David Elkouss
QuTech
TU Delft
d.elkousscoronas@tudelft.nl

Key distribution and the CHSH game

David Elkouss is assistant professor at QuTech at TU Delft, where he works, among others, on quantum key distribution. In this article, Elkouss reviews the relation between the violation of a Bell inequality and device independent quantum key distribution, by departing from the so-called CHSH inequality and linking it with a protocol for key distribution.

Quantum key distribution (QKD) [3,8] allows distributing information-theoretically secure keys to two distant parties. The only required assumptions are the validity of quantum theory and a characterization of the devices used for implementing the key distribution protocol. Hence, whenever the characterization is not precise enough, it can be exploited via side-channel attacks that do not break the distribution protocol but profit from the device imperfections. An alternative paradigm is device-independent quantum key distribution (diQKD) [8]. In diQKD the required assumptions are milder, i.e. it is enough to assume quantum theory to be correct. However, in contrast with QKD, the implementation of diQKD remains elusive. Recently, the first loophole-free Bell experiments have been implemented. These implementations promise to bring diQKD close to reality.

Here, we begin from basic principles and review the relation between the violation of a Bell inequality and the feasibility of diQKD. The structure of the article is as follows: We first describe the setting of the CHSH inequality as a non-local game [5], and how the winning probability achievable by Alice and Bob is limited if they play with a local strategy. Then we introduce the formalism of quantum information and show that with quantum resources Alice and Bob can achieve a larger winning probability. In a real experiment, one necessarily only encounters a finite number of samples, hence the winning probability can never be estimated with certainty. Thereafter, we argue how it is still possible to make a rigorous statement about the type of strategy played by Alice and Bob. Finally, we link winning probabilities beyond the local strategy limit with the distribution of secret keys.

The CHSH game and its classical value

In this section, we describe a non-local game and derive the maximum winning probability for classical or local players. This game was first introduced by John Clauser, Michael Horne, Abner Shimony, and Richard Holt in [7] and thereafter has been known as the CHSH game.

First, let us introduce the scenario. The CHSH game is an example of a bipartite non-local game. That is, a game played by two parties or players. We call them Alice and Bob. Both are located in two separated locations such that during each round of the game they cannot exchange information. This locality restriction might be enforced because they are spatially separated or because we assume that we have well characterized their laboratories and can conclude that they do not leak during the game execution. For a review on non-local games see [5].

Alice and Bob have a binary-input binary-output box. It receives respectively $x,y \in \{0,1\}$ and outputs $a,b \in \{0,1\}$, see Figure 1. We can imagine a box with two buttons and whenever the player pushes a button the box outputs a bit. The rules of the CHSH game are as follows. The inputs x, y are chosen uniformly at random and Alice and Bob are free to choose any strategy for their boxes to output the values a, b. They win the game whenever $x \cdot y = a \oplus b$, where $a \oplus b$ indicates $a + b \bmod 2$, and they lose otherwise.

Let us first focus on local or classical strategies. We call a strategy local or classical if there exists some shared source of randomness (possibly trivial) between the players such that

$$\Pr(a,b \mid x,y,\lambda) = \Pr(a \mid x,\lambda)\Pr(b \mid y,\lambda)$$

where $\Pr(a,b \mid x,y,\lambda)$ is the probability that the boxes output a, b given x, y and λ, the outcome of the shared randomness.

Before we analyze the maximum winning probability, we may wonder what is the role of randomness. A strategy is de-

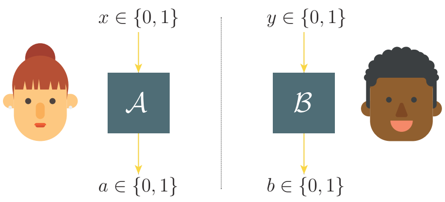

Figure 1 In the CHSH game, two space-like separated parties, that we call Alice and Bob receive two binary inputs $x,y \in \{0,1\}$ and produce two binary outputs $a,b \in \{0,1\}$. Alice and Bob win the game if $x \cdot y = a \oplus b$, where $a \oplus b = a + b \bmod 2$.

terministic if $\Pr(a,b\,|\,x,y)$ takes only values zero or one. Any non-deterministic local strategy can be implemented with shared randomness in such a way that $\Pr(a,b\,|\,x,y,\lambda)$ takes only values zero or one. Hence, the winning probability can be written in the form

$$p_{\text{win}} = \sum_{\lambda} \Pr(\lambda) \sum_{x,y} \frac{1}{4} \sum_{a,b:x\cdot y = a\oplus b} \Pr(a,b\,|\,x,y,\lambda)$$

where $\Pr(a,b\,|\,x,y,\lambda)$ is deterministic. Can non-deterministic strategies help Alice and Bob achieve better winning probabilities than deterministic strategies? It is easy to see that for any probabilistic strategy we can upper bound the winning probability by:

$$p_{\text{win}} \leq \max{}_{\lambda} \sum_{x,y} \frac{1}{4} \sum_{a,b:x\cdot y = a\oplus b} \Pr(a,b\,|\,x,y,\lambda)$$

where the right-hand side is the winning probability of a deterministic strategy.

Now we can investigate what is the maximum value achievable with a local strategy. From the argument above, we only need to consider deterministic strategies. Alice and Bob have only four different choices for choosing their outputs. Either they fix the output to zero or one, either they output the input or they flip it. Hence, combining Alice and Bob choices there are only sixteen different deterministic strategies. For instance, let us suppose that Alice chooses $a = x$ and Bob chooses $b = 0$. Then, they win whenever the input is $(x,y) = (0,0)$, $(x,y) = (0,1)$ and $(x,y) = (1,1)$ but they lose when $(x,y) = (1,0)$. Since all inputs are chosen with equal probability, they win with probability $p_{\text{win}} = 0.75$. Can they do any better? It is a matter of checking the remaining fifteen combinations of strategies, but it turns out that it is not possible. The best winning probability that can be achieved by a local strategy is three over four. We call this best probability the classical value of the game and we denote it by p^*_{win}.

The quantum value of CHSH

Let us do a detour to introduce some rudiments of quantum information. This is necessary in order to talk about the quantum value of the CHSH game. We first see how to represent quantum states and then we discuss a class of measurements known as projective measurements. We point the interested reader to [11] for an in-depth introduction to quantum information.

A qubit represents a two-level quantum mechanical system, for instance the polarization of a photon. We can describe the state of the two-level system by a vector in $\mathbb{C}^2$, that we can write as

$$\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} = \alpha_0 \begin{pmatrix}1\\0\end{pmatrix} + \alpha_1 \begin{pmatrix}0\\1\end{pmatrix}$$

with $\alpha_0, \alpha_1 \in \mathbb{C}$ and such that $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The reasons for restricting to unit vectors will become clear later.

The so-called ket notation introduced by Dirac allows for a more compact description of quantum systems. We can rewrite the state of a qubit $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ where

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

Of course, there is nothing particular about the canonical or computational basis. For any orthonormal basis given by v and $v^{\perp}$, we can find the complex coefficients $\beta_v, \beta_{v^{\perp}}$ such that $|\phi\rangle = \beta_v|v\rangle + \beta_{v^{\perp}}|v^{\perp}\rangle$.

A two-qubit system can be described by a unit vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$. We can write its state using ket notation in an analogous way to one qubit systems. Let

$$|0\rangle_A|0\rangle_B = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |0\rangle_A|1\rangle_B = \begin{pmatrix}0\\1\\0\\0\end{pmatrix},$$
$$|1\rangle_A|0\rangle_B = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |1\rangle_A|1\rangle_B = \begin{pmatrix}0\\0\\0\\1\end{pmatrix},$$

be the ket representation of each vector of the computational basis. Then an arbitrary state is of the form

$$|\phi\rangle_{AB} = \sum_{i,j\in\{0,1\}} \alpha_{ij}|i\rangle_A|j\rangle_B.$$

Now, let us assume that we have two one-qubit systems A and B with state $|\phi\rangle_A = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi\rangle_B = \beta_0|0\rangle + \beta_1|1\rangle$. We can describe the joint composite system, $|\omega\rangle_{AB}$, by taking the tensor product of $|\phi\rangle_A$ and $|\psi\rangle_B$:

$$\begin{aligned}|\omega\rangle_{AB} &= |\phi\rangle_A \otimes |\psi\rangle_B\\ &= \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \otimes \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\\ &= \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}\\ &= \sum_{i,j\in\{0,1\}} \alpha_i\beta_j|i\rangle_A|j\rangle_B.\end{aligned}$$

The natural question is if all two qubit states can be written in this form. The answer is no, but whenever this is the case and we can write the state of a two-qubit state as the tensor product of two one-qubit states we say that the state is a product state. Otherwise, we say that the state is *entangled*. A very important consequence of this definition is that it is not possible to describe the individual qubit systems of an entangled state with a ket. The individual qubit systems of an entangled state do not have a definite state. Alternatively, if a qubit system has a definite state (can be described by a ket) it can not be part of an entangled state. We call a system with a definite state a *pure* state.

The next step in our brief introduction to quantum information is measurement. We only consider a subclass of measurements called rank-one projective measurements. These measurements are specified by a measurement basis and can be understood as reading in which element of the basis the state is. The outcome of such a measurement is probabilistic. Let an arbitrary d-level quantum system be given by

$$|\phi\rangle = \sum_{i=0}^{d-1} \alpha_i |u\rangle_i$$

and let us suppose that we measure this state in the basis given by $\{|u\rangle_i\}_{i=0}^{d-1}$. Then, the probability that we obtain measurement outcome i is $|\alpha_i|^2$. The restriction to unit vectors guarantees that the sum over all possible outcomes $\sum_i |\alpha_i|^2 = 1$ as expected.

Now let us show how entanglement can help Alice and Bob obtain a winning probability in the CHSH game larger than the classical value. For this, let us assume that Alice and Bob share the following quantum state, known as the maximally entangled state, before the beginning of the game:

$$|\phi\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}} \tag{1}$$

Let us define the following measurement bases:

$$\begin{aligned}&A_0 = \{|0\rangle, |1\rangle\},\\ &A_1 = \left\{\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}, \tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}\\ &B_0 = \{\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle,\\ &\qquad -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle\} \text{ and}\\ &B_1 = \{\cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle,\\ &\qquad \sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle\}.\end{aligned}$$

The strategy of Alice and Bob is, given the inputs x and y, measure in the bases A_x and B_y. Let us compute the winning probability with this strategy.

$$\begin{aligned}&\Pr(\text{win} \mid x=0, y=0)\\ &\quad= \Pr(a=0, b=0 \mid x=0, y=0)\\ &\qquad+ \Pr(a=1, b=1 \mid x=0, y=0)\\ &\quad= \cos^2\frac{\pi}{8}.\end{aligned}$$

We can also easily verify that

$$\begin{aligned}&\Pr(\text{win} \mid x=0, y=1)\\ &\quad= \Pr(\text{win} \mid x=0, y=1)\\ &\quad= \Pr(\text{win} \mid x=1, y=0)\\ &\quad= \Pr(\text{win} \mid x=1, y=1)\\ &\quad= \cos^2\frac{\pi}{8} \approx 0.85.\end{aligned}$$

We do not prove it here, but it turns out that the strategy that we just analyzed is optimal. That is, it is not possible, within the formalism of quantum mechanics, to achieve a larger winning probability [6]. Hence, in particular, there exists no quantum strategy that allows Alice and Bob to win the game with probability one. Moreover, the maximally entangled state is unique in achieving it, this will be crucial for the purpose of key distillation. More precisely, if Alice and Bob achieve the optimal winning probability then they can conclude that up to a local unitary transformation they share a maximally entangled state. This result can be made robust. That is, if the winning probability of CHSH is close to the optimal value, then Alice and Bob can conclude that their state is close to the optimal state [10]. This closeness is quantified according to some distance measure between quantum states that goes beyond the scope of this introduction [11].

Non-locality with finite data

In the previous sections, we have derived the optimal winning probabilities under the assumption of local or quantum strategies. In particular, we have seen that there are quantum strategies that yield strictly larger winning probabilities than local strategies. This is a fundamental theoretical statement, but by itself, it is not very useful. In a real experiment, one observes a finite sequence of inputs and outputs. With this finite number of runs, it is possible to compute the frequency of wins, but the true probability is beyond reach. Is it then possible to decide that an experimental implementation is governed by a non-local strategy?

The solution is to perform a hypothesis test where the null hypothesis is that the experiment is run by a local strategy. Then the CHSH game is played some predefined number of times n and the number of wins c is recorded. With this value, it is possible to compute the probability of obtaining the same or a larger number of wins under the assumption that the null hypothesis is true. If this probability is below some number decided in advance, the null hypothesis is discarded. Let us now make explicit the computation of this probability. Let C_i be a random variable that takes value one if Alice and Bob win the i-th game and zero otherwise. Then conditioned to the occurrence of any sequence of outcomes in the first $i-1$ rounds of CHSH the winning probability remains bounded by the classical value [4]:

$$\Pr(C_i = 1 \mid C_1 \ldots C_{i-1}) \leq p^*_{\text{win}}.$$

The intuition behind this statement is that the previous sequence of outcomes can be regarded as an instance of shared randomness. Building on top of this it is possible to show that for all local strategies

$$\Pr(C \geq c) \leq \sum_{k=c}^{n} \binom{n}{k} (p^*_{\text{win}})^k (1-p^*_{\text{win}})^{n-k}, \quad (2)$$

where the right-hand side of Eq. (2) is the tail of a binomial distribution with parameters n and p^*_{win}. This tail, which is the probability that the binomial takes a value equal or larger than c can be computed numerically. In practice, if the winning probability is above the classical value, the right-hand side decreases very fast. For a fixed frequency of wins above p^*_{win}, the tail decreases exponentially fast to zero, see Figure 2. A similar result holds even if the inputs of the CHSH game are not chosen uniformly at random but they have a small bias [4,9].

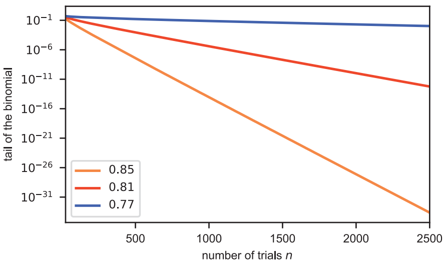

Figure 2 Evaluation of the right-hand side of Eq. (2) for different values of frequencies of wins above the classical value.

Key distillation

In this section, we relate the winning probability with the possibility of distilling secret keys. For the purpose of this discussion we say that a protocol produces a perfect key of n bits if it is distributed uniformly at random over the set of strings of length n, Alice and Bob share the same string with probability one and the probability that any third party guesses the value of the string is no better than a random guess, i.e. the guessing probability is at most 2^{-n}. This definition can be made robust by allowing close to uniform distributions in terms of the variational distance and close to random guesses.

Let us assume that Alice and Bob share a maximally entangled state (see Eq. (1)). Then, we know that since it is a pure state, it needs to be in tensor product form with any additional system that belongs to Eve. Moreover, if two states are in product form, then it is not possible to infer information about one by measuring the other. You can convince yourself by writing a product state and computing the joint probability distribution after measuring each state in some basis. Moreover, if Alice and Bob now measure the state in the computational basis they obtain a uniformly random bit and in consequence they share a perfect secret key.

The problem in practice is that it is not possible a priori to know what is the state shared by Alice and Bob without relying on additional assumptions. However, as we saw in the previous section, if Alice and Bob observe a frequency of wins close to the quantum value of CHSH, they can conclude that they share states close to the maximally entangled state. Hence, if Alice and Bob have access to some source that provides them with maximally entangled states they could try to distil a key as follows. In each round, both Alice and Bob decide randomly whether they play the CHSH game or they try to distil key by measuring in the computational basis. After n rounds, they share their random choices and compute the number of wins in the CHSH game. If the number of wins is large enough they can conclude that they shared maximally entangled states with high probability and that the values measured in the distillation rounds constitute a secret key. Of course, making this intuition rigorous is rather challenging, see [1] for a recent proof.

Even if the protocol that we describe below is dubbed device-independent there are some assumptions that need to be made. Let us go over them. First, there is some classical information that Alice and Bob need to exchange during the protocol. This information, although not secret, should arrive undistorted at the other party. For this, Alice and Bob can use an authenticated classical communications channel. Alternatively, they can themselves implement an authenticated channel if they share in advance a small secret key. Second, both Alice and Bob's laboratories are assumed to be secure, i.e. no information leaks during or after the protocol. Note, however, that no assumption is made on the measurement or preparation devices that can be completely uncharacterized. In this sense, the protocol is device-independent.

The following protocol is a version of the Ekert protocol [8] proposed in [12]:

1. Alice generates a uniformly random string of measurement bases $X=(x_0,\ldots,x_{n-1})\in\{0,1\}^n$ and measures sequentially in the basis given by A_x. The device outputs a string of measurement outcomes $A=(a_0,\ldots,a_{n-1})\in\{0,1\}^n$.
2. Bob generates a uniformly random string of measurement bases $Y\in\{0,1,2\}^n$ and measures sequentially in the basis given by B_y, where $B_2=A_0$. The device outputs a string of measurement outcomes $B=(b_0,\ldots,b_{n-1})\in\{0,1\}^n$.
3. Alice and Bob communicate to each other the measurement strings X and Y over the classic communications channel.
4. Alice chooses a random subset of $S\subset\{0,1,\ldots,n-1\}$ of size $|S|=n/2$ and sends S to Bob. Alice and Bob compute the following sets: $T=\{i\in S, y_i\neq 2\}$, $U=\{i\in S, x_i=0, y_i=2\}$ and $V=\{i\notin S, x_i=0, y_i=2\}$.
5. Alice and Bob compute the number of CHSH wins and mismatches on the sets T and U:
$$f_{\text{win}}=\frac{|\{i\in T, x_iy_i=a_i\oplus b_i\}|}{|T|},$$
$$f_{\text{error}}=\frac{|\{i\in U, x_i\neq y_i\}|}{|U|}.$$
If f_{win} and $1-f_{\text{error}}$ are not above some predetermined threshold the protocol aborts.
6. Alice and Bob perform a sequence of classical postprocessing steps to distil a secret key [13].

Using this protocol, for n large enough Alice and Bob can distil secret keys at a rate that scales linearly with n and is a function only of the frequencies of wins and mismatches f_{win} and f_{error} [1].

Summary and further reading

We introduced several topics. Let us summarize and point to appropriate sources for further reading. First, we presented the CHSH game and showed that the maximum winning probability with local strategies is 0.75. In order to discuss the winning probability with quantum resources, we briefly introduced some rudiments of quantum information and showed that the maximally entangled state achieves a strictly larger winning probability than the local value. We point the reader to the review paper [5] for more information on non-local games and to [11] for a thorough introduction to quantum information.

Then, we argued that in a real experiment it is not possible to observe probabilities, but it is still possible to conclude that Alice and Bob are implementing a non-local strategy. Moreover, for a large enough number of games, if the frequency of wins is close to the optimal value it is possible to conclude that Alice and Bob share a state close to the maximally entangled state. We concluded by introducing the concept of secret key and arguing that the maximally entangled state can be used to produce a secret key. Finally, we presented a protocol for key distribution that randomly intercalates rounds of CHSH and key production. We point the reader to [13] for an in-depth discussion of (non-device-independent) QKD and to [1] for a security proof of diQKD.

References

1 R. Arnon-Friedman, R. Renner and T. Vidick, Simple and tight device-independent security proofs, arXiv:1607.01797, 2016.

2 J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy,* Cambridge University Press, 2004.

3 C.H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *International Conference on Computers, Systems & Signal Processing,* Bangalore, India, 1984.

4 P. Bierhorst, A robust mathematical model for a loophole-free Clauser–Horne experiment, *Journal of Physics A: Mathematical and Theoretical* 48(19) (2015).

5 N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Bell nonlocality, *Reviews of Modern Physics* 86(2) (2014).

6 B.S. Cirel'son, Quantum generalizations of Bell's inequality, *Letters in Mathematical Physics* 4(2) (1980).

7 J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt, Proposed experiment to test local hidden-variable theories, *Physical Review Letters* 23(15) (1969).

8 A.K. Ekert, Quantum cryptography based on Bell's theorem, *Physical Review Letters* 67(6) (1991).

9 D. Elkouss and S. Wehner, (Nearly) optimal P values for all Bell inequalities, *NPJ Quantum Information* 2 (2016), 16026.

10 M. McKague, T.H. Yang and V. Scarani, Robust self-testing of the singlet, *Journal of Physics A: Mathematical and Theoretical,* 45(45) (2012).

11 M.A. Nielsen and I.L. Chuang, *Quantum Information and Quantum Computation,* Cambridge University Press, 2000.

12 S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar and V. Scarani, Device-independent quantum key distribution secure against collective attacks, *New Journal of Physics* 11(4) (2009), 045021.

13 M. Tomamichel and A. Leverrier, A rigorous and complete proof of finite key security of quantum key distribution, arXiv:1506.08458, 2015.

14 U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, *Physical Review Letters* 113(14) (2014).