Title: Tomography without trusted apparatus

Date: Aug 29, 2008 02:00 PM

URL: http://pirsa.org/08080046

Abstract: I will talk about \'self-testing\' quantum apparatus.

Tomography with untrusted apparatus?

Michele Mosca

Based on self-testing work with F. Magniez, D. Mayers, M. McKague, H. Ollivier

29 August 2008

Why do we want to test quantum apparatus?

Tomography with untrusted apparatus?

Michele Mosca

Based on self-testing work with F. Magniez, D. Mayers, M. McKague, H. Ollivier

29 August 2008

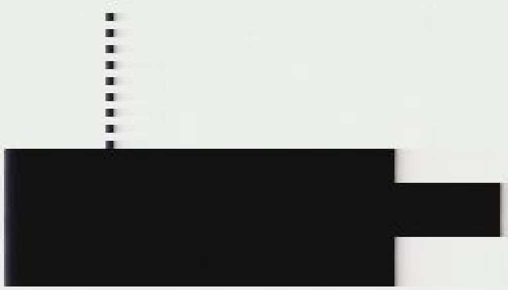
Why do we want to test quantum apparatus?

Why do we want to test quantum apparatus?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

Why do we want to test quantum apparatus?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

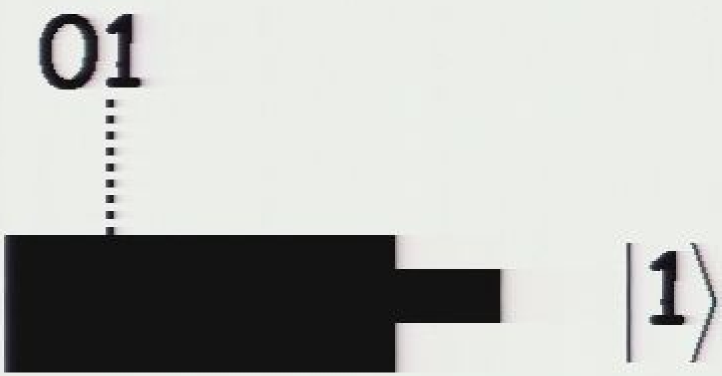


Why do we want to test quantum apparatus?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

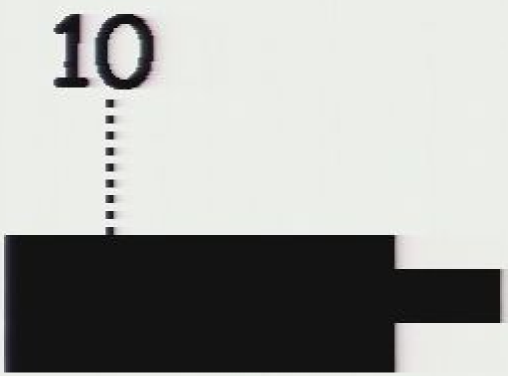
Why do we want to test quantum apparatus?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.



Why do we want to test quantum apparatus?

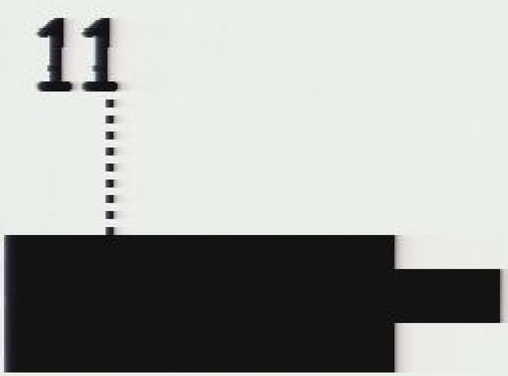
Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.



$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Why do we want to test quantum apparatus?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.



$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Why do we want to test quantum apparatus?

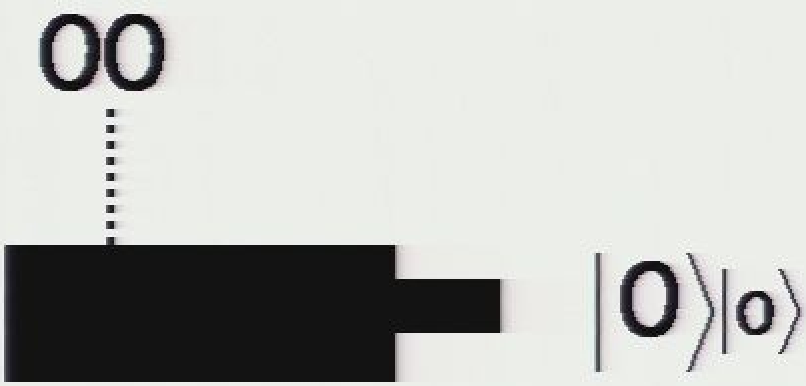
Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

Why should you trust this component?

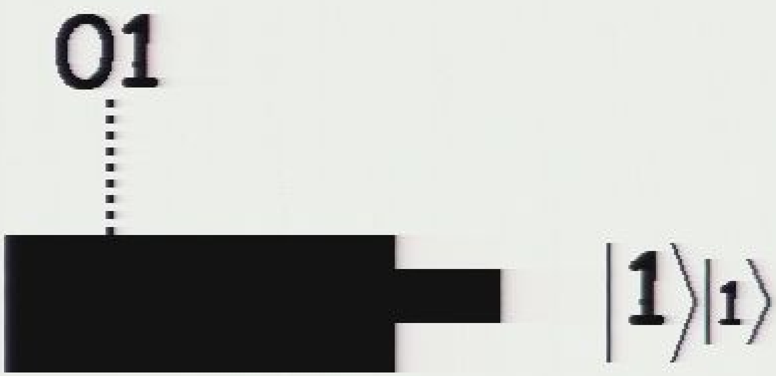
Why not?
What if what we really have is implementing the following?

Why not?

What if what we really have is implementing the following?



Why not?
What if what we really have is implementing the following?



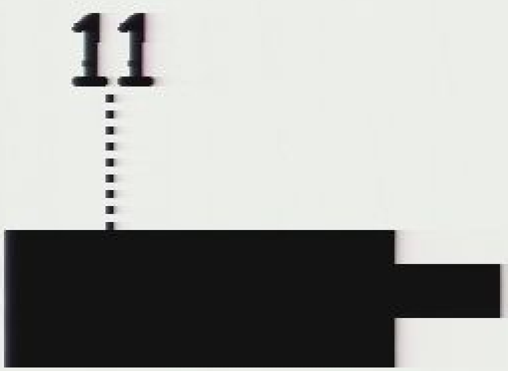
Why not?

What if what we really have is implementing the following?

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}|2\rangle$$

Why not?

What if what we really have is implementing the following?



$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}|3\rangle$$

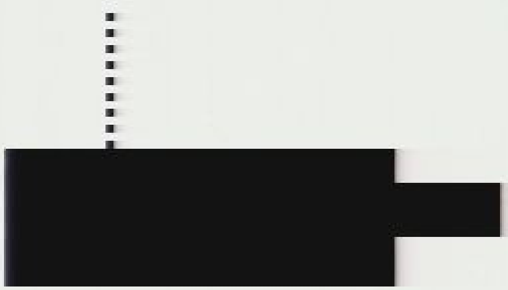
Why not?
What if what we really have is implementing the following?

"side-channels"

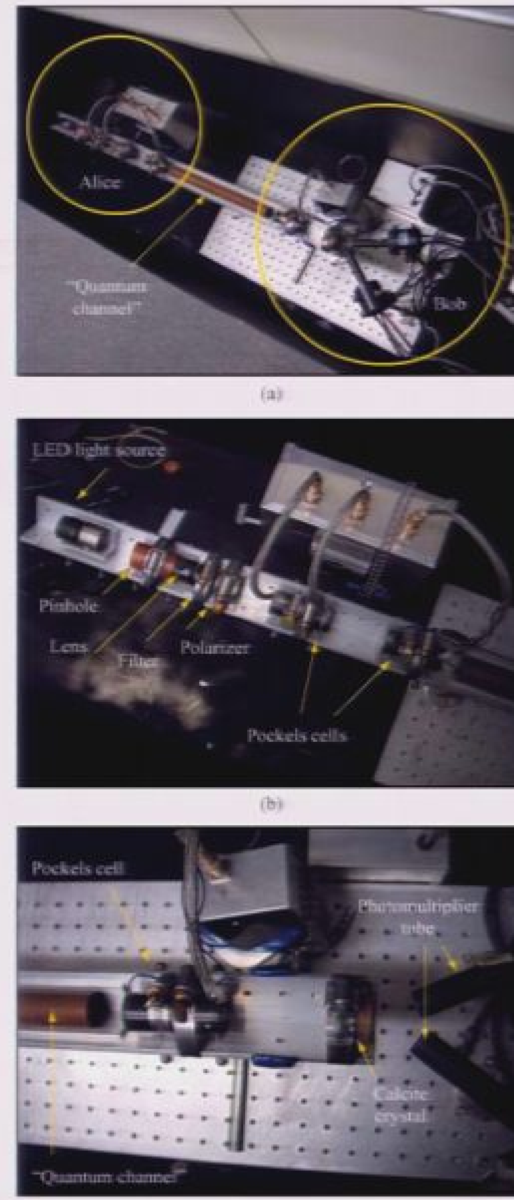
http://www.research.ibm.com/journal/rd/481/smolin.html

C. H. Bennett, F. Bessett, G. Brassard, L. Salvail, and J. Smolin, " Experimental Quantum Cryptography," J. Cryptol. 5, No. 1, 3–28 (1992).

Why not?
What if what we really have is impl the following?



"side-channel



(c)

Figure 1

The apparatus used to perform the fi[illegible] cryptography experiment: (a) The entire apparatus; (b) detailed view of Alice; (c) detailed view of Bob.

http://www.research.ibm.com/journal/rd/481/smolin.html

C. H. Bennett, F. Bessett, G. Brassard, L. Salvail, and J. Smolin, “ Experimental Quantum Cryptography,” J. Cryptol. 5, No. 1, 3–28 (1992).

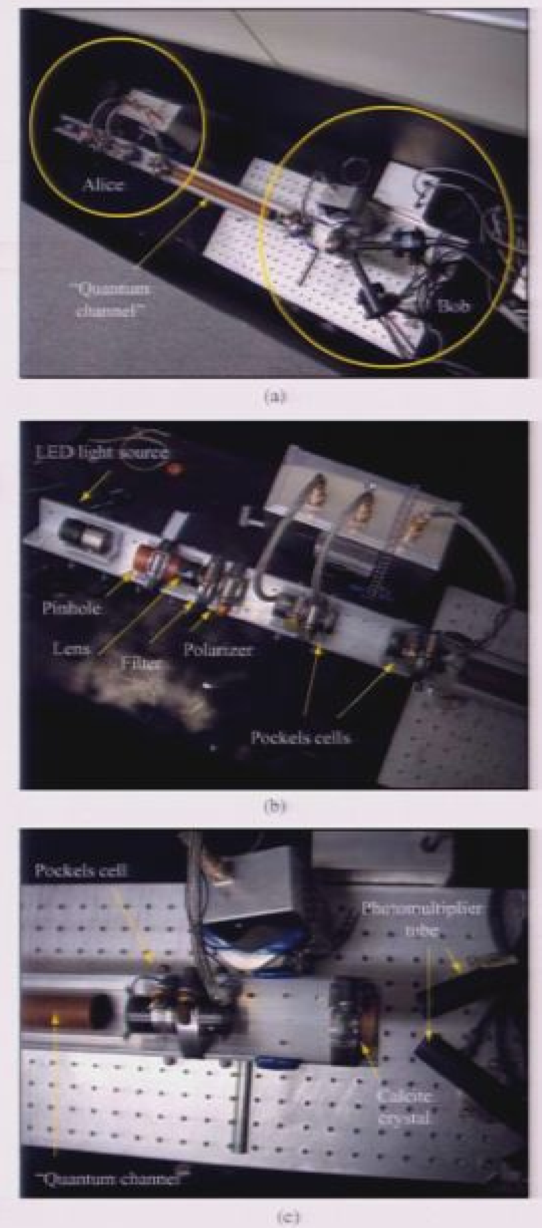


Figure 1

The apparatus used to perform the fi... cryptography experiment: (a) The entire apparatus; (b) detailed view of Alice; (c) detailed view of Bob.

Why not?
What if what we really have is impl
the following?

“side-channel

(see Zhao et al. arXiv:0704.3253)

We need to make our assumptions and testing procedures explicit.

We need to make our assumptions and testing procedures explicit.

We also don't want to rely on some other untrusted apparatus (e.g. in order to "just" do tomography).

SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1524–1540, October 1997

QUANTUM COMPUTABILITY*

LEONARD M. ADLEMAN[†], JONATHAN DEMARRAIS[†], AND MING-DEH A. HUANG[†]

Abstract. In this paper some theoretical and (potentially) practical aspects of quantum computing are considered. Using the tools of transcendental number theory it is demonstrated that quantum Turing machines (QTM) with rational amplitudes are sufficient to define the class of bounded error quantum polynomial time (BQP) introduced by Bernstein and Vazirani [*Proc. 25th ACM Symposium on Theory of Computation*, 1993, pp. 11–20, *SIAM J. Comput.*, 26 (1997), pp. 1411–1473]. On the other hand, if quantum Turing machines are allowed unrestricted amplitudes (i.e., arbitrary complex amplitudes), then the corresponding BQP class has uncountable cardinality and contains sets of all Turing degrees. In contrast, allowing unrestricted amplitudes does not increase the power of computation for error-free quantum polynomial time (EQP). Moreover, with unrestricted amplitudes, BQP is not equal to EQP. The relationship between quantum complexity classes and classical complexity classes is also investigated. It is shown that when quantum Turing machines are restricted to have transition amplitudes which are algebraic numbers, BQP, EQP, and nondeterministic quantum polynomial time (NQP) are all contained in PP, hence in $P^{\#P}$ and PSPACE. A potentially practical issue of designing "machine independent" quantum programs is also addressed. A single ("almost universal") quantum algorithm based on Shor's method for factoring integers is developed which would run correctly on almost all quantum computers, even if the underlying unitary transformations are unknown to the programmer and the device builder.

Key words. quantum Turing machines, quantum complexity classes

AMS subject classifications. 68Q05, 68Q10, 68Q15

PII. S0097539795293639

A model of quantum computation where the computer does a tomography of some of its components

SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1524–1540, October 1997

QUANTUM COMPUTABILITY*

LEONARD M. ADLEMAN†, JONATHAN DEMARRAIS†, AND MING-DEH A. HUANG†

Abstract. In this paper some theoretical and (potentially) practical aspects of quantum computing are considered. Using the tools of transcendental number theory it is demonstrated that quantum Turing machines (QTM) with rational amplitudes are sufficient to define the class of bounded error quantum polynomial time (BQP) introduced by Bernstein and Vazirani [*Proc. 25th ACM Symposium on Theory of Computation*, 1993, pp. 11–20, *SIAM J. Comput.*, 26 (1997), pp. 1411–1473]. On the other hand, if quantum Turing machines are allowed unrestricted amplitudes (i.e., arbitrary complex amplitudes), then the corresponding BQP class has uncountable cardinality and contains sets of all Turing degrees. In contrast, allowing unrestricted amplitudes does not increase the power of computation for error-free quantum polynomial time (EQP). Moreover, with unrestricted amplitudes, BQP is not equal to EQP. The relationship between quantum complexity classes and classical complexity classes is also investigated. It is shown that when quantum Turing machines are restricted to have transition amplitudes which are algebraic numbers, BQP, EQP, and nondeterministic quantum polynomial time (NQP) are all contained in PP, hence in $P^{\#P}$ and PSPACE. A potentially practical issue of designing "machine independent" quantum programs is also addressed. A single ("almost universal") quantum algorithm based on Shor's method for factoring integers is developed which would run correctly on almost all quantum computers, even if the underlying unitary transformations are unknown to the programmer and the device builder.

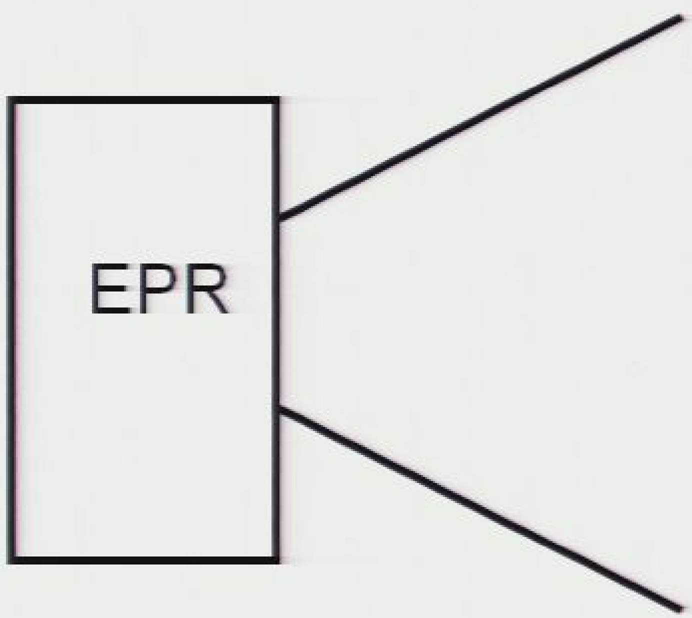
Key words. quantum Turing machines, quantum complexity classes

AMS subject classifications. 68Q05, 68Q10, 68Q15

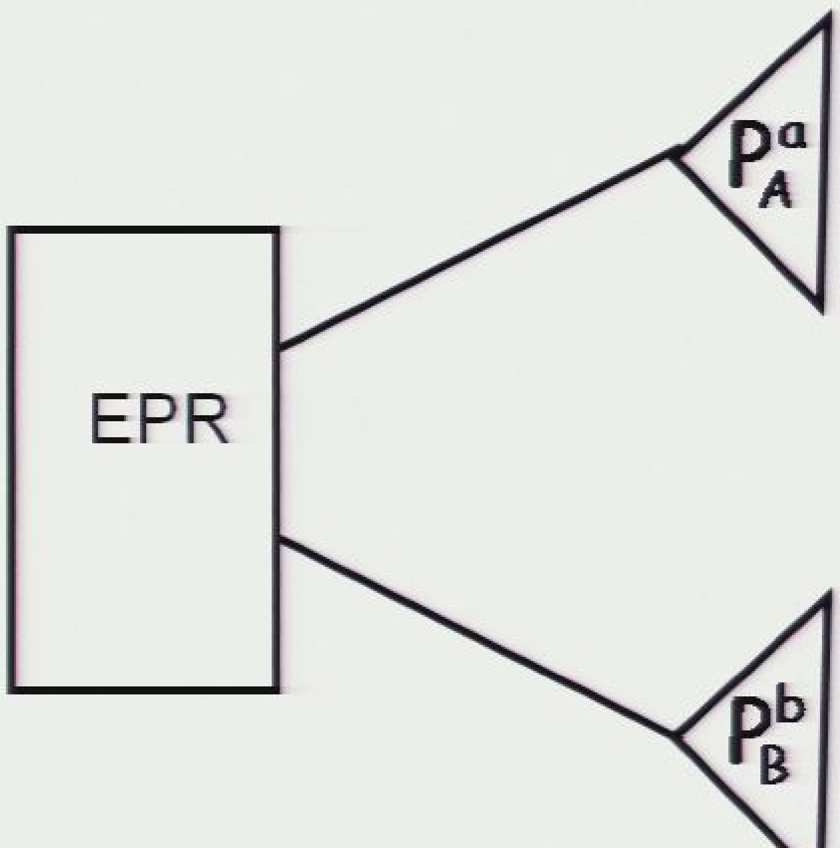
PII. S0097539795293639

*Mayers and Yao devised a scheme for “self”-testing **sources** for the purposes of QKD.*

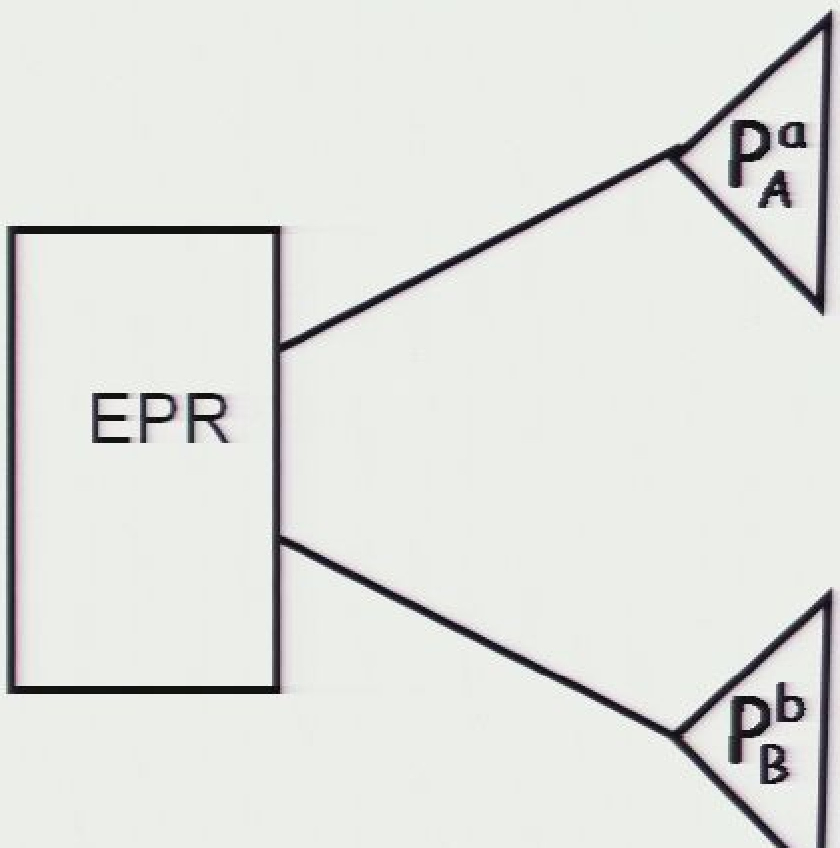
*Mayers and Yao devised a scheme for “self”-testing **sources** for the purposes of QKD.*



Mayers and Yao devised a scheme for “self”-testing ***sources*** *for the purposes of QKD.*



*Mayers and Yao devised a scheme for “self”-testing **sources** for the purposes of QKD.*



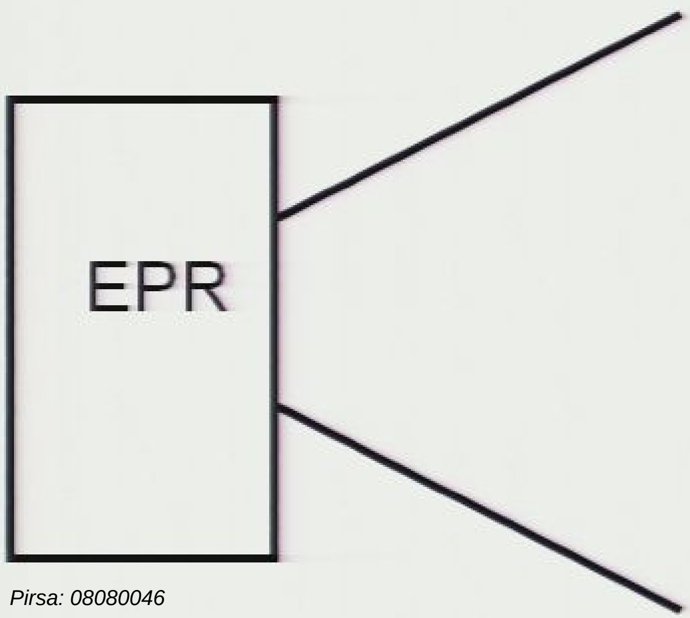
$$P^0 + P^{\pi/2} = I$$

$$P^{\pi/8} + P^{5\pi/8} = I$$

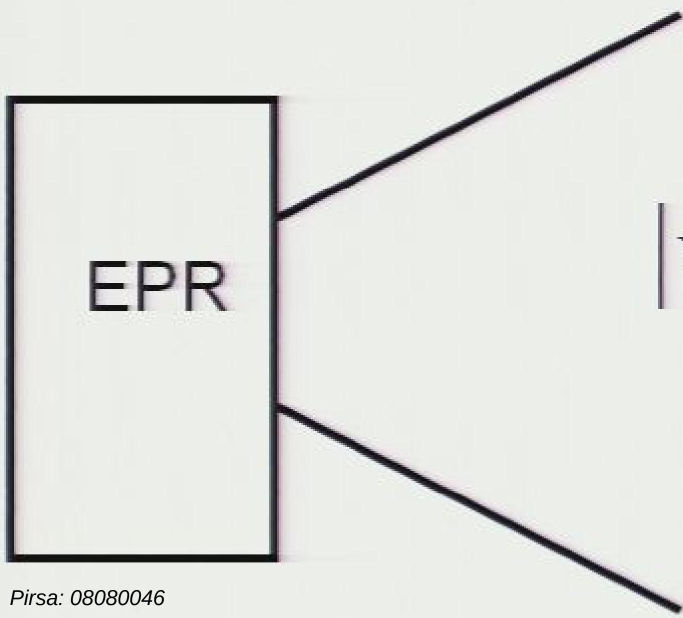
$$P^{\pi/4} + P^{3\pi/4} = I$$

the statistics are consistent with $|\varphi\rangle = |00\rangle + |11\rangle$ then
e output of the sources is locally unitarily equivalent to
state containing $|\varphi\rangle$, and the projections are
onsistent with measuring the EPR pair.

the statistics are consistent with $|\varphi\rangle = |00\rangle + |11\rangle$ then
ne output of the sources is locally unitarily equivalent to
state containing $|\varphi\rangle$, and the projections are
onsistent with measuring the EPR pair.



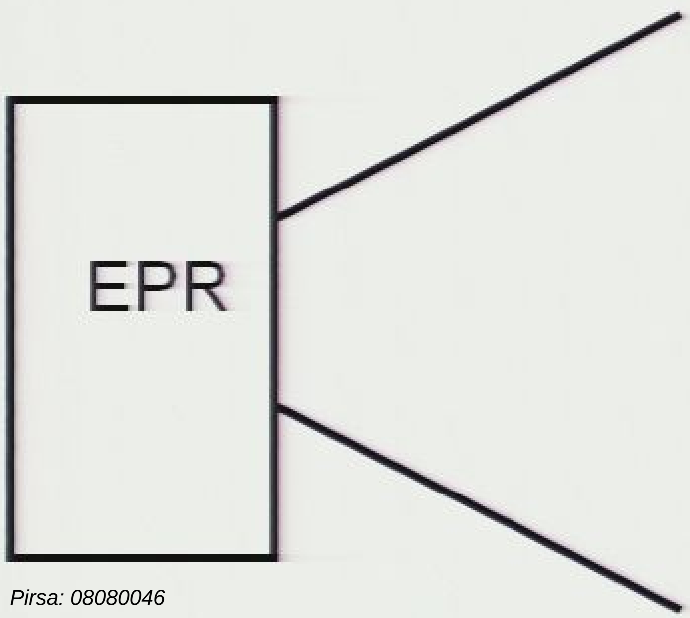
the statistics are consistent with $|\varphi\rangle = |00\rangle + |11\rangle$ then
e output of the sources is locally unitarily equivalent to
state containing $|\varphi\rangle$, and the projections are
onsistent with measuring the EPR pair.



$$|\psi\rangle_{AB}$$

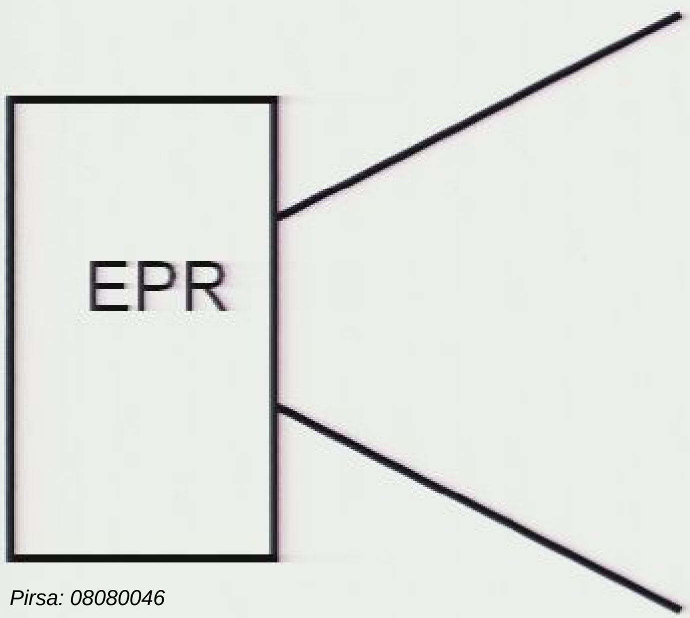
$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$

Application of this result



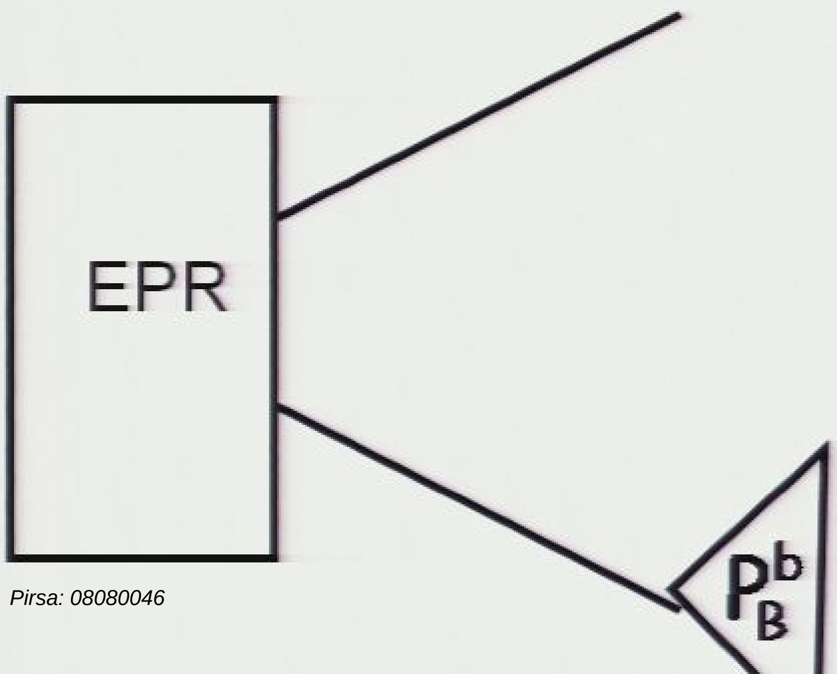
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B \left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB} \right)$$



Application of this result

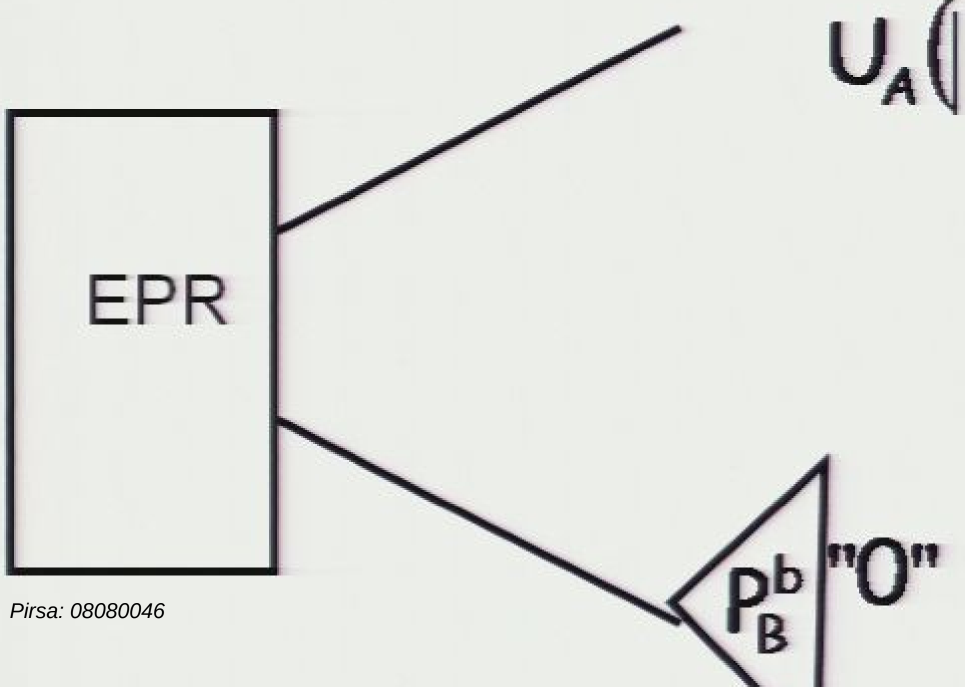
$$|\Psi\rangle_{AB} = U_A \otimes U_B \left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB} \right)$$



Application of this result

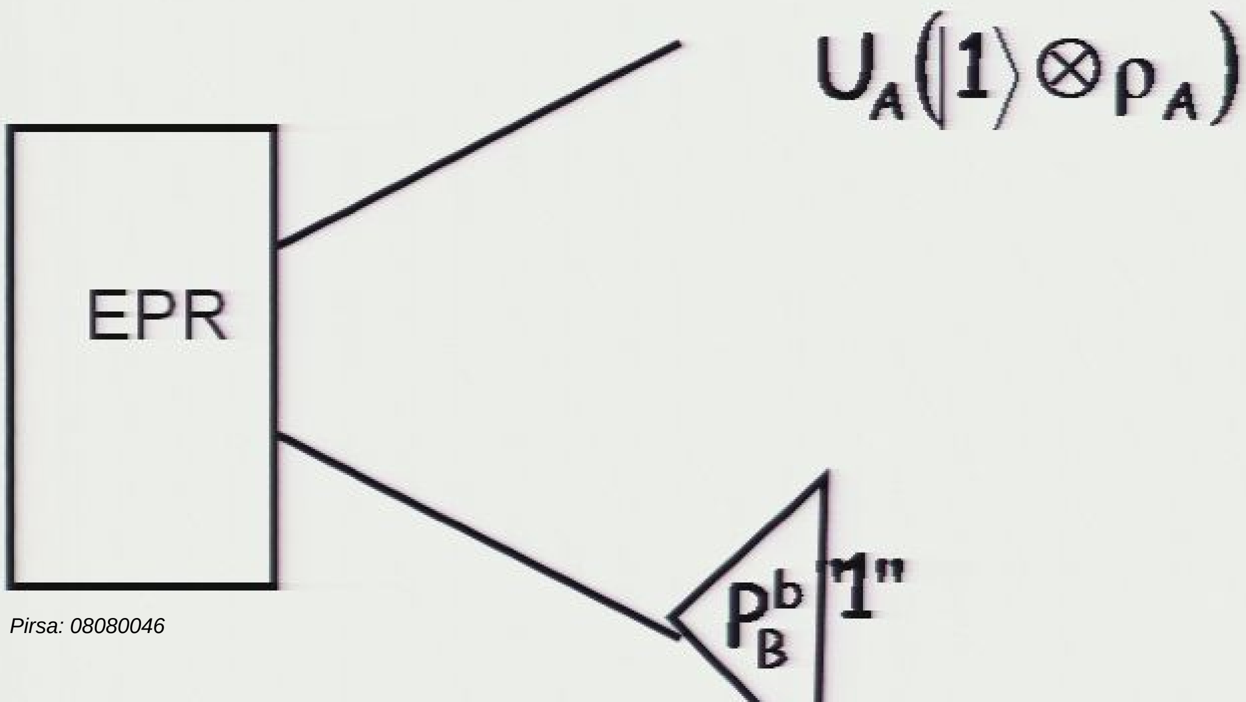
$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$

$$U_A\left(|0\rangle \otimes \rho_A\right)$$



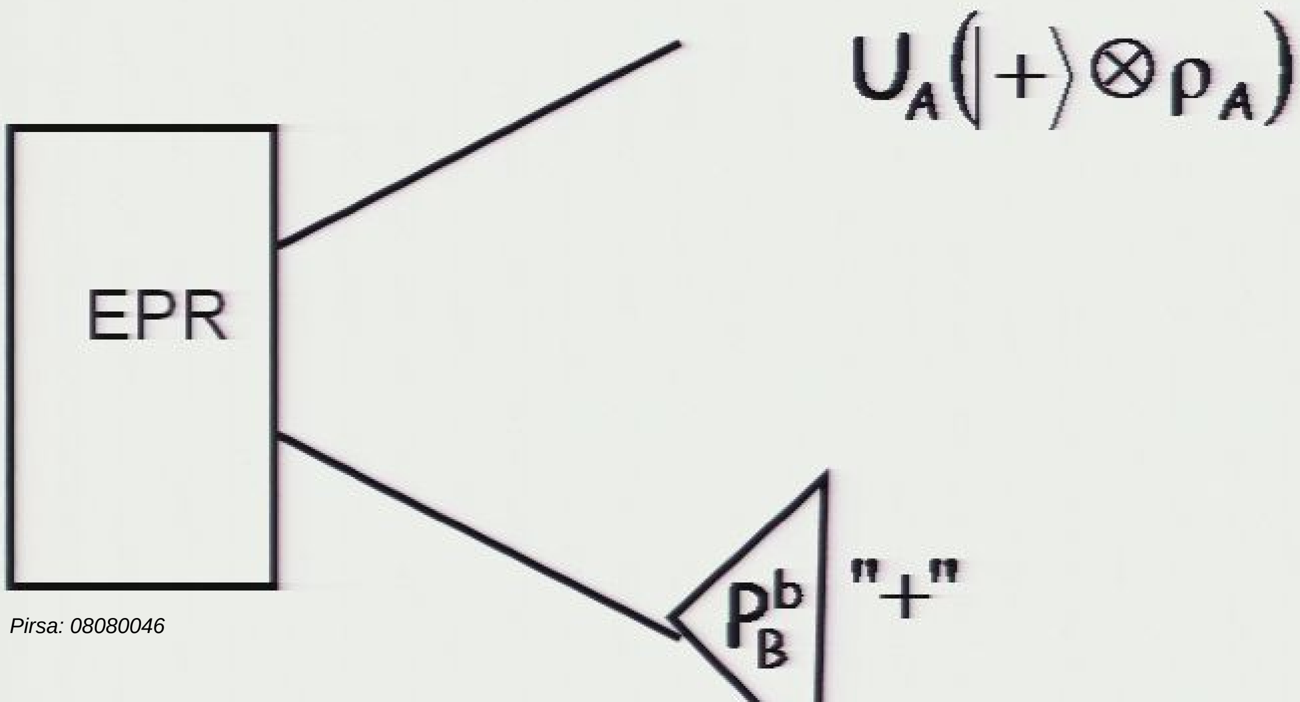
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



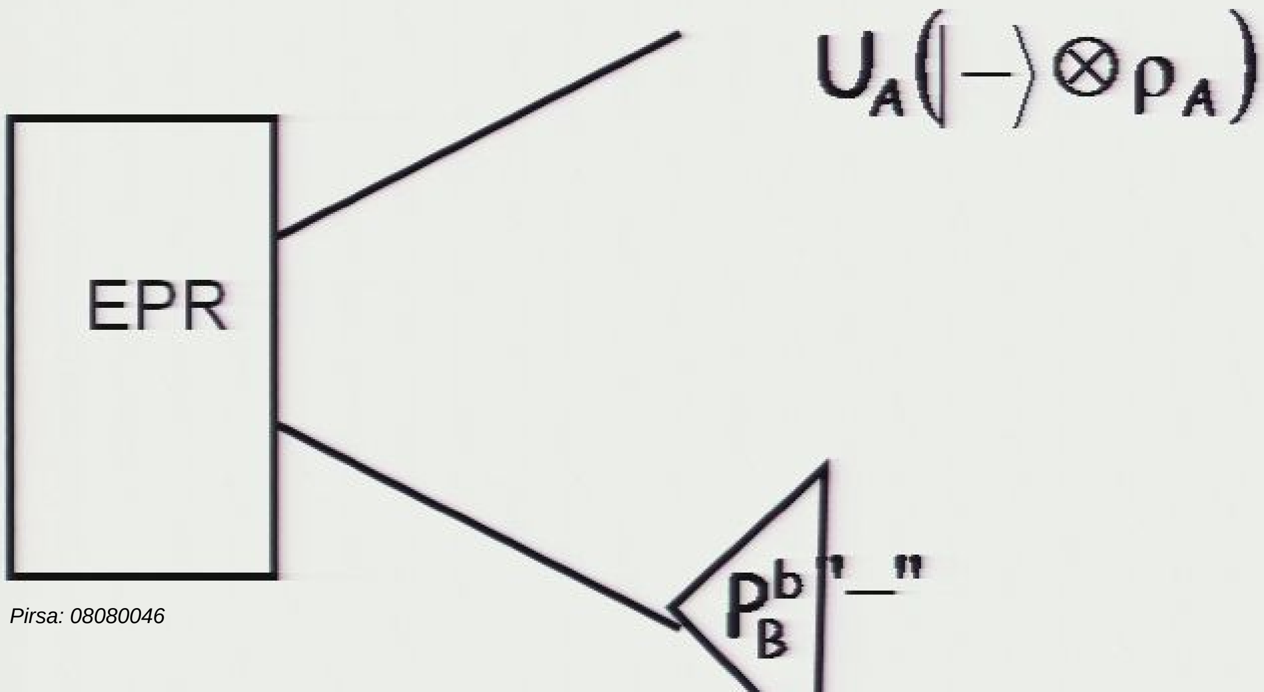
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



he main assumptions of Mayers and Yao are

Locality (i.e. measurements at A commute with those at B)

Repeatability of experiments

Trusted classical apparatus

Trusted local random number generators.

he main assumptions of Mayers and Yao are

- Locality (i.e. measurements at A commute with those at B)
- Repeatability of experiments
- Trusted classical apparatus
- Trusted local random number generators.

However, the results are not “robust”. The results hold exactly if the statistics are satisfied exactly.

Any realistic application will need to be robust.

he main assumptions of Mayers and Yao are

Locality (i.e. measurements at A commute with those at B)

Repeatability of experiments

Trusted classical apparatus

Trusted local random number generators.

However, the results are not “robust”. The results hold exactly if the statistics are satisfied exactly.

Any realistic application will need to be robust.

ssuming robustness) This might be the only way, using only these assumptions, to verifiably securely prepare BB84 states for QKD

Why else do we want to test?

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why should you trust this result?

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why should you trust this result?

Or, suppose we have proved one of the Clay Institute $1M Millennium problem by a proof that needs to be run on a quantum computer.

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why should you trust this result?

Or, suppose we have proved one of the Clay Institute $1M Millennium problem by a proof that needs to be run on a quantum computer.

Should they pay us?

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

What else was known?

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why should you trust this result?

Or, suppose we have proved one of the Clay Institute $1M Millennium problem by a proof that needs to be run on a quantum computer.

Should they pay us?

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

5) The ability to use the same gate more than once in the same experiment

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

5) The ability to use the same gate more than once in the same experiment
6) The ability to prepare and measure '0' and '1'

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

5) The ability to use the same gate more than once in the same experiment
6) The ability to prepare and measure '0' and '1'
7) The dimension of the physical systems storing the qubits was known (i.e. 2-level systems)

What needs to be done?

We wish to remove assumptions 5,6 and 7.

What needs to be done?

We wish to remove assumptions 5,6 and 7.

We wish to still have a "composable" technique for self-testing a large circuit; since we want it to be efficient.

One step in that direction

What needs to be done?

We wish to remove assumptions 5,6 and 7.

We wish to still have a "composable" technique for self-testing a large circuit; since we want it to be efficient.

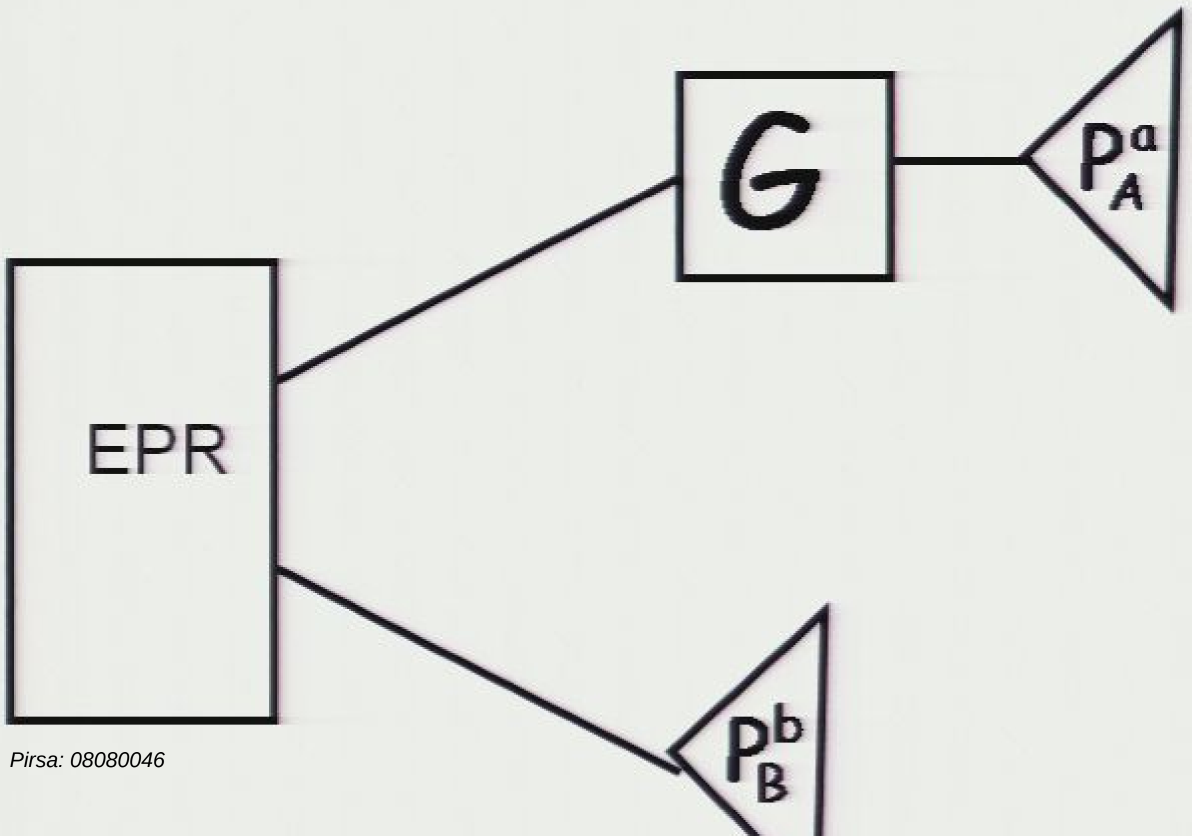
One step in that direction

One step in that direction

We can combine the EPR self-test of Mayers-Yao with DMMS-style gate testing

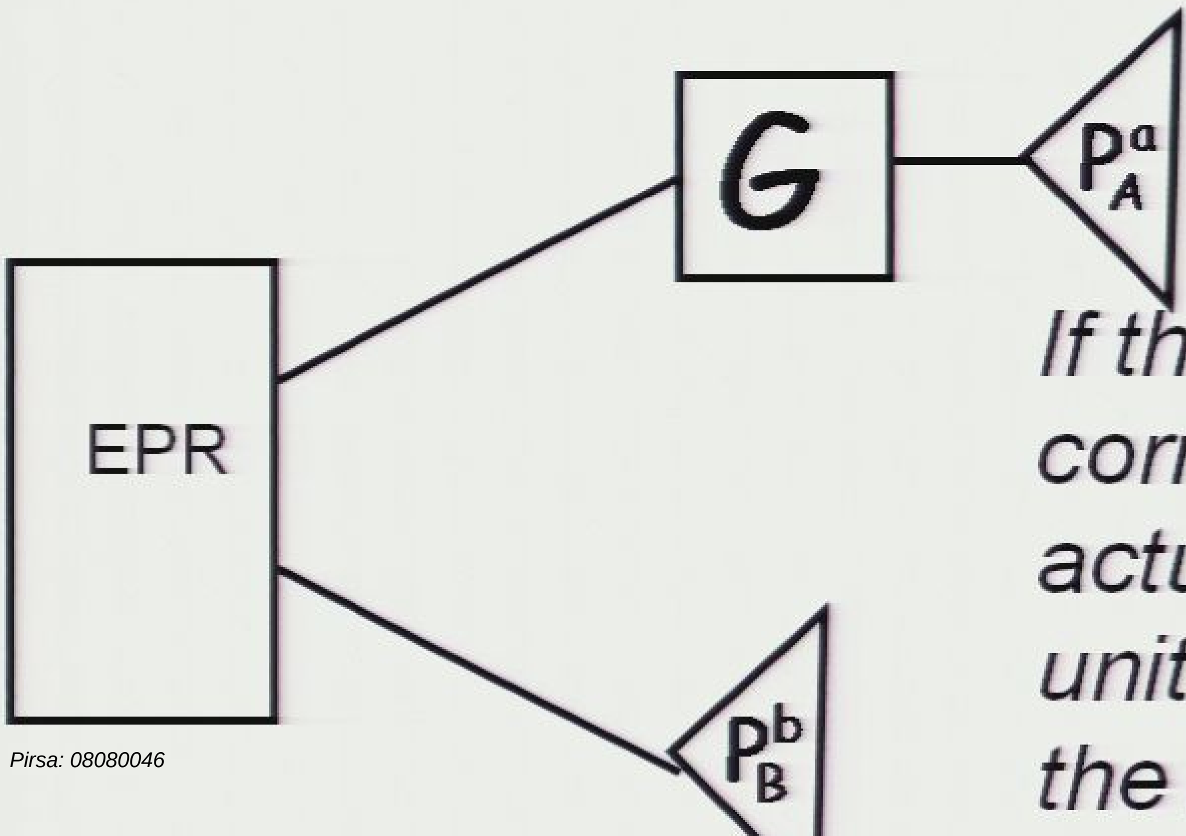
One step in that direction

We can combine the EPR self-test of Mayers-Yao with DMMS-style gate testing



One step in that direction

We can combine the EPR self-test of Mayers-Yao with DMMS-style gate testing



If the statistics are correct, then the actual gate G is locally unitarily equivalent to the ideal gate, T.

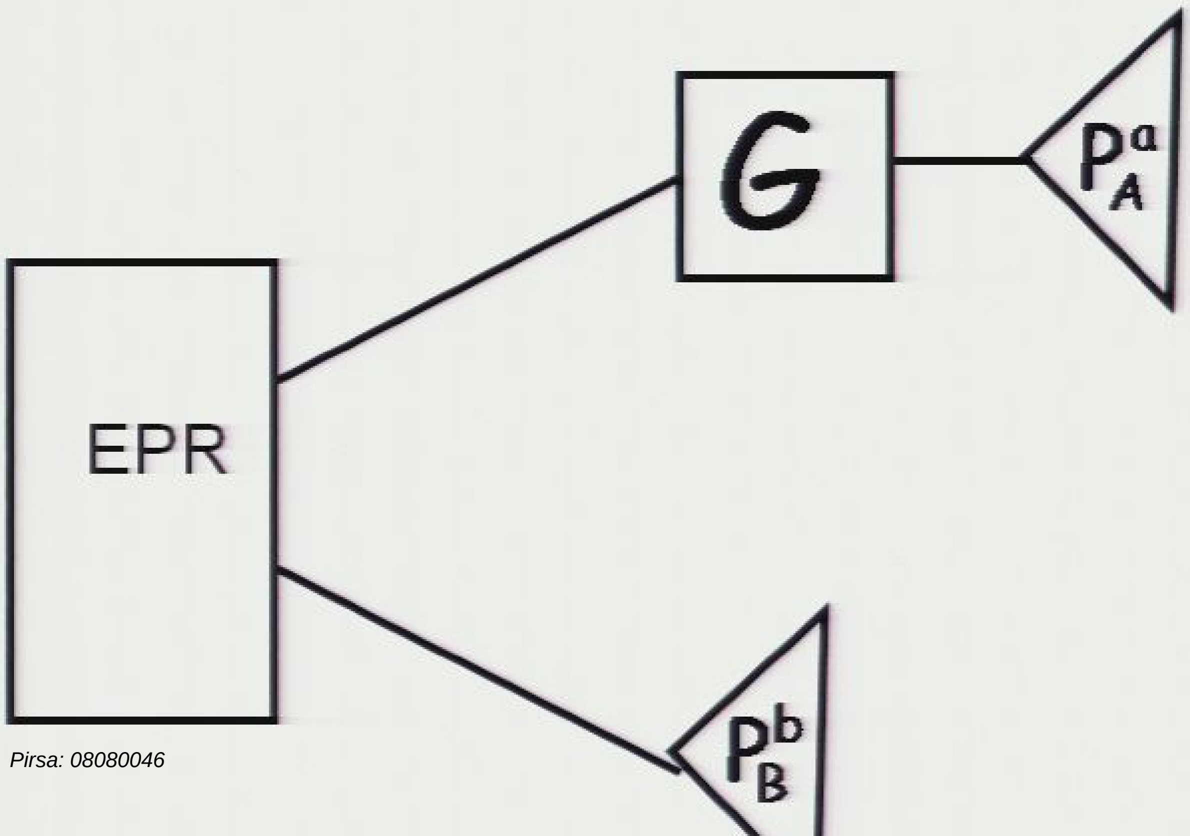
Still not composable…

Still not composable…

The following does not necessarily compose

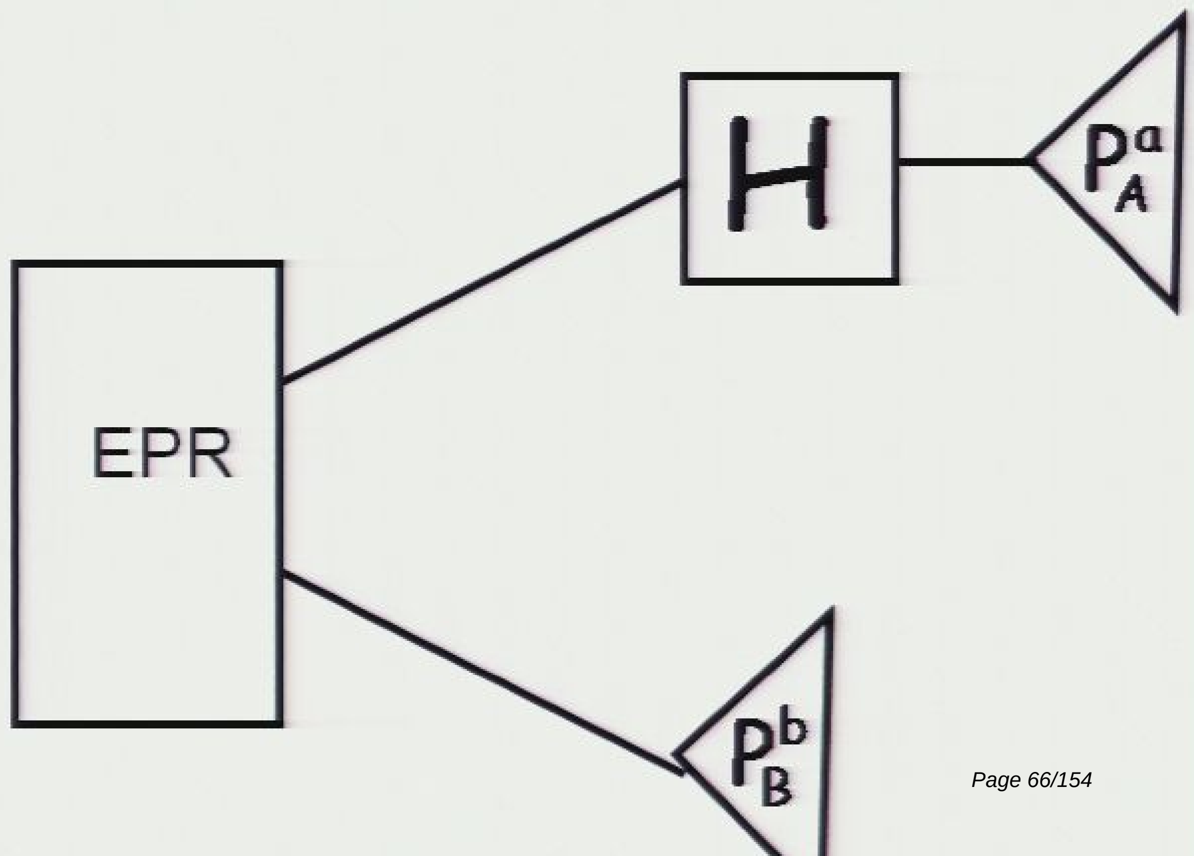
Still not composable…

The following does not necessarily compose



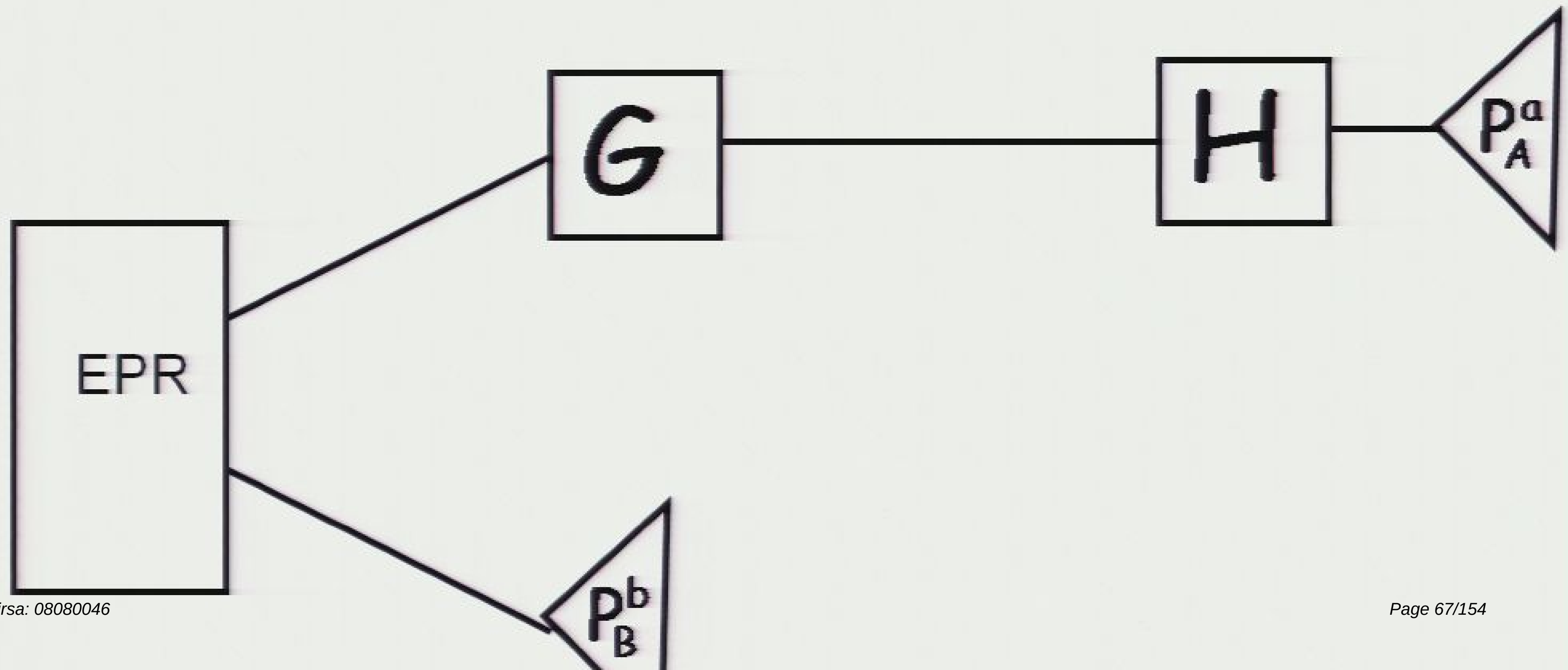
Still not composable…

The following does not necessarily compose



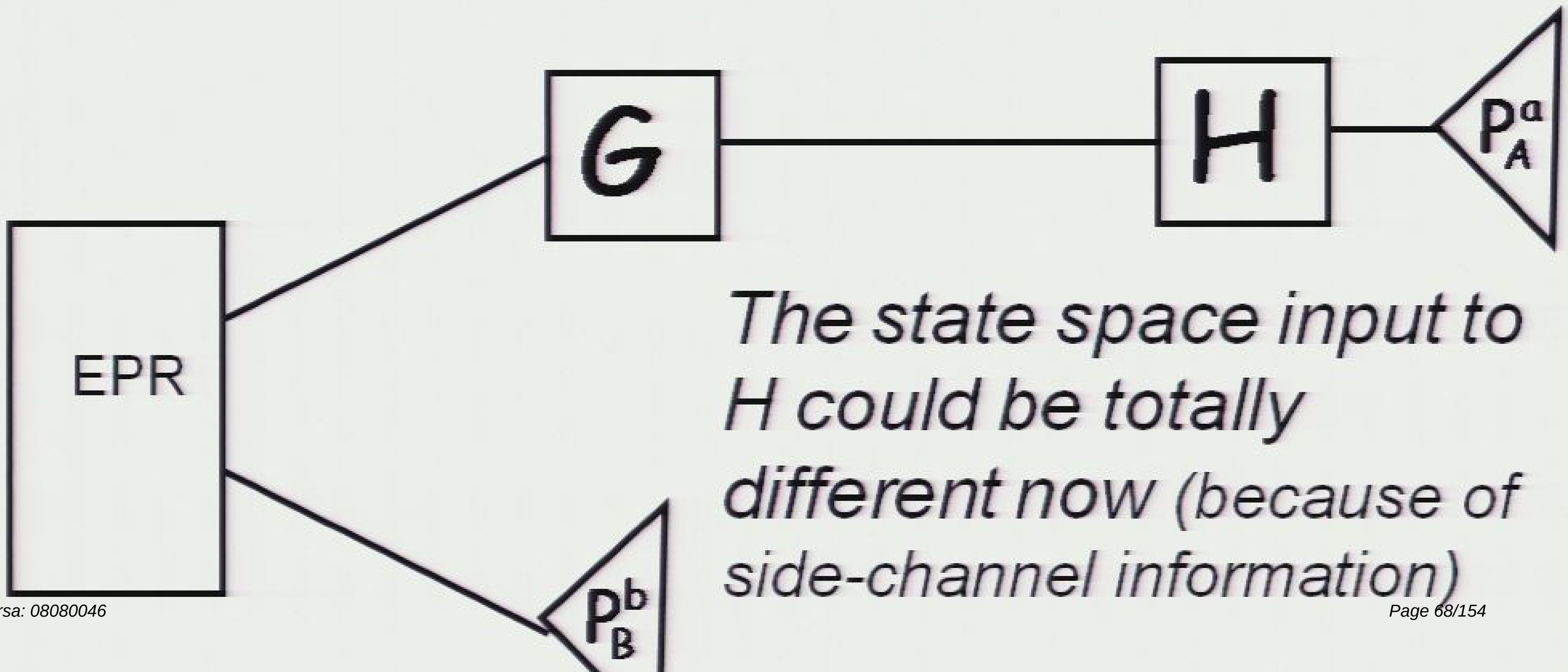
Still not composable…

The following does not necessarily compose



Still not composable...

The following does not necessarily compose



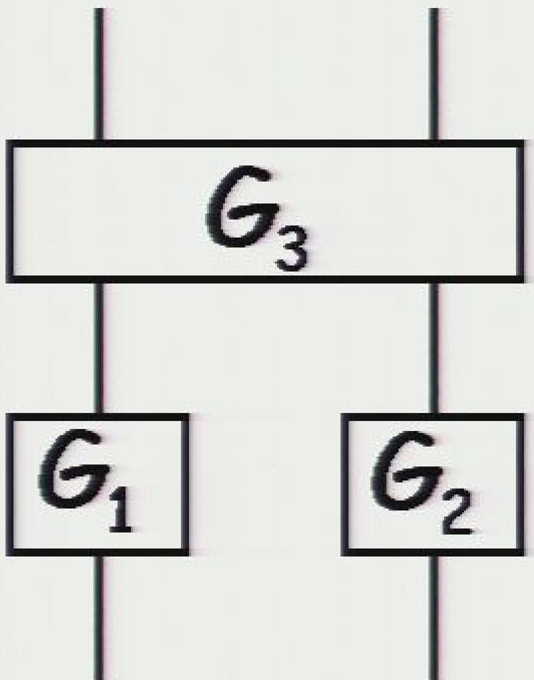
The state space input to H could be totally different now (because of side-channel information)

Goal

We ultimately wish to test the performance of an entire circuit (note that the circuits now flow up)

Goal

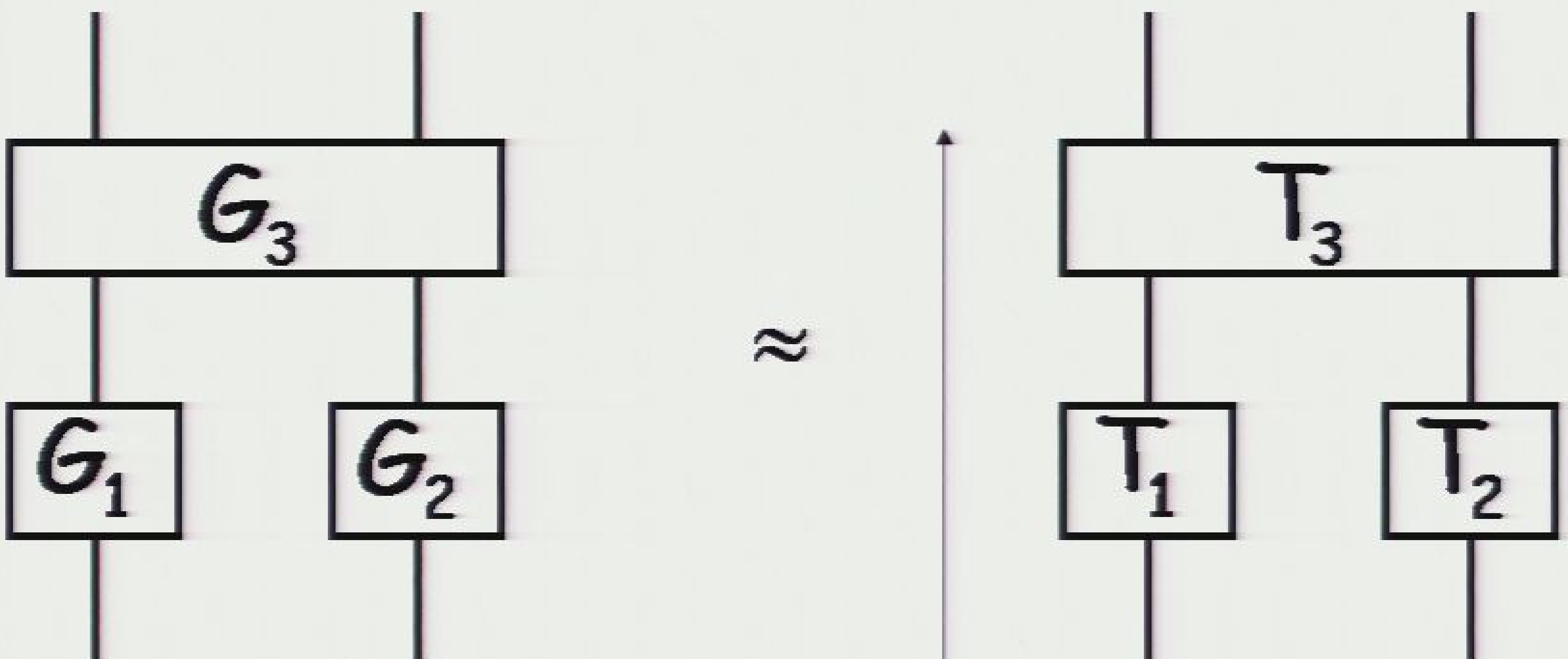
We ultimately wish to test the performance of an entire circuit *(note that the circuits now flow up)*



"actual physical gates"

Goal

We ultimately wish to test the performance of an entire circuit (note that the circuits now flow up)



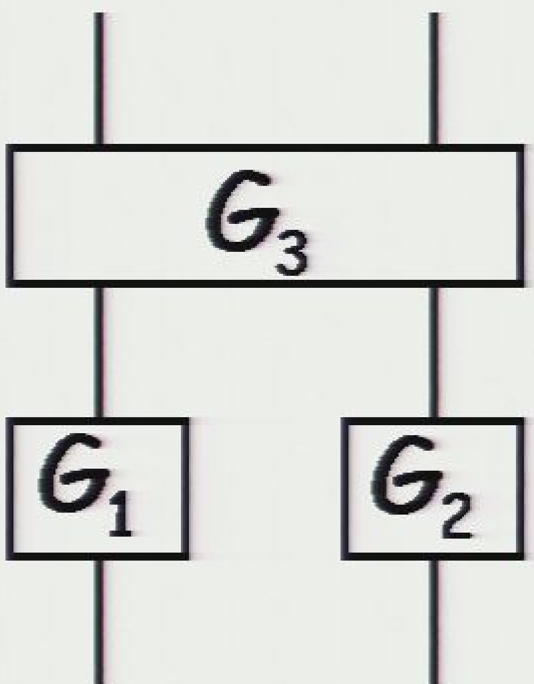
"actual physical gates" *"ideal gates"*

example

Suppose we wish to run the following circuit

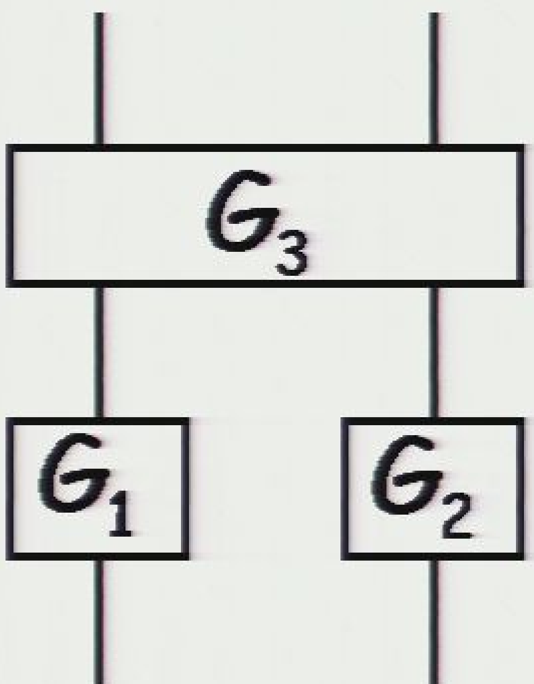
example

Suppose we wish to run the following circuit



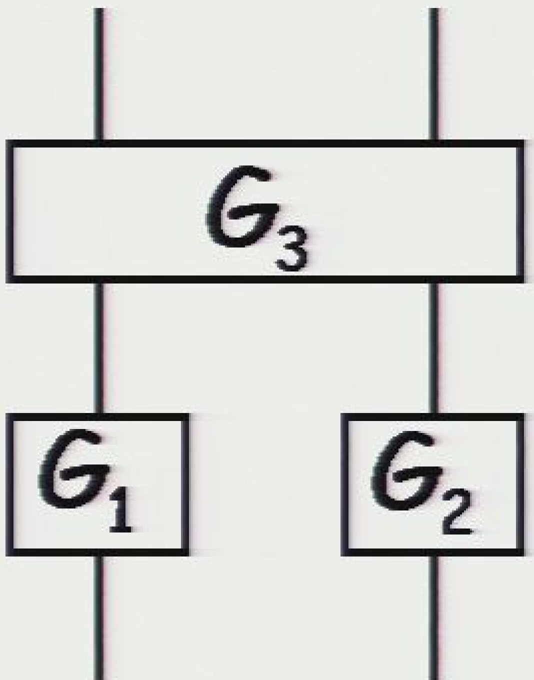
example

Suppose we wish to run the following circuit



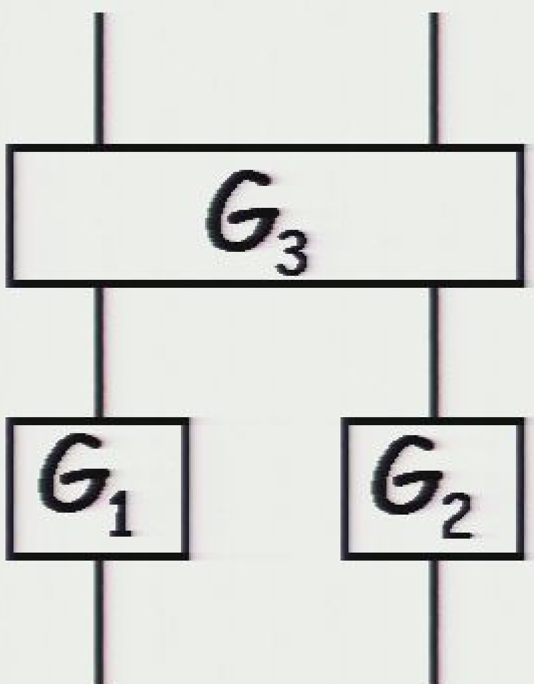
example

Suppose we wish to run the following circuit



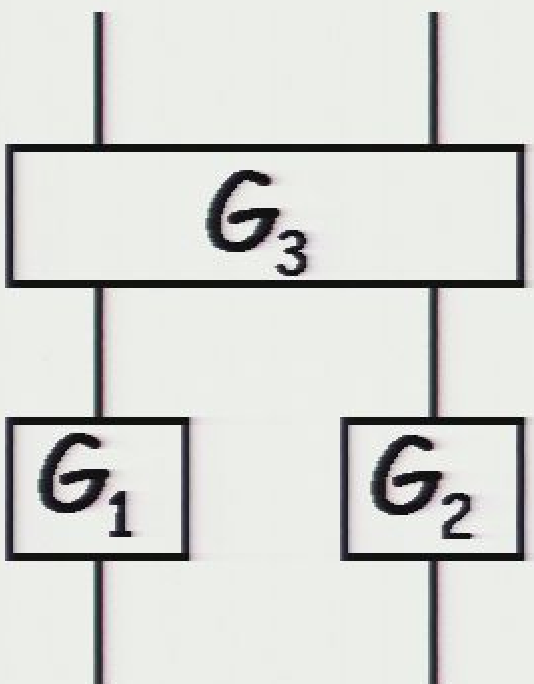
example

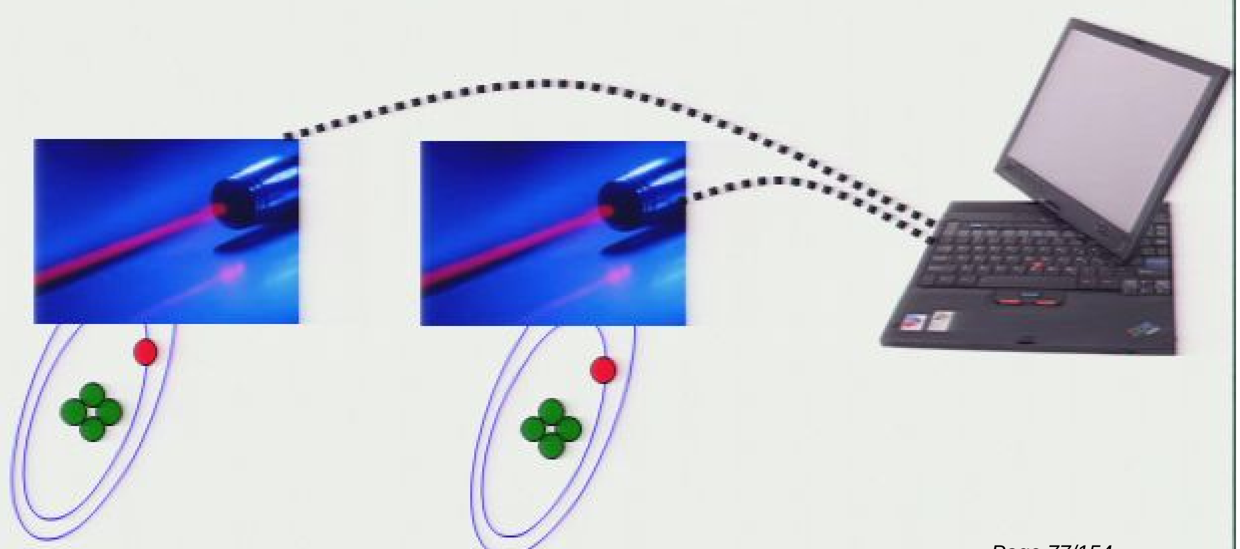
Suppose we wish to run the following circuit



example

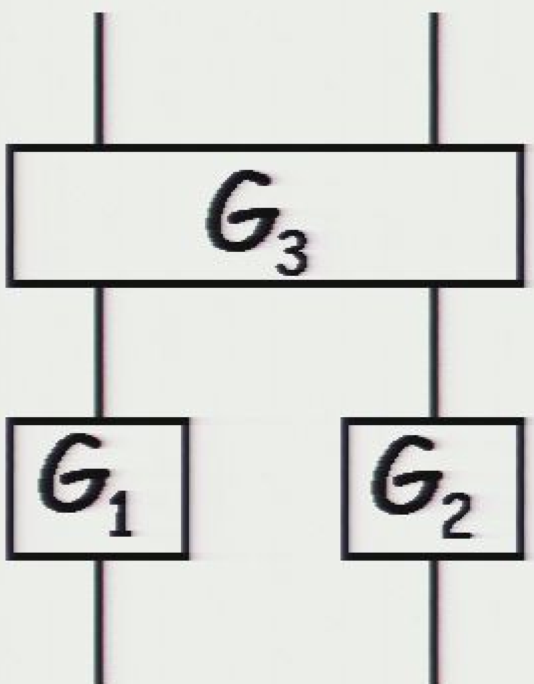
Suppose we wish to run the following circuit





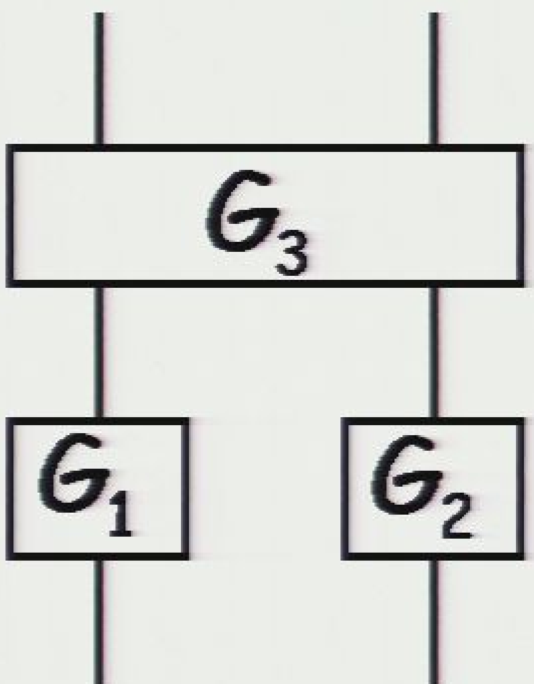
example

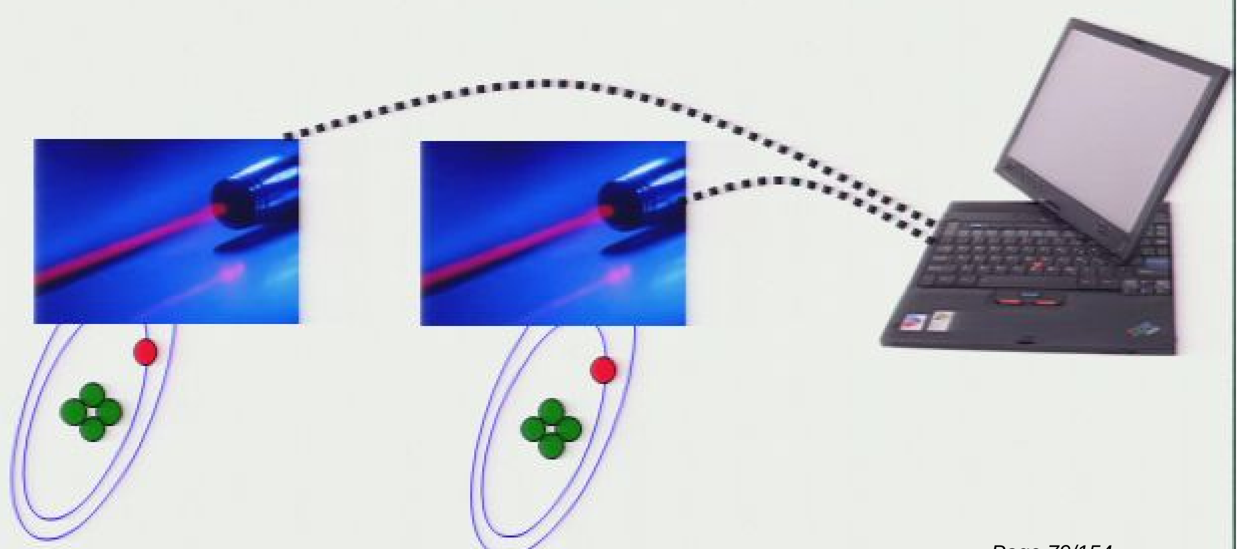
Suppose we wish to run the following circuit



example

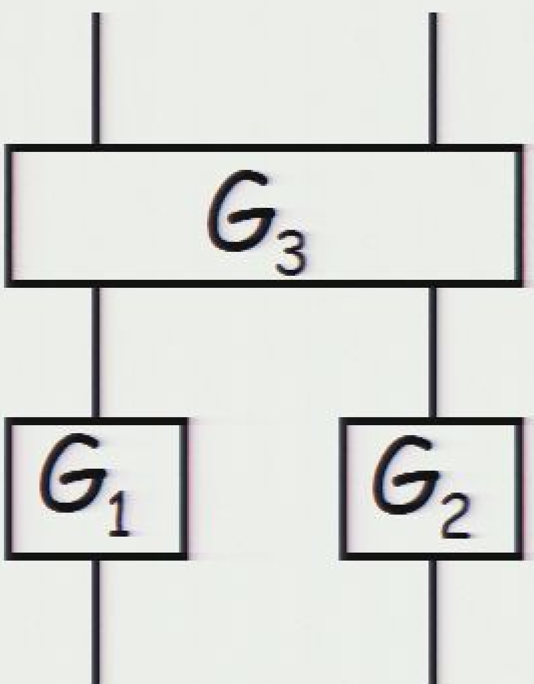
Suppose we wish to run the following circuit

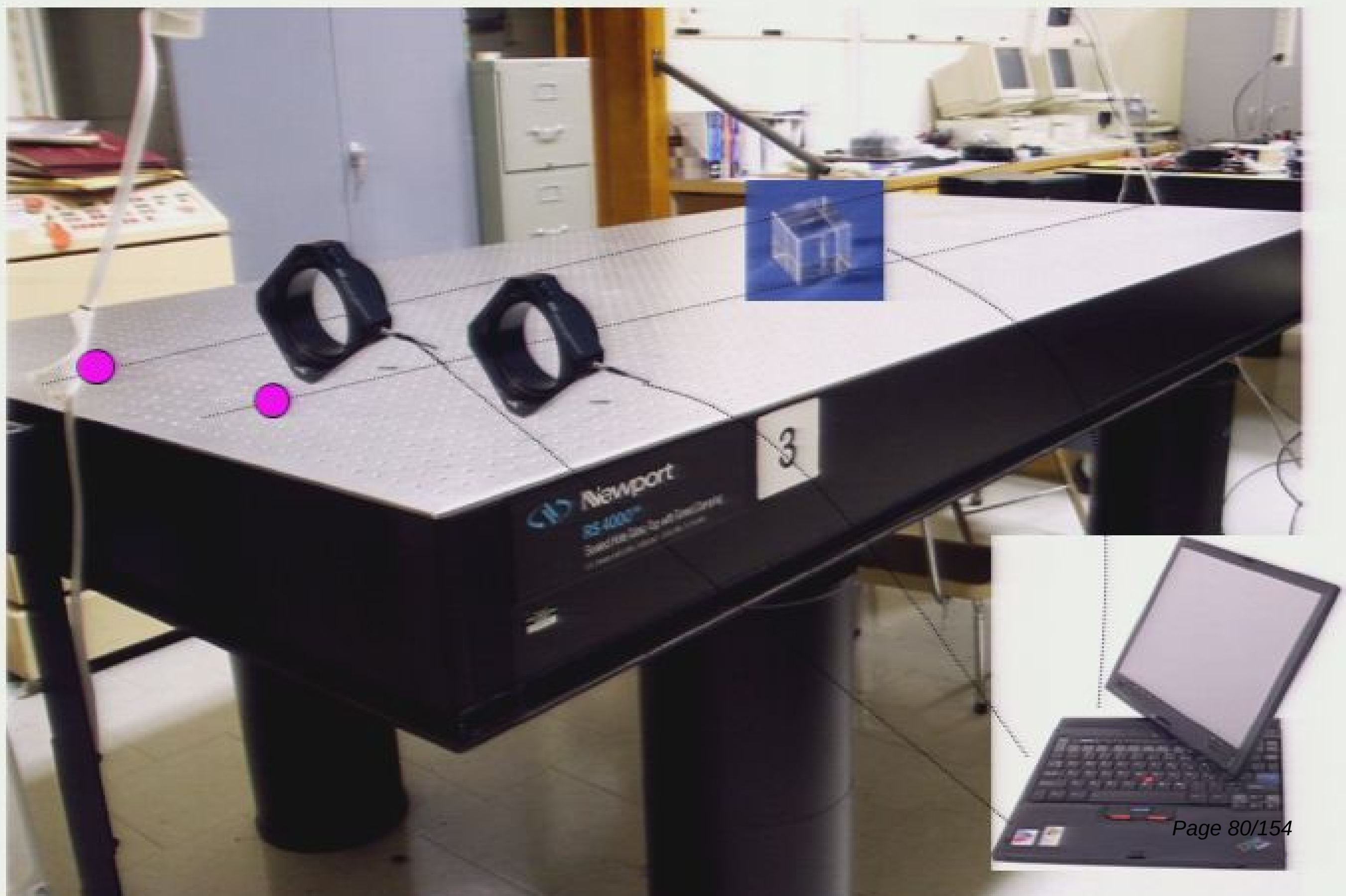




Example 2

Suppose we wish to run the following circuit





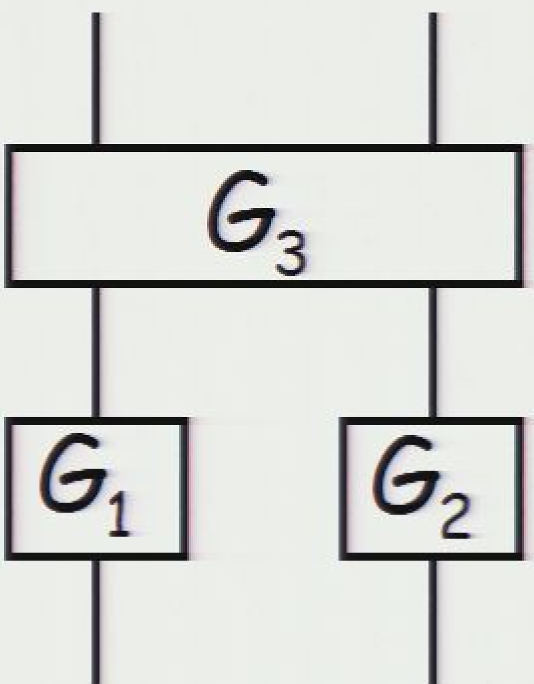
Another major challenge

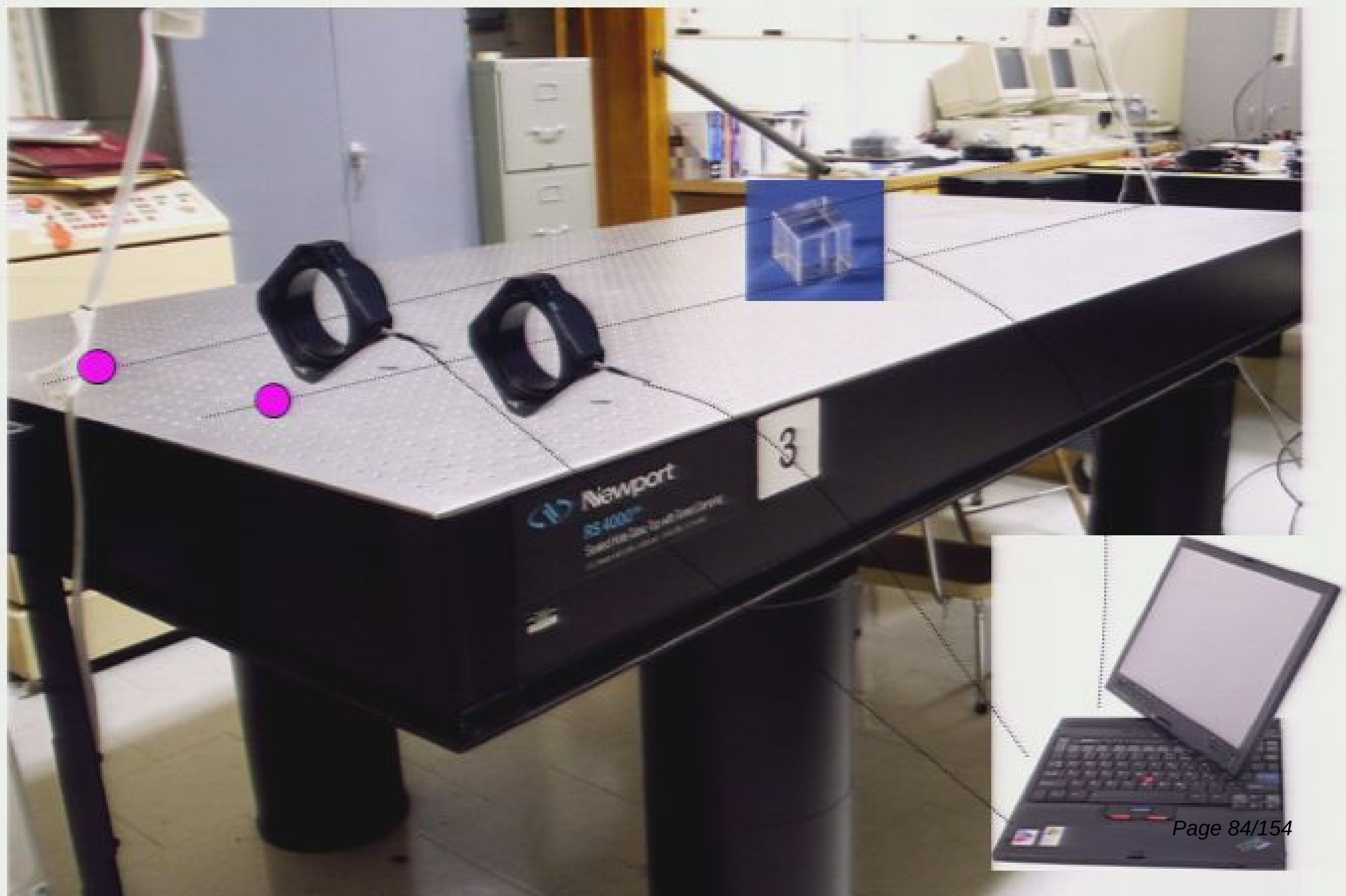
Another major challenge

Another major challenge

Example 2

Suppose we wish to run the following circuit





Another major challenge

No finite set of tests will lead to a foolproof test. Why not?

Another major challenge

No finite set of tests will lead to a foolproof test. Why not?

The gates can communicate the full (classical) history of their past to future gates in hidden degrees of freedom. Thus each gate knows the history of its input qubit(s), and can recognize when its history is no longer part of a test.

Another major challenge

No finite set of tests will lead to a foolproof test. Why not?

The gates can communicate the full (classical) history of their past to future gates in hidden degrees of freedom. Thus each gate knows the history of its input qubit(s), and can recognize when its history is no longer part of a test.

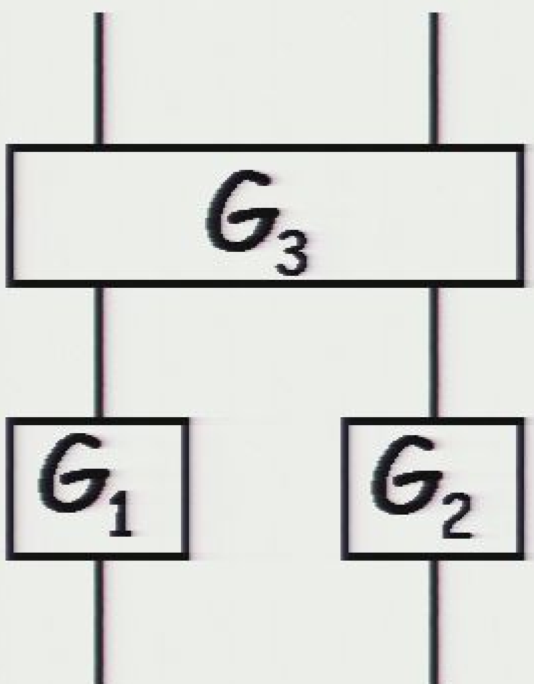
Hint: Every circuit we would wish to run needs to also be part of a test.

example

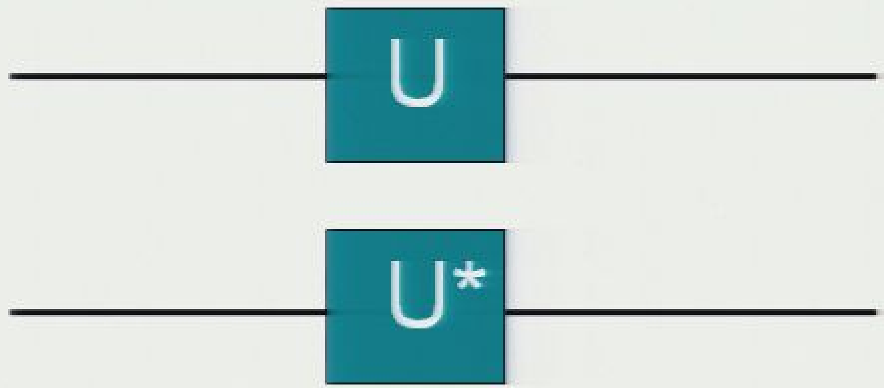
Suppose we wish to run the following circuit

example

Suppose we wish to run the following circuit

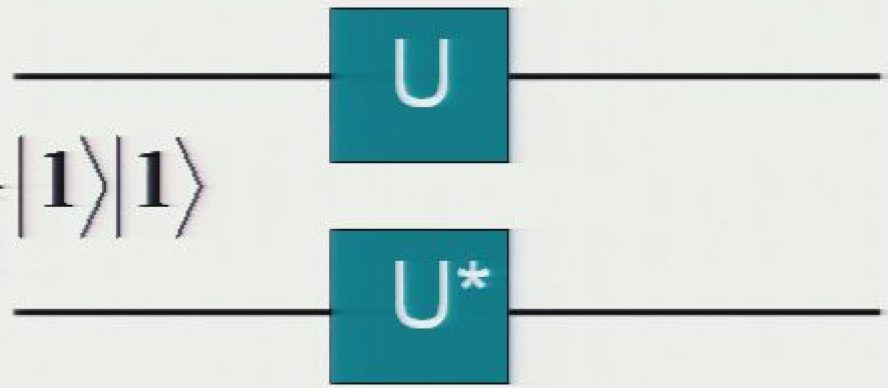


Property of EPR pairs



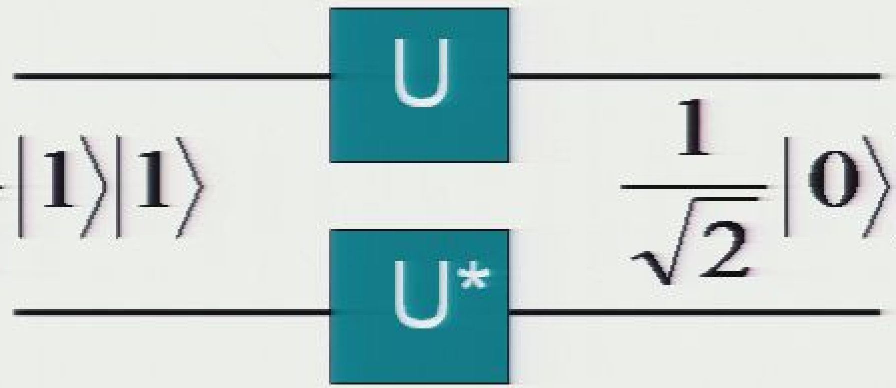
Property of EPR pairs

$$\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$



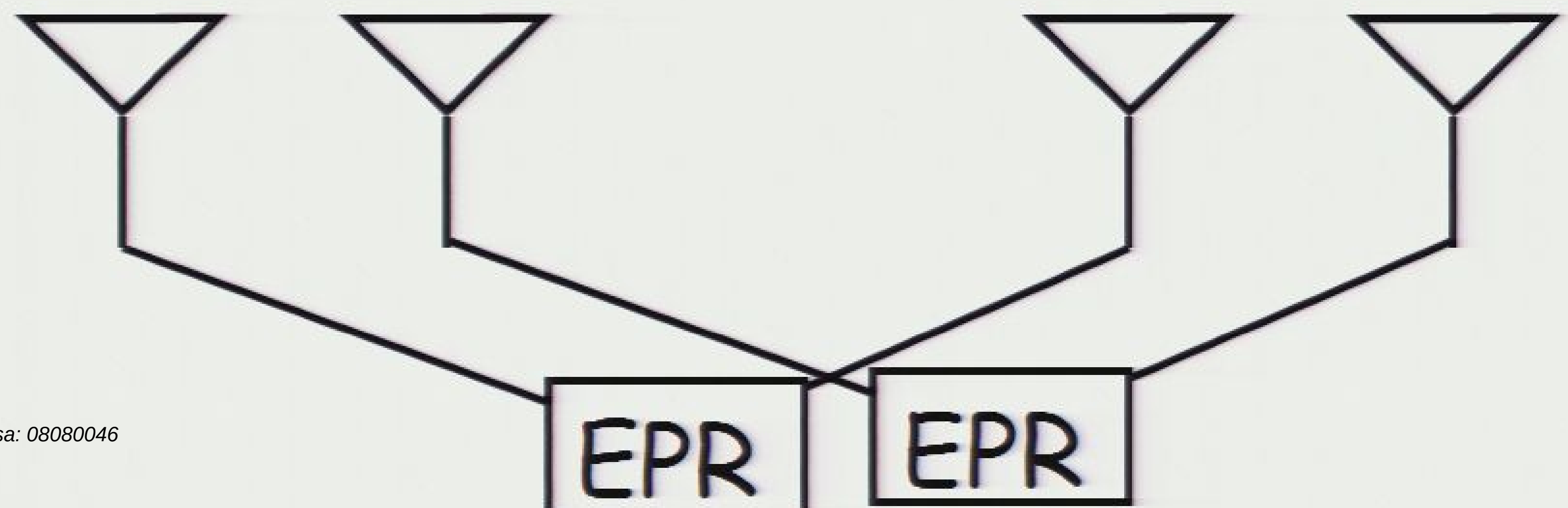
Property of EPR pairs

$$\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

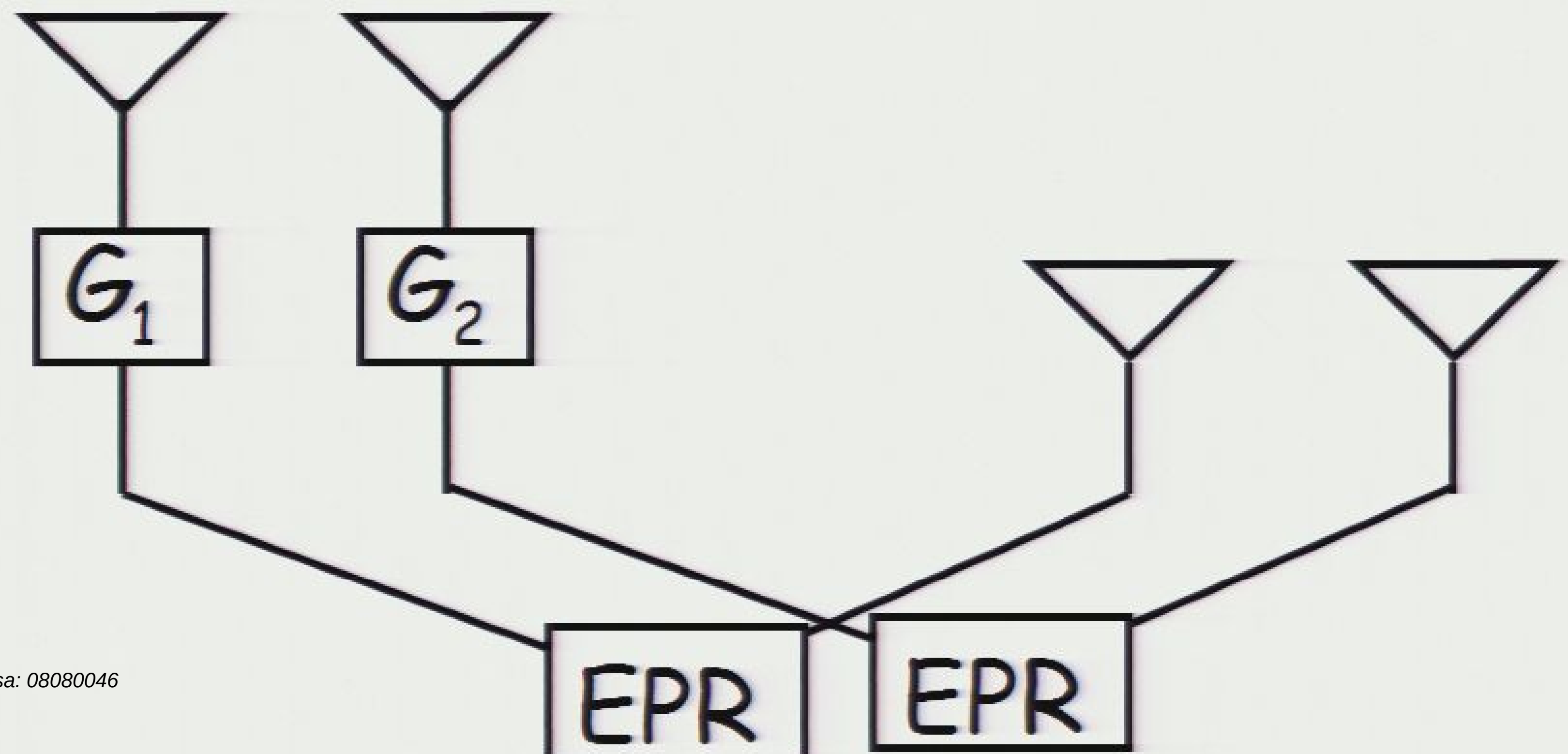


$$\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

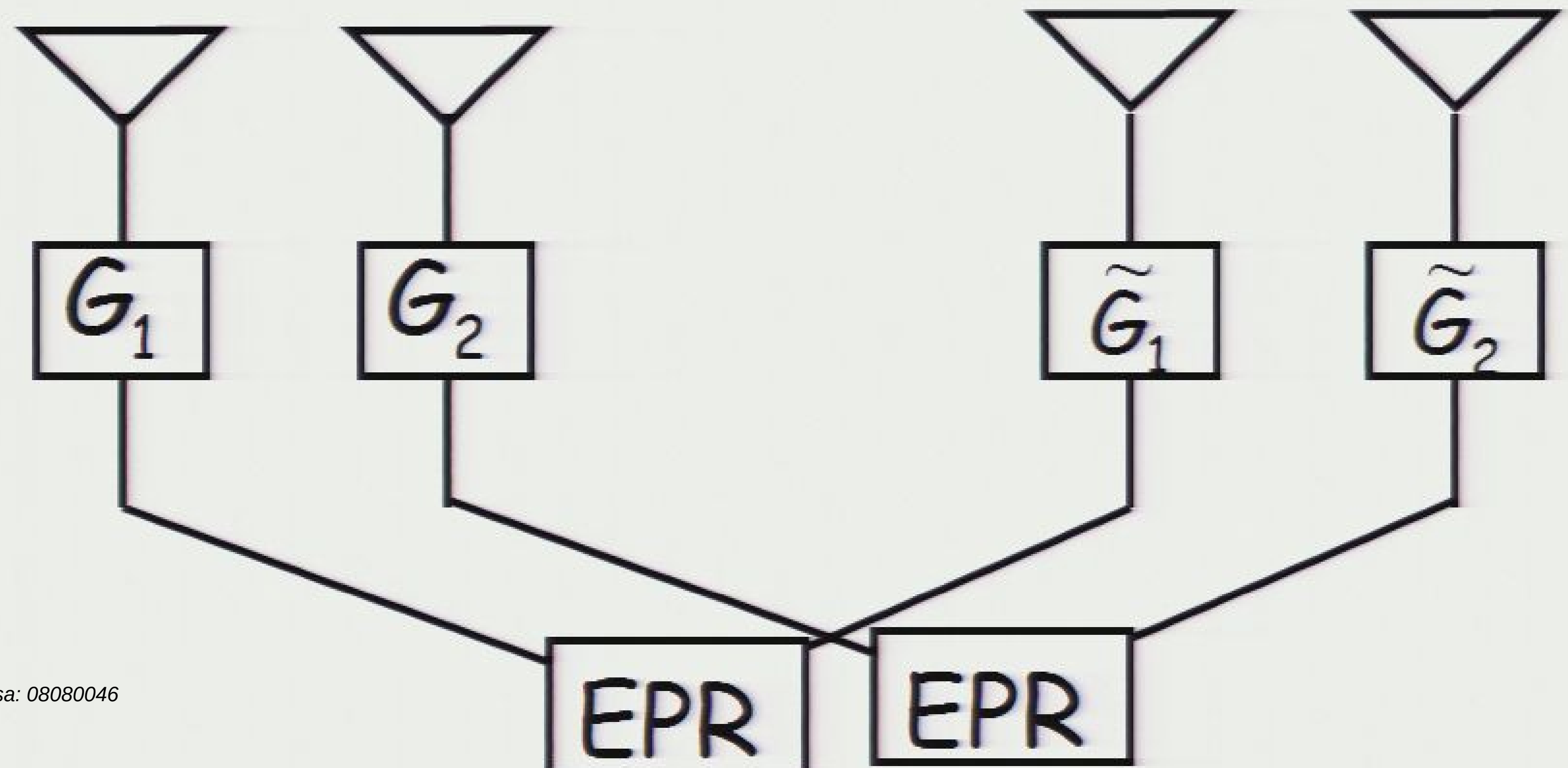
example



“tomography test”

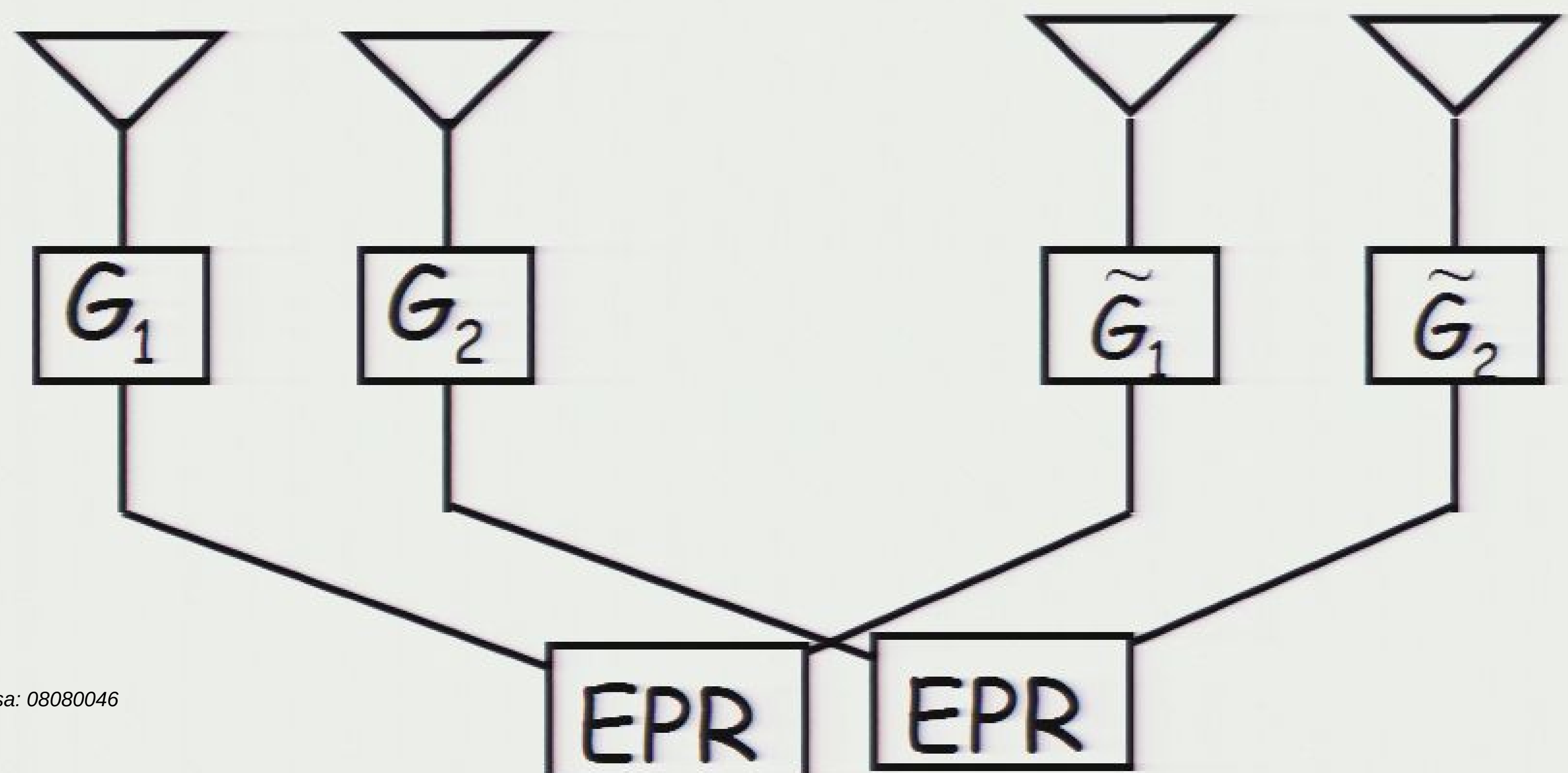


"conspiracy test"

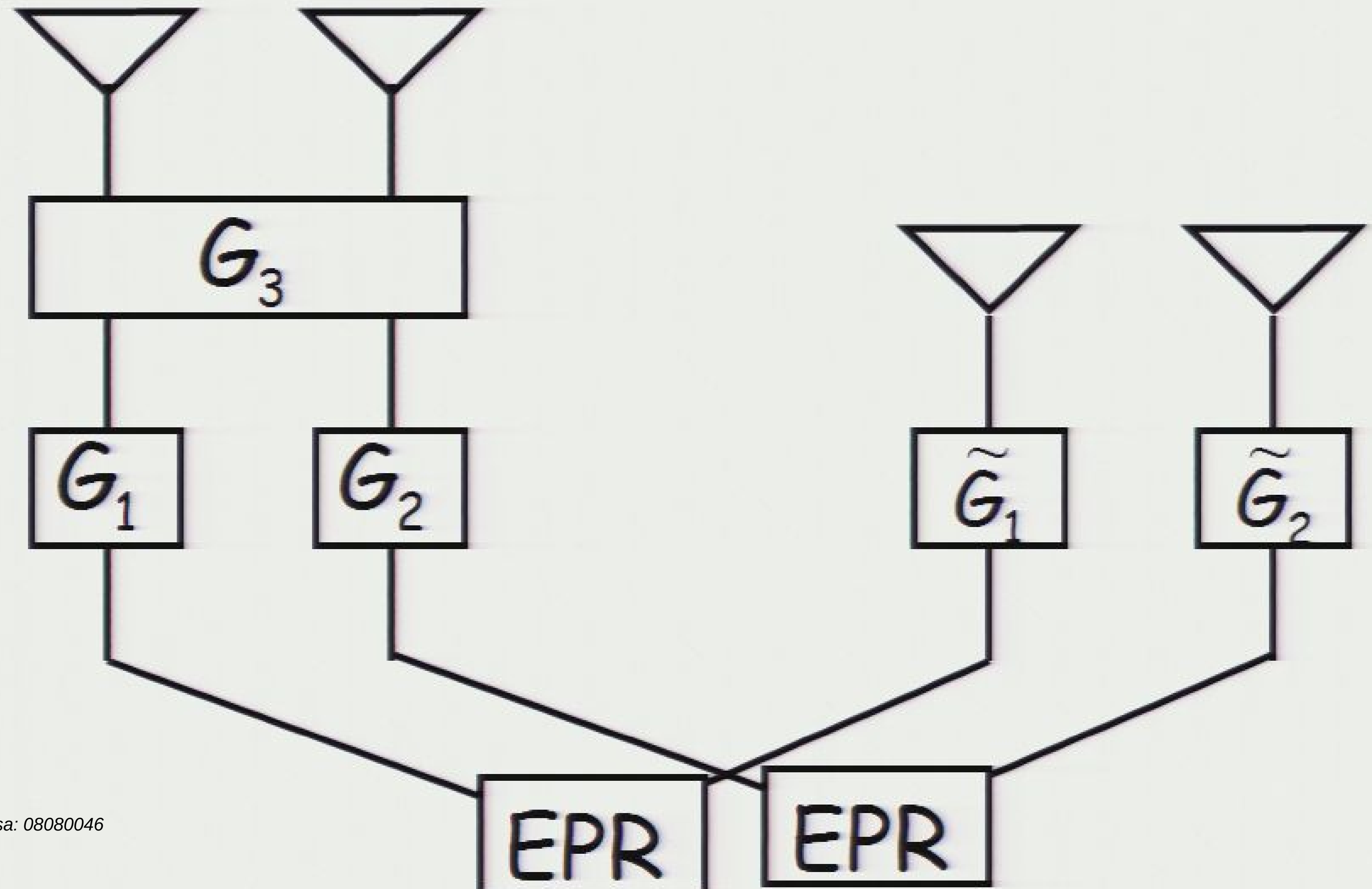


“conspiracy test”

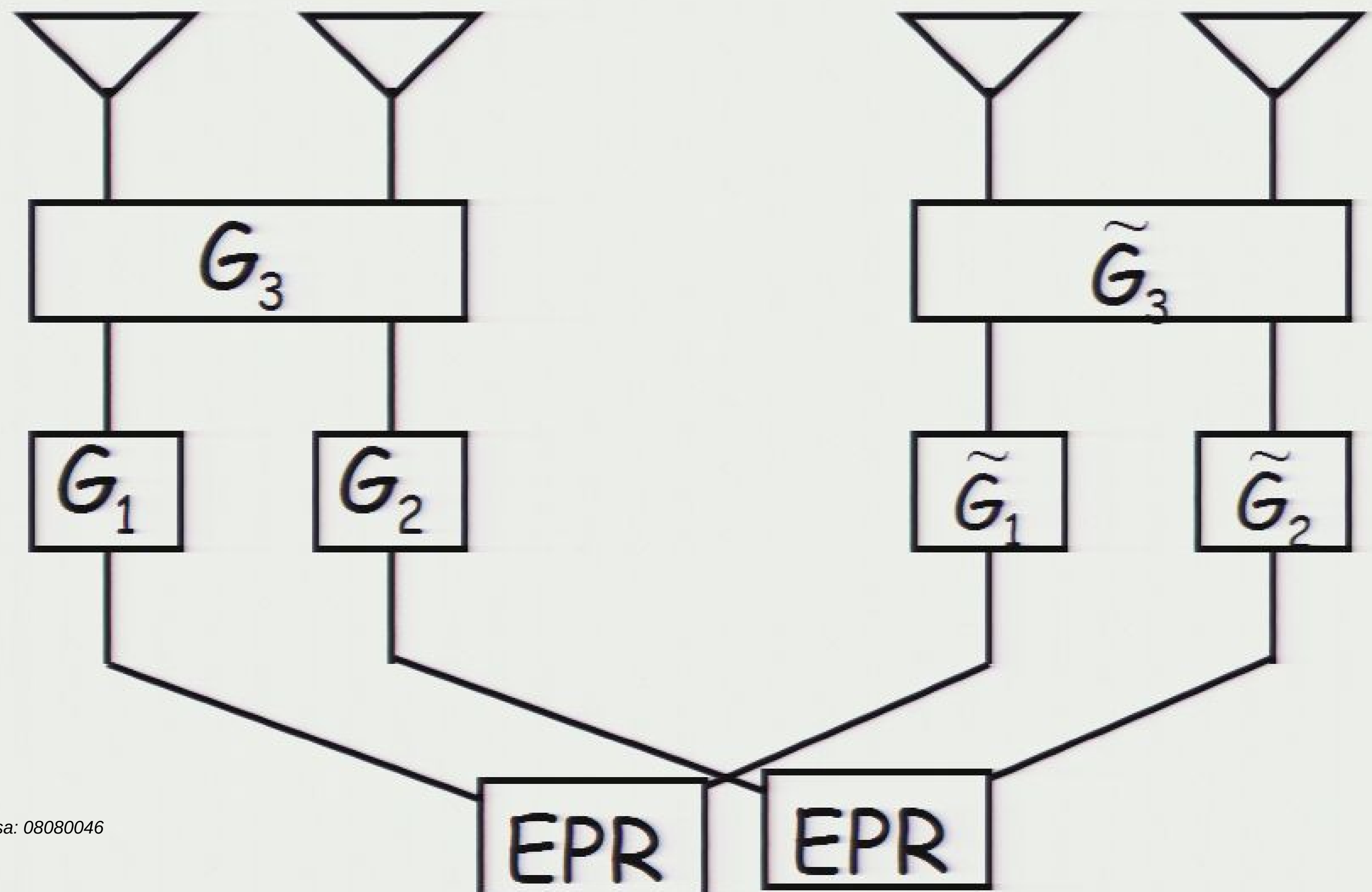
If $\widetilde{G}_1 = G_1^*$*, then this should recreate two EPR pairs.*



Tomography test

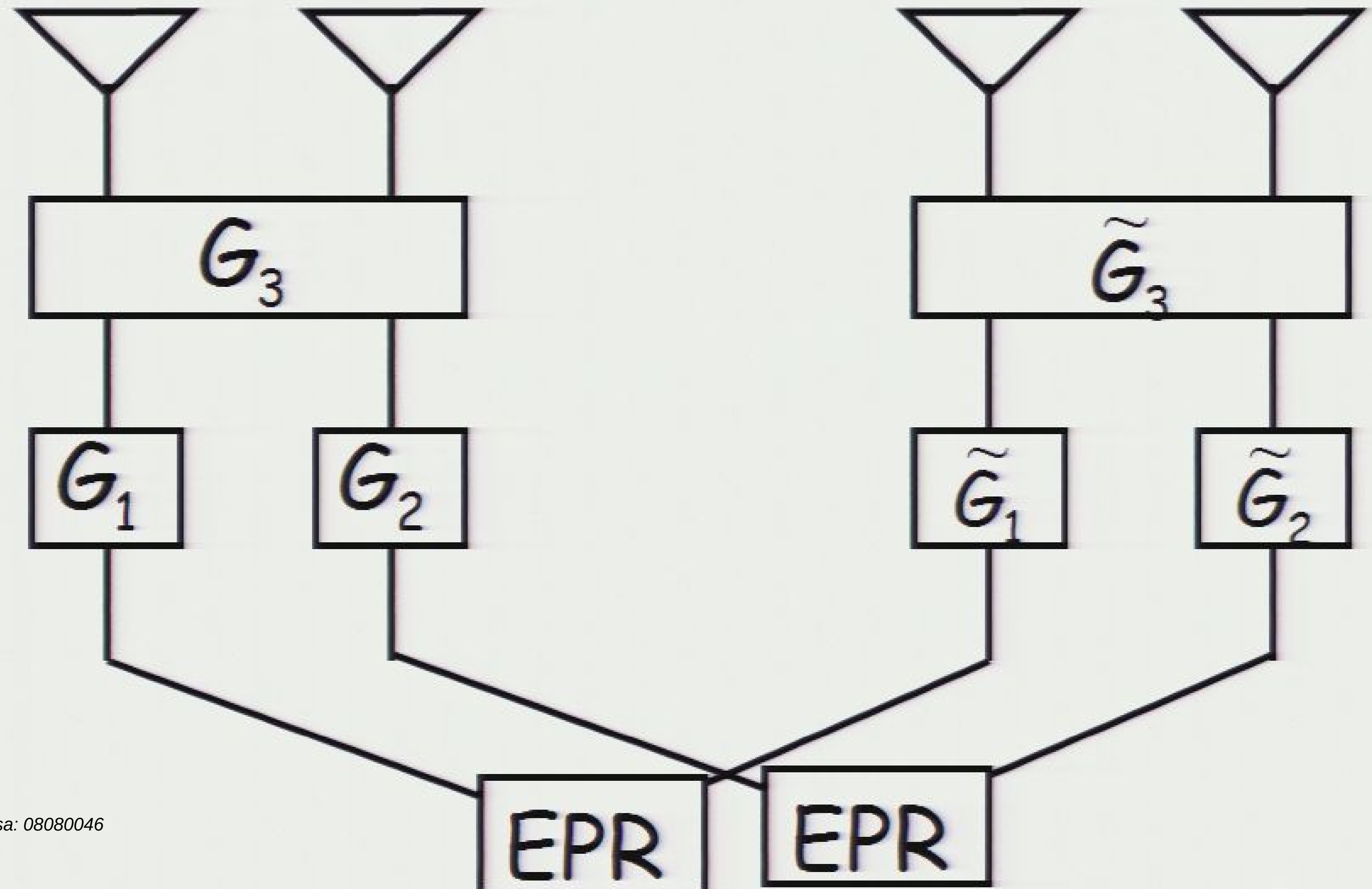


Conspiracy test



Some technical points

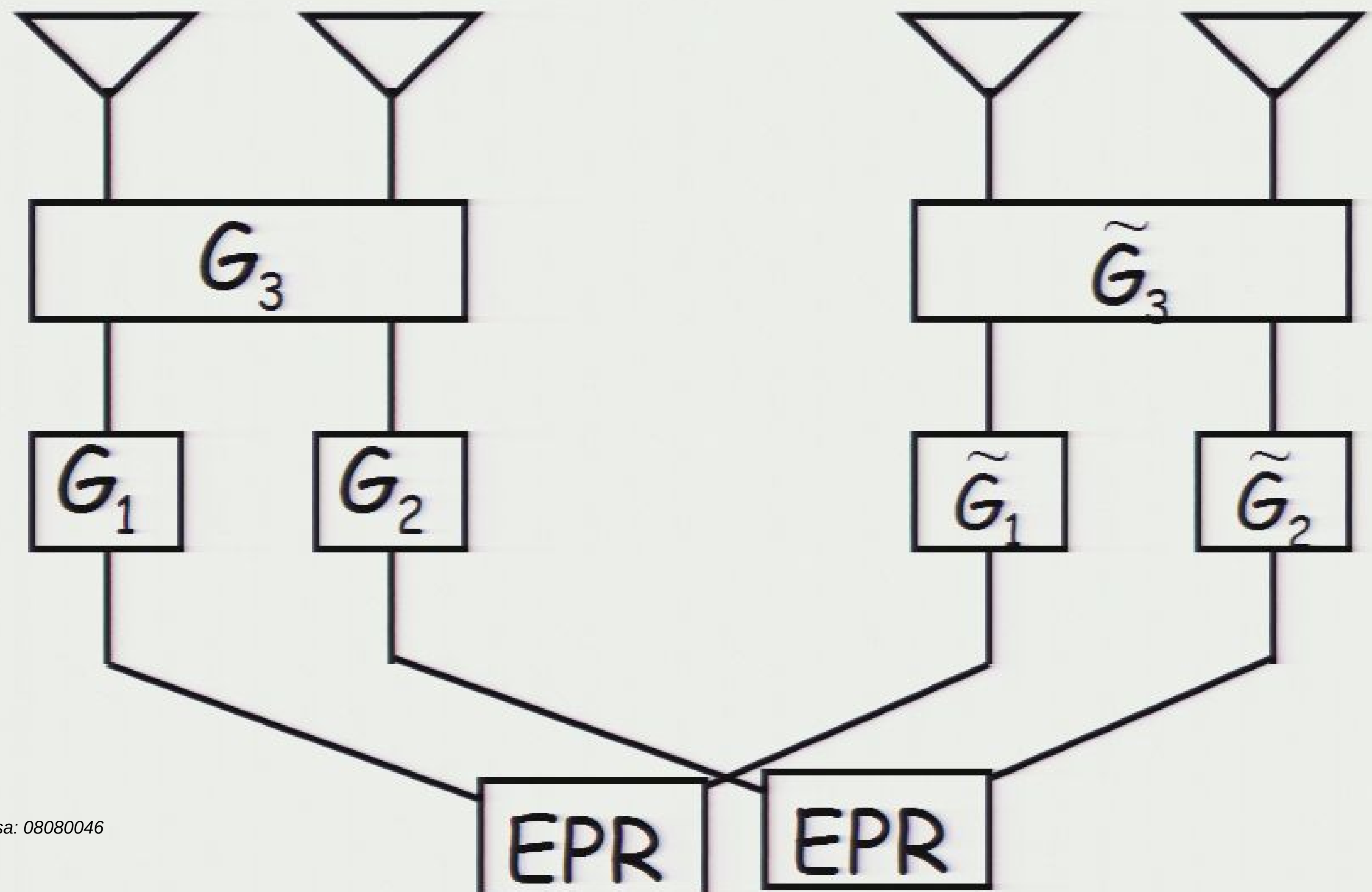
Conspiracy test

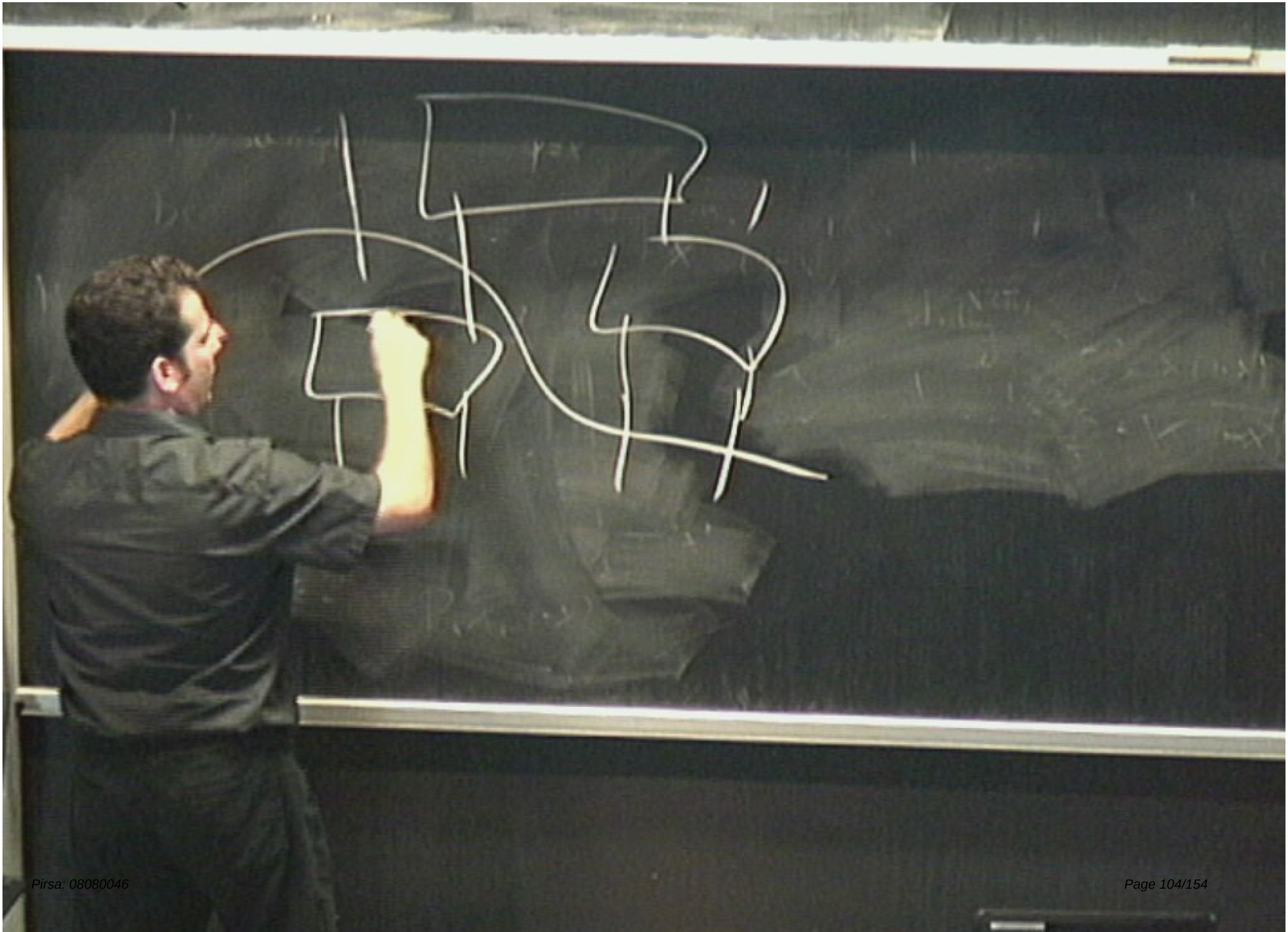


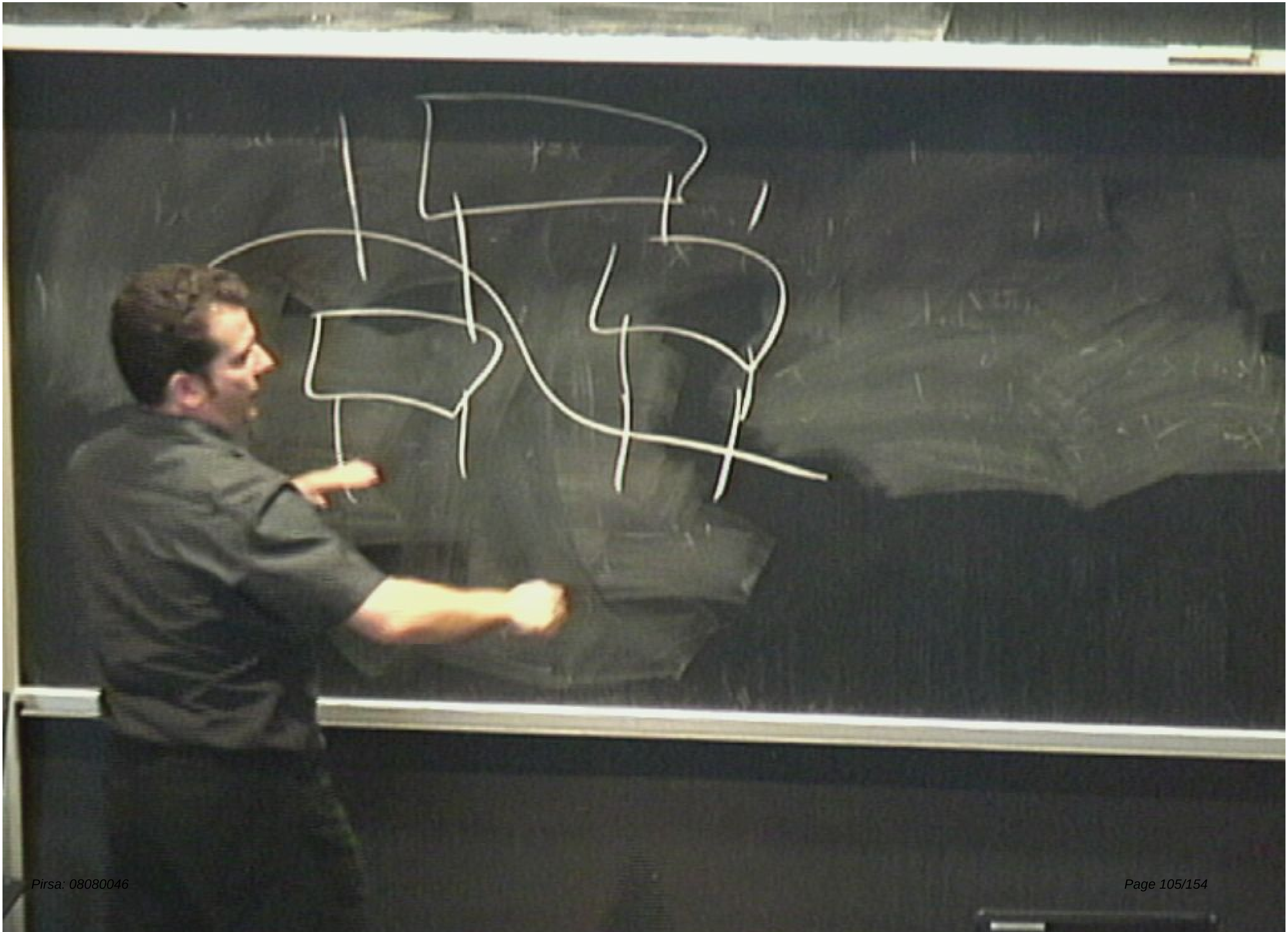
Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

Conspiracy test

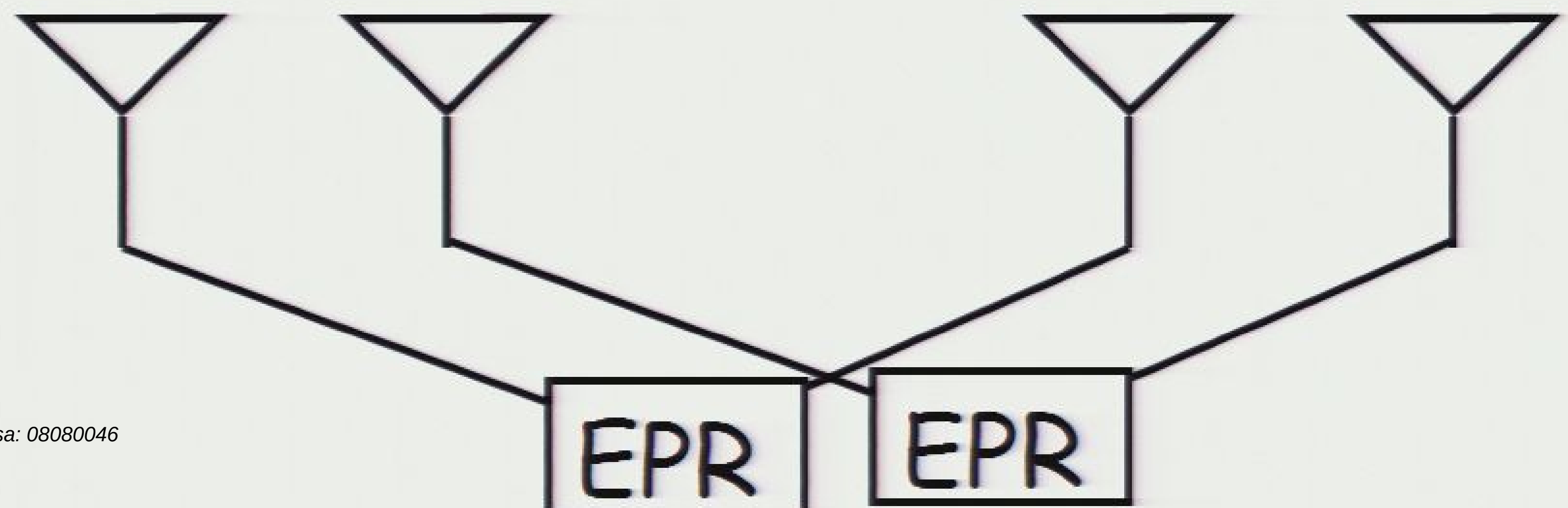






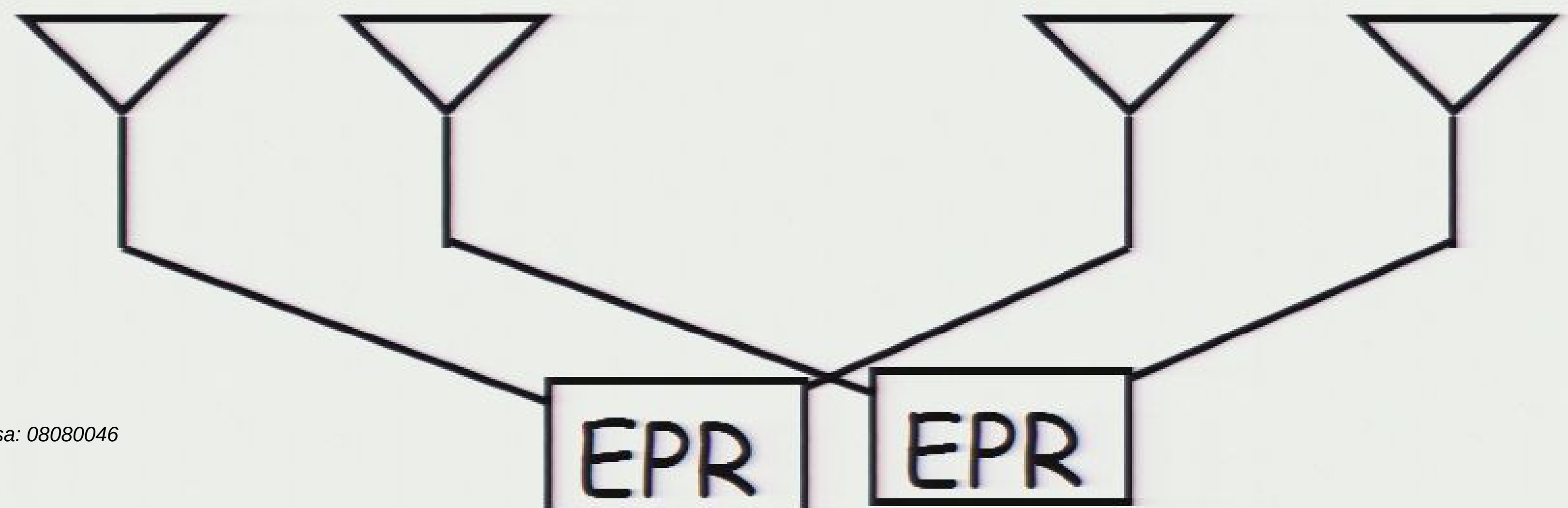
example

Verify the initial qubit sources.

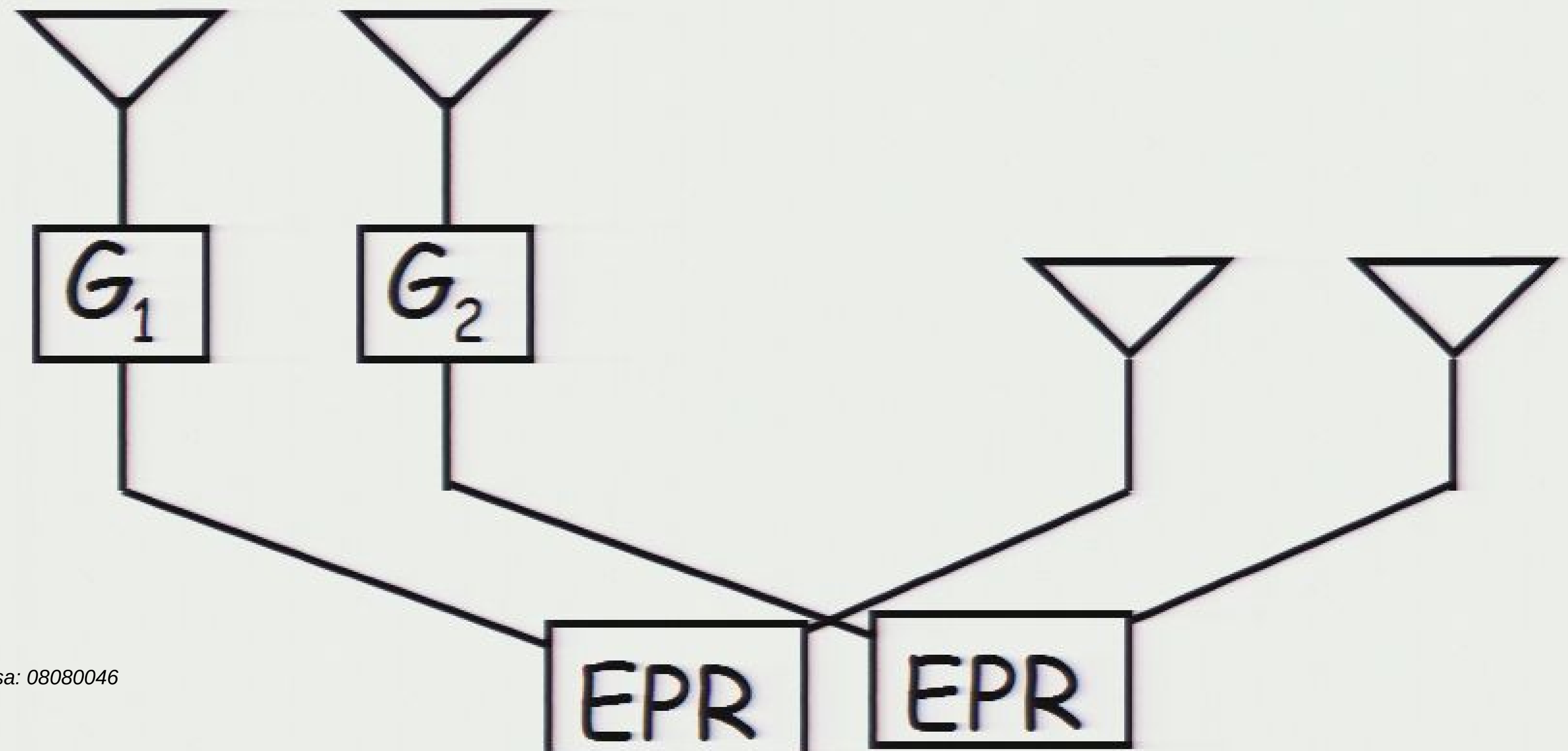


example

Verify the initial qubit sources.

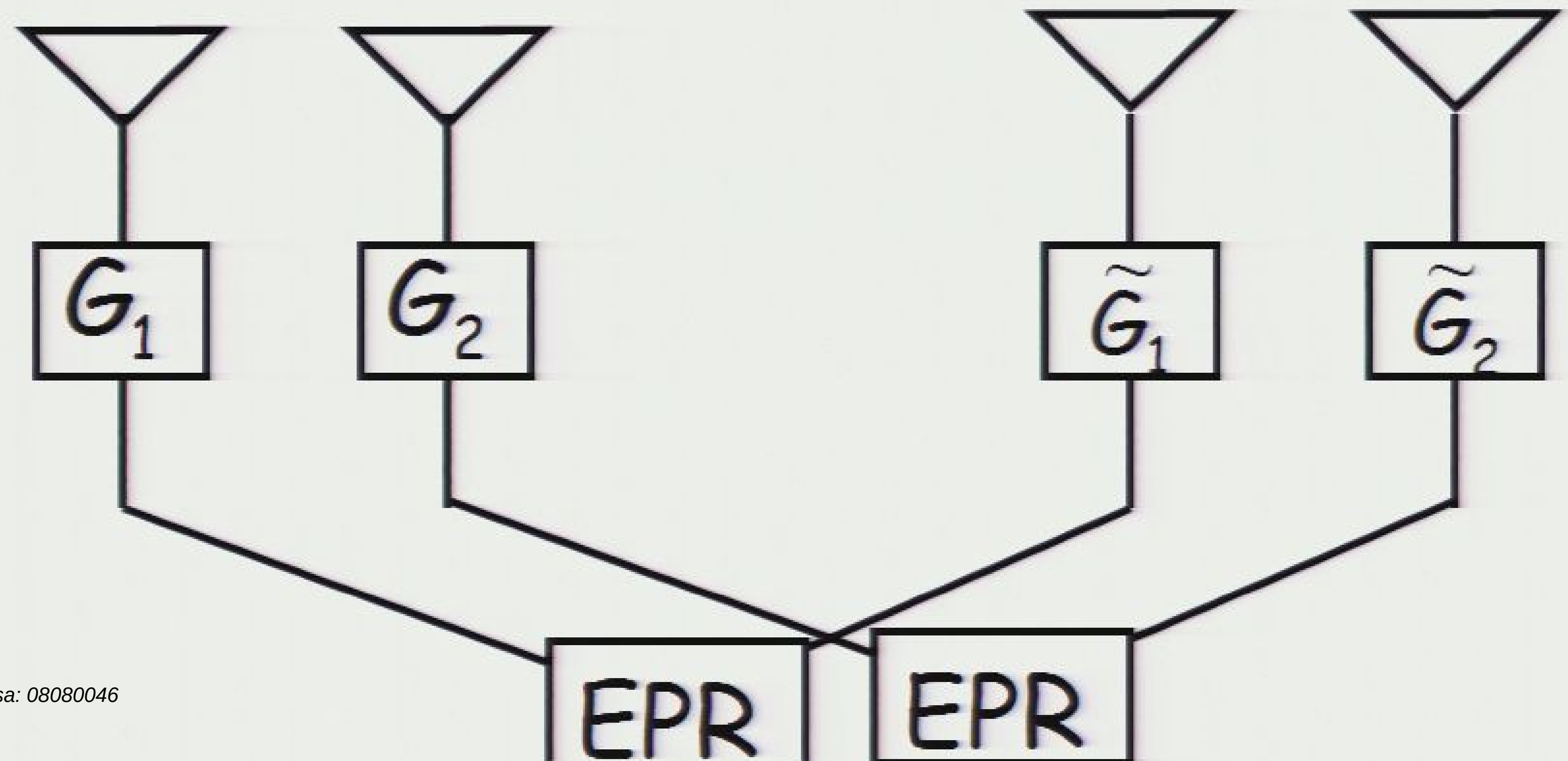


“tomography test”

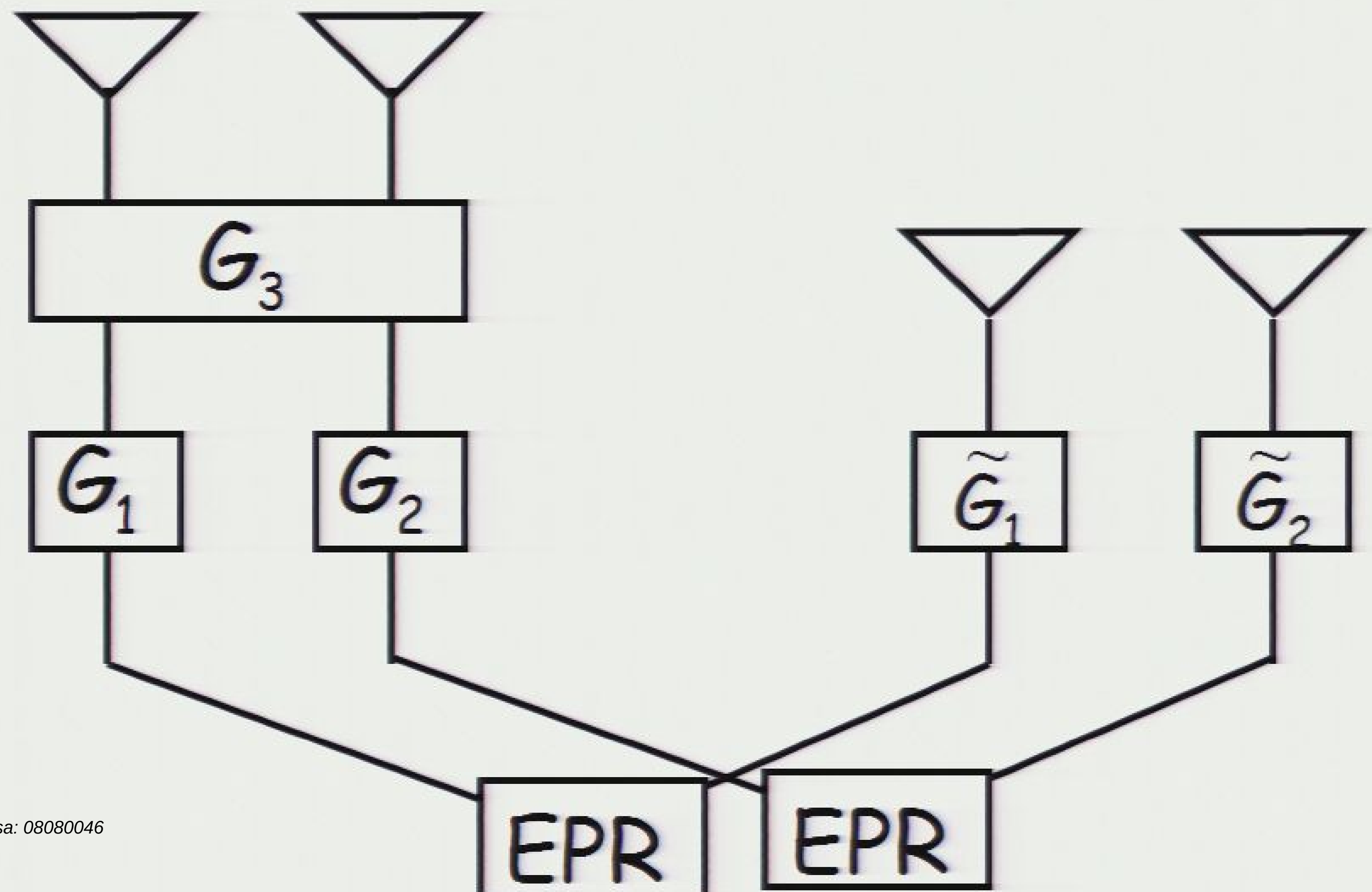


"conspiracy test"

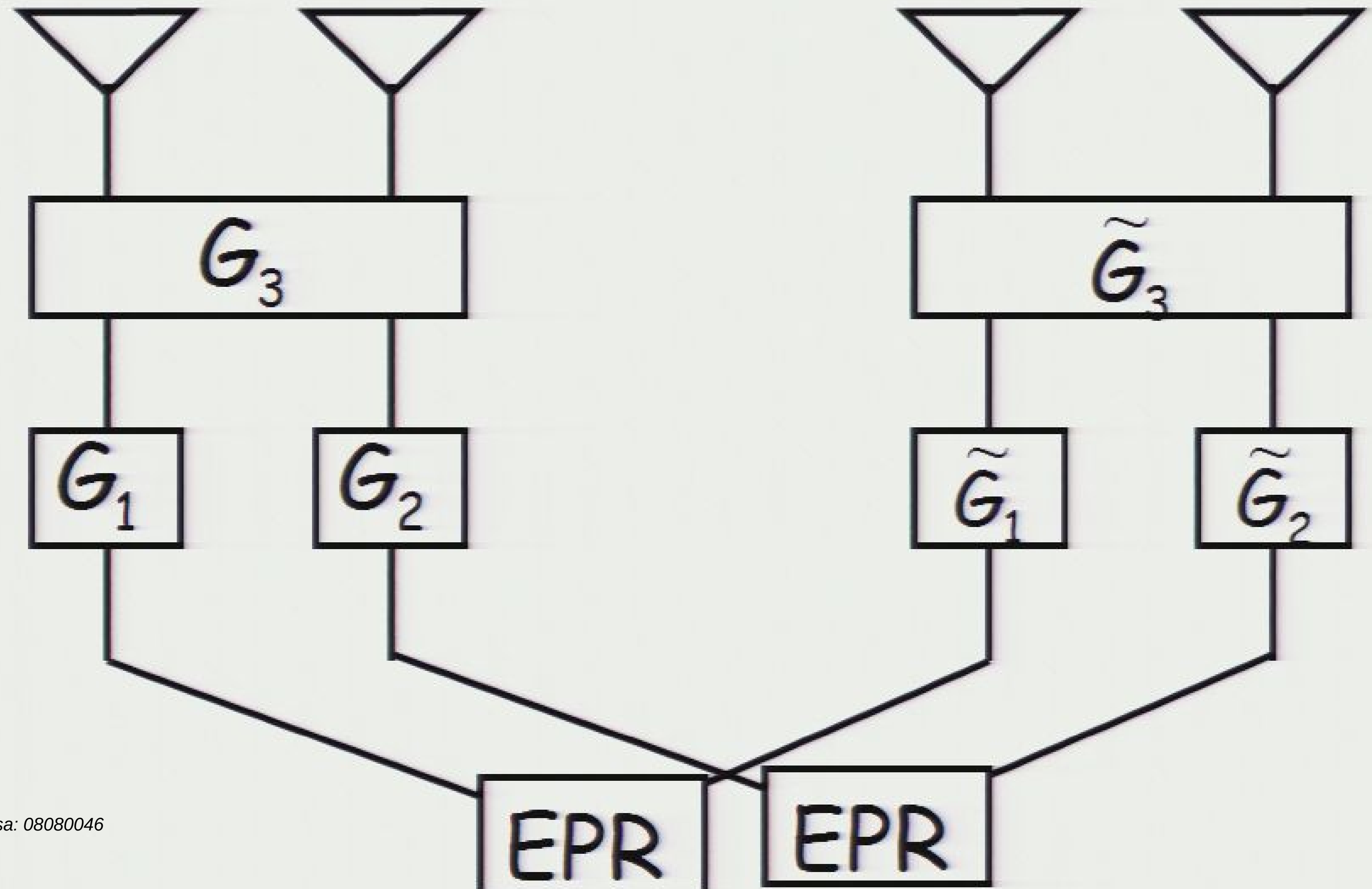
If $\tilde{G}_1 = G_1^*$, *then this should recreate two EPR pairs.*



Tomography test



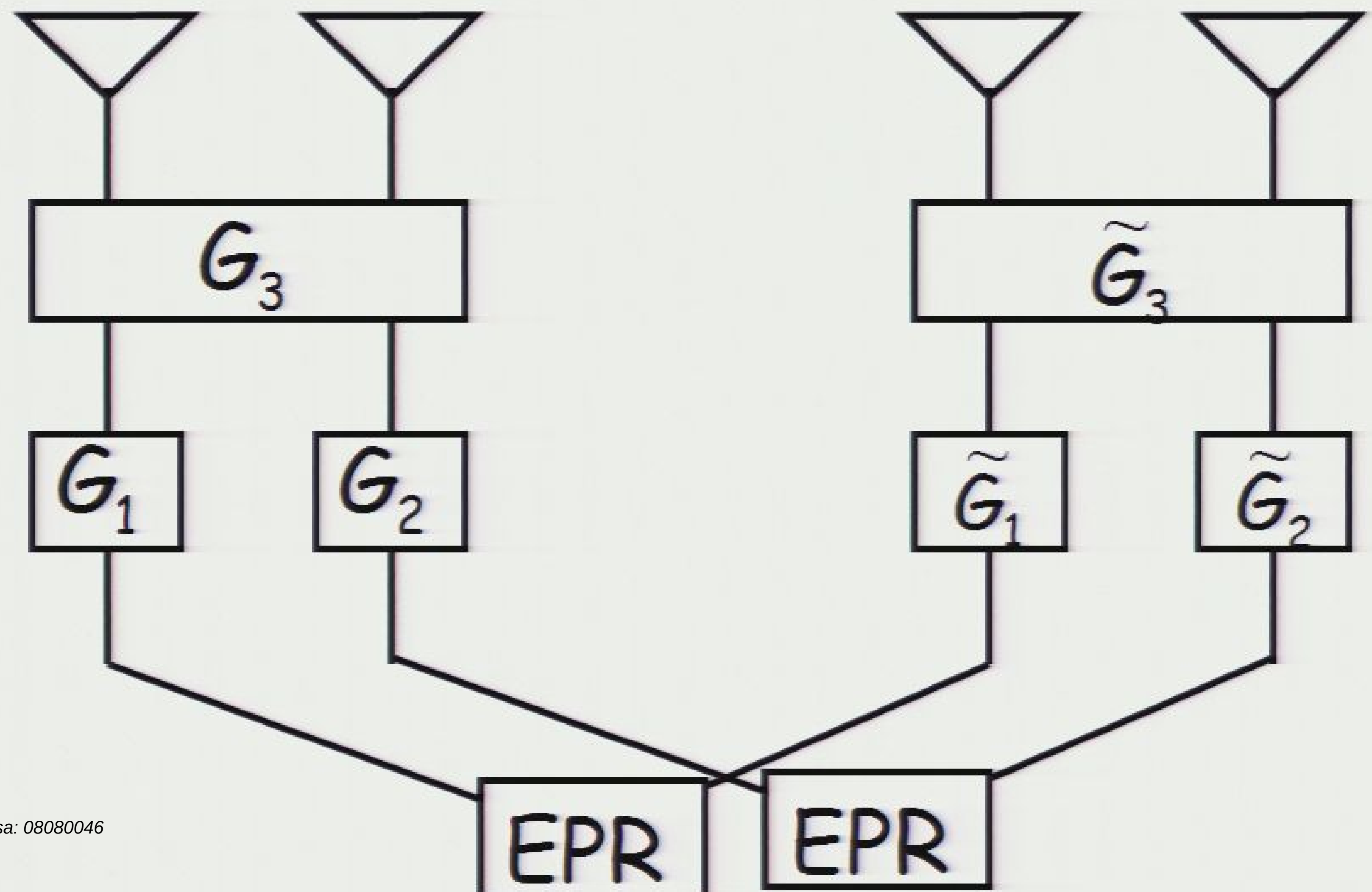
Conspiracy test

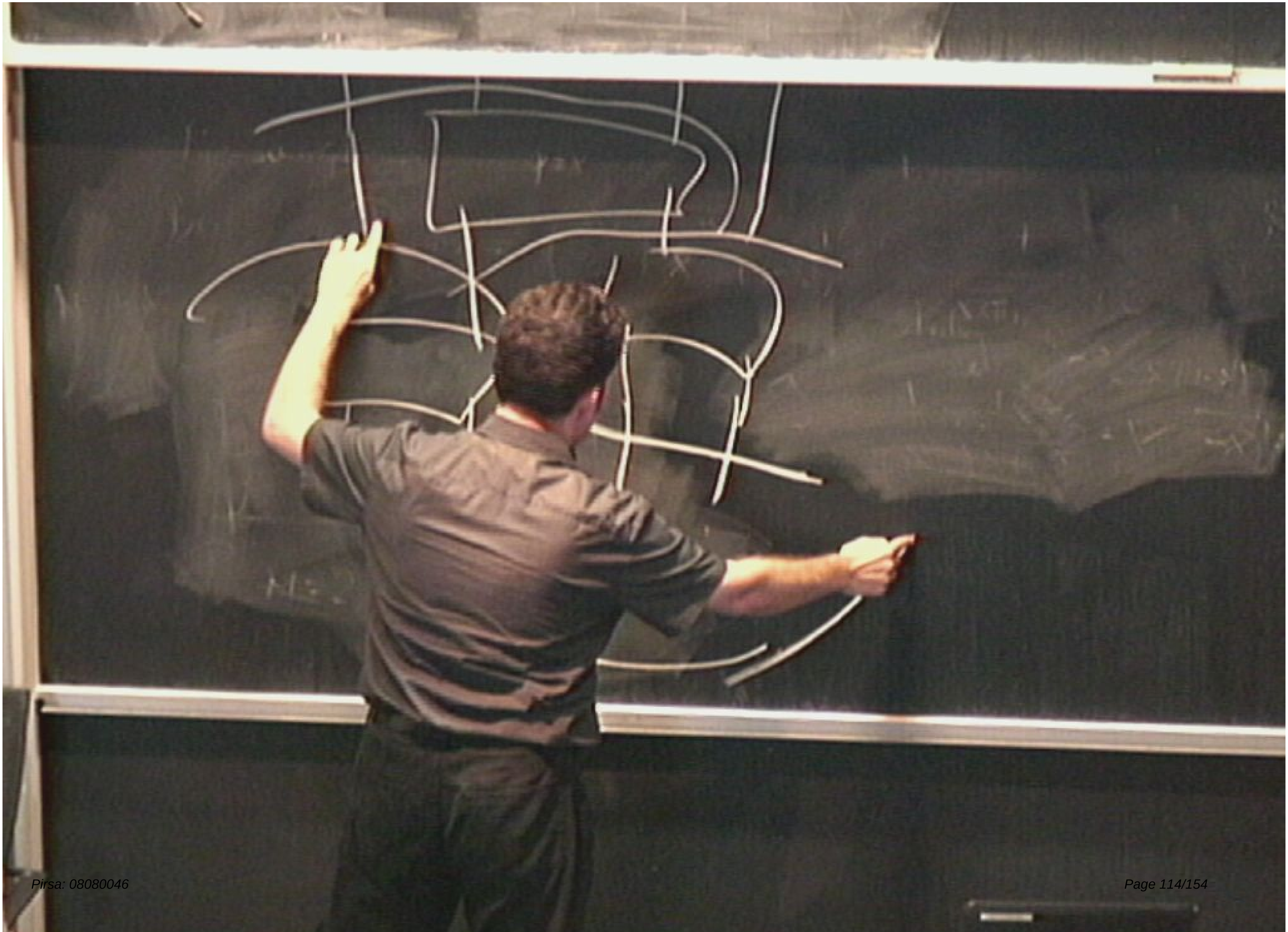


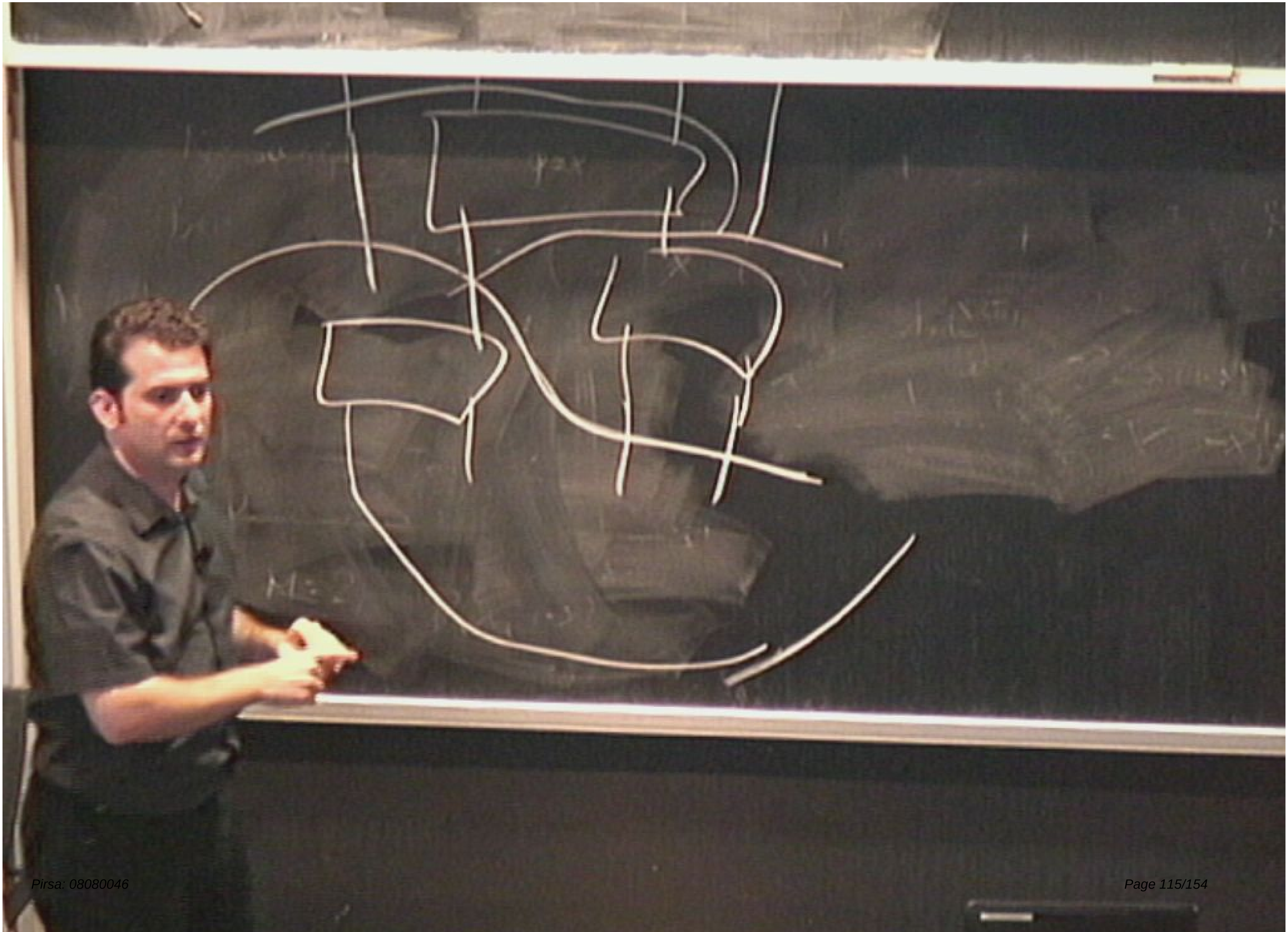
Some technical points

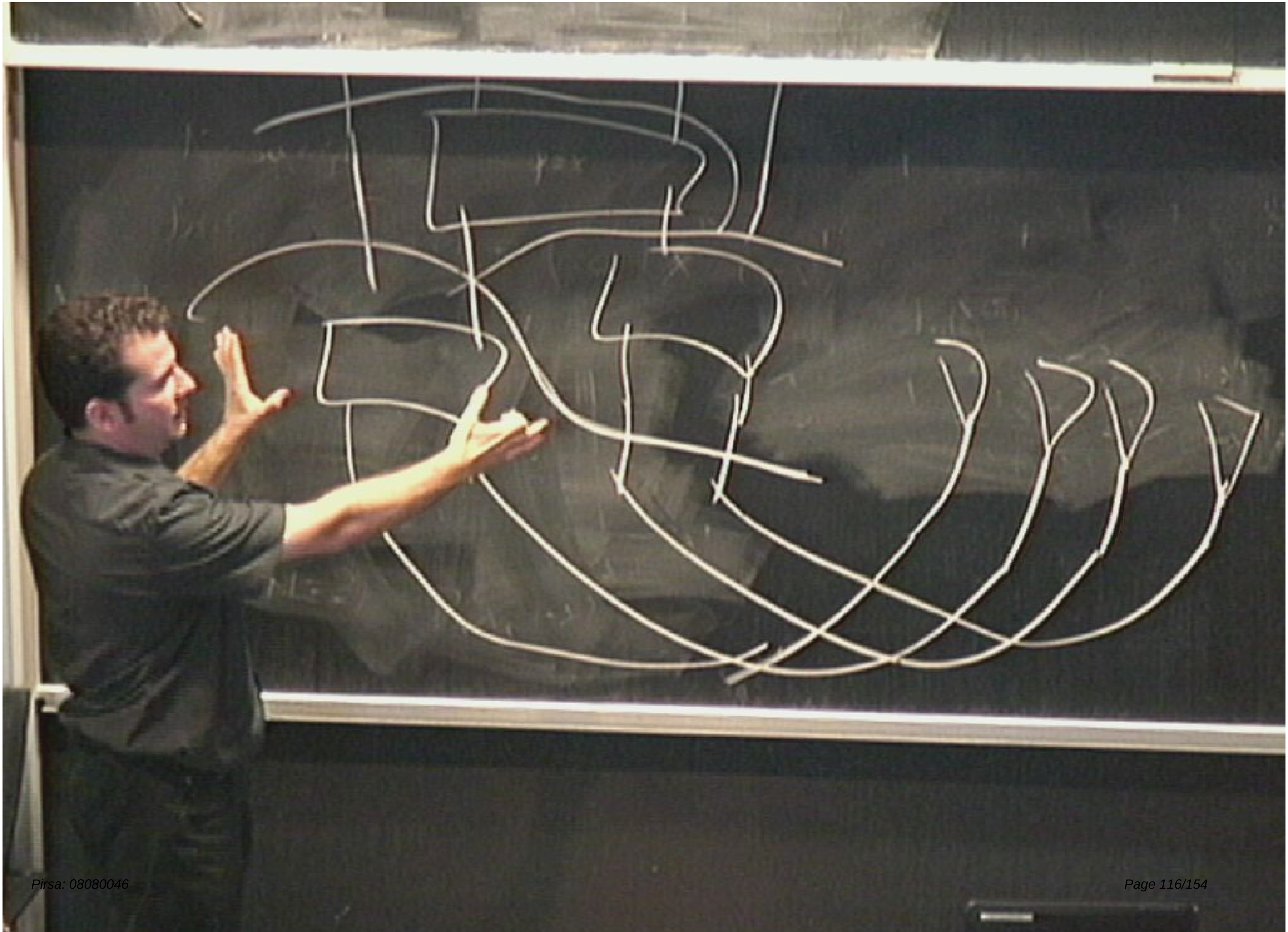
Our procedure is only good for verifying gates and states with real coefficients.

Conspiracy test

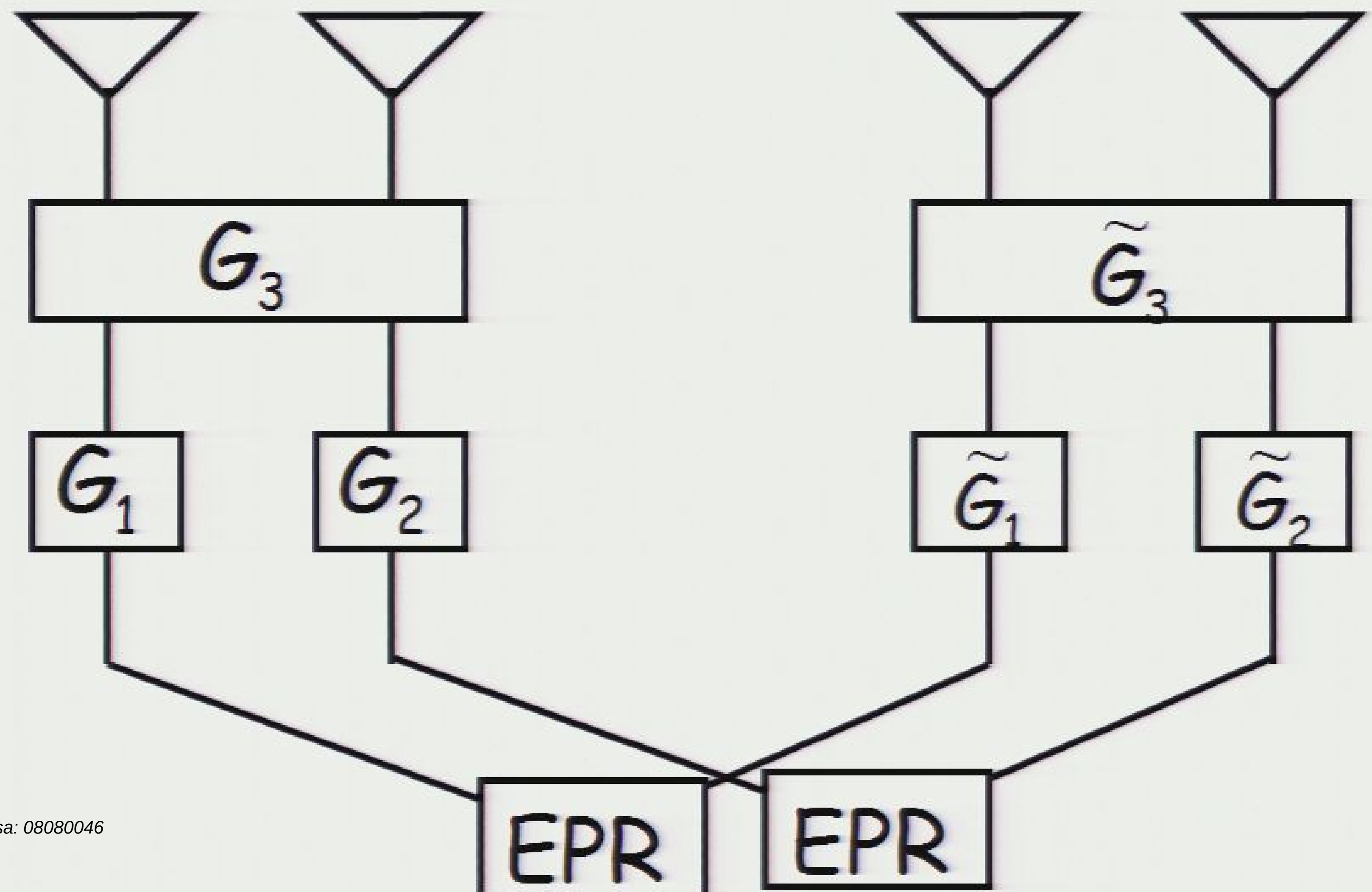








Conspiracy test



Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

*NB We are not **assuming** that our gates or states only have real coefficients.*

We are merely saying that we do not have a procedure in the case of non-real coefficients.

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

NB We are not ***assuming*** *that our gates or states only have real coefficients.*

We are merely saying that we do not have a procedure in the case of non-real coefficients.

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

This is not for lack of trying. There is a fundamental reason for this:

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

This is not for lack of trying. There is a fundamental reason for this:

complex bit can be simulated by 2 real bits (see .g. Rudolph and Grover quant-ph/0210187; non-ocal version given in a few minutes). But the two ystems are not "equivalent" according to our otion of equivalence. E.g. inner products are not reserved

Other technical points

Our tools include defining a notion of "simulation" and "equivalence".

Other technical points

Our tools include defining a notion of "simulation" and "equivalence".

Under the right conditions, simulation implies equivalence, and we are able to get our main results.

Precise statement of our main result

Let $T^1, T^2, \cdots, T^k \in U(2^n)$ *(acting on a constant number of qubits each)*

$x \in \{0,1\}^n, \varepsilon > 0, \gamma > 0$

Precise statement of our main result

Let $T^1, T^2, \cdots, T^k \in U(2^n)$ (acting on a constant number of qubits each)

$x \in \{0,1\}^n, \varepsilon > 0, \gamma > 0$

If $\mathrm{CircuitTest}(T^1, T^2, \cdots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \cdots T^2 T^1 |x\rangle$ *in the computational basis.*

Precise statement of our main result

If $\mathsf{CircuitTest}(T^1, T^2, \cdots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \ldots T^2 T^1 |x\rangle$ *in the computational basis.*

The number of experiments is in $O\left(\frac{kn}{\varepsilon}\log\left(\frac{n}{\gamma}\right)\right)$

The problem with imaginary amplitudes

Precise statement of our main result

If $\mathsf{CircuitTest}(T^1, T^2, \cdots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \ldots T^2 T^1 |x\rangle$ *in the computational basis.*

The number of experiments is in $O\left(\frac{kn}{\varepsilon}\log\left(\frac{n}{\gamma}\right)\right)$

The problem with imaginary amplitudes

The problem with imaginary amplitudes

The problem with imaginary amplitudes

The problem with imaginary amplitudes

$$|0\rangle \leftrightarrow |0\rangle|\mathbf{0}\rangle$$

The problem with imaginary amplitudes

$$|0\rangle \leftrightarrow |0\rangle|\mathbf{0}\rangle$$

$$i|0\rangle \leftrightarrow |0\rangle|1\rangle$$

$$|1\rangle \leftrightarrow |1\rangle|\mathbf{0}\rangle$$

$$i|1\rangle \leftrightarrow |1\rangle|1\rangle$$

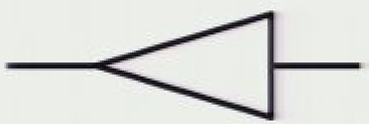
The problem with imaginary amplitudes

$$|0\rangle \leftrightarrow |0\rangle|\mathbf{0}\rangle$$

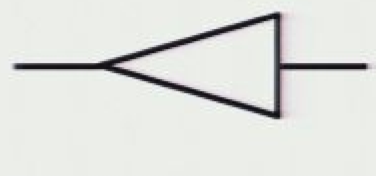
$$i|0\rangle \leftrightarrow |0\rangle|1\rangle$$

$$|1\rangle \leftrightarrow |1\rangle|\mathbf{0}\rangle$$

$$i|1\rangle \leftrightarrow |1\rangle|1\rangle$$



$$\leftrightarrow$$



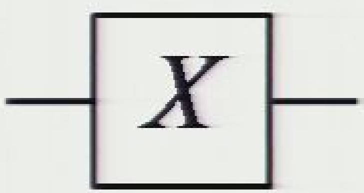
The problem with imaginary amplitudes

$$|0\rangle \leftrightarrow |0\rangle|\mathbf{0}\rangle$$

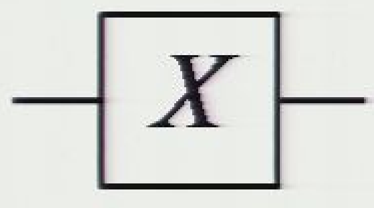
$$i|0\rangle \leftrightarrow |0\rangle|1\rangle$$

$$|1\rangle \leftrightarrow |1\rangle|\mathbf{0}\rangle$$

$$i|1\rangle \leftrightarrow |1\rangle|1\rangle$$



$$\leftrightarrow$$



The problem with imaginary amplitudes

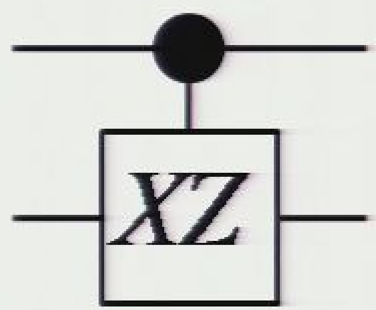
$$|0\rangle \leftrightarrow |0\rangle|\mathbf{0}\rangle$$

$$i|0\rangle \leftrightarrow |0\rangle|1\rangle$$

$$|1\rangle \leftrightarrow |1\rangle|\mathbf{0}\rangle$$

$$i|1\rangle \leftrightarrow |1\rangle|1\rangle$$

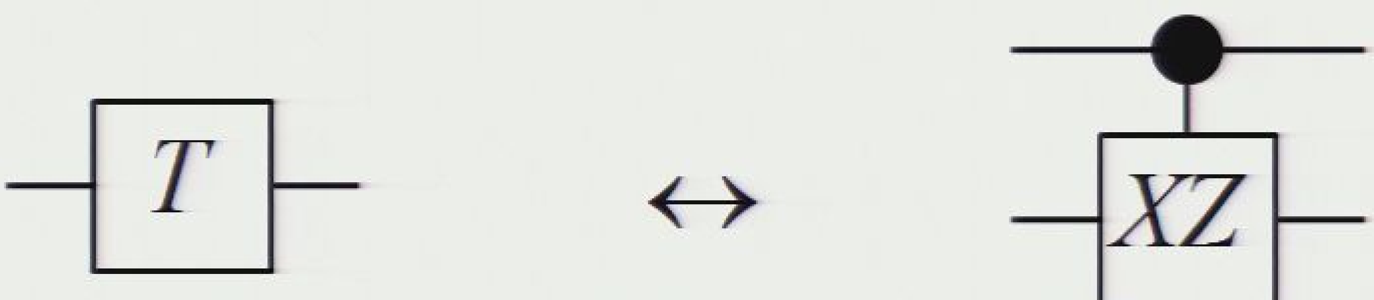
$$\leftrightarrow$$



The problem with imaginary amplitudes

$$\left|x_1x_2\ldots x_n\right\rangle \leftrightarrow \left|x_1x_2\ldots x_n\right\rangle\left|\mathbf{0}\right\rangle$$

$$i\left|x_1x_2\ldots x_n\right\rangle \leftrightarrow \left|x_1x_2\ldots x_n\right\rangle\left|1\right\rangle$$



Test against this conspiracy?

$$\left|x_1 x_2 \ldots x_n\right\rangle \leftrightarrow \left|x_1 x_2 \ldots x_n\right\rangle \left|\mathbf{0}\right\rangle$$

$$i\left|x_1 x_2 \ldots x_n\right\rangle \leftrightarrow \left|x_1 x_2 \ldots x_n\right\rangle \left|1\right\rangle$$

Test against this conspiracy?

$$\left|x_1x_2\ldots x_n\right\rangle \leftrightarrow \left|x_1x_2\ldots x_n\right\rangle\left|\mathbf{0}\right\rangle$$

$$i\left|x_1x_2\ldots x_n\right\rangle \leftrightarrow \left|x_1x_2\ldots x_n\right\rangle\left|1\right\rangle$$

Note that the "extra" hidden qubit is required to be at any location that applies a non-real gate.

Test against this conspiracy?

$$\left|x_1 x_2 \ldots x_n\right\rangle \leftrightarrow \left|x_1 x_2 \ldots x_n\right\rangle \left|\mathbf{0}\right\rangle$$

$$i\left|x_1 x_2 \ldots x_n\right\rangle \leftrightarrow \left|x_1 x_2 \ldots x_n\right\rangle \left|1\right\rangle$$

Note that the "extra" hidden qubit is required to be at any location that applies a non-real gate.

BUT, this violates our locality assumption.

Test against this conspiracy?

$$\left|x_1 x_2 \ldots x_n\right\rangle \leftrightarrow \left|x_1 x_2 \ldots x_n\right\rangle \left|\mathbf{0}\right\rangle$$

$$i\left|x_1 x_2 \ldots x_n\right\rangle \leftrightarrow \left|x_1 x_2 \ldots x_n\right\rangle \left|1\right\rangle$$

Note that the "extra" hidden qubit is required to be at any location that applies a non-real gate.

BUT, this violates our locality assumption.

Can we get around this problem?

A “local” conspiracy (with M. McKague, also independently found by Pironio/Navascues/etc.)

$$|x_1x_2\ldots x_n\rangle \leftrightarrow |x_1x_2\ldots x_n\rangle|\mathbf{0}\rangle$$

$$i|x_1x_2\ldots x_n\rangle \leftrightarrow |x_1x_2\ldots x_n\rangle|\mathbf{1}\rangle$$

$$|\mathbf{0}\rangle = \sum_{h(y)\ even} (-1)^{h(y)/2} |y_1y_2\ldots y_n\rangle$$

$$|\mathbf{1}\rangle = \sum_{h(y)\ odd} (-1)^{(h(y)-1)/2} |y_1y_2\ldots y_n\rangle$$

A “local” conspiracy (with M. McKague, also independently found by Pironio/Navascues/etc.)

$$|x_1x_2\ldots x_n\rangle \leftrightarrow |x_1x_2\ldots x_n\rangle|\mathbf{0}\rangle$$

$$i|x_1x_2\ldots x_n\rangle \leftrightarrow |x_1x_2\ldots x_n\rangle|\mathbf{1}\rangle$$

Ve replace the extra qubit with n qubits in the ntangled state:

$$|\mathbf{0}\rangle = \sum_{h(y)\ even} (-1)^{h(y)/2}|y_1y_2\ldots y_n\rangle$$

$$|\mathbf{1}\rangle = \sum_{h(y)\ odd} (-1)^{h(y)-1/2}|y_1y_2\ldots y_n\rangle$$

What does this conspiracy mean?

lo "black-box" test with our assumptions will be
ble to verify a set of states/ operations/
neasurements are unitarily equivalent to some
on-real states/ operations/ measurements.

Some open problems and future directions

- *Apply these techniques to actual experiments (e.g. with poor photon detectors). Modify as needed.*

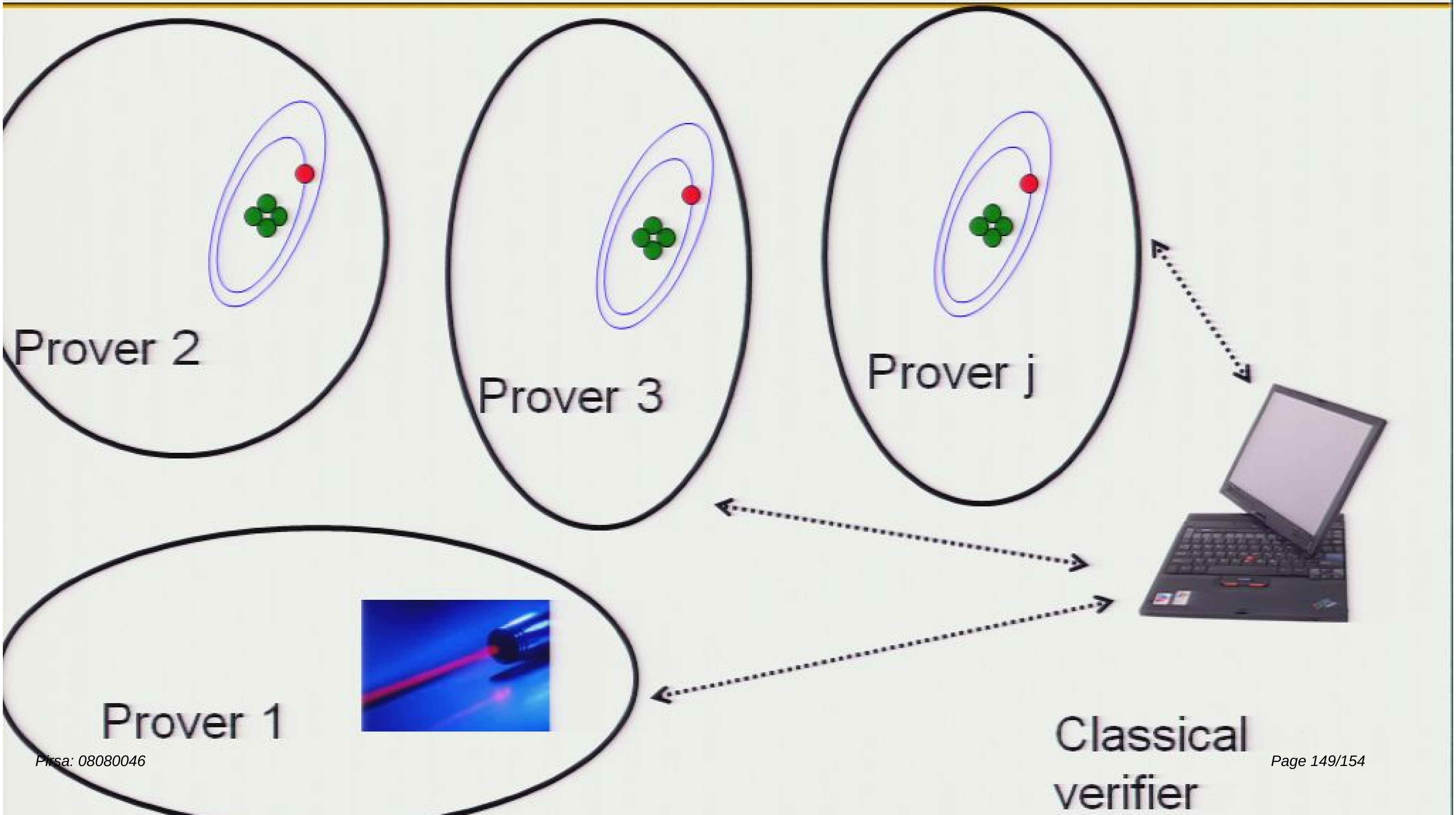
Some open problems and future directions

- *Apply these techniques to actual experiments (e.g. with poor photon detectors). Modify as needed.*
- *Can we improve the asymptotics?*

Some open problems and future directions

- *Apply these techniques to actual experiments (e.g. with poor photon detectors). Modify as needed.*
- *Can we improve the asymptotics?*
- *Relationship to "device-independent" security proofs (Acin et al. quant-ph/0702152)?*

Multi-prover interactive proof paradigm



Thanks to our sponsors…

NSERC
CRSNG

Ontario

Ontario Centres of Excellence

Government of Canada
Gouvernement du Canada

Sun microsystems

MITACS

QuantumWorks

25 years cifar
…dian Institute for

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

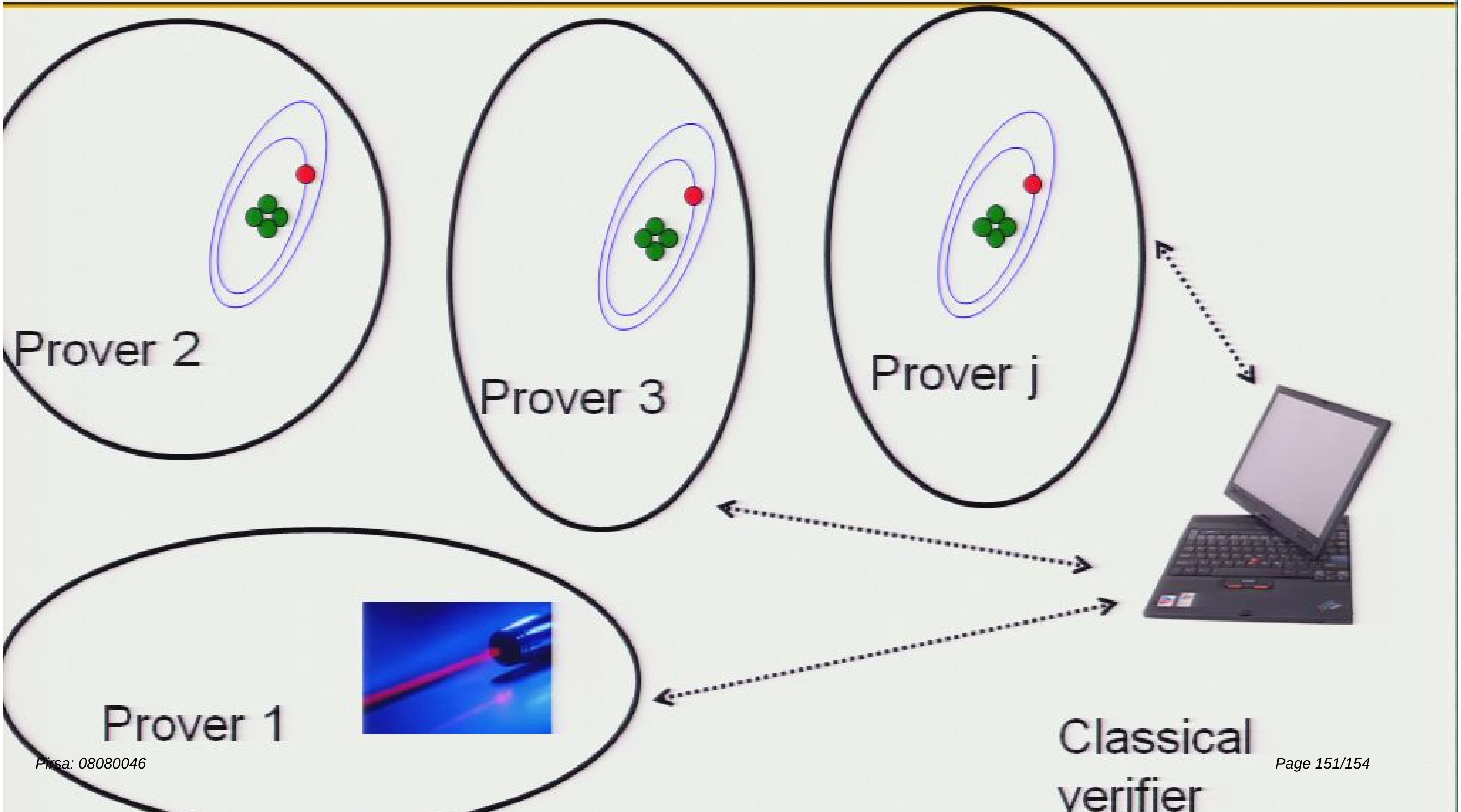
Canada Foundation for Innovation
Fondation canadienne pour l'innovation

SCIENCE TO SHAPE THE FUTURE OF THE ARMY

NATIONAL SECURITY AGENCY

DTO

Multi-prover interactive proof paradigm



Some open problems and future directions

- *Apply these techniques to actual experiments (e.g. with poor photon detectors). Modify as needed.*
- *Can we improve the asymptotics?*
- *Relationship to "device-independent" security proofs (Acin et al. quant-ph/0702152)?*

Some open problems and future directions

- *Apply these techniques to actual experiments (e.g. with poor photon detectors). Modify as needed.*
- *Can we improve the asymptotics?*
- *Relationship to "device-independent" security proofs (Acin et al. quant-ph/0702152)?*

Some open problems and future directions

- *Apply these techniques to actual experiments (e.g. with poor photon detectors). Modify as needed.*
- *Can we improve the asymptotics?*
- *Relationship to "device-independent" security proofs* (Acin et al. quant-ph/0702152)?

Click to add notes