Title: The impossibility of partially local hidden variable models for quantum theory and the relation to cryptography

Date: Dec 12, 2008 11:50 AM

URL: http://pirsa.org/08120037

Abstract: More than 40 years ago, Bell ruled out completely local hidden variable models as an explanation for quantum correlations. However, a new type of hidden variable model has recently been brought to light by the work of Leggett. Such a model has both local and non-local parts. Roughly speaking, having a local part means that the measurement outcomes can be guessed with better than 50% success. In this talk, I will explain that there exist quantum correlations for which any hidden variable model must have a trivial local part. I will then discuss how an extension of the original theorem implies that these correlations can be used to enhance the quality of a private random string.

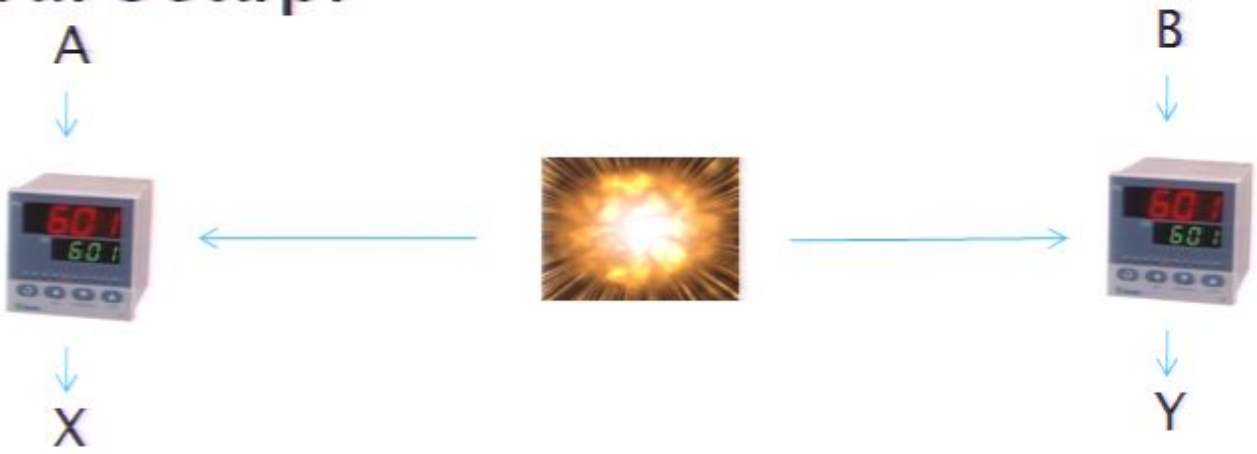
The impossibility of partially local hidden variable models for quantum theory and the relation to cryptography

Roger Colbeck (ETH Zurich)

(based on work with Renato Renner
PRL 101 050403)

Hidden Variable Models

- General Setup:



- Scenario described by distribution P(X,Y|A,B).
- In quantum theory, X and Y are not determined until measured.
- Can the correlations be explained with a hidden variable model?

Hidden Variable Models

- We introduce U, V and W as hidden variables:

- These variables (if known) would determine the outcomes completely:

  i.e., X=f(A,B,U,V,W) and Y=g(A,B,U,V,W).

Hidden Variable Models

- In the Bell model (completely local), X=f(A,U), Y=g(B,V). This is incompatible with QM.
- Conversely, a completely non-local theory is compatible with all quantum correlations.
- What about in-between models with a local and non-local part?

Mixed models

- We have X=f(A,B,U,V,W) and Y=g(A,B,U,V,W).
- To give the model a local part, we restrict P(X|ABUV)=P(X|AU) (and similarly for Y).
- A local part essentially means that given knowledge of local parameters only, we have some knowledge about X.

No local part

- For a particular set of quantum correlations, it can be shown that P(X|AU) is uniform (and therefore independent of A and U).
- Hence, hidden variable models for quantum mechanics have no local part.
- In other words, even given access to all the local parameters, the outcomes of the measurement devices are completely unpredictable.

Mixed models

- We have X=f(A,B,U,V,W) and Y=g(A,B,U,V,W).
- To give the model a local part, we restrict P(X|ABUV)=P(X|AU) (and similarly for Y).
- A local part essentially means that given knowledge of local parameters only, we have some knowledge about X.

No local part

- For a particular set of quantum correlations, it can be shown that P(X|AU) is uniform (and therefore independent of A and U).
- Hence, hidden variable models for quantum mechanics have no local part.
- In other words, even given access to all the local parameters, the outcomes of the measurement devices are completely unpredictable.

Mixed models

- We have X=f(A,B,U,V,W) and Y=g(A,B,U,V,W).
- To give the model a local part, we restrict P(X|ABUV)=P(X|AU) (and similarly for Y).
- A local part essentially means that given knowledge of local parameters only, we have some knowledge about X.

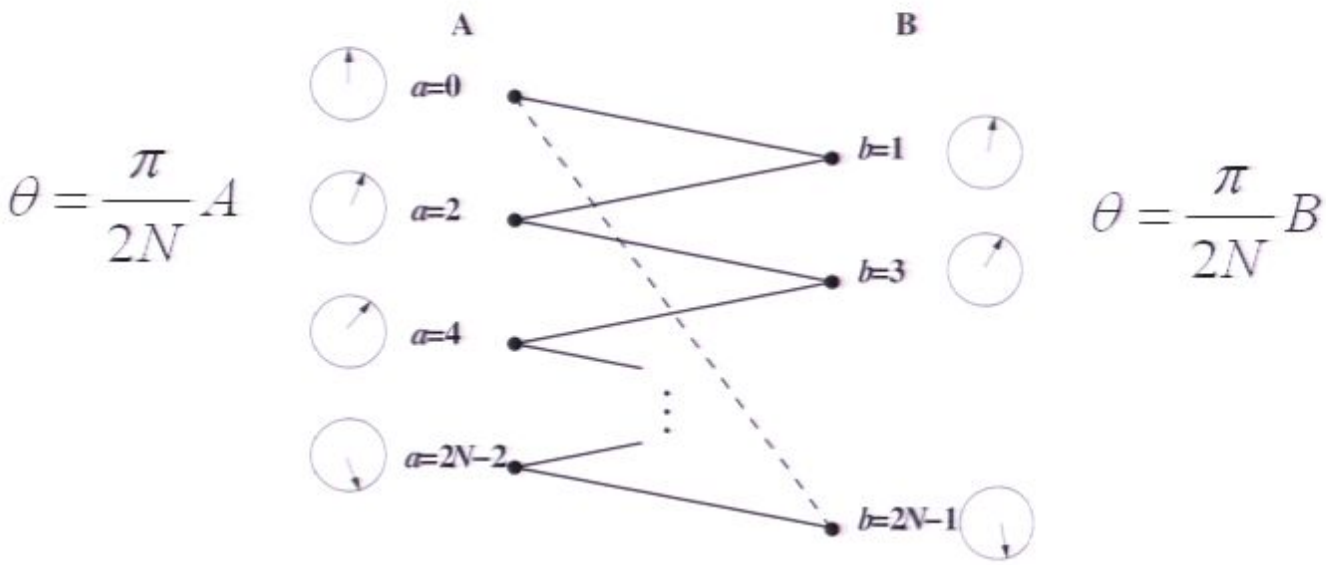
No local part

- For a particular set of quantum correlations, it can be shown that P(X|AU) is uniform (and therefore independent of A and U).
- Hence, hidden variable models for quantum mechanics have no local part.
- In other words, even given access to all the local parameters, the outcomes of the measurement devices are completely unpredictable.

Chained Bell Inequalities

- In order to show our result, we use chained Bell inequalities:

$$I_N := P(X = Y \mid 0, 2N-1) + \sum_{|A-B|=1} P(X \neq Y \mid A, B) \geq 1$$



Main Theorem

- In the original version of the theorem, we show that, for any non-signalling distribution and for A and B independent of the hidden variables, that, for all a, b

$$D(P_{XU|a}, P_{\overline{X}} \times P_U) \leq \frac{I_N}{2},$$

$$D(P_{YV|v}, P_{\overline{Y}} \times P_V) \leq \frac{I_N}{2}.$$

$P_{\overline{X}}$ denotes the uniform distribution on X and D is the variational distance.

Significance of D

- D is a measure of the distance between two distributions; the smaller D is, the closer the two distributions.
- D directly determines the maximum probability of correctly distinguishing the two distributions. $P_{guess} = \frac{1}{2}(1+D)$.
- If two distributions have distance D, they behave identically in all situations, except with probability at most D.

No local part

- Quantum mechanics allows us to obtain $I_N \approx \pi^2 / 8N \xrightarrow{N\to\infty} 0$. Hence, $D(P_{XU|a}, P_{\bar{X}} \times P_U)$ can be bounded by an arbitrarily small number.

- In the limit, we have $P_{XU|a} = P_{\bar{X}} \times P_U$, i.e. X is uniformly distributed, and independent of U.

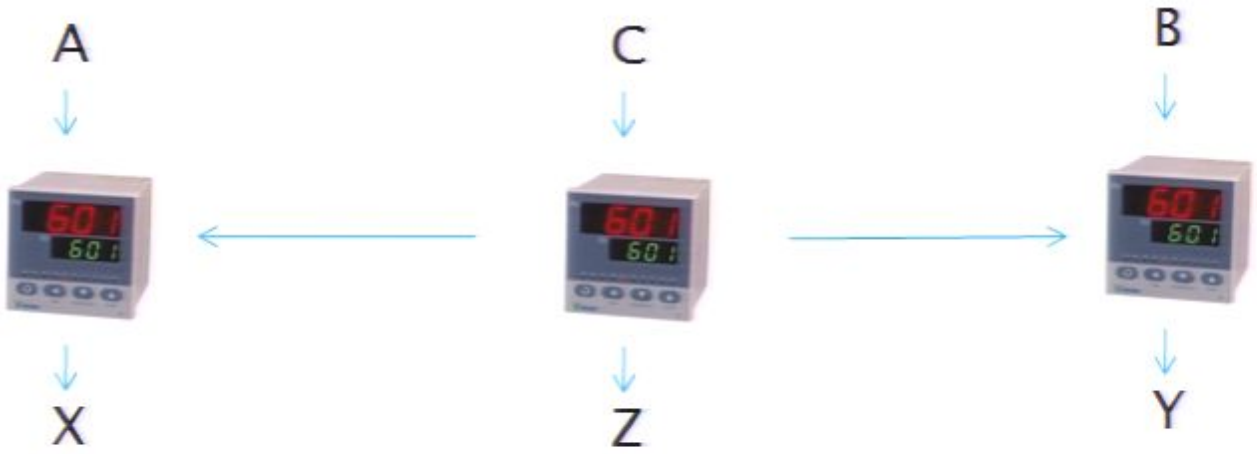
- In other words, there is no local part.

Cryptographic Setting

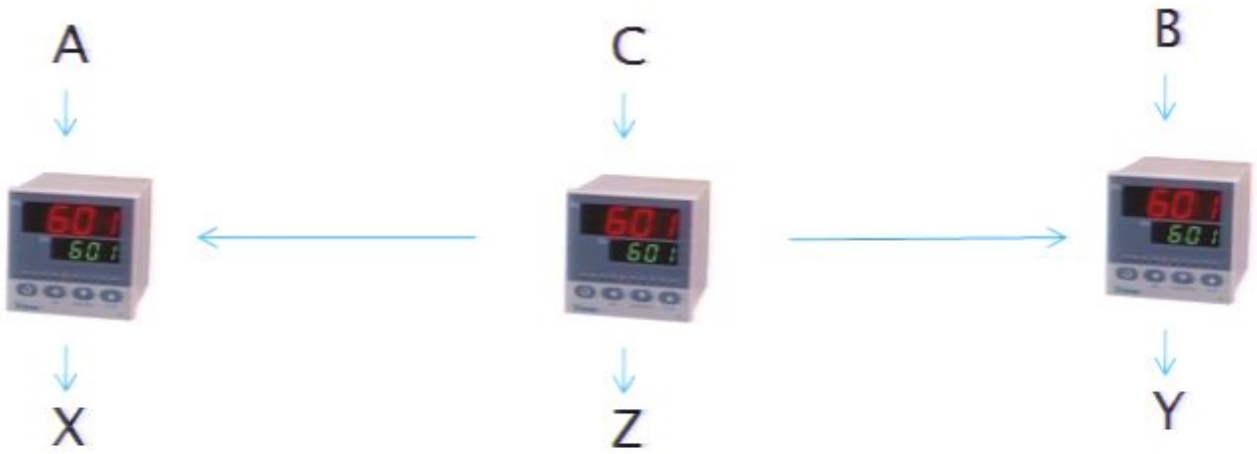
- Now consider the use of these correlations for cryptography, i.e. Alice and Bob use them to establish a shared private key.

Cryptographic Setting

- We replace the source with a system held by an Eavesdropper, Eve.

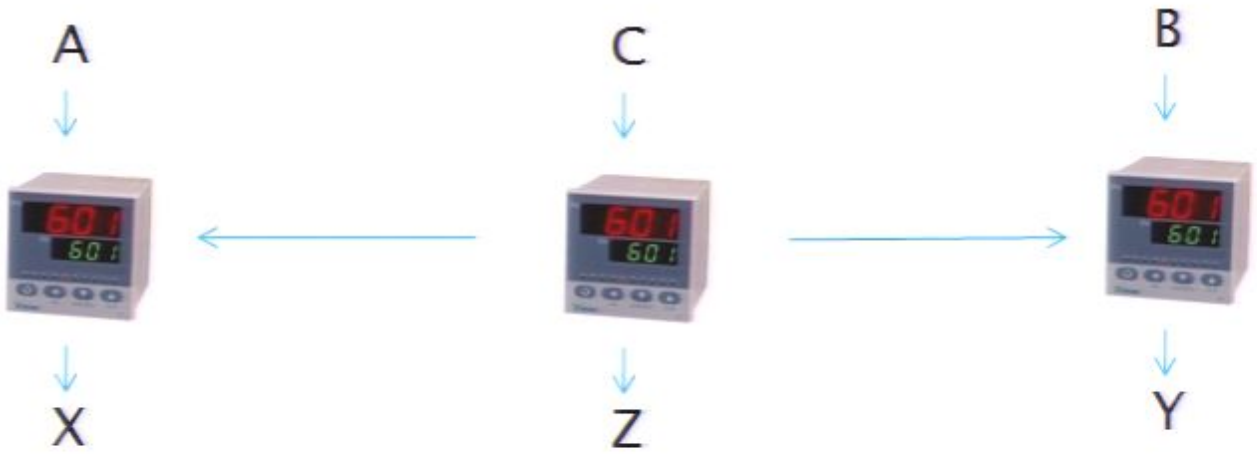


Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

Cryptographic Setting

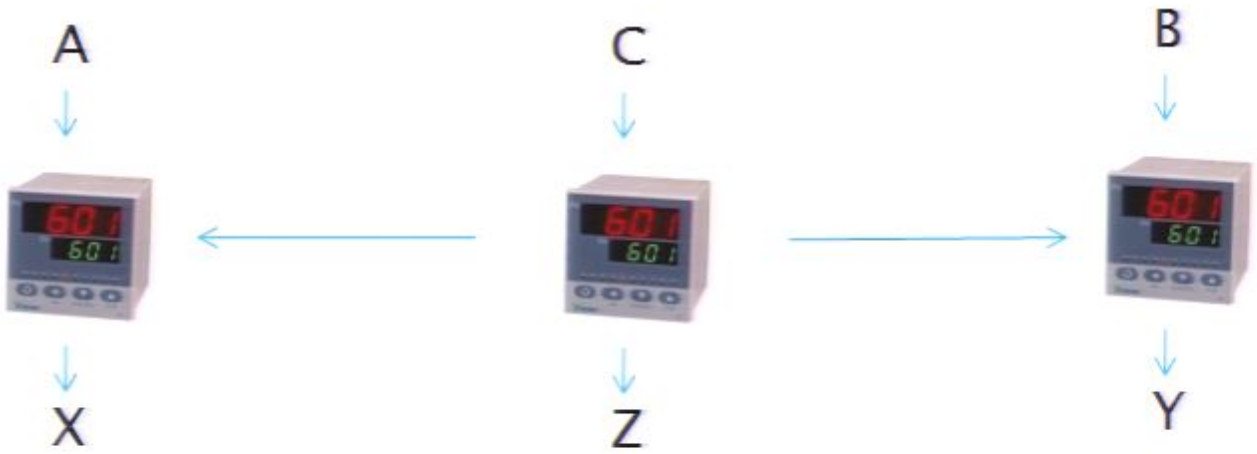


- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

Stronger Theorem

- In the original theorem, we bounded $D(P_{XU|a}, P_{\overline{X}} \times P_U)$ assuming that the choice of measurement, A, is independent of the local hidden variables.
- If the hidden variables could be chosen knowing A and B, then a completely local hidden variable model is possible.
- Amazingly, we can show that even if U and V are almost completely dependent on A and B, then the output is close to uniform.

Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

No local part

- Quantum mechanics allows us to obtain $I_N \approx \pi^2 / 8N \xrightarrow{N\to\infty} 0$. Hence, $D(P_{XU|a}, P_{\bar{X}} \times P_U)$ can be bounded by an arbitrarily small number.

- In the limit, we have $P_{XU|a} = P_{\bar{X}} \times P_U$, i.e. X is uniformly distributed, and independent of U.

- In other words, there is no local part.

Significance of D

- D is a measure of the distance between two distributions; the smaller D is, the closer the two distributions.
- D directly determines the maximum probability of correctly distinguishing the two distributions. $P_{guess} = \frac{1}{2}(1+D)$.
- If two distributions have distance D, they behave identically in all situations, except with probability at most D.

Main Theorem

- In the original version of the theorem, we show that, for any non-signalling distribution and for A and B independent of the hidden variables, that, for all a, b

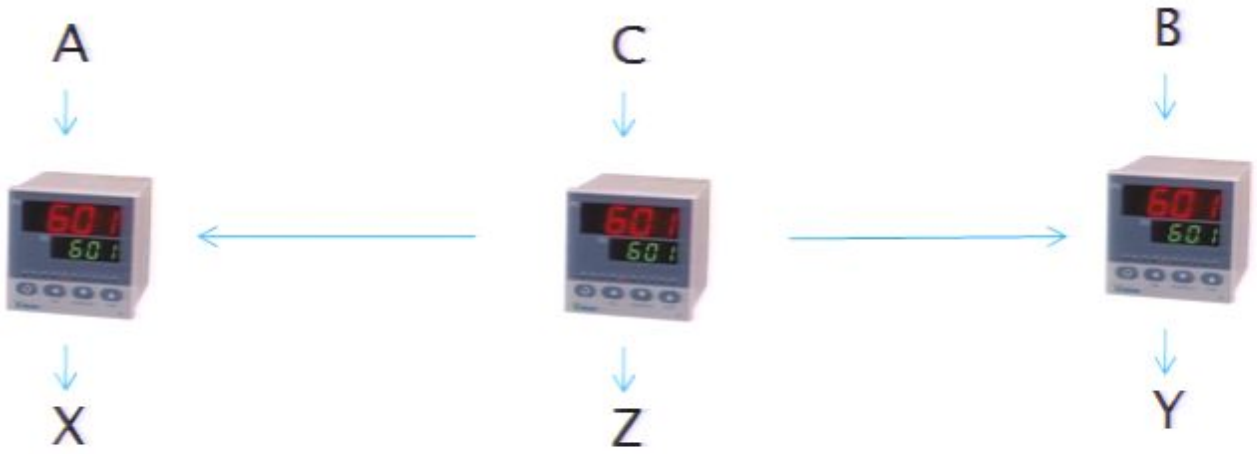
$$D(P_{XU|a}, P_{\overline{X}} \times P_U) \leq \frac{I_N}{2},$$

$$D(P_{YV|v}, P_{\overline{Y}} \times P_V) \leq \frac{I_N}{2}.$$

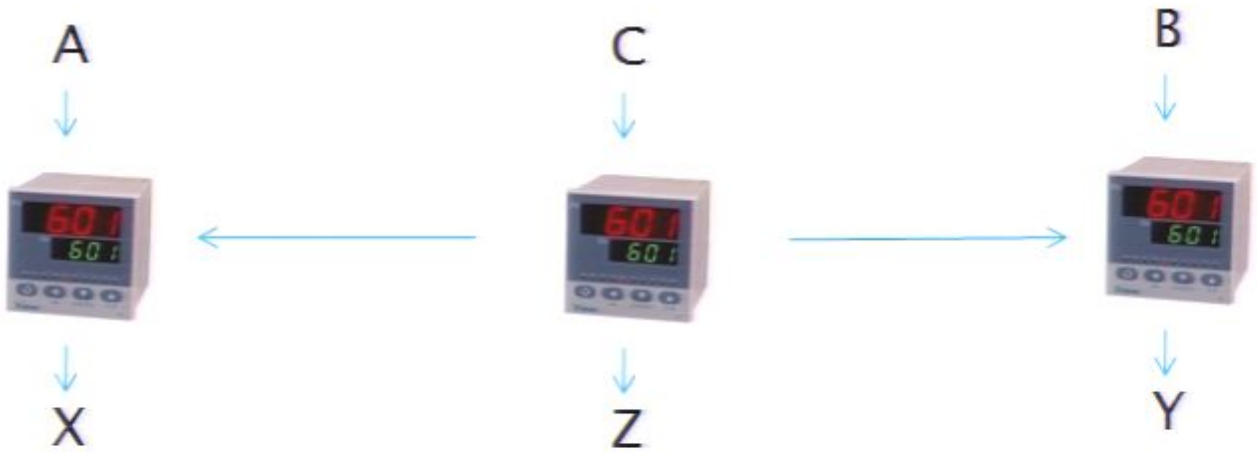
$P_{\overline{X}}$ denotes the uniform distribution on X and D is the variational distance.

Cryptographic Setting

- We replace the source with a system held by an Eavesdropper, Eve.

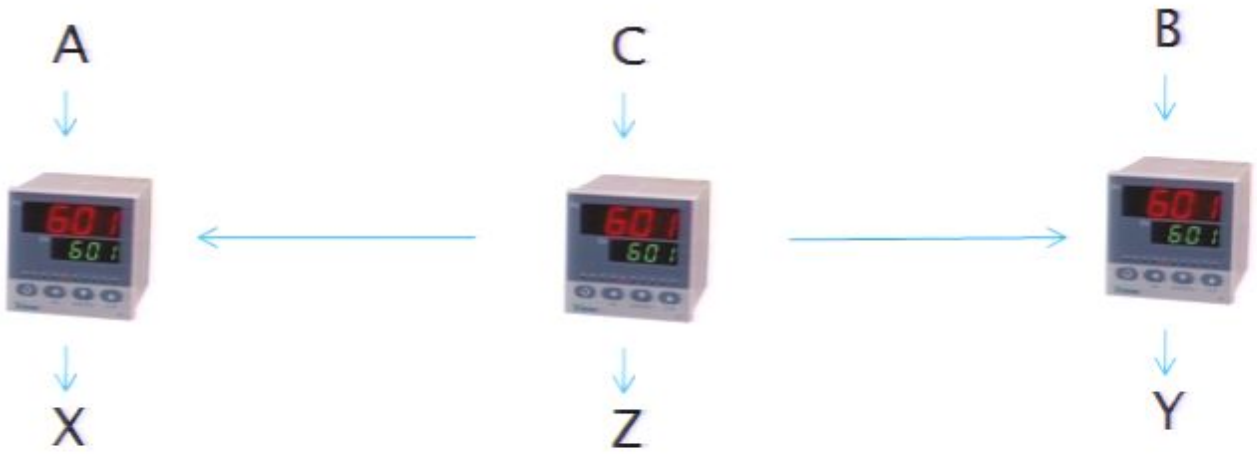


Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

Stronger Theorem

- In the original theorem, we bounded $D(P_{XU|a}, P_{\overline{X}} \times P_U)$ assuming that the choice of measurement, A, is independent of the local hidden variables.
- If the hidden variables could be chosen knowing A and B, then a completely local hidden variable model is possible.
- Amazingly, we can show that even if U and V are almost completely dependent on A and B, then the output is close to uniform.

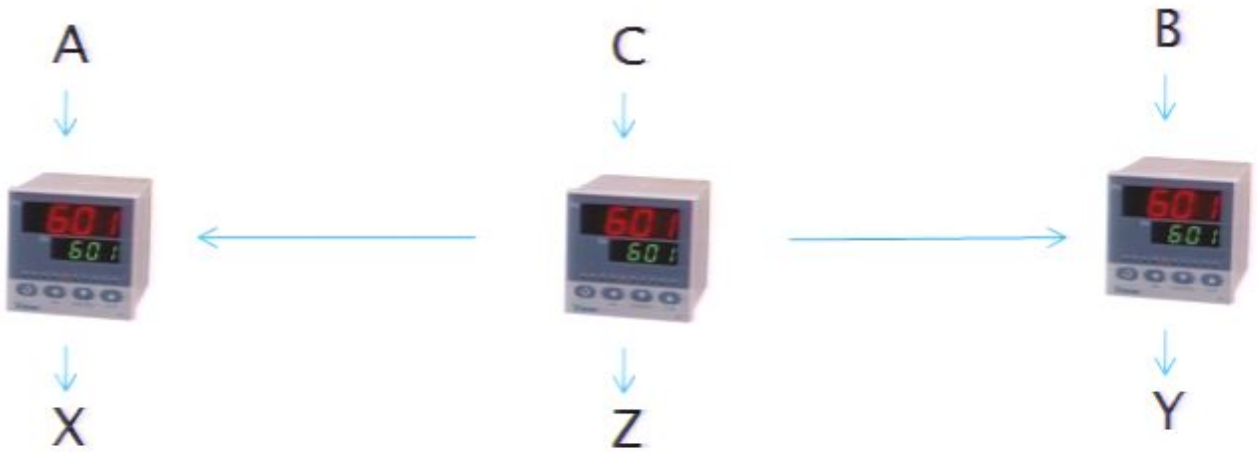
Stronger Theorem

- For any distribution P(XYZ|ABC) that is non-signalling between Alice and Bob, we have

$$D(P_{XZC|ab}, P_{\overline{X}} \times P_{ZC|ab}) \leq \frac{I_N}{2}.$$

- In other words, even if C and Z can depend on A and B, if I_N is small, then X is close to uniform.
- This shows that if Alice and Bob have strings of low privacy, they can enhance this privacy.

Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

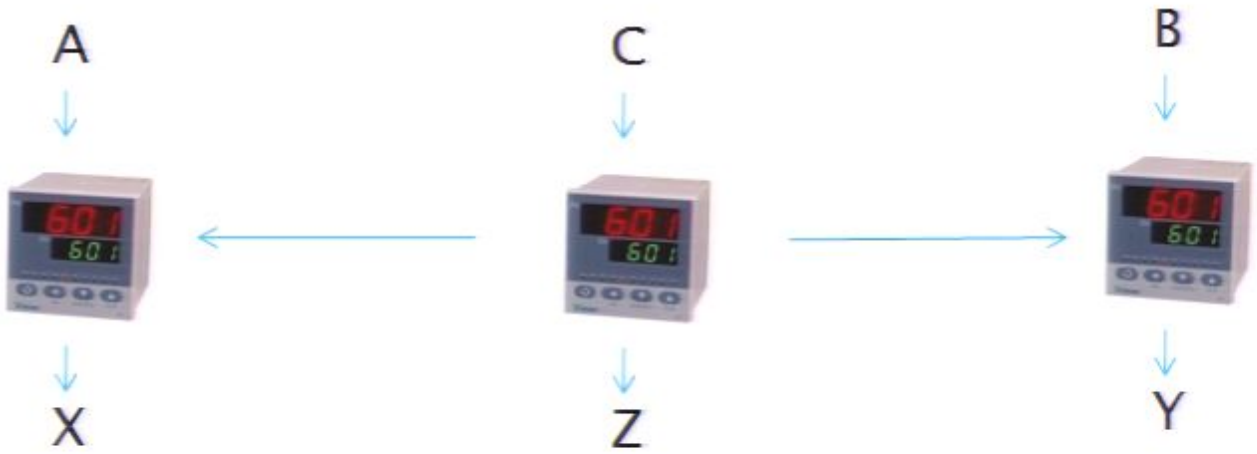
Stronger Theorem

- For any distribution P(XYZ|ABC) that is non-signalling between Alice and Bob, we have

$$D(P_{XZC|ab}, P_{\bar{X}} \times P_{ZC|ab}) \leq \frac{I_N}{2}.$$

- In other words, even if C and Z can depend on A and B, if I_N is small, then X is close to uniform.
- This shows that if Alice and Bob have strings of low privacy, they can enhance this privacy.

Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

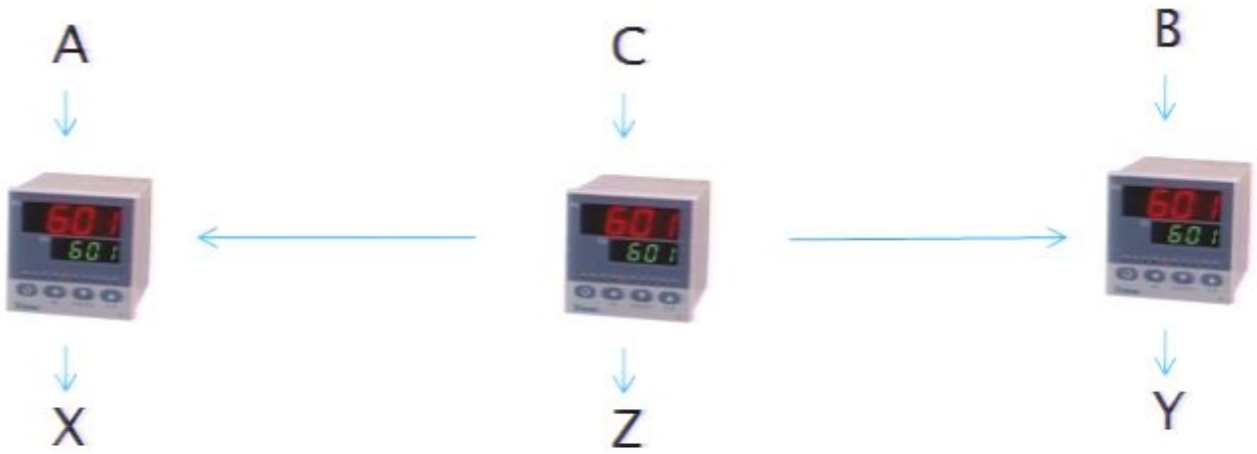
Stronger Theorem

- For any distribution P(XYZ|ABC) that is non-signalling between Alice and Bob, we have

$$D(P_{XZC|ab}, P_{\overline{X}} \times P_{ZC|ab}) \leq \frac{I_N}{2}.$$

- In other words, even if C and Z can depend on A and B, if I_N is small, then X is close to uniform.
- This shows that if Alice and Bob have strings of low privacy, they can enhance this privacy.

Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

Stronger Theorem

- In the original theorem, we bounded $D(P_{XU|a}, P_{\overline{X}} \times P_U)$ assuming that the choice of measurement, A, is independent of the local hidden variables.
- If the hidden variables could be chosen knowing A and B, then a completely local hidden variable model is possible.
- Amazingly, we can show that even if U and V are almost completely dependent on A and B, then the output is close to uniform.

Stronger Theorem

- For any distribution P(XYZ|ABC) that is non-signalling between Alice and Bob, we have

$$D(P_{XZC|ab}, P_{\overline{X}} \times P_{ZC|ab}) \leq \frac{I_N}{2}.$$

- In other words, even if C and Z can depend on A and B, if I_N is small, then X is close to uniform.
- This shows that if Alice and Bob have strings of low privacy, they can enhance this privacy.

Summary

- To explain quantum correlations with a hidden variable model, such a hidden variable model cannot have a local part.
- The local part is related to the knowledge an eavesdropper could have on the privacy of a string. Correlations with no local part are completely private.
- A stronger version of the theorem shows that these correlations can be used to enhance privacy.

Stronger Theorem

- For any distribution P(XYZ|ABC) that is non-signalling between Alice and Bob, we have

$$D(P_{XZC|ab}, P_{\overline{X}} \times P_{ZC|ab}) \leq \frac{I_N}{2}.$$

- In other words, even if C and Z can depend on A and B, if I_N is small, then X is close to uniform.
- This shows that if Alice and Bob have strings of low privacy, they can enhance this privacy.

Summary

- To explain quantum correlations with a hidden variable model, such a hidden variable model cannot have a local part.
- The local part is related to the knowledge an eavesdropper could have on the privacy of a string. Correlations with no local part are completely private.
- A stronger version of the theorem shows that these correlations can be used to enhance privacy.

Stronger Theorem

- For any distribution P(XYZ|ABC) that is non-signalling between Alice and Bob, we have

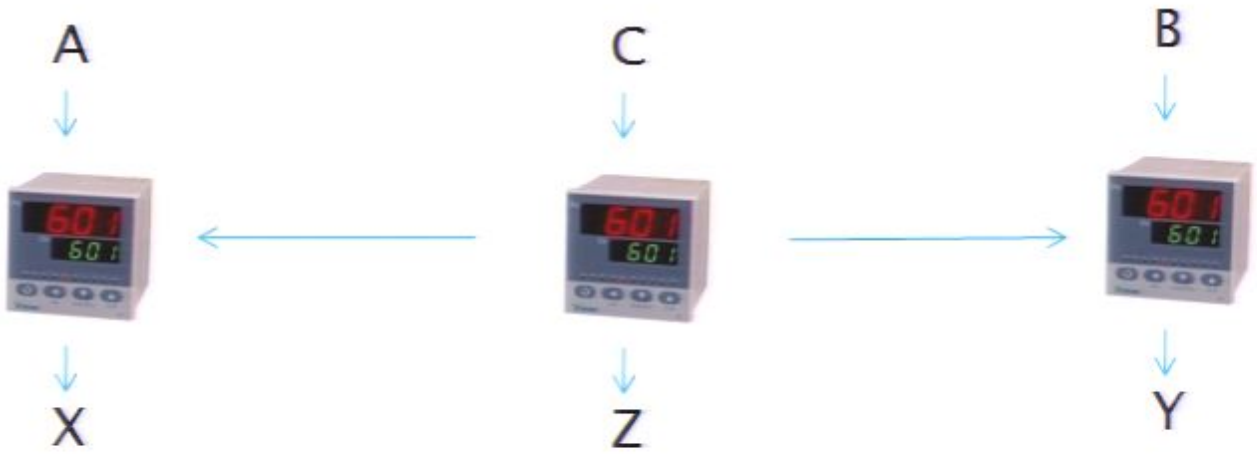
$$D(P_{XZC|ab}, P_{\overline{X}} \times P_{ZC|ab}) \leq \frac{I_N}{2}.$$

- In other words, even if C and Z can depend on A and B, if I_N is small, then X is close to uniform.
- This shows that if Alice and Bob have strings of low privacy, they can enhance this privacy.

Stronger Theorem

- In the original theorem, we bounded $D(P_{XU|a}, P_{\overline{X}} \times P_U)$ assuming that the choice of measurement, A, is independent of the local hidden variables.
- If the hidden variables could be chosen knowing A and B, then a completely local hidden variable model is possible.
- Amazingly, we can show that even if U and V are almost completely dependent on A and B, then the output is close to uniform.

Cryptographic Setting



- We assume that the entire setup is created by Eve, and demand security even if so.
- If Alice and Bob can verify that I_N is small, then they are assured of the key's security.

Stronger Theorem

- In the original theorem, we bounded $D(P_{XU|a}, P_{\overline{X}} \times P_U)$ assuming that the choice of measurement, A, is independent of the local hidden variables.
- If the hidden variables could be chosen knowing A and B, then a completely local hidden variable model is possible.
- Amazingly, we can show that even if U and V are almost completely dependent on A and B, then the output is close to uniform.

Cryptographic Setting

- We replace the source with a system held by an Eavesdropper, Eve.