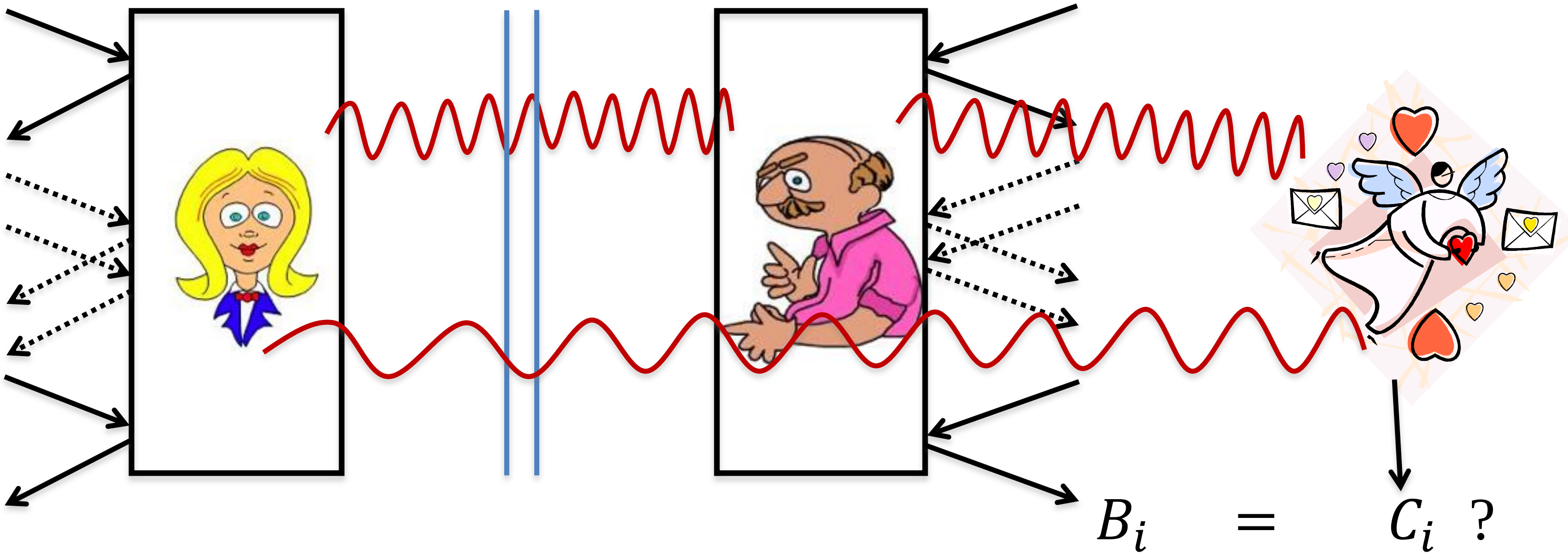
Then: $H_\infty^\epsilon(B|E) \geq n$ *(for any quantum E)*

- Recall parameters: $m = poly(n/\epsilon)$ rounds of interaction, $polylog(n, 1/\epsilon)$ bits of randomness to select inputs
  $\rightarrow$ Exponential expansion for $\epsilon = 1/poly(n)$

- [FGS'12,PM'12] also obtain exponential expansion, based on [PAM+10]
  (Use *two pairs* of devices, *assume no entanglement between the pairs)*

- Lower bound on $H_\infty^\epsilon(B|E)$ implies protocol is composable

Quantum adversaries



- Suppose Bob's outputs are random, but…

  …Eve has a measurement on her system that produces identical outcomes!

- Ex: ABE share m copies of $|\Psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

  Most of Bob's inputs are "0": Eve can bet on his measurement being B_0

  $\rightarrow$ B,E get same outcome whenever $Y_i = 0$

- Catch: trace out Eve $\Rightarrow$ A,B in separable state!
- Monogamy: high correlation b/w B,E $\Rightarrow$ no entanglement b/w A,B

Proof strategy

The certification theorem: Suppose that

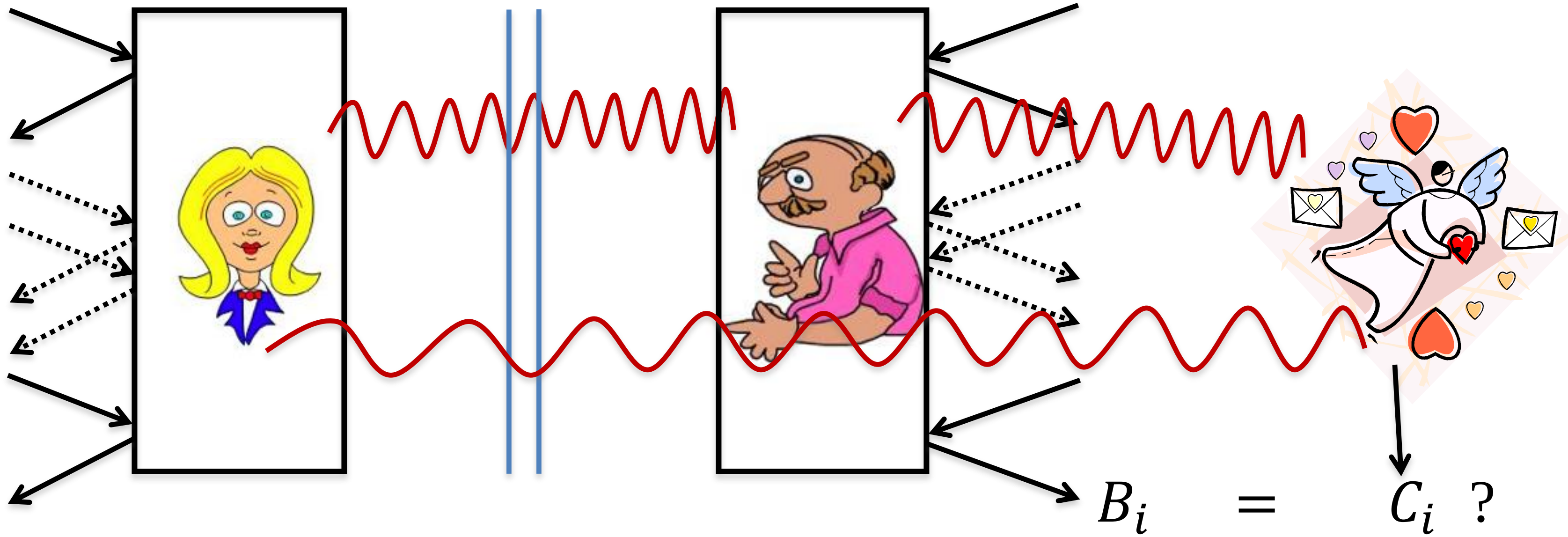
1. The initial randomness was perfectly uniform
2. The devices did not communicate
3. Quantum mechanics is correct
4. The experimenter's test passes

Then: $H_\infty^\epsilon(B|E) \geq n$ *(for any quantum E)*

Suppose (1),(2),(3),(4) hold, but $H_\infty^\epsilon(B_1 \cdots B_m|E) \ll n$

1. Easy case: $\exists i, H_\infty^\epsilon(B_i|E) \ll n/m \ll 1$
   - Derive contradiction with no-signaling condition in i-th block
2. General case: $H_\infty^\epsilon(B|E) \ll n$
   - Exploit assumption using "quantum reconstruction paradigm"
   - Enables reduction to easy case: identify "good i" such that Eve can predict B_i

Easy case: $\exists i \in [m], p_{guess}(B_i|E) \geq 0.99$



- Can always measure Eve first → her prediction acts as "anchor" for $\mathrm{B_i}$
  Most of the time, block i is a dummy block: $Y_i = 0$.
  → on input $Y_i = 0$, Bob is almost *deterministic*

- Small chance that block i is a check block:
  Can Alice, Bob satisfy CHSH constraints if Bob's output on input 0 is fixed?

- Determinism incompatible with Bell inequality violation
  [PAM+10] gave quantitative argument for general Bell inequalities
  → We give direct intuitive argument based on "guessing game"

Proof strategy

The certification theorem: Suppose that

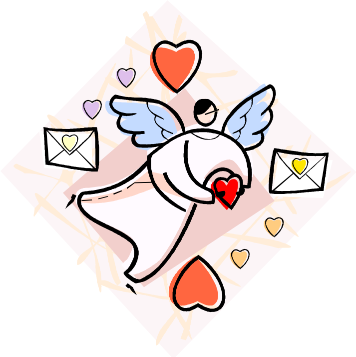
1. The initial randomness was perfectly uniform
2. The devices did not communicate
3. Quantum mechanics is correct
4. The experimenter's test passes

Then: $H_\infty^\epsilon(B|E) \geq n$ *(for any quantum* E*)*

Suppose (1),(2),(3),(4) hold, but $H_\infty^\epsilon(B|E) \ll n$

1. Easy case: $\exists i, H_\infty^\epsilon(B_i|E) \ll 1$
   - Derive contradiction with no-signaling condition in i-th block ✓
2. General case: $H_\infty^\epsilon(B|E) \ll n$
   - Exploit assumption through "quantum reconstruction paradigm"
   - Enables reduction to easy case: identify "good i" such that Eve can predict B_i

General case: $H_\infty^\epsilon(B|E) \ll n$



- ~~Idea 0:~~ $\cancel{p_{guess}(B|E) = 2^{-H_\infty(B|E)} \gg 2^{-n}}$
  $\rightarrow$ Eve can guess *complete* string B, but with *very low success*

- Idea 1: use *smoothed* min-entropy $H_\infty^\epsilon(B|E) \ll n$
  Operational interpretation: Eve can break any n-bit extractor on B, with advantage $\epsilon = poly^{-1}(n) \gg 2^{-n}$

- Idea 2: deduce existence of "improved" Eve:
  Eve can guess $\hat{B} \approx B$ with succ. $\approx \epsilon$ (some caveats)
  Based on "quantum reconstruction paradigm"

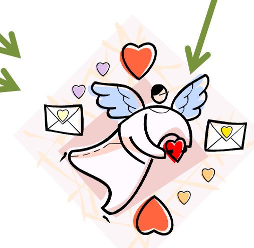
- Boosted success from 2^{-n} to ϵ!
  $\rightarrow$ Reduce to easy case: identify "good" block i such that Eve can predict B_i
  (need to condition on event of probability $\approx \epsilon$, instead of $\approx 2^{-n}$)

A "quantum reconstruction paradigm"

Lemma [DVPR'11,VV'12]: Assume $B \in \{0,1\}^m$ such that $H_\infty^\epsilon(B|E) \ll n$. Then there exists $O(n\log(1/\epsilon))$ indices $A \subseteq [m]$ such that, *given* B_A, Eve can *predict* $\hat{B}$ such that $\mathrm{d}(\hat{B}, B) \le 0.01$, with success $O(poly(\epsilon/m))$.

B:

0	1	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	0	1	0	1	0



At most 1% errors,
with probability $\geq (\epsilon/m)^4$

$\hat{B}$:

0	1	**1**	1	1	0	**0**	0	1	1	0	1	**0**	0	1	1	1	0	**0**	1	0	1	0

A "quantum reconstruction paradigm"

Lemma [DVPR'11,VV'12]: Assume $B \in \{0,1\}^m$ such that $H_\infty^\epsilon(B|E) \ll n$. Then there exists $O(n\log(1/\epsilon))$ indices $A \subseteq [m]$ such that, *given* B_A, Eve can *predict* $\hat{B}$ such that $\mathrm{d}(\hat{B}, B) \leq 0.01$, with success $O(poly(\epsilon/m))$.

- Introduced in [Tre'01] to analyze *classical* extractors
- [DV'11,DVPR'12] Adaptation to quantum setting challenging: reconstruction requires repeated measurement of E
- [KT06]: can assume Eve applies specific measurement (PGM) → simultaneously refines all required measurements

Proof strategy

The certification theorem: Suppose that

1. The initial randomness was perfectly uniform
2. The devices did not communicate
3. Quantum mechanics is correct
4. The experimenter's test passes

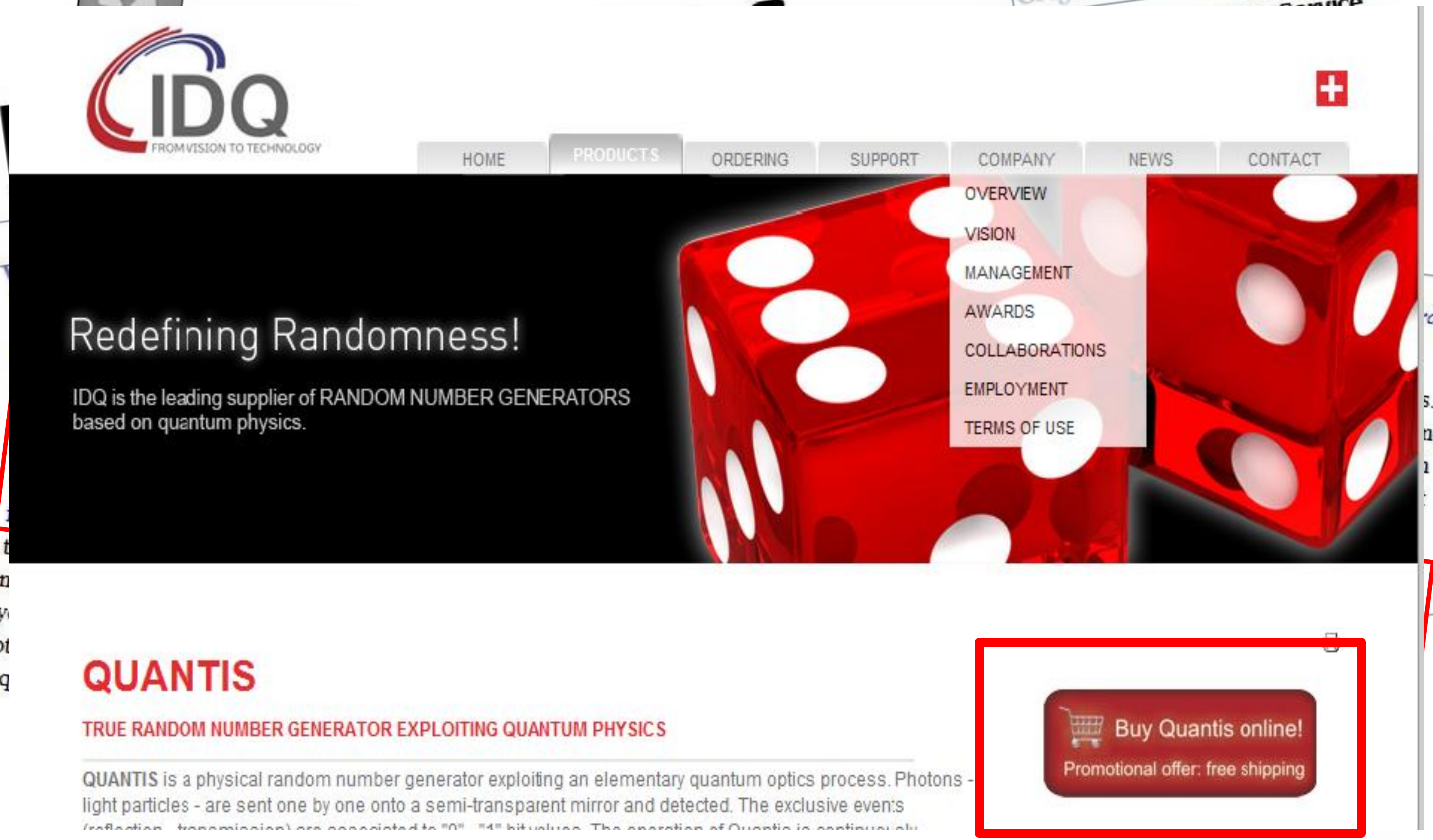
Then: $H_\infty^\epsilon(B|E) \geq n$ *(for any quantum E)*

Suppose (1),(2),(3),(4) hold, but $H_\infty^\epsilon(B|E) \ll n$

1. Easy case: $\exists i, H_\infty^\epsilon(B_i|E) \ll 1$
   – Derive contradiction with no-signaling condition in i-th block
2. General case: $H_\infty^\epsilon(B|E) \ll n$
   – Exploit assumption through "quantum reconstruction paradigm"
   – Enables reduction to easy case: identify "good i" such that Eve can predict B_i

Questions

- How much can we sell this for?



Questions

- Applications? *Implementations*?
  - Can the protocol be made robust to noise?
    To imperfections in the initial randomness?
  - Improve efficiency

- What is the maximum stretch?
  - Doubly exponential expansion?
  - *Unbounded* expansion?

- Other models/assumptions
  - "Free will amplification" [Colbeck-Renner'11]
  - Certified randomness generation under other assumptions

God does not play dice with the Universe.

Albert Einstein

Stop telling God what to do with his dice.

Niels Bohr