Bell Inequalities:
What do we know about them and why should cryptographers care

Ronald de Wolf

Centrum Wiskunde & Informatica

and University of Amsterdam

Overview

Overview

1. The weirdness of quantum mechanics:
   Bell inequalities & their violation

Overview

1. The weirdness of quantum mechanics:
   Bell inequalities & their violation

2. Why should cryptographers care?

Overview

1. The weirdness of quantum mechanics:
   Bell inequalities & their violation

2. Why should cryptographers care?

3. What do we know about Bell inequalities?

Part 1:

Quantum mechanics:
Bell inequalities & their violation

The weirdness of quantum mechanics

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

- If Alice measures her qubit,
  the joint state immediately collapses to $|00\rangle$ or $|11\rangle$

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right)$$

- If Alice measures her qubit,
  the joint state immediately collapses to $|00\rangle$ or $|11\rangle$
- Einstein's complaint (EPR'35)

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

- If Alice measures her qubit,
  the joint state immediately collapses to $|00\rangle$ or $|11\rangle$
- Einstein's complaint (EPR'35): This seems to violate either locality (no instantaneous action at a distance)

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

- If Alice measures her qubit,
the joint state immediately collapses to $|00\rangle$ or $|11\rangle$
- Einstein's complaint (EPR'35): This seems to violate either locality (no instantaneous action at a distance) or realism (objects have well-defined properties, even before they are measured)

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

- If Alice measures her qubit,
the joint state immediately collapses to $|00\rangle$ or $|11\rangle$
- Einstein's complaint (EPR'35): This seems to violate either locality (no instantaneous action at a distance) or realism (objects have well-defined properties, even before they are measured)
- But there is local-realist model for this: shared coin flip

The weirdness of quantum mechanics

- EPR-pair: two entangled particles in joint state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- If Alice measures her qubit, the joint state immediately collapses to $|00\rangle$ or $|11\rangle$
- Einstein's complaint (EPR'35): This seems to violate either locality (no instantaneous action at a distance) or realism (objects have well-defined properties, even before they are measured)
- But there is local-realist model for this: shared coin flip
- Bell'64: there are other quantum predictions that cannot be reproduced by local-realist models

General setup

General setup

- Alice receives input x, Bob receives y

General setup

- Alice receives input x, Bob receives y, distributed $\sim \pi$

General setup

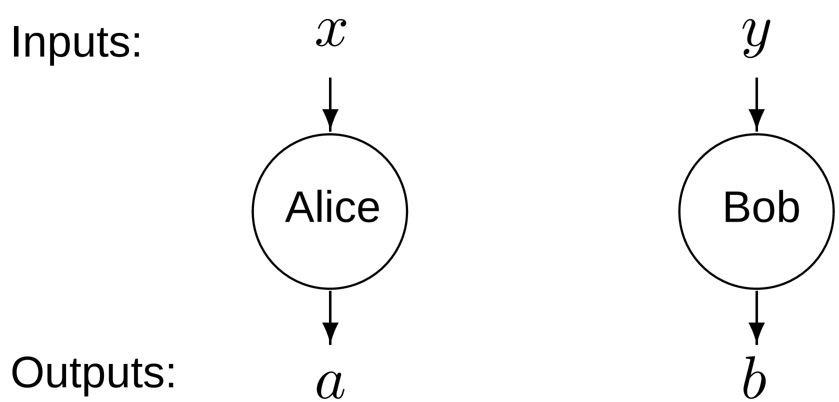
- Alice receives input x, Bob receives y, distributed $\sim \pi$
  They produce outputs a and b

General setup

- Alice receives input x, Bob receives y, distributed $\sim \pi$
  They produce outputs a and b
  Some outputs a, b win the game on inputs x, y

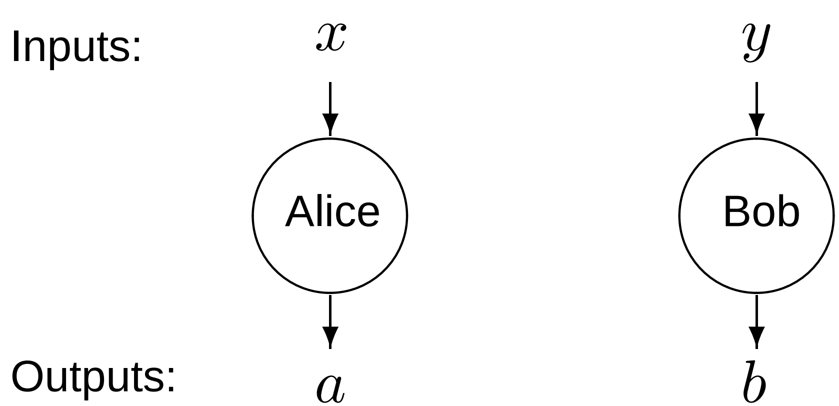
General setup

- Alice receives input x, Bob receives y, distributed $\sim \pi$
  They produce outputs a and b
  Some outputs a, b win the game on inputs x, y



General setup

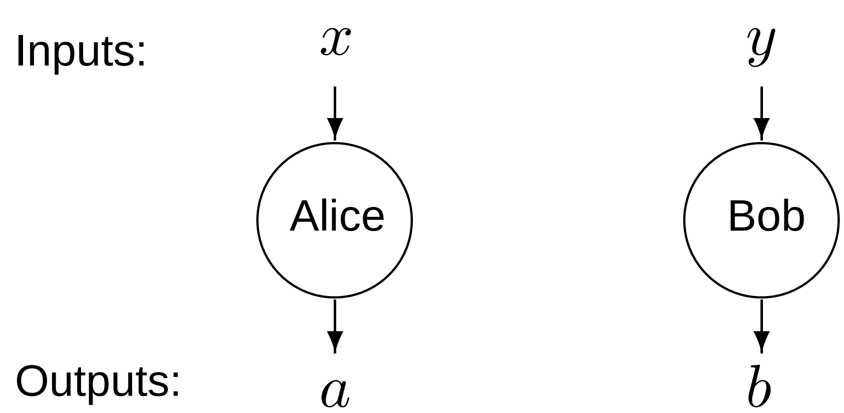
- Alice receives input x, Bob receives y, distributed $\sim \pi$
  They produce outputs a and b
  Some outputs a, b win the game on inputs x, y



- Classical value $\omega(G)$: maximal winning probability among classical protocols (shared randomness)

General setup

- Alice receives input x, Bob receives y, distributed $\sim \pi$
  They produce outputs a and b
  Some outputs a, b win the game on inputs x, y



- Classical value $\omega(G)$: maximal winning probability among classical protocols (shared randomness)
- Entangled value $\omega^*(G)$: maximal winning probability among quantum protocols (shared entanglement)

Example 1: CHSH'69

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0,1\}$ and $y \in \{0,1\}$

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0, 1\}$ and $y \in \{0, 1\}$
- Alice and Bob output $a \in \{0, 1\}$ and $b \in \{0, 1\}$

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0,1\}$ and $y \in \{0,1\}$
- Alice and Bob output $a \in \{0,1\}$ and $b \in \{0,1\}$, and win if $a \oplus b = x \wedge y$

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0,1\}$ and $y \in \{0,1\}$
- Alice and Bob output $a \in \{0,1\}$ and $b \in \{0,1\}$, and win if $a \oplus b = x \wedge y$
- Best classical strategy wins with probability 0.75 ($\omega(G) = 0.75$)

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0,1\}$ and $y \in \{0,1\}$
- Alice and Bob output $a \in \{0,1\}$ and $b \in \{0,1\}$, and win if $a \oplus b = x \wedge y$
- Best classical strategy wins with probability 0.75 ($\omega(G) = 0.75$)
- Best quantum strategy wins with prob $\cos(\pi/8)^2 \approx 0.85$

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0,1\}$ and $y \in \{0,1\}$
- Alice and Bob output $a \in \{0,1\}$ and $b \in \{0,1\}$, and win if $a \oplus b = x \wedge y$
- Best classical strategy wins with probability 0.75 ($\omega(G) = 0.75$)
- Best quantum strategy wins with prob $\cos(\pi/8)^2 \approx 0.85$ using one EPR-pair ($\omega_2^*(G) \approx 0.85$)

Example 1: CHSH'69

- Uniform distribution on inputs $x \in \{0, 1\}$ and $y \in \{0, 1\}$
- Alice and Bob output $a \in \{0, 1\}$ and $b \in \{0, 1\}$, and win if $a \oplus b = x \wedge y$
- Best classical strategy wins with probability 0.75 ($\omega(G) = 0.75$)
- Best quantum strategy wins with prob $\cos(\pi/8)^2 \approx 0.85$ using one EPR-pair ($\omega_2^*(G) \approx 0.85$)
- Hence the output-distributions of the quantum protocol cannot be reproduced by classical protocols

Example 1: CHSH’69

- Uniform distribution on inputs $x \in \{0, 1\}$ and $y \in \{0, 1\}$
- Alice and Bob output $a \in \{0, 1\}$ and $b \in \{0, 1\}$, and win if $a \oplus b = x \wedge y$
- Best classical strategy wins with probability 0.75 ($\omega(G) = 0.75$)
- Best quantum strategy wins with prob $\cos(\pi/8)^2 \approx 0.85$ using one EPR-pair ($\omega_2^*(G) \approx 0.85$)
- Hence the output-distributions of the quantum protocol cannot be reproduced by classical protocols
- When implemented, such experiments show that nature is not classical (i.e., not local-realist)

Example 1: CHSH experiment

Example 1: CHSH experiment

- CHSH and related games were implemented by Aspect et al. in '81,'82, using entangled photon-pairs

Example 1: CHSH experiment

- CHSH and related games were implemented by Aspect et al. in ’81,’82, using entangled photon-pairs
- Outcomes conform to quantum mechanical predictions, so they seem to refute local realism

Example 1: CHSH experiment

- CHSH and related games were implemented by Aspect et al. in ’81,’82, using entangled photon-pairs
- Outcomes conform to quantum mechanical predictions, so they seem to refute local realism
- Experiments are not perfect:

Example 1: CHSH experiment

- CHSH and related games were implemented by Aspect et al. in ’81,’82, using entangled photon-pairs
- Outcomes conform to quantum mechanical predictions, so they seem to refute local realism
- Experiments are not perfect:

1. Locality loophole: Alice and Bob shouldn’t be able to communicate during the experiment

Example 1: CHSH experiment

- CHSH and related games were implemented by Aspect et al. in ’81,’82, using entangled photon-pairs
- Outcomes conform to quantum mechanical predictions, so they seem to refute local realism
- Experiments are not perfect:
  1. Locality loophole: Alice and Bob shouldn’t be able to communicate during the experiment
  2. Detection loophole: photon channels and detectors are not perfect, if the error is too big then local-realist explanations become possible (but implausible)

Example 1: CHSH experiment

- CHSH and related games were implemented by Aspect et al. in ’81,’82, using entangled photon-pairs
- Outcomes conform to quantum mechanical predictions, so they seem to refute local realism
- Experiments are not perfect:
  1. Locality loophole: Alice and Bob shouldn’t be able to communicate during the experiment
  2. Detection loophole: photon channels and detectors are not perfect, if the error is too big then local-realist explanations become possible (but implausible)
- Hard to close both loopholes simultaneously:
  to close locality loophole distance between Alice and Bob should be large, but then detection-error goes up

Example 2: Magic square game

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity

- Clearly impossible:

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity

- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

- Alice gets row-index $x \in \{1, 2, 3\}$, Bob column-index y

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

- Alice gets row-index $x \in \{1, 2, 3\}$, Bob column-index y
  Reply: row $a = a_1 a_2 a_3$ must have even parity,

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

- Alice gets row-index $x \in \{1, 2, 3\}$, Bob column-index y
  Reply: row $a = a_1 a_2 a_3$ must have even parity,
  column $b = b_1 b_2 b_3$ must have odd parity

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

- Alice gets row-index $x \in \{1, 2, 3\}$, Bob column-index y
Reply: row $a = a_1 a_2 a_3$ must have even parity,
column $b = b_1 b_2 b_3$ must have odd parity,
they must agree where row/column overlap: $a_y = b_x$

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

- Alice gets row-index $x \in \{1, 2, 3\}$, Bob column-index y
  Reply: row $a = a_1 a_2 a_3$ must have even parity,
  column $b = b_1 b_2 b_3$ must have odd parity,
  they must agree where row/column overlap: $a_y = b_x$
- A perfect classical strategy would correspond to a magic square, which doesn't exist: $\omega(G) = 8/9$

Example 2: Magic square game

- Idea: try to fill a 3×3 square with bits, such that each row has even parity, each column has odd parity
- Clearly impossible:

0	0	0
0	0	0
1	1	0

0	0	0
0	0	0
1	1	1

- Alice gets row-index $x \in \{1, 2, 3\}$, Bob column-index y
  Reply: row $a = a_1 a_2 a_3$ must have even parity,
  column $b = b_1 b_2 b_3$ must have odd parity,
  they must agree where row/column overlap: $a_y = b_x$
- A perfect classical strategy would correspond to a magic square, which doesn't exist: $\omega(G) = 8/9$
- Can win with prob 1 using 2 EPR-pairs: $\omega_4^*(G) = 1$

Part 2:

Why should cryptographers care?

Making crypto protocols

Breaking crypto protocols

Quantum key distribution

Quantum key distribution

- Entanglement-based version of BB84 (Ekert'91)

Quantum key distribution

- Entanglement-based version of BB84 (Ekert'91)

1. Some source distributes n EPR-pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Quantum key distribution

- Entanglement-based version of BB84 (Ekert'91)

1. Some source distributes n EPR-pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Alice and Bob measure their qubits in randomly chosen bases (computational or diagonal)

Quantum key distribution

- Entanglement-based version of BB84 (Ekert'91)

1. Some source distributes n EPR-pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Alice and Bob measure their qubits in randomly chosen bases (computational or diagonal)
3. They test (over public authenticated classical channel) results for a subset: should be equal for qubits measured in same basis, uniform otherwise

Quantum key distribution

- Entanglement-based version of BB84 (Ekert'91)

1. Some source distributes n EPR-pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Alice and Bob measure their qubits in randomly chosen bases (computational or diagonal)
3. They test (over public authenticated classical channel) results for a subset: should be equal for qubits measured in same basis, uniform otherwise
4. If the error is too big, blame Eve and abort.
   Else: raw key is remaining bits that were measured in same basis

Quantum key distribution

- Entanglement-based version of BB84 (Ekert'91)
  1. Some source distributes n EPR-pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  2. Alice and Bob measure their qubits in randomly chosen bases (computational or diagonal)
  3. They test (over public authenticated classical channel) results for a subset: should be equal for qubits measured in same basis, uniform otherwise
  4. If the error is too big, blame Eve and abort. Else: raw key is remaining bits that were measured in same basis
- Information-theoretically secure *if* Alice and Bob can trust that they measure qubits in the chosen basis

Insecurity of QKD

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis
- Example: instead of an EPR-pair, Eve gives them two shared random bits

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis
- Example: instead of an EPR-pair, Eve gives them two shared random bits
- For measurement in comput. basis: measure 1st bit

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis
- Example: instead of an EPR-pair, Eve gives them two shared random bits
- For measurement in comput. basis: measure 1st bit
  For measurement in diagonal basis: measure 2nd bit

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis
- Example: instead of an EPR-pair, Eve gives them two shared random bits
- For measurement in comput. basis: measure 1st bit
  For measurement in diagonal basis: measure 2nd bit
- If A & B measure system in same basis they get same random bit, else get independent random bits

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis
- Example: instead of an EPR-pair, Eve gives them two shared random bits
- For measurement in comput. basis: measure 1st bit
  For measurement in diagonal basis: measure 2nd bit
- If A & B measure system in same basis they get same random bit, else get independent random bits
- This gives correct statistics without any entanglement!

Insecurity of QKD

- The previous scheme is wholly insecure if Alice and Bob cannot trust that they measure qubits in chosen basis
- Example: instead of an EPR-pair, Eve gives them two shared random bits
- For measurement in comput. basis: measure 1st bit
  For measurement in diagonal basis: measure 2nd bit
- If A & B measure system in same basis they get same random bit, else get independent random bits
- This gives correct statistics without any entanglement!
- Eve could have a perfect copy without being detected

Solution: test Bell inequality violation

Solution: test Bell inequality violation

- Solution (Barrett-Hardy-Kent’05): instead Alice and Bob test the EPR-pairs by testing Bell inequality violations

Solution: test Bell inequality violation

- Solution (Barrett-Hardy-Kent'05): instead Alice and Bob test the EPR-pairs by testing Bell inequality violations
- 1. For each of the n "EPR-pairs" Alice and Bob themselves choose random inputs x, y and run CHSH-strategy

Solution: test Bell inequality violation

- Solution (Barrett-Hardy-Kent'05): instead Alice and Bob test the EPR-pairs by testing Bell inequality violations
- 1. For each of the n "EPR-pairs" Alice and Bob themselves choose random inputs x, y and run CHSH-strategy
  2. Test (over public channel) for a subset that statistics conform to what EPR-pairs should give

Solution: test Bell inequality violation

- Solution (Barrett-Hardy-Kent'05): instead Alice and Bob test the EPR-pairs by testing Bell inequality violations
- 1. For each of the n "EPR-pairs" Alice and Bob themselves choose random inputs x, y and run CHSH-strategy
  2. Test (over public channel) for a subset that statistics conform to what EPR-pairs should give
  3. If test is passed, raw key is derived from the remaining bits

Solution: test Bell inequality violation

- Solution (Barrett-Hardy-Kent'05): instead Alice and Bob test the EPR-pairs by testing Bell inequality violations
- 1. For each of the n "EPR-pairs" Alice and Bob themselves choose random inputs x, y and run CHSH-strategy
  2. Test (over public channel) for a subset that statistics conform to what EPR-pairs should give
  3. If test is passed, raw key is derived from the remaining bits
- Test can only be passed if they share entanglement

Solution: test Bell inequality violation

- Solution (Barrett-Hardy-Kent'05): instead Alice and Bob test the EPR-pairs by testing Bell inequality violations
- 1. For each of the n "EPR-pairs" Alice and Bob themselves choose random inputs x, y and run CHSH-strategy
  2. Test (over public channel) for a subset that statistics conform to what EPR-pairs should give
  3. If test is passed, raw key is derived from the remaining bits
- Test can only be passed if they share entanglement, but then they can distill shared secret key from the remaining bits

Device-independent crypto

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements
- Two issues:

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements
- Two issues:
  1. There are security proofs under the assumption that Alice's and Bob's qubits are measured separately

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements
- Two issues:
  1. There are security proofs under the assumption that Alice's and Bob's qubits are measured separately, but not for the most general coherent attacks (yet)

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements
- Two issues:
  1. There are security proofs under the assumption that Alice's and Bob's qubits are measured separately, but not for the most general coherent attacks (yet)
  2. Locality loophole is no problem (isolated labs)

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements
- Two issues:
  1. There are security proofs under the assumption that Alice's and Bob's qubits are measured separately, but not for the most general coherent attacks (yet)
  2. Locality loophole is no problem (isolated labs); detection loophole is a bigger problem

Device-independent crypto

- New approach to quantum crypto, fewer assumptions:
  1. Parties are constrained by QM
  2. Parties have private source of randomness
  3. A & B's labs are isolated: no info leaks in or out

  But adversary may control states and measurements
- Two issues:
  1. There are security proofs under the assumption that Alice's and Bob's qubits are measured separately, but not for the most general coherent attacks (yet)
  2. Locality loophole is no problem (isolated labs); detection loophole is a bigger problem
- Applications besides QKD: random-number generation, bit commitment and coin flipping

Breaking parallel repetition

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification: Suppose Alice and Bob can win a game with prob $c < 1$

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel
- Raz's parallel repetition theorem:
  probability to win all games goes down as $c^{\Omega(k)}$

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel
- Raz's parallel repetition theorem:
  probability to win all games goes down as $c^{\Omega(k)}$
- Problem: even if classically $c < 1$, entanglement can make winning probability equal to 1

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel
- Raz's parallel repetition theorem:
  probability to win all games goes down as $c^{\Omega(k)}$
- Problem: even if classically $c < 1$, entanglement can make winning probability equal to 1
- Example: repeat magic square game k times:

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel
- Raz's parallel repetition theorem:
  probability to win all games goes down as $c^{\Omega(k)}$
- Problem: even if classically $c < 1$, entanglement can make winning probability equal to 1
- Example: repeat magic square game k times:
  1. Classical winning probability $\leq (8/9)^{\Omega(k)}$

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel
- Raz's parallel repetition theorem:
  probability to win all games goes down as $c^{\Omega(k)}$
- Problem: even if classically $c < 1$, entanglement can make winning probability equal to 1
- Example: repeat magic square game k times:
  1. Classical winning probability $\leq (8/9)^{\Omega(k)}$
  2. Quantum winning probability remains 1
     if Alice and Bob share $2k$ EPR-pairs

Breaking parallel repetition

- Parallel repetition often used for hardness-amplification:
  Suppose Alice and Bob can win a game with prob $c < 1$
  Let them try to win k instances of the game in parallel
- Raz's parallel repetition theorem:
  probability to win all games goes down as $c^{\Omega(k)}$
- Problem: even if classically $c < 1$, entanglement can make winning probability equal to 1
- Example: repeat magic square game k times:
  1. Classical winning probability $\leq (8/9)^{\Omega(k)}$
  2. Quantum winning probability remains 1
     if Alice and Bob share $2k$ EPR-pairs
- Classical hardness-amplification fails here!

Part 3:

What do we know about Bell inequalities?

How large can the violation be?

How large can the violation be?

- Bell inequality violation: $\omega^*(G) > \omega(G)$

How large can the violation be?

- Bell inequality violation: $\omega^*(G) > \omega(G)$
- CHSH game: $\omega_2^*(G) \approx 0.85$ vs $\omega(G) = 0.75$

How large can the violation be?

- Bell inequality violation: $\omega^*(G) > \omega(G)$
- CHSH game: $\omega_2^*(G) \approx 0.85$ vs $\omega(G) = 0.75$
- Magic square: $\omega_4^*(G) = 1$ vs $\omega(G) = 8/9$

How large can the violation be?

- Bell inequality violation: $\omega^*(G) > \omega(G)$
- CHSH game: $\omega_2^*(G) \approx 0.85$ vs $\omega(G) = 0.75$
- Magic square: $\omega_4^*(G) = 1$ vs $\omega(G) = 8/9$
- How large can $\frac{\omega_n^*(G)}{\omega(G)}$ be, as a function of the allowed entanglement-dimension n?

How large can the violation be?

- Bell inequality violation: $\omega^*(G) > \omega(G)$
- CHSH game: $\omega_2^*(G) \approx 0.85$ vs $\omega(G) = 0.75$
- Magic square: $\omega_4^*(G) = 1$ vs $\omega(G) = 8/9$
- How large can $\dfrac{\omega_n^*(G)}{\omega(G)}$ be, as a function of the allowed entanglement-dimension n?

1. JPPVW'09: at most $O(n)$ for all G

How large can the violation be?

- Bell inequality violation: $\omega^*(G) > \omega(G)$
- CHSH game: $\omega_2^*(G) \approx 0.85$ vs $\omega(G) = 0.75$
- Magic square: $\omega_4^*(G) = 1$ vs $\omega(G) = 8/9$
- How large can $\frac{\omega_n^*(G)}{\omega(G)}$ be, as a function of the allowed entanglement-dimension n?

1. JPPVW'09: at most $O(n)$ for all G
2. BRSW'11: there is a G with $\frac{\omega_n^*(G)}{\omega(G)} \geq \frac{n}{(\log n)^2}$

XOR-games: constant improvement

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1)

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1), and winning condition: $a \cdot b = c_{xy}$. Example: CHSH

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1), and winning condition: $a \cdot b = c_{xy}$. Example: CHSH
- For classical strategies $a : x \mapsto a(x)$ and $b : y \mapsto b(y)$, Alice and Bob win on input x, y iff $c_{xy} a(x) b(y) = 1$

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1), and winning condition: $a \cdot b = c_{xy}$. Example: CHSH
- For classical strategies $a : x \mapsto a(x)$ and $b : y \mapsto b(y)$, Alice and Bob win on input x, y iff $c_{xy} a(x) b(y) = 1$
- For $M(x,y) = \pi(x,y) c_{xy}$, $\omega(G) = \max_{a,b} \sum_{x,y} M(x,y) a(x) b(y)$

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1), and winning condition: $a \cdot b = c_{xy}$. Example: CHSH
- For classical strategies $a : x \mapsto a(x)$ and $b : y \mapsto b(y)$, Alice and Bob win on input x, y iff $c_{xy} a(x) b(y) = 1$
- For $M(x,y) = \pi(x,y) c_{xy}$, $\omega(G) = \max_{a,b} \sum_{x,y} M(x,y) a(x) b(y)$
- Using results of Tsirelson:

$$\omega^*(G) = \max_{d, A(x), B(y) \in S^{d-1}} \sum_{x,y} M(x,y) \langle A(x), B(y) \rangle$$

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1), and winning condition: $a \cdot b = c_{xy}$. Example: CHSH
- For classical strategies $a : x \mapsto a(x)$ and $b : y \mapsto b(y)$, Alice and Bob win on input x, y iff $c_{xy} a(x) b(y) = 1$
- For $M(x,y) = \pi(x,y) c_{xy}$, $\omega(G) = \max_{a,b} \sum_{x,y} M(x,y) a(x) b(y)$
- Using results of Tsirelson:

$$\omega^*(G) = \max_{d, A(x), B(y) \in S^{d-1}} \sum_{x,y} M(x,y) \langle A(x), B(y) \rangle$$

- Grothendieck's inequality says $\omega^*(G) \leq K_G \omega(G)$

XOR-games: constant improvement

- XOR-game: the outputs a and b are bits (viewed as ± 1), and winning condition: $a \cdot b = c_{xy}$. Example: CHSH
- For classical strategies $a : x \mapsto a(x)$ and $b : y \mapsto b(y)$, Alice and Bob win on input x, y iff $c_{xy} a(x) b(y) = 1$
- For $M(x,y) = \pi(x,y) c_{xy}$, $\omega(G) = \max_{a,b} \sum_{x,y} M(x,y) a(x) b(y)$
- Using results of Tsirelson:

$$\omega^*(G) = \max_{d, A(x), B(y) \in S^{d-1}} \sum_{x,y} M(x,y) \langle A(x), B(y) \rangle$$

- Grothendieck's inequality says $\omega^*(G) \leq K_G \omega(G)$
- Quantum advantage not much bigger than classical!

Max violation as function of #outputs

Max violation as function of #outputs

- XOR-games: constant number of outputs, limited Bell inequality violation

Max violation as function of #outputs

- XOR-games: constant number of outputs, limited Bell inequality violation

- More generally, the maximal Bell inequality violation is limited by the number k of outputs of each player:

Max violation as function of #outputs

- XOR-games: constant number of outputs, limited Bell inequality violation
- More generally, the maximal Bell inequality violation is limited by the number k of outputs of each player:

1. Junge & Palazuelos'10: $\dfrac{\omega^*(G)}{\omega(G)} = O(k)$ for all G

Max violation as function of #outputs

- XOR-games: constant number of outputs, limited Bell inequality violation
- More generally, the maximal Bell inequality violation is limited by the number k of outputs of each player:

1. Junge & Palazuelos'10: $\dfrac{\omega^*(G)}{\omega(G)} = O(k)$ for all G
2. BRSW'11: there is a G with $\dfrac{\omega^*(G)}{\omega(G)} \geq \dfrac{k}{(\log k)^2}$

What kind of entanglement?

What kind of entanglement?

- For many purposes, EPR-pairs are the most general kind of entanglement

What kind of entanglement?

- For many purposes, EPR-pairs are the most general kind of entanglement
- Other kinds of entanglement can be derived from this with local operations and classical communication

What kind of entanglement?

- For many purposes, EPR-pairs are the most general kind of entanglement
- Other kinds of entanglement can be derived from this with local operations and classical communication
- Not for Bell inequalities: there are games where

What kind of entanglement?

- For many purposes, EPR-pairs are the most general kind of entanglement
- Other kinds of entanglement can be derived from this with local operations and classical communication
- Not for Bell inequalities: there are games where
  - no violation if Alice and Bob share EPR-pairs

What kind of entanglement?

- For many purposes, EPR-pairs are the most general kind of entanglement
- Other kinds of entanglement can be derived from this with local operations and classical communication
- Not for Bell inequalities: there are games where
  - no violation if Alice and Bob share EPR-pairs
  - large violation if they share other, non-maximally entangled state (Junge & Palazuelos'10, Regev'10)

Summary

Summary

- Bell inequality violations show that local realism is untenable view of nature

Summary

- Bell inequality violations show that local realism is untenable view of nature
- Relevance for crypto:

Summary

- Bell inequality violations show that local realism is untenable view of nature

- Relevance for crypto:

  1. Positive: device-independent cryptography

Summary

- Bell inequality violations show that local realism is untenable view of nature
- Relevance for crypto:
  1. Positive: device-independent cryptography
  2. Negative: hardness amplification can fail

Summary

- Bell inequality violations show that local realism is untenable view of nature
- Relevance for crypto:
  1. Positive: device-independent cryptography
  2. Negative: hardness amplification can fail
- What do we know:

Summary

- Bell inequality violations show that local realism is untenable view of nature
- Relevance for crypto:
  1. Positive: device-independent cryptography
  2. Negative: hardness amplification can fail
- What do we know:
  1. Essentially tight examples of Bell ineq violations

Summary

- Bell inequality violations show that local realism is untenable view of nature

- Relevance for crypto:
  1. Positive: device-independent cryptography
  2. Negative: hardness amplification can fail

- What do we know:
  1. Essentially tight examples of Bell ineq violations, as a function of entanglement-dimension, and as a function of number of outputs

Summary

- Bell inequality violations show that
  local realism is untenable view of nature

- Relevance for crypto:
  1. Positive: device-independent cryptography
  2. Negative: hardness amplification can fail

- What do we know:
  1. Essentially tight examples of Bell ineq violations, as a function of entanglement-dimension, and as a function of number of outputs
  2. EPR-pairs not always the best type of entanglement