量子和相对论密码学：基于物理原理的信息安全

Quantum and Relativistic Cryptography: Security Based on Physical

施尧耘　Yaoyun Shi

阿里云首席量子技术科学家，之江实验室副主任

Aliyun and Zhijiang Laboratory

Claim 1.

All cryptographic protocols are secure.

As long as the assumptions are met.

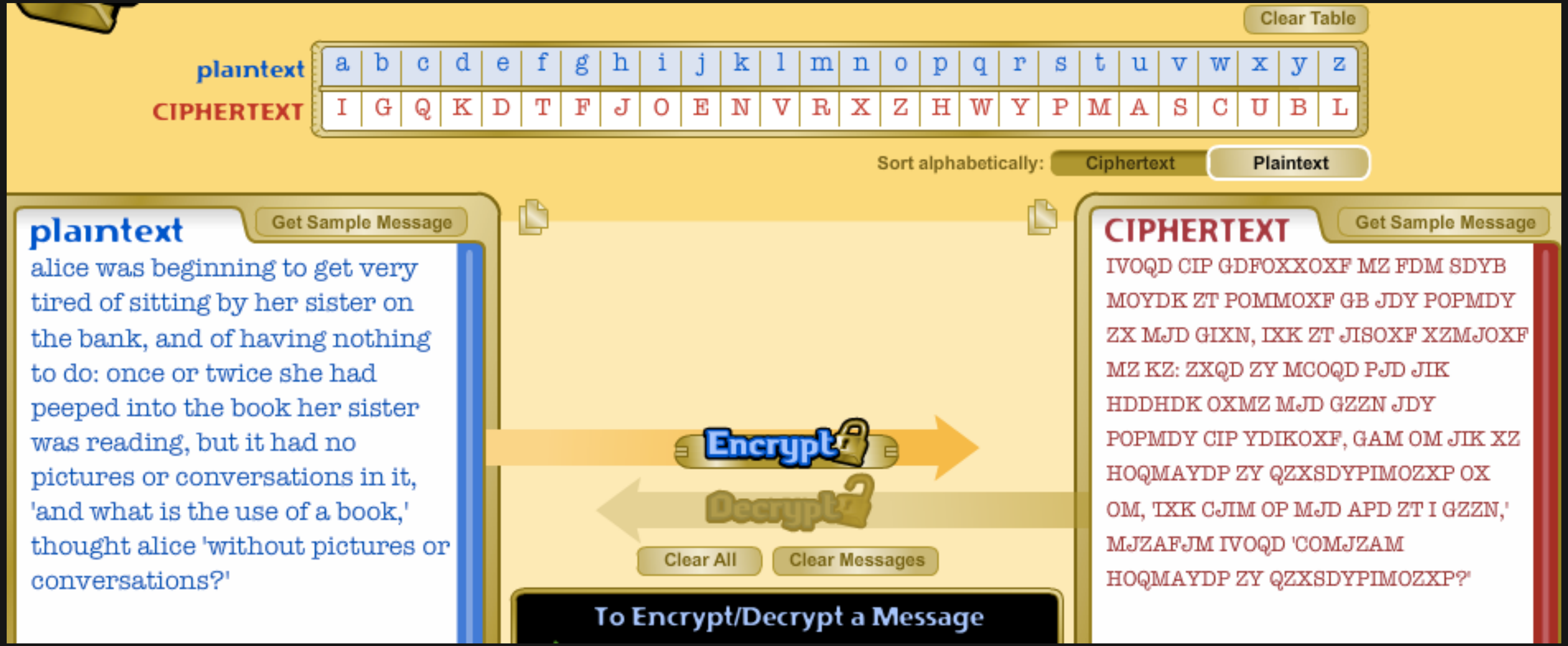
A central goal in crypto research: minimize assumptions.

Claim 2.

Cryptography today is as secure as it was thousands of years ago.

The same assumption:
nobody is smart enough to crack it.

Example: Substitution table



CryptoClub.org

Example: RSA

Widely used public-key cryptosystem

Turing Award 2002

Integer-factorization breaks RSA

No efficient classical algorithm known
No proof of hardness

Example: Diffie-Hellman-Merkle Key Exchange Protocol

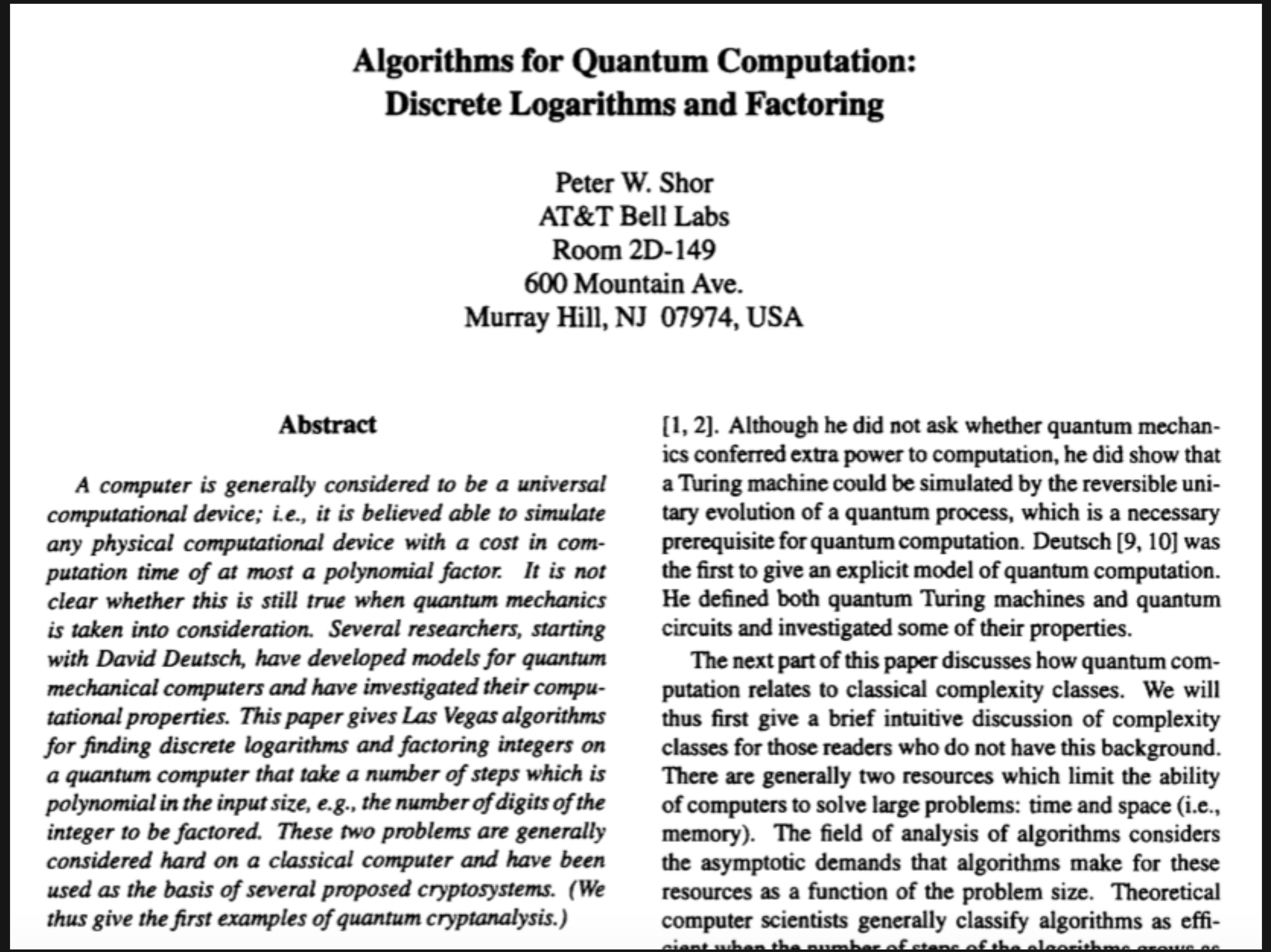
Widely used protocol

Turing Award 2015

Solving Discrete-Logarithm breaks it

No efficient classical algorithm known
No proof of hardness

Quantum computer will break both RSA and D-H-M



Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as effi-

“Computational Assumption”: assuming Adversary’s computational power is limited

Computational Assumption

All public-key cryptography requires the assumption

Security may be broken by advances in computing power or in algorithms

“Unconditional/Information-Theoretical Security”: without Computational Assumption

A central question:
Is unconditional security possible?

Not for many tasks

A way out: assuming fundamental physical laws; Reduce security to the correctness of physical theories

Key Examples in this Talk

Quantum:
Key Distribution

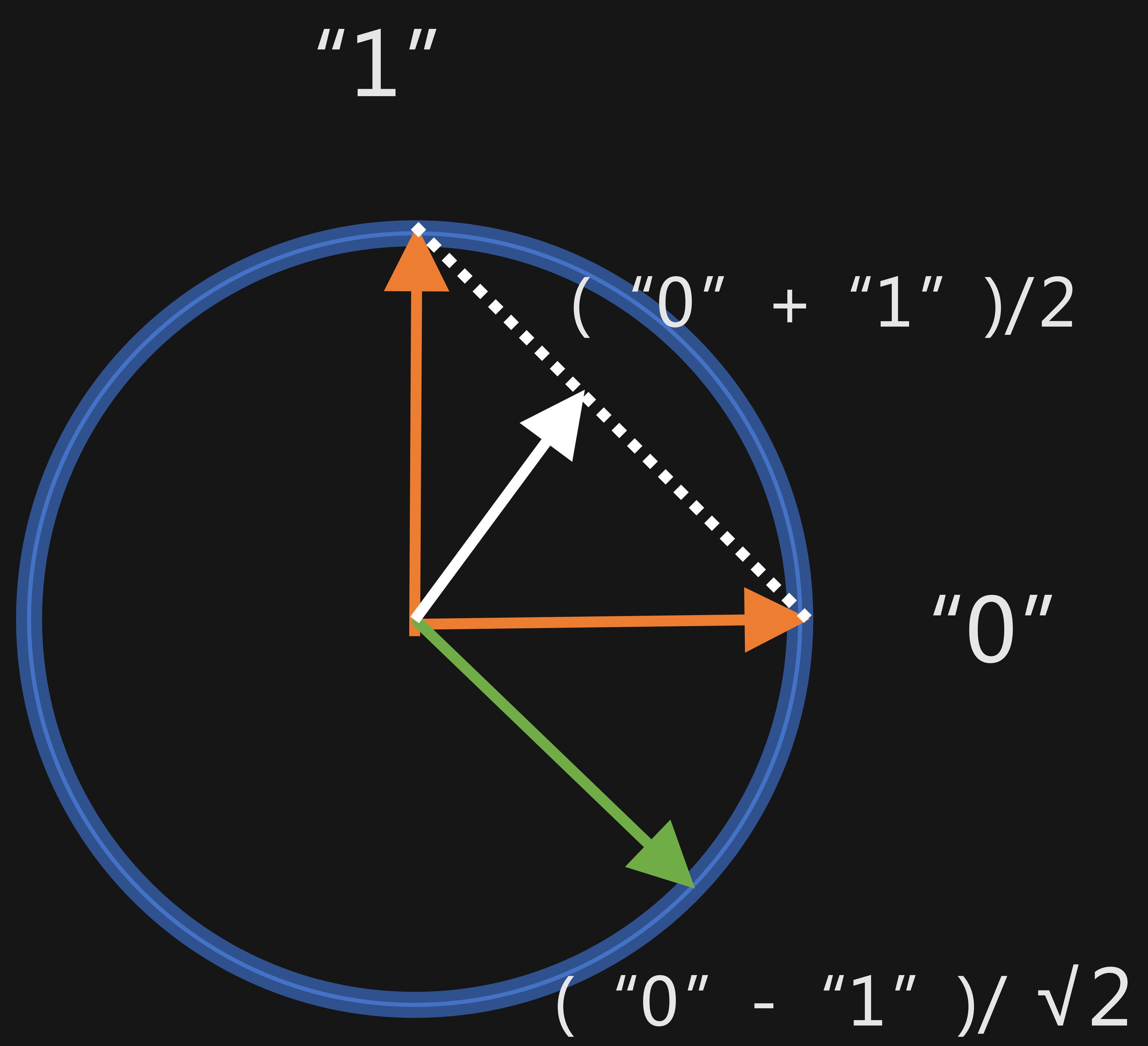
Quantum + Relativistic:
Untrusted-Device Q.
Key Distribution

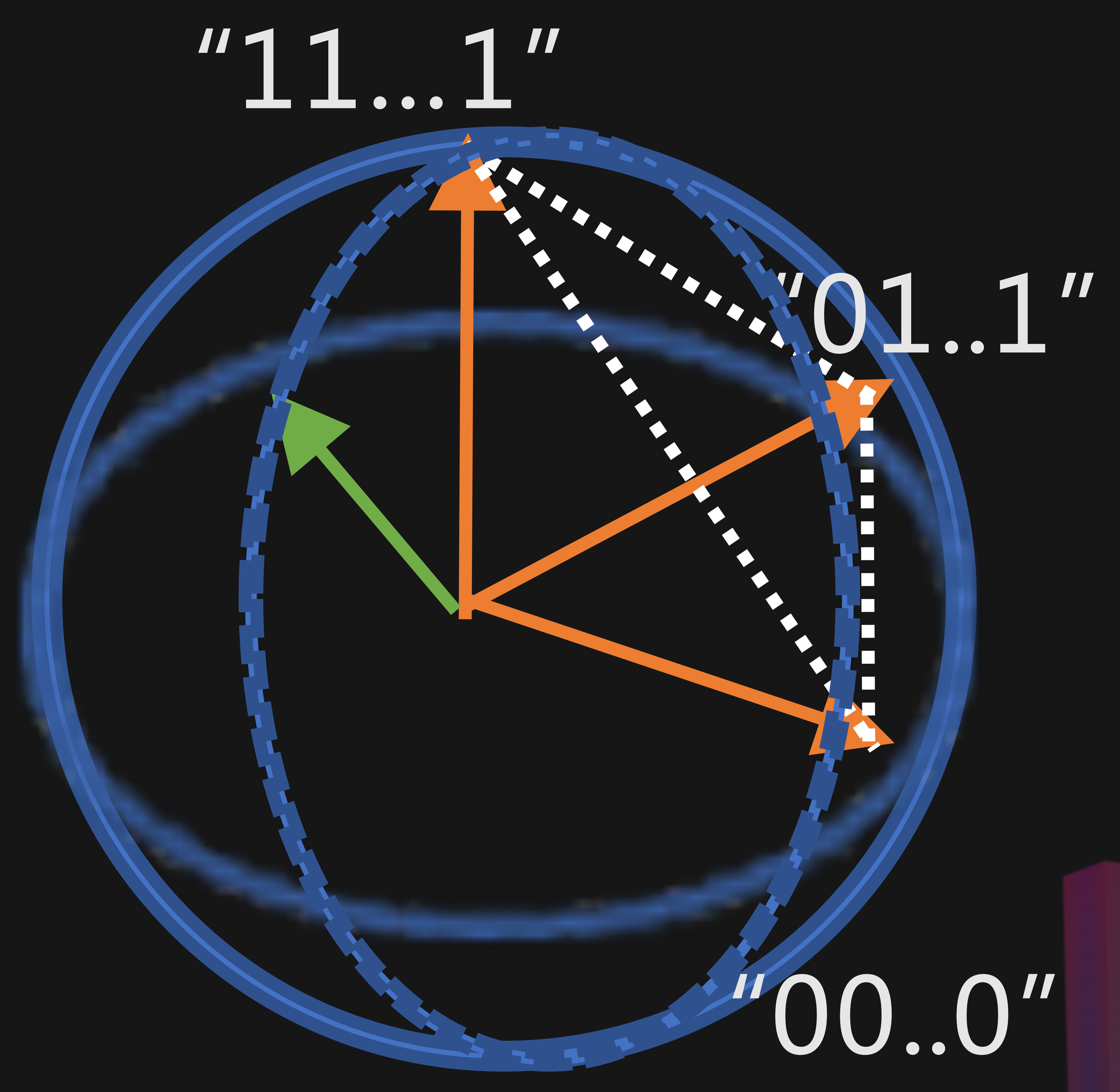
Quantum Cryptography: Assume that quantum mechanics is correct (Honest Party can apply q.) & Complete (Adversary cannot do more than q. m. allows)

Quantum States

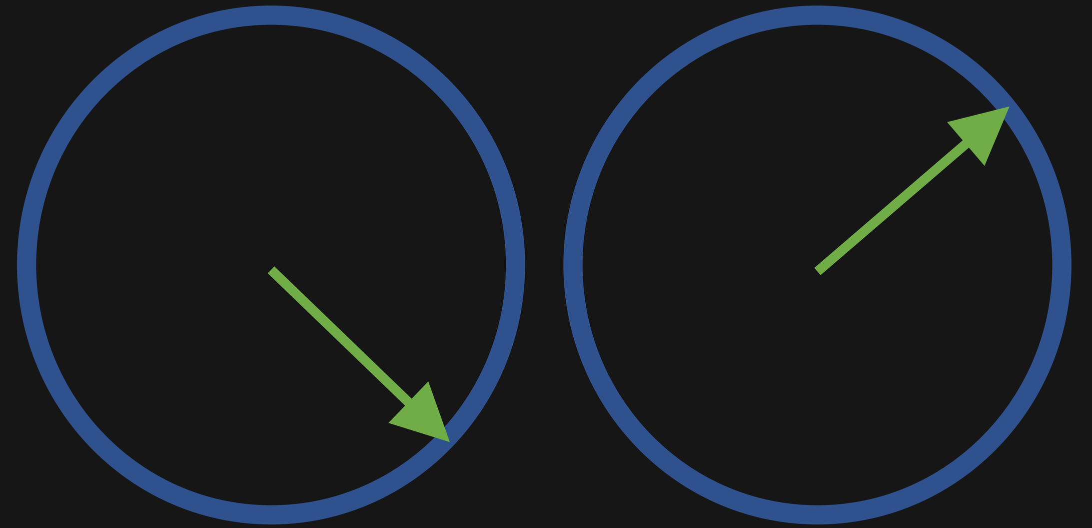
- 1 classical bit = “0” or “1”
- 1 random bit = a probabilistic mixture of “0” and “1”
- 1 quantum bit (qubit) = a length 1 linear combination of “0” and “1”

- N classical bits : 2^N possibilities ”00..0”,.. “11..1”
- N random bits : a probabilistic mixture of these
- N qubits : a length 1 linear combination of these





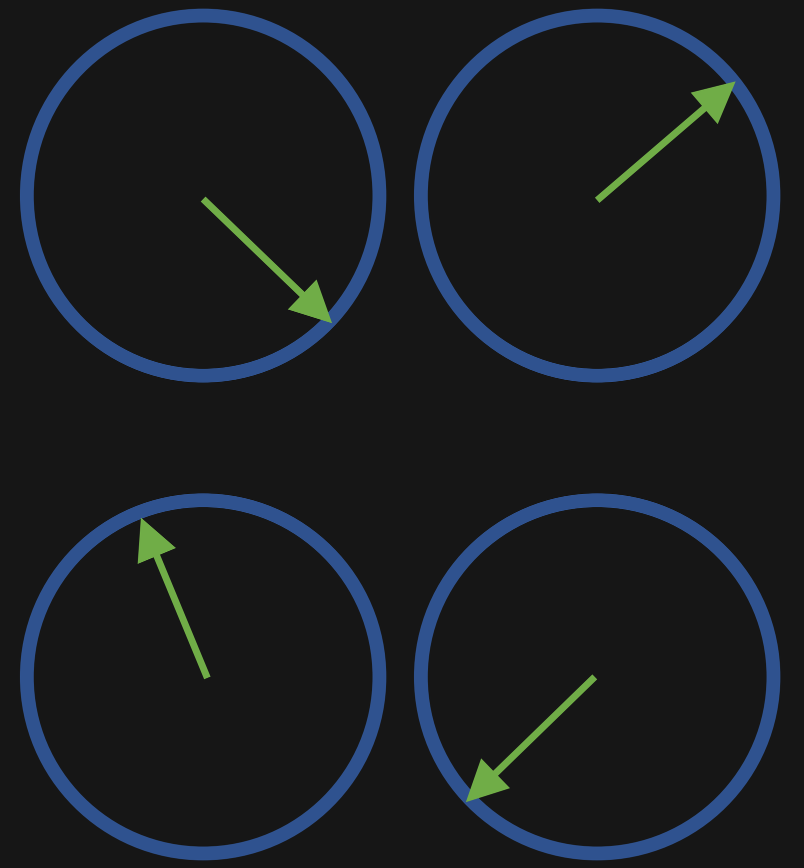
Quantum Entanglement



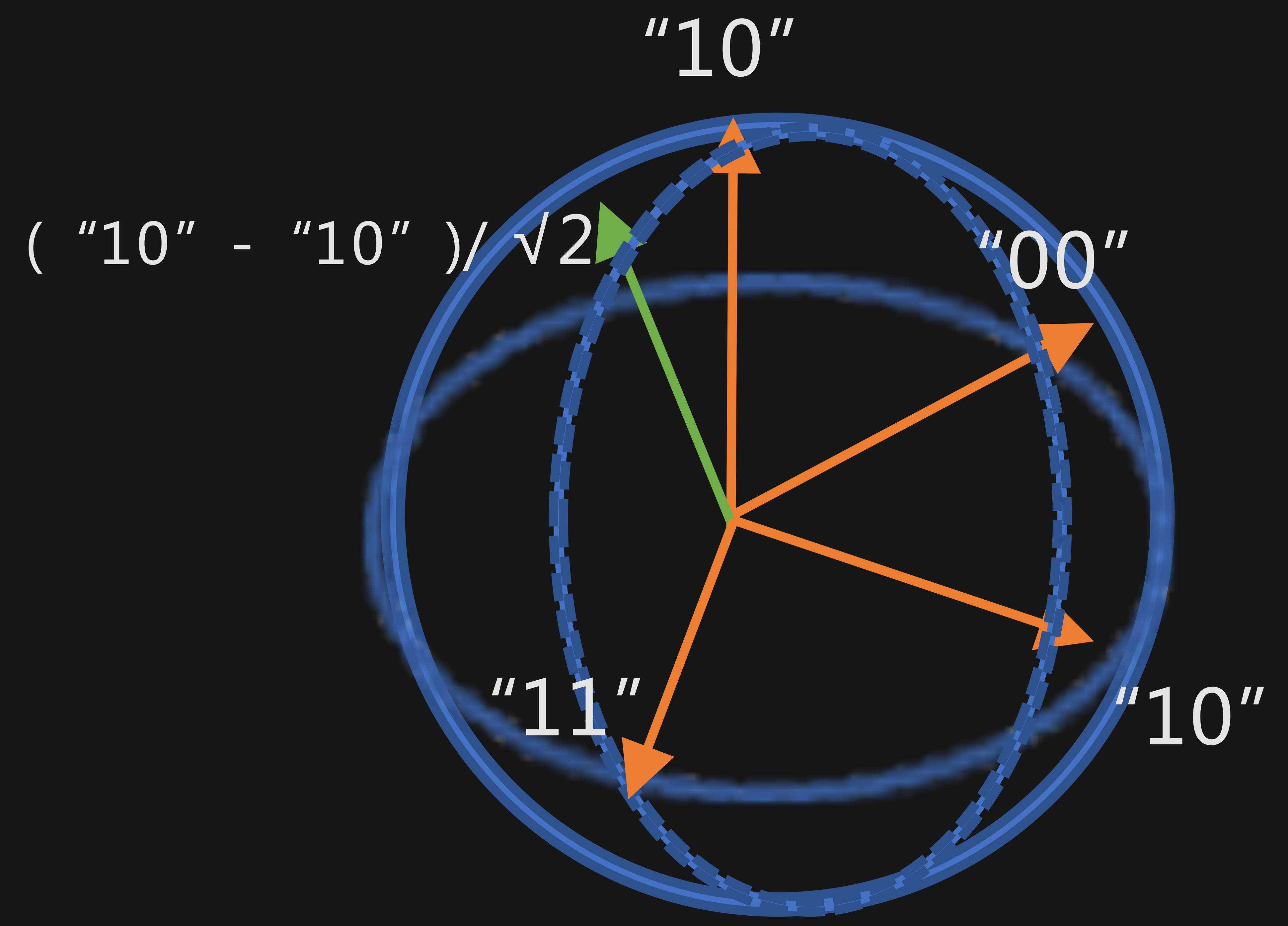
No correlation

½ probability

½ probability



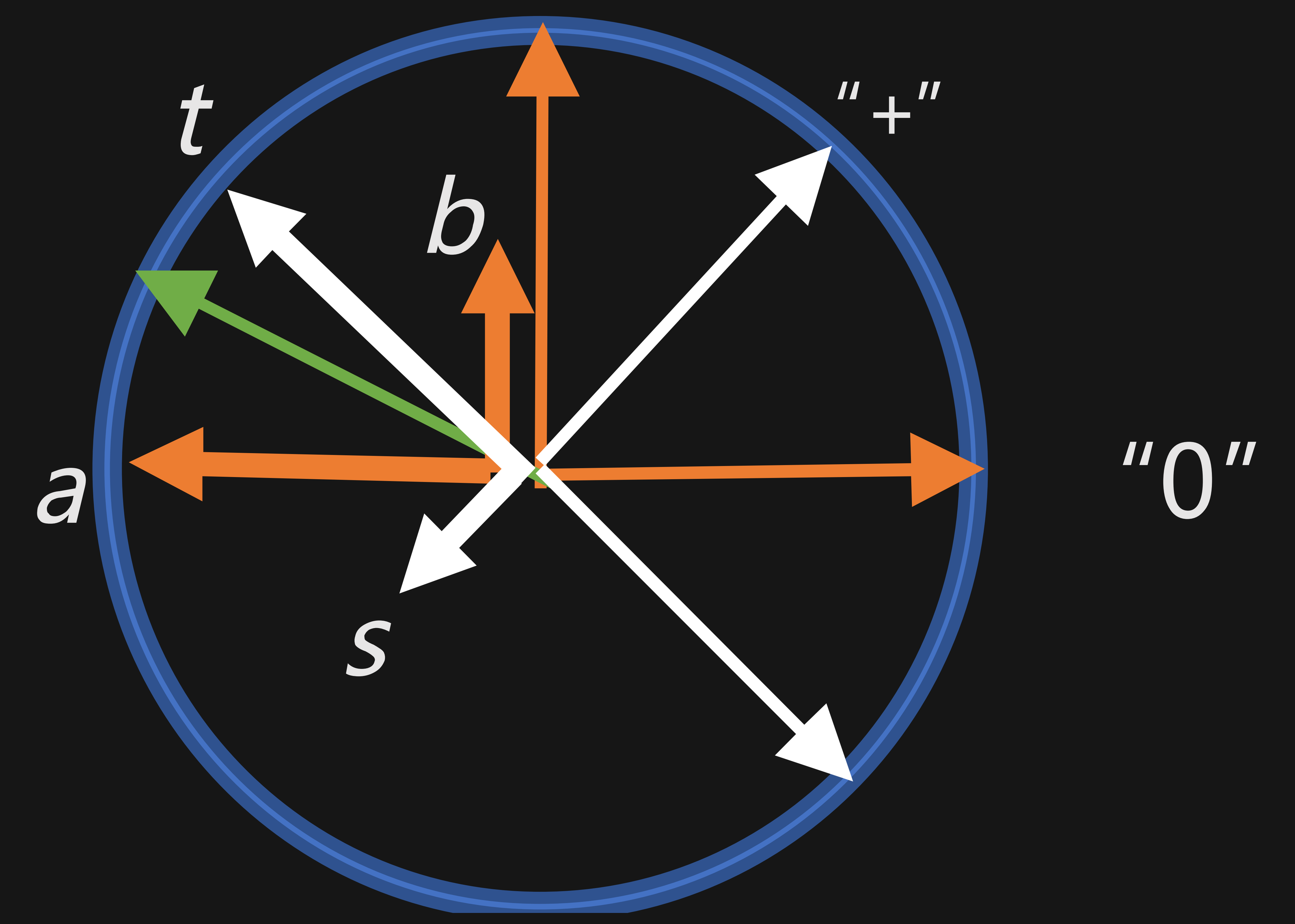
Classical correlation

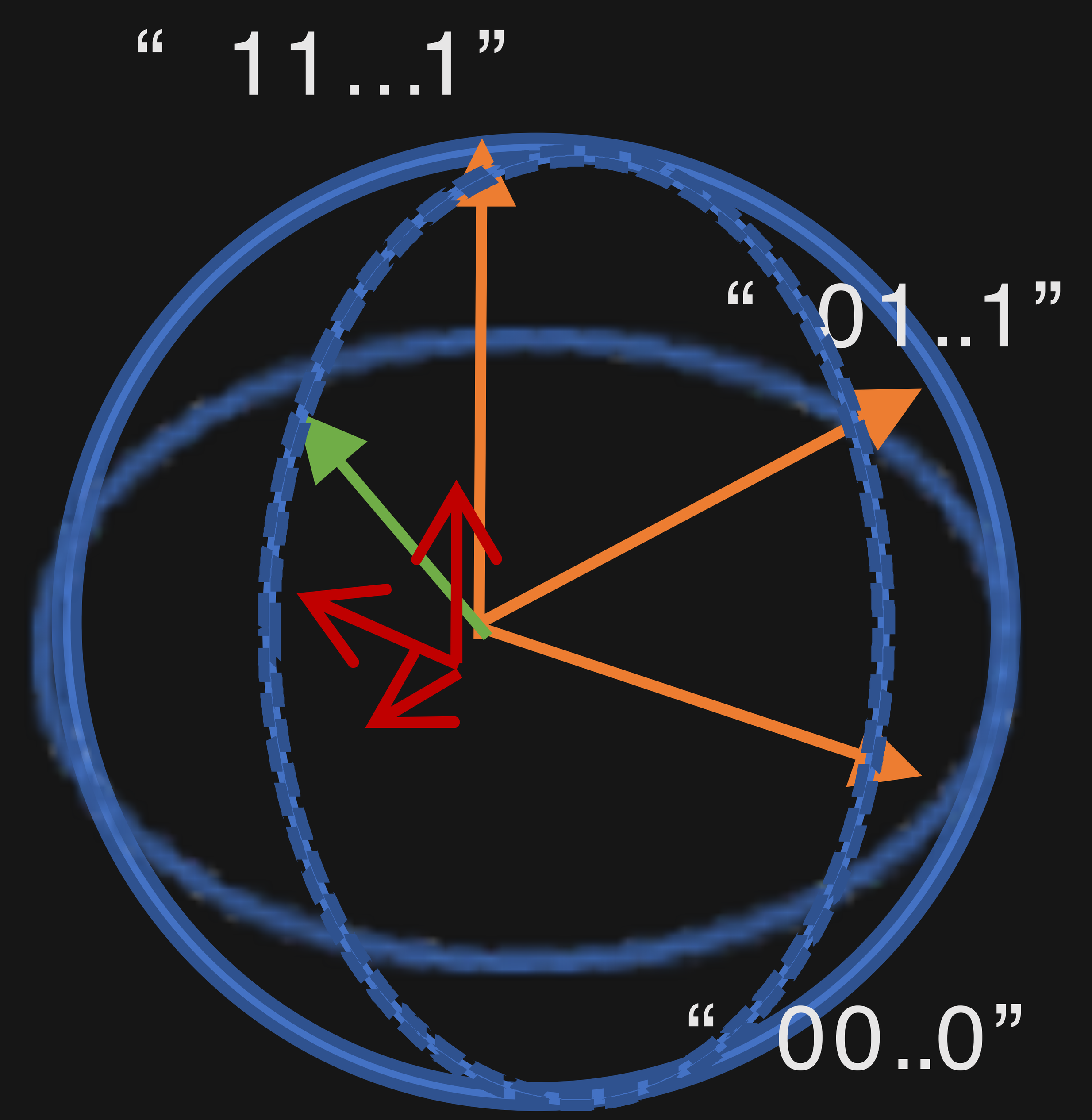


Quantum entanglement
≠ any classical correlation

Quantum Measurement: classical read-out

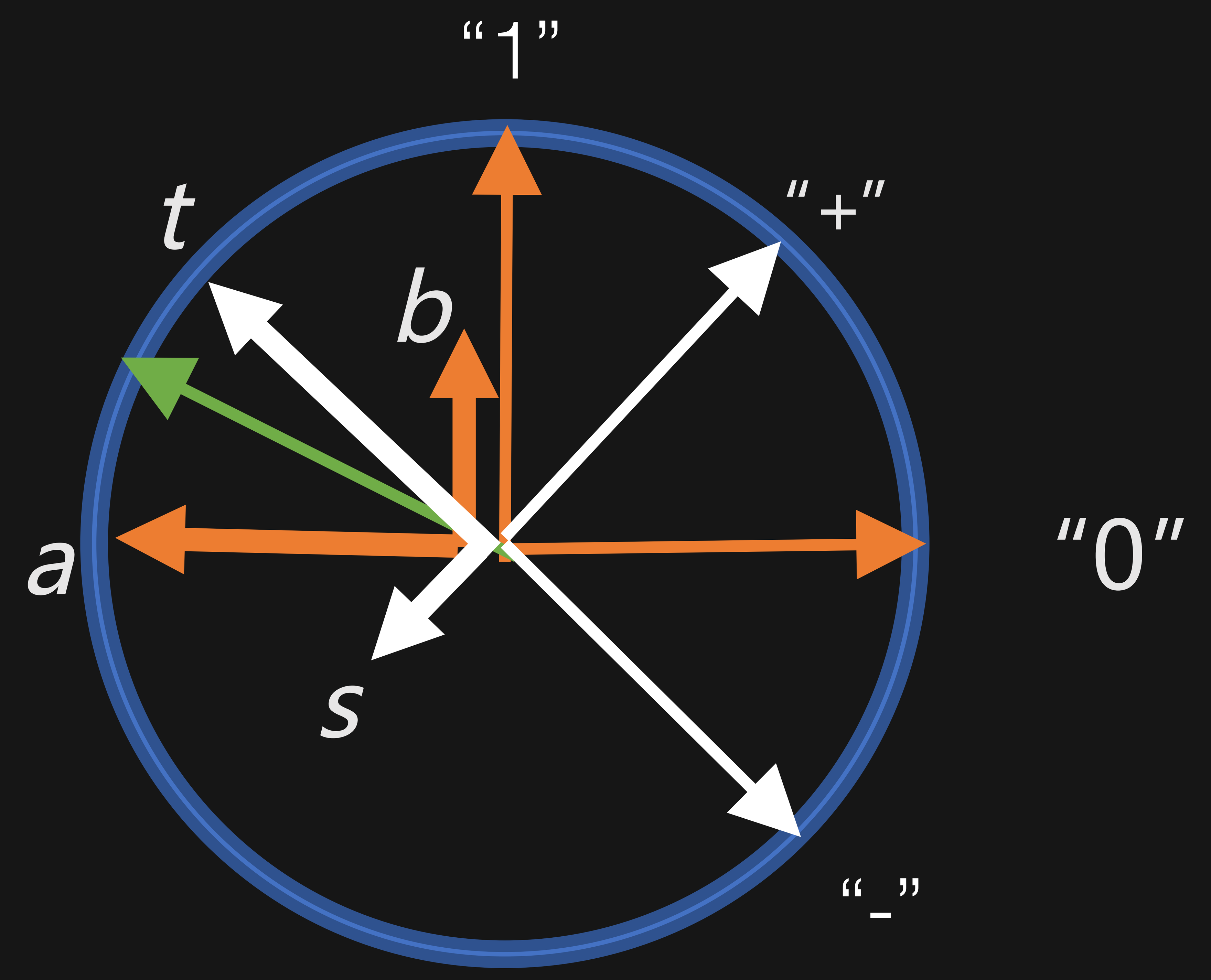
- Measurement = projection to an orthonormal basis
- Each base vector = an observed outcome
- Assign a probability to each outcome
- The state becomes the observed outcome state





Example: measuring a 1 qubit state ϕ

- Using {“0”, “1”}:
  W. prob. = |a|², observe “0”, ϕ becomes “0”
  W. prob. = |b|², observe “1”, ϕ becomes “1”
- Using {“+”, “-”}:
  W. prob. = |s|², observe “+”, ϕ becomes “+”
  W. prob. = |t|², observe “-”, ϕ becomes “-”



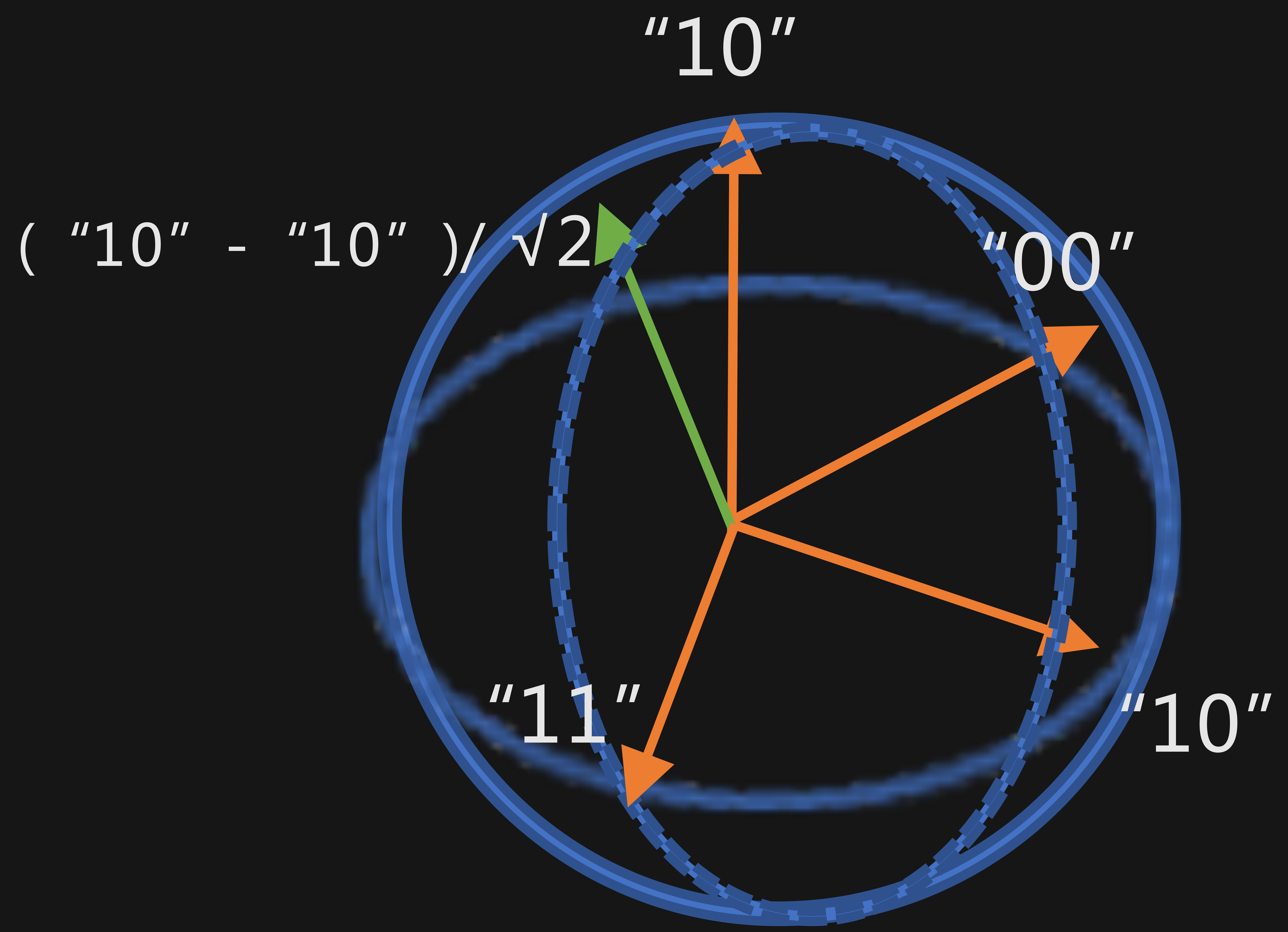
Measuring both particles in the EPR State
(“01”- “10”)/√2:

- Both using {“0”, “1”}: equal chance in {“01”, “10”}
- Both using {“+”, “-”}: equal chance in {“+-”, “-+”}
- Both using any orthonormal {“⬆”,”⬇”}: equal chance in

  {“⬆⬇”, “⬇⬆”}

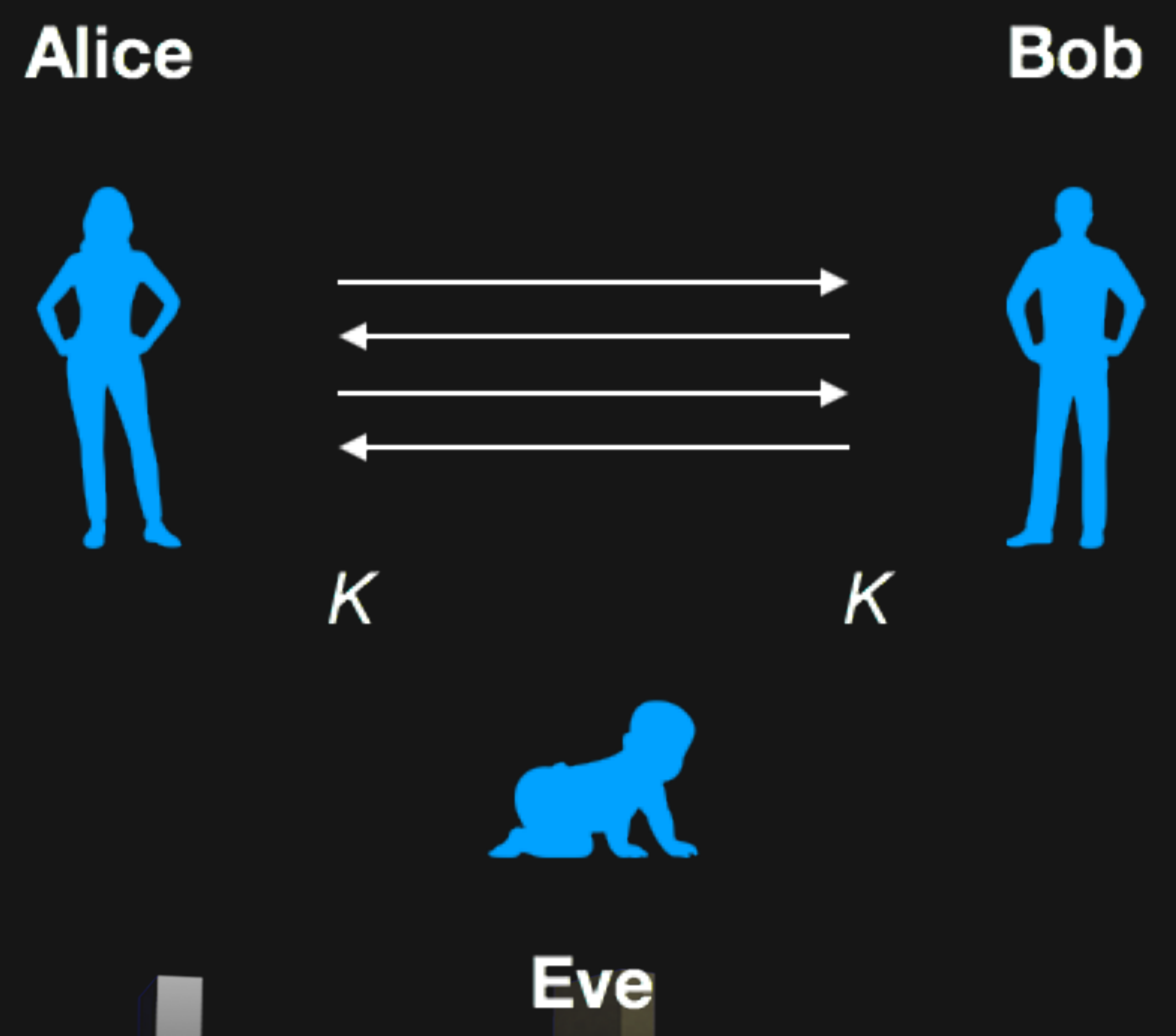
The results are always the opposite!

- One uses {“0”, “1”}, the other uses {“+”, “-”}
  uniformly random



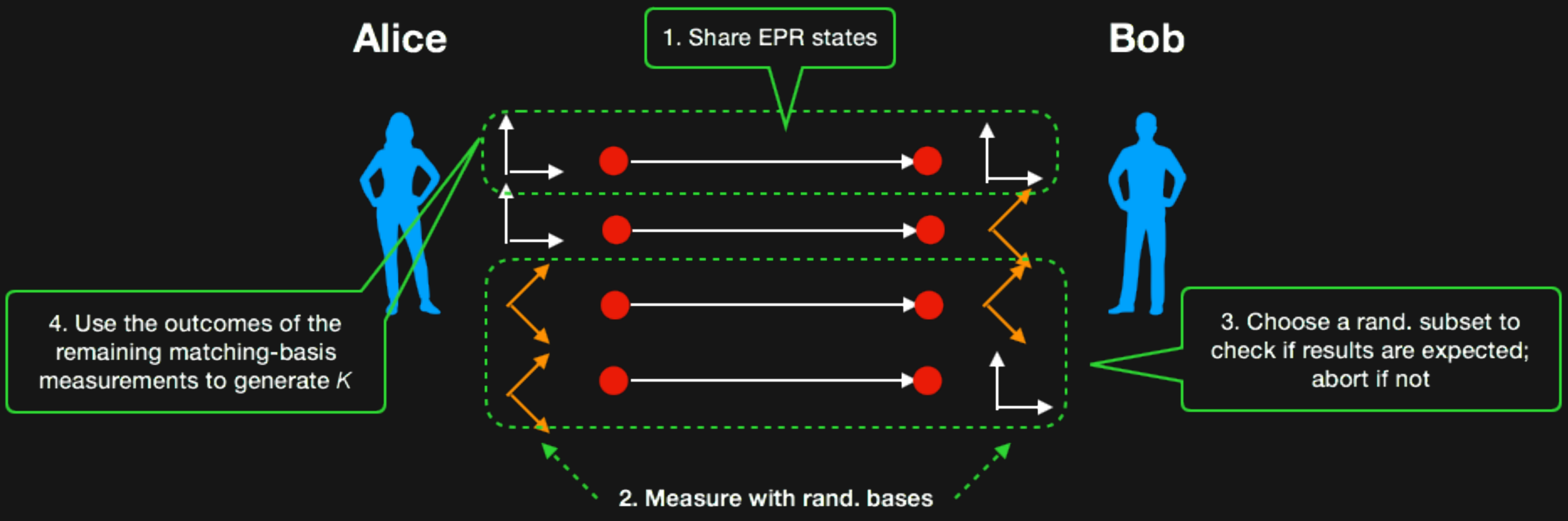
Key Exchange

- Alice and Bob talk to each other while Eve is listening
- Alice & Bob want to establish a secret *K* unknown to Eve



- Classically impossible because Eve can copy the whole conversation
- Quantum possible as Eve has measure message to gain info, thusdisturbing the system, risking being caught

Quantum Key Distribution [BB84, E91]

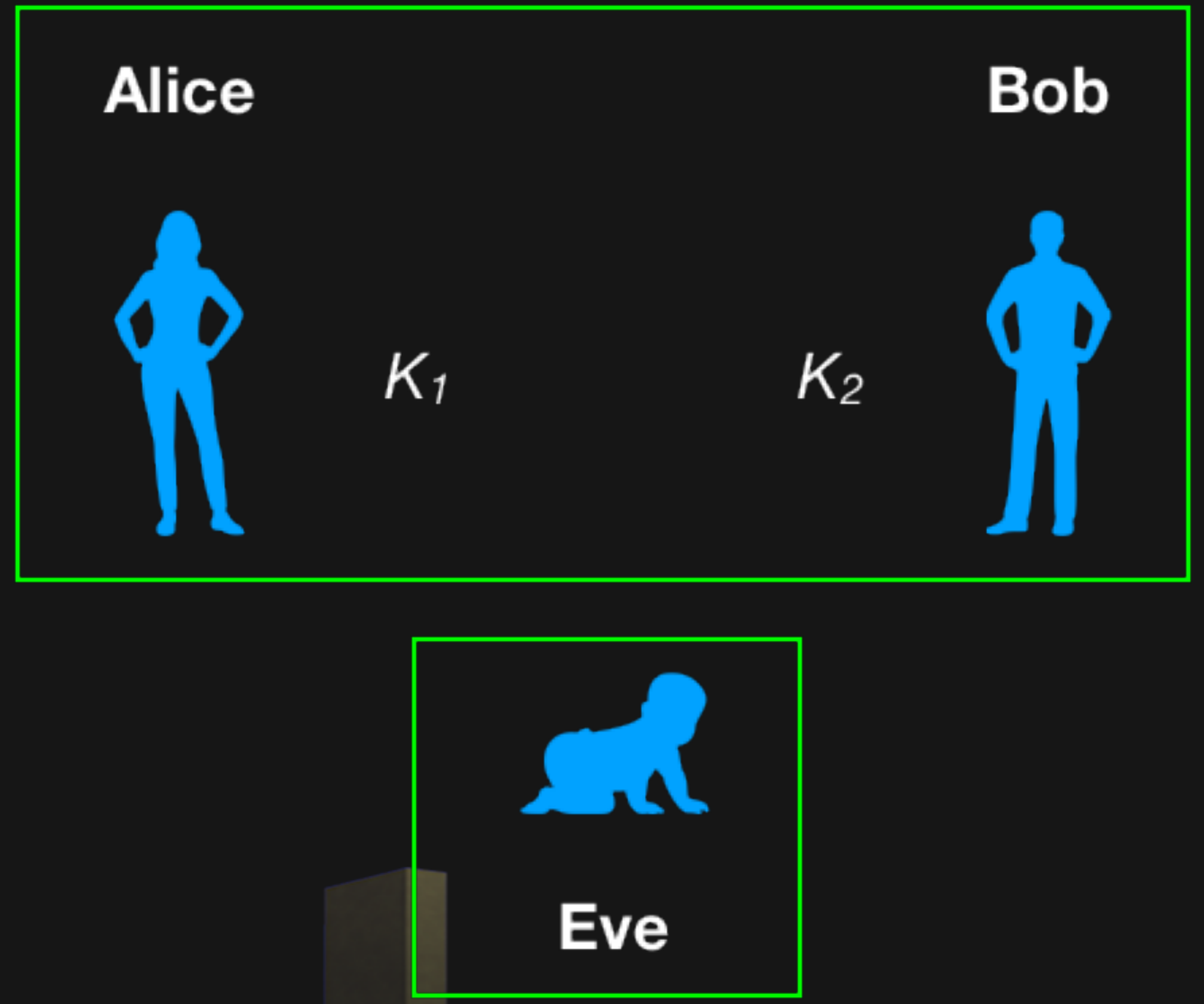


Security of QKD

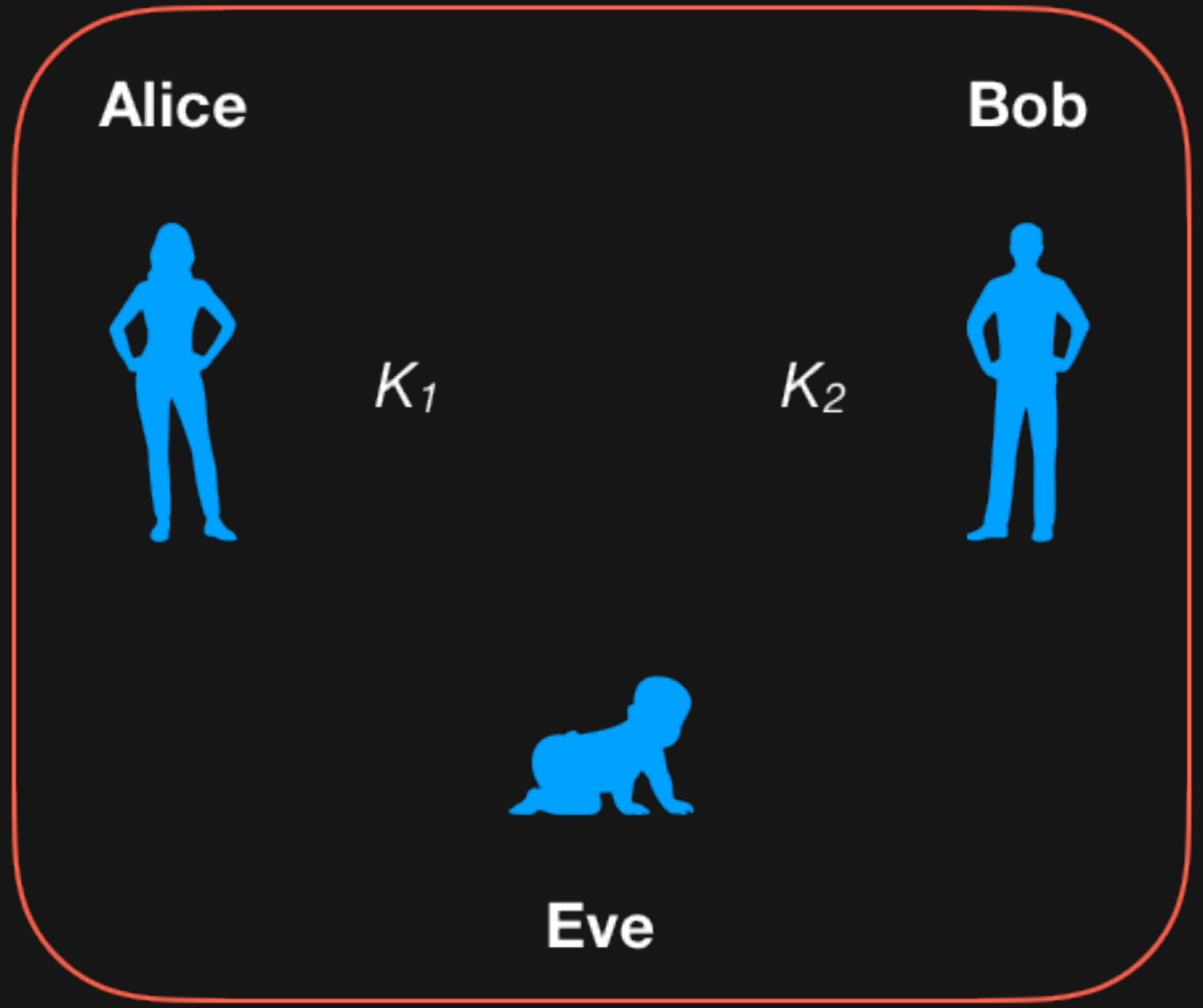
[LC'01, M'01, Renner'05]

- If Eve is honest, Success with high prob.
- Final state approximately a mixture of secure & Success and Abort

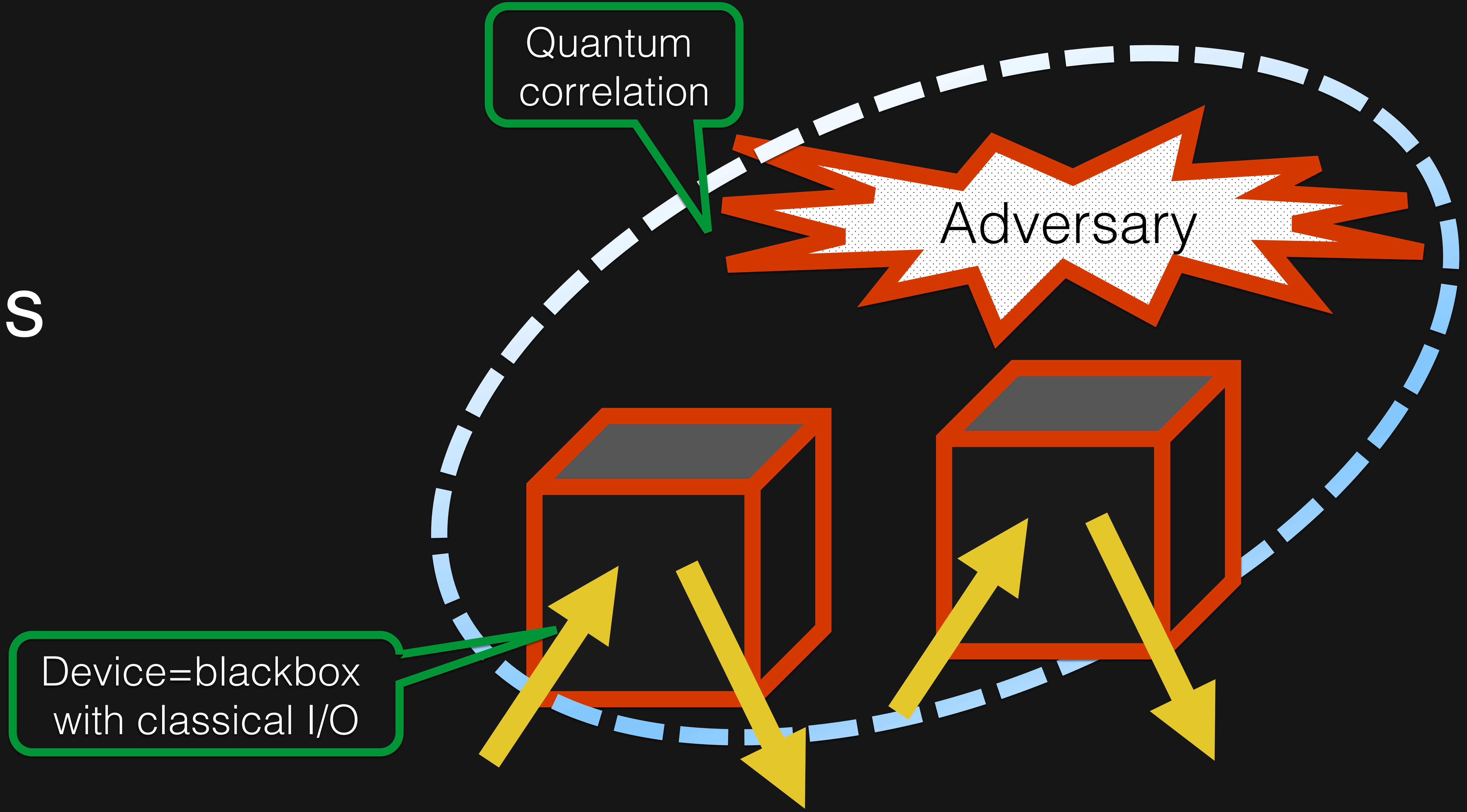
Success: approximately
K1=K2=uniform;
No correlation with Eve



Abort
Arbitrary correlation

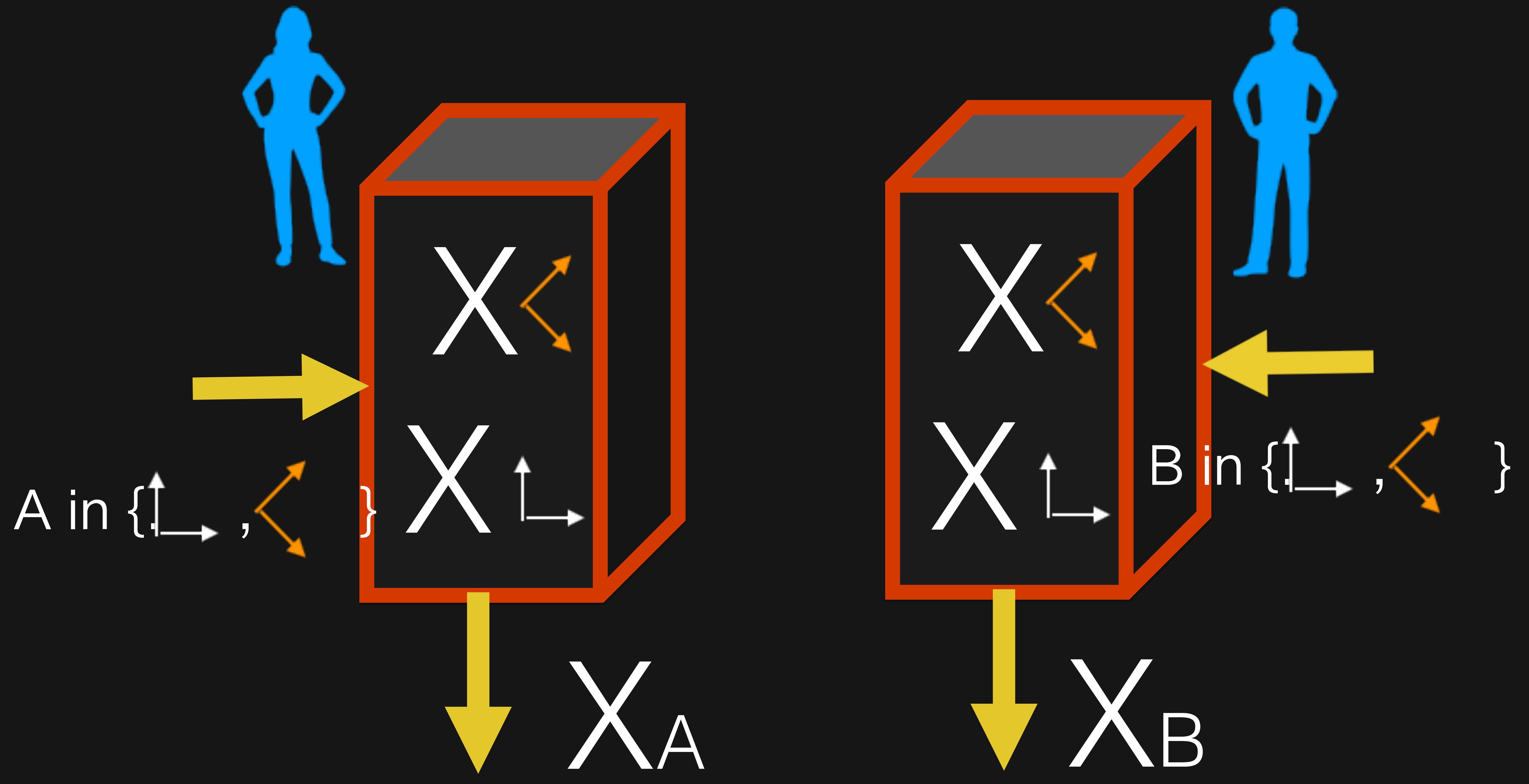


How do we know that the quantum devices are functioning well?



Faking the EPR correlation (for the “0/1” and “+/-” measurements)

The X variables are uniform and independent



Quantum Self-Testing: Some quantum correlations cannot be faked; implementation may assume relativity

Nonlocal games: making use of relativity to forbid communication

The Magic Square Game (MSG)

- Impossible constraints

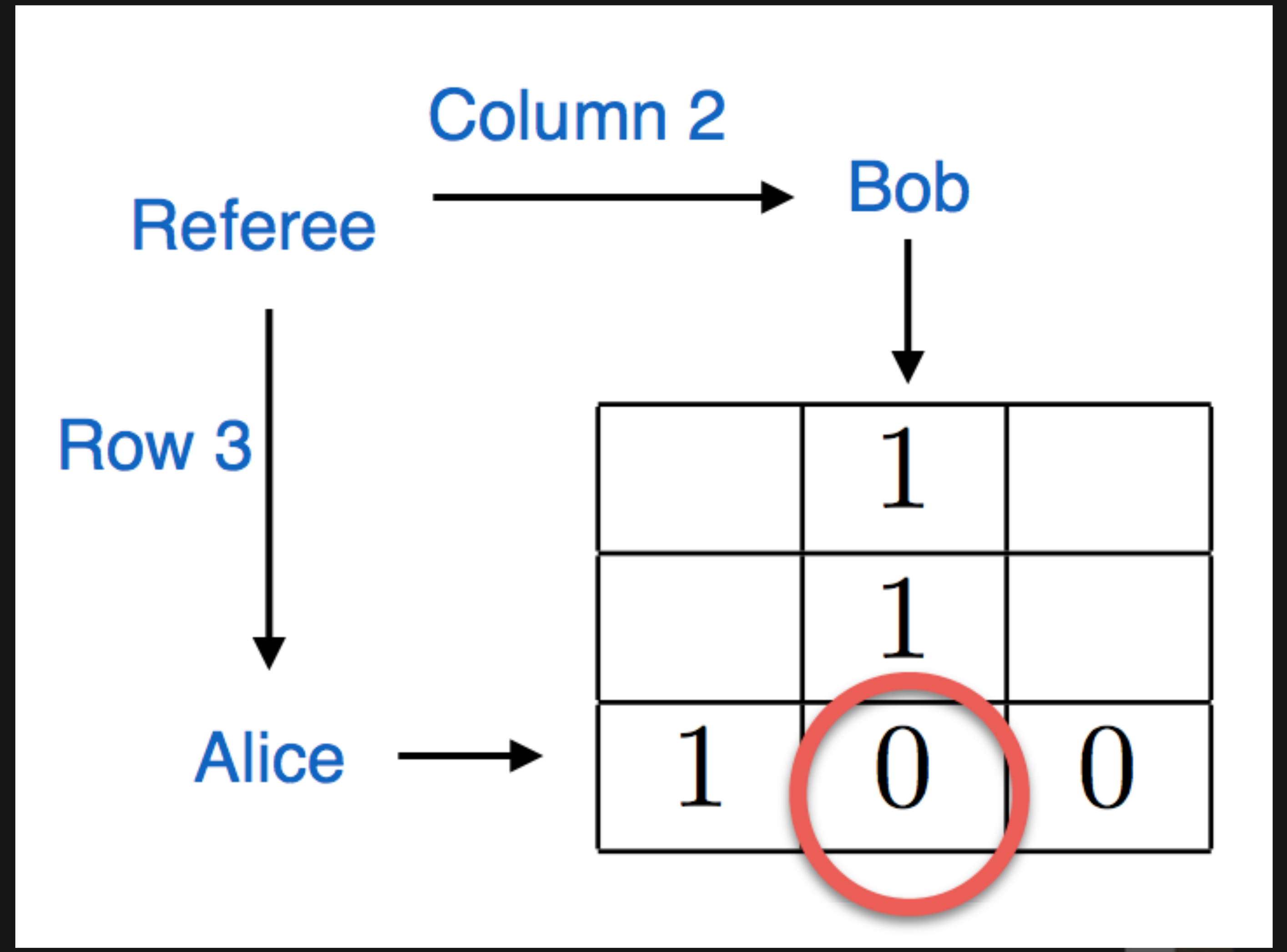
Game:

- Referee -> Alice a rand. row index
- Referee -> Bob a rand. column index
- Both return 3 bits
- Pass: if
  intersection bit is consistent, &
  row and column sums are correct

Each row sums to odd

1	1	1
0	1	0
1	0	0/1?

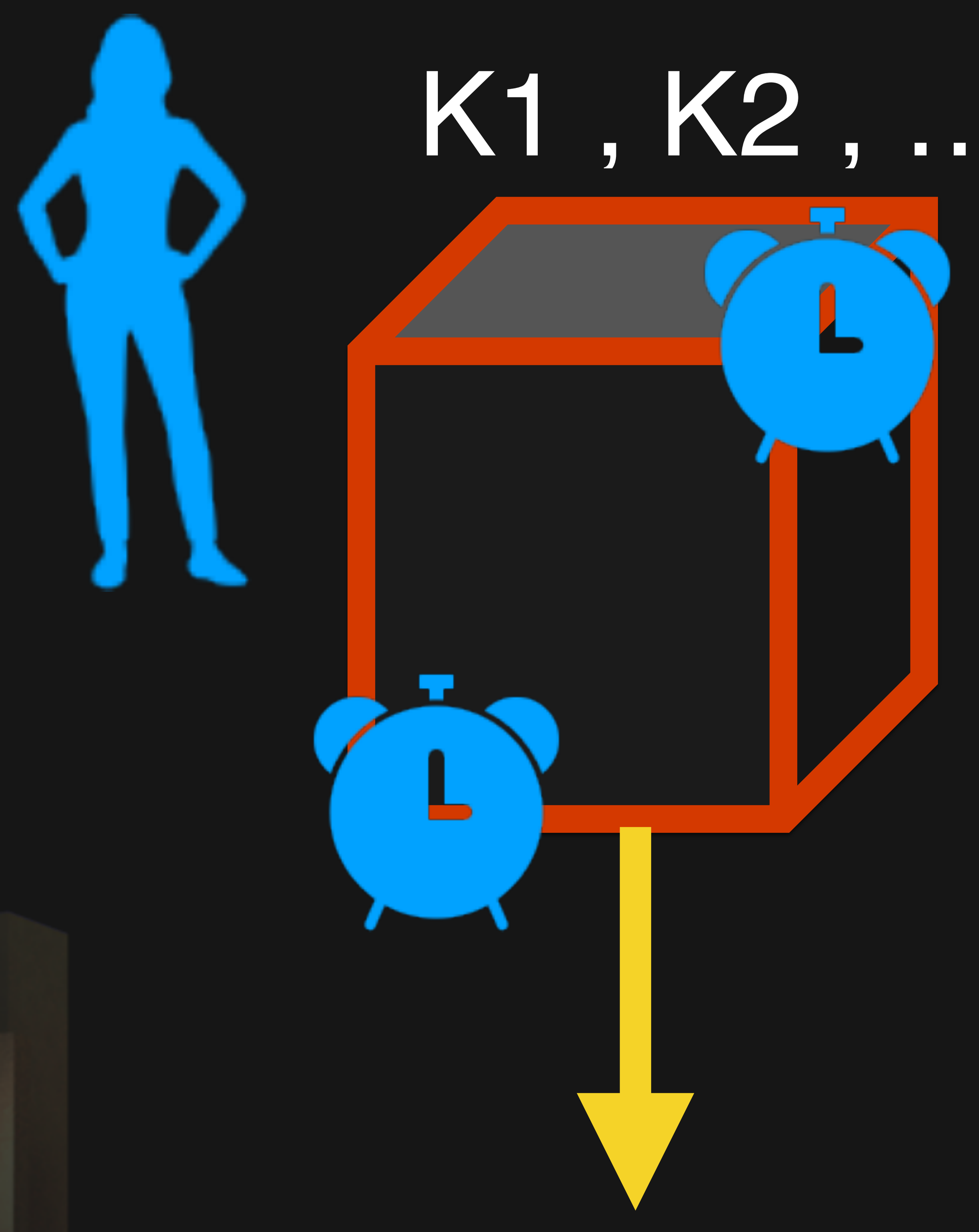
Each column sums to even



MSG: all classical algorithm fails ≥1/9 chance;
q. can win with certainty
All sufficiently good q.
strategies are essentially the same

Parallel Device-Independent QKD using MSG [Jain, Miller, Shi’17]

K1 , K2 , … , Kn



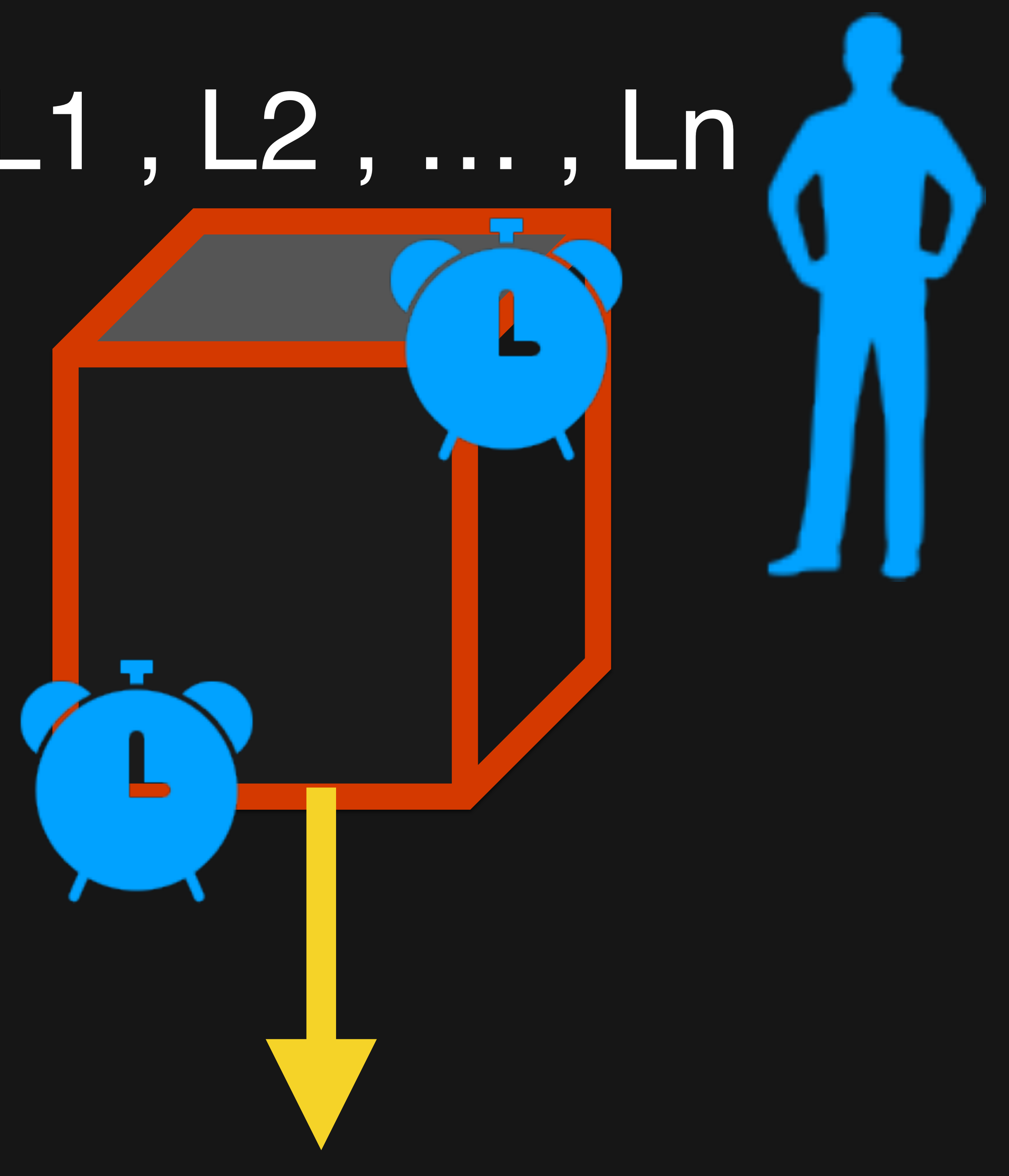
R1 , R2 , … , Rn

1. Alice and Bob generate random local input

2. Within enough time for communication, their boxes output corresponding rows and columns

3. Check correctness using a subset; use rest for generating key

L1 , L2 , … , Ln



C1 ,C2 , … , Cn

Conclusion: Quantum Cryptography can reach unconditional security where classical crypto can’t.

Conclusion: Relativity can also enable otherwise impossible tasks (e.g. to remove trust on q. devices).

Other major quantum and relativistic protocols

Delegated Q. Computation

[Broadbent et al.'09]

Bit Commitment

- Relativistic; classical security
- Quantum security open
  [Chakraborty,et. Al. '13;
  Fehr et a. '16]

Certifying Location

- Relativistic; classical security
- Quantum security open
  [Buhrman et al.'14]

Weak Coin Flipping

- Quantum security
- Construction not efficient
  [Mochon'05]

An open problem: defining identity (QKD assumes ID authentication)

THANKS

THANKS

THANKS

THANKS