dr Jędrzej Kaniewski
Faculty of Physics, University of Warsaw
Pasteura 5, 02-093 Warsaw

Summary of Professional Accomplishments

1. Name

Jędrzej Kaniewski

2. Diplomas, degrees conferred in specific areas of science or arts, including the name of the institution which conferred the degree, year of degree conferment, title of the PhD dissertation

Bachelor of Arts in Natural Sciences (University of Cambridge, 2011)
Master of Advanced Study in Mathematics (University of Cambridge, 2011)
PhD in Physics (National University of Singapore, 2015)
Thesis title: Relativistic quantum cryptography

3. Information on employment in research institutes or faculties/departments or school of arts

In 2011 I finished a 4-year undergraduate course at the University of Cambridge. In December 2011 I started a PhD at the National University of Singapore under the supervision of prof. Stephanie Wehner. I defended my PhD in December 2015. Although during all this time I was formally a PhD student in Singapore, in October 2014 my research group relocated to the Technical University in Delft in the Netherlands and I spent the last year of my PhD there.

In January 2016 I joined the group of prof. Matthias Christandl at the University of Copenhagen as a postdoc. Between March 2017 and June 2018 my employment was fully funded by the Individual Fellowship of Marie Skłodowska-Curie Actions awarded by the European Commission.

Between July 2018 and June 2019 I was employed as an assistant professor in the Centre for Theoretical Physics of the Polish Academy of Sciences. My employment was fully funded from a POLONEZ grant awarded by the National Science Centre, Poland.

Since July 2019 I am employed as an assistant professor at the Faculty of Physics of the University of Warsaw, where my employment is fully funded from a HOMING grant from the Foundation for Polish Science. In 2020 I was awarded a SONATA grant from the National Science Centre, Poland, which will extend my employment until the end of 2023.

4. Description of the achievements, set out in art. 219 para 1 point 2 of the Act

The habilitation cycle consists of 9 scientific papers published in international physics journals, which focus on certification of quantum devices and, more specifically, on a problem known as self-testing.

Certification of quantum devices revolves around the following question: how to demonstrate that an a priori unknown quantum device operates according to a given theoretical specification in an efficient manner? This problem can be formulated in multiple ways depending on the kind of device that we wish to certify (e.g. a source of quantum states, a measurement device or a quantum logical gate) and the scenario in which the certification process should be implemented (what kind of tools do we have access to? what assumptions are we happy to make?).

The standard scenario is the so-called tomographic scenario, in which an unknown quantum device is tested using other (trusted) devices, e.g. we test a source of quantum states using a trusted measurement device. In this case the certification problem becomes essentially a calibration problem and we encounter the usual obstacle: how to calibrate the first device?

It turns out that some forms of certification are possible even if we do not have access to any trusted devices. In our case we focus on the so-called Bell scenario (see Figure 1), in which two quantum devices share an entangled quantum state. Each device can locally perform one out of a few possible quantum measurements. It is worth stressing that our interaction with each device is fully classical: both choosing which measurement to perform and reading the measurement outcome happen through the exchange of classical information.

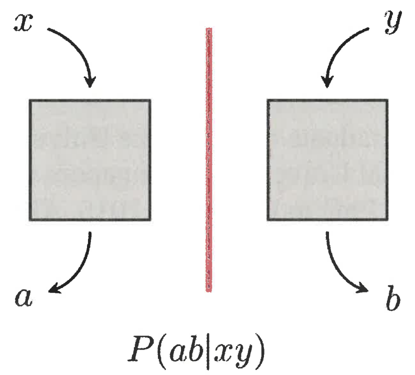

Figure 1: A bipartite Bell scenario. Two non-communicating quantum devices perform measurements denoted by x, y and produce outcomes denoted by a, b. Conclusions drawn in this scenario are based only on the observed statistics denoted by P(ab|xy) and the assumption the two devices do not communicate during the experiment.

An extraordinary feature of the Bell scenario is the ability to conduct an experiment, which allows us to distinguish quantum devices from classical devices under just one assumption, namely that the devices do not communicate during the experiment. If we observe correlations that cannot be explained by any classical theory, we say that we have violated some Bell inequality and this phenomenon is of fundamental importance for the foundations of quantum mechanics. These theoretical findings have been verified in numerous experiments using different physical implementations.

The original goal of the Bell test was to find a simple physical situation in which quantum mechanics can be distinguished from classical theories under minimal assumptions. Certification of quantum devices in Bell scenarios should be seen as a subsequent step in this direction: if we are capable of concluding that there is something non-classical happening in our experiment, then if we additionally assume that our devices are quantum, we should be able to draw further conclusions regarding these devices. A typical task in a Bell test is to certify entanglement between devices (entanglement is necessary to produce Bell inequality violations).

Self-testing is the most complete form of certification in the Bell scenario. In the noiseless case it allows us to uniquely identify the quantum state and the measurements performed (up to two natural classes of transformations, which can never be ruled out). This stems from the fact that in the Bell scenario some particularly strong quantum correlations can be implemented in a unique manner, which is a highly non-trivial statement.

In the habiliation cycle I have worked on the following research questions:

1. What quantum structures (states, measurements) can be self-tested?
2. How does the concept of self-testing behave in realistic scenarios, i.e. in the presence of noise?
3. Can we extend the concept of self-testing to other quantum scenarios and what assumptions are necessary to do so?
4. Do there exist cases in which self-testing is not possible and novel, weaker forms of certification must be introduced to formulate correct conclusions?

Below I present a detailed description of all the achievements described in the habilitation cycle (chronological order).

In paper [1] I focus on the problem of self-testing using the Clauser-Horne-Shimony-Holt (CHSH) and Mermin inequalities. It is known that the maximal violation of the CHSH inequality requires the presence of a maximally-entangled state of two qubits. The goal of this work was to analyse to what extent the self-testing of the quantum state is robust to noise. In this work I have introduced a new method of self-testing based on operator inequalities and I demonstrated its usefulness for the inequalities mentioned above. In the case of the CHSH inequality, where the maximal quantum value equals $2\sqrt{2}\approx 2.83$, while the classical value equals 2, I have shown that a non-trivial state certification is possible if the observed violation exceeds the threshold of ≈2.11 (previously it was known that this threshold equals at least ≈2.39). The Mermin inequality is a tripartite inequality and its maximal violation requires a three-qubit Greenberger-Horne-Zeilinger (GHZ) state. The quantum value of the Mermin inequality equals 4 and in this work I have shown that it is possible to certify closeness to the GHZ state if the observed violation exceeds $2\sqrt{2}$. This threshold value can be easily explained by noting that it can be attained using only bipartite entanglement (bipartite entanglement cannot yield a non-trivial closeness statement to a GHZ state, which contains tripartite entanglement). This shows that the bound derived for the Mermin inequality is tight.
Applicant's contribution: Paper [1] is a single-author paper.

In paper [2] I consider the question of self-testing of quantum measurements. It is worth mentioning that previous works focused on self-testing of states and self-testing of measurements was treated as an auxiliary result of lesser importance. Therefore, it was not even clear what definition to adopt for the purpose of self-testing the measurements. I have considered the problem of self-testing of a pair of two-outcome (binary) measurements and I noticed that the self-testing definition can be based entirely on the commutation relations between them. It is known that the more two observable non-commute, the more incompatible they are. In this work I have shown that for a pair of binary observables satisfying a specific commutation relation allows us to deduce that they are equivalent to a specific pair of qubit

measurements. From these commutation relations I have constructed a family of measures, which I then used for the purpose of certifying unknown observables. The main conclusion of this work is that every pair of binary observables on a qubit can be certified and, moreover, the self-testing procedure is robust to noise: even a small violation of some Bell inequality leads to a quantitative conclusion about the incompatibility of the unknown measurements. Moreover, this approach allowed me to analyse a family of multipartite Bell inequalities known as the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequalities. This family is indexed by integers $n \geq 2$. For $n=2$ we recover the CHSH inequality, while for $n=3$ we recover the Mermin inequality. In this work I have shown that for any *n* this inequality exhibits the self-testing property. In other words, to achieve the maximal violation one requires an *n*-qubit GHZ state, while the local measurements must correspond to maximally anticommuting observables (e.g. the Pauli matrices **X** i **Z**).
Applicant's contribution: Paper [2] is a single-author paper.

In paper [3] together with collaborators from the University of Geneva, Institute for Nuclear Research in Debrecen (Hungary) and Perimeter Institute in Waterloo (Canada) we have shown that the concept of self-testing can be extended to scenarios different than Bell scenarios. We have shown that this phenomenon occurs in a non-trivial form in "prepare-and-measure" scenarios (see Figure 2) if as an additional assumption we impose a bound on the dimension of the quantum system transmitted between the devices. In this work we have focused on the simplest case, i.e. the quantum random access code in which 2 classical bits are encoded in a single qubit. We have shown that the optimal quantum strategy in this task is unique (up to the choice of basis, i.e. a unitary operation) and consists of encoding the four possible combinations in four pure states which geometrically form a square in the Bloch sphere and then performing measurements in two mutually unbiased bases on a qubit. The standard optimal strategy employs measurements corresponding to the eigenbases of the Pauli **X** and **Z** operators and then the prepared states must correspond to the eigenvectors of the (**X** ± **Z**) operators. In this work we have also shown that strategies that approach the optimal performance must be in a well-defined sense close to the optimal strategy. To do so we have constructed two independent argument showing that: (1) the prepared quantum states must be approximately pure and form a square on the Bloch sphere; (2) the measurements must be approximately rank-1 and projective and mutually unbiased. The first of these arguments used a method I proposed in paper [1] for self-testing in Bell scenarios.
Applicant's contribution: The idea to extend the concept of self-testing to "prepare-and-measure" scenarios came from the collaborators from Geneva, while I was invited to join the project due to my expertise in the field of self-testing. Together with the first author we have derived the analytical relations and I was also responsible for adapting the method from paper [1] to a new scenario.

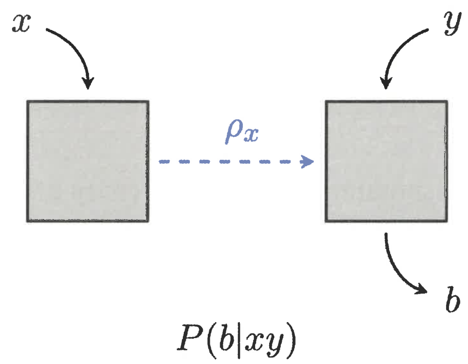

Figure 2: A "prepare-and-measure" scenario. A source of quantum state receives classical information x and produces a quantum state of fixed dimension. A measurement device performs a measurement denoted by y and returns an outcome b. Conclusions in this scenario are based solely on the observed statistics P(b|xy) and the assumption that the dimension of the transmitted quantum state is bounded.

In paper [4] together with researchers from the University of Geneva we have extended the concept of self-testing to the Bell scenario of three devices, where the quantum states are generated by two independent sources (see Figure 3). The goal of this scenario was to show under minimal assumptions that device B, which receives quantum states from two independent sources implements an entanglement swapping procedure. We have shown that if devices A and C exhibit the maximal violation of a certain variant of the CHSH inequality (the exact form depends on the classical outcome produced by device B), then indeed we are capable of fully characterising the unknown quantum systems based only on the assumption of independent sources. We have also considered the case where the violation is not maximal. To do so we had to define what it means for a quantum measurement acting on a tensor product of two Hilbert spaces to be equivalent (or at least similar) to a Bell basis measurement on two qubits. The definition we adopted is based on completely positive unital maps. For such a definition we have shown that if devices A and C exhibit a large (but not necessarily maximal) violation of the CHSH inequality, then the measurement performed by device B must be similar to a Bell basis measurement. The mathematical derivation uses the main result of paper [1] as one of the ingredients.
Applicant's contribution: Together with the first author we have derived an analytical characterisation of all the devices in the noiseless case. I have shown how to adapt the method from paper [1] to the scenario with two independent sources, which required finding an analytical solution to a family of semidefinite programs.

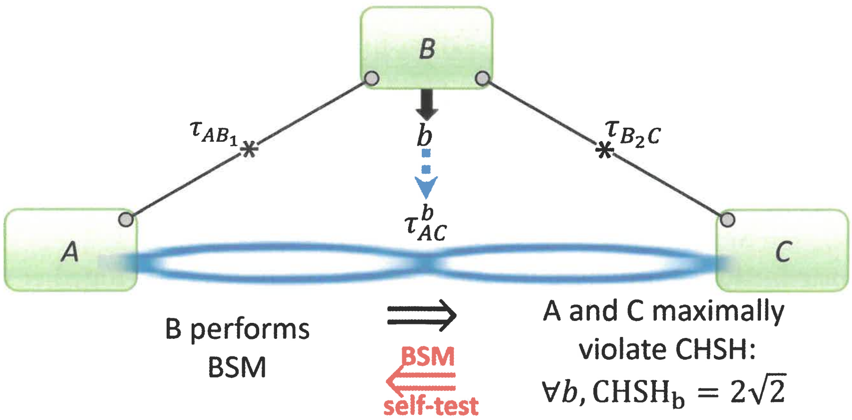

Figure 3: A Bell scenario with two independent sources in which one can certify entangled quantum measurements.

In paper [5] together with a collaborator from the University of Gdańsk (Mate Farkas, whose PhD thesis I co-supervised) we have shown that self-testing in "prepare-and-measure" scenarios can be proven for high-dimensional quantum random access codes. We have considered the standard case in which 2 classical dits (dit = a unit of classical information taking *d* possible values) are encoded in 1 qudit (qudit = a *d*-dimensional quantum system). Previously it was known that if in such a task the measurement device is restricted to measurements in a basis (i.e. measurements which are projective and rank-1), then the optimal measurements correspond to mutually unbiased bases. The first result of our work is that the performance cannot be improved by using the most general quantum measurements. Moreover, we have shown that the optimal performance is possible only if the measurements performed correspond to measurements in a pair of mutually unbiased bases. We have also managed to show that strategies whose performance is close to optimal must be close to the optimal strategy. More specifically, we have shown that the following statements must hold approximately: (1) the measurement operators must be rank-1, (2) the traces of the products of the measurement operators must be uniformly distributed, (3) the measurements must be as incompatible as mutually unbiased bases and (4) measurements must lead to the strongest possible uncertainty relations. For the cases of $d=3$ i $d=4$ certification is possible at a realistic level of noise and our theoretical findings were later confirmed in an experiment ("Self-Testing Mutually Unbiased Bases in Higher Dimensions with Space-Division Multiplexing Optical Fiber Technology", Farkas et al., Physical Review Applied **15**, 014028 (2021)). The mathematical argument is based only on elementary properties of matrices, which implies that the argument can be applied to any value of *d* and for every value of *d* we obtain a non-trivial robustness to noise (although the robustness decreases as the dimension increases). It is worth stressing that although our analysis provides detailed results on the measurement operators, it does not correspond to a certification up to a unitary (in higher dimensions not all pairs of mutually unbiased bases are unitarily equivalent). This observation was crucial and led us to the results published in paper [9].
Applicant's contribution: Together with the first author we have derived analytical self-testing relations.

In paper [6] together with collaborators from the University of Amsterdam we have generalised the self-testing method proposed in paper [1]. In the original work this method was used to derive a strong certification statement for the two-qubit maximally-entangled state based on the violation of the CHSH inequality. In this work we have used the same method to certify partially-entangled two-qubit states using the tilted-CHSH inequality. We have shown that also in this case we obtain results strongly resistant against noise. Moreover, we have shown that self-testing based on the CHSH inequality is possible only if the observed violation equals at least ≈ 2.0014. Results published in this work started in the master's thesis of Tim Coopmans, which prof. Christian Schaffner and myself have jointly supervised.
Applicant's contribution: I proposed the main idea of the project and together with the first author we have derived the analytical relations. I have also supervised the numerical calculations. Together we have constructed the argument showing that self-testing is only possible above a certain threshold.

In paper [7] together with collaborators we have introduced a new family of Bell inequalities tailored to measurements in mutually unbiased bases. We have shown that if *d* is a prime larger than 2, we can construct a Bell inequality whose maximal quantum value is achieved by the maximally-entangled state of local dimension *d* and measurements constituting a specific arrangement of mutually unbiased bases (we need *d* such bases, whose existence is guaranteed since *d* is a prime). Moreover, in the simplest case of $d=3$ we have given a proof for self-testing. This is one of the first arguments, where self-testing of high-dimensional systems is proven directly without relying on some self-testing results for two-qubit states. In this case by considering the sum-of-squares decomposition of the Bell operator, we have managed to fully characterise the optimal pairs of measurements through algebraic relations, for which we could find explicit solutions (this argument is a generalisation of the argument used in paper [2] to analyse pairs of binary observables).
Applicant's contribution: Together with prof. Augusiak and dr Tura we have derived the new construction of Bell inequalities. I have derived the self-testing result for $d=3$ on my own.

Paper [8] is based on an observation made while working on the geometry of the quantum set of correlations. We have noticed that there exist relatively simple Bell inequalities (3 measurement settings and 2 outcomes on each device), whose maximal violation can be achieved in many inequivalent ways. All these realisations are based on a maximally-entangled state of two qubits, but the measurements performed differ. In this work I have managed to fully characterise the quantum realisations which achieve the maximal violation. I have achieved this by decomposing the Bell operators as a sum of squares and deriving algebraic relations that need to by satisfied by optimal measurement operators. Then, I managed to solve these algebraic relations using a method similar to the one presented in paper [2], but since in this scenario we are characterising 3 observables (instead of 2), these algebraic relations do not lead to a single solution, but to a 1-parameter family of solutions (all of them still act on a single qubit). Having fully characterised the observables, I could construct the Bell operator and show for which combinations of measurements the maximal violation is possible. It turned out that in all the cases one needs a maximally-entangled state of two qubits, which proves the existence of a new, weak form of self-testing, which allows us to certify the state, even though we cannot fully characterise the measurements. I have also analysed the situation in which we observe a non-maximal violation of the Bell inequality. It turns out that an approximate certification of the state is possible and the numerical results suggest that this scenario is similar to the standard scenarios in which strong self-testing is possible, e.g. the CHSH scenario. Similarly, the analysis of randomness which we can certify did not exhibit a significant difference from the standard cases. This suggests that this new weak form of self-testing might still be sufficient for many concrete applications.
Applicant's contribution: Paper [8] is a single-author paper.

In paper [9] together with collaborators we have proposed a new construction of Bell inequalities. This construction allows us to obtain Bell inequalities, which are maximally violated by specific symmetric arrangements of measurements. For every dimension $d \geq 2$ we are capable of constructing a Bell inequality which is maximally violated by: (1) an arbitrary pair of mutually unbiased bases (see Figure 4) and (2) a set of symmetric informationally-complete projectors. In both cases the required state is a maximally-entangled state of local dimension *d*. Both families of inequalities can be used in device-independent cryptography. We have shown that the family based on mutually unbiased bases allows one to implement a quantum key distribution protocol, while the family based on symmetric projectors can be used for efficient randomness generation. In both cases we have performed numerical calculations,

which confirmed that for $d=3$ both protocols are useful at a realistic level of noise. We have also showed that both families can be used to certify the measurements, while the mutually unbiased bases inequalities can also be used to certify the state. Therefore, we have shown that there exist extremal points (in the convex geometry sense) of the quantum set, which do not fulfil the self-testing condition, which constitutes the most important result of this work from the foundational point of view. The argument leading to certification shows that the inequalities for mutually unbiased bases are maximally violated by a unique probability point, which means that this is an exposed point and, therefore, extremal. However, since in higher dimensions (e.g. $d=4$) there exist pairs of mutually unbiased bases which are not unitarily equivalent, which was mentioned in the context of paper [5], this point can be implemented by many inequivalent quantum realisations. Our result demonstrates that it is natural to define an entire hierarchy of certification conditions in which the standard definition corresponds to the most restrictive variant. Moreover, we have shown that a natural family of measurements, which we dubbed the mutually unbiased measurements, is non-trivial and contains measurements which are not simply a direct sum of mutully unbiased bases.
Applicant's contribution: The idea to construct a Bell inequality for symmetric informationally-complete projectors is due to dr Tavakoli. I have shown that this construction can be applied to mutually unbiased bases. Together with dr Farkas we have derived the analytical certification relations and investigated the structure of mutually unbiased measurements.

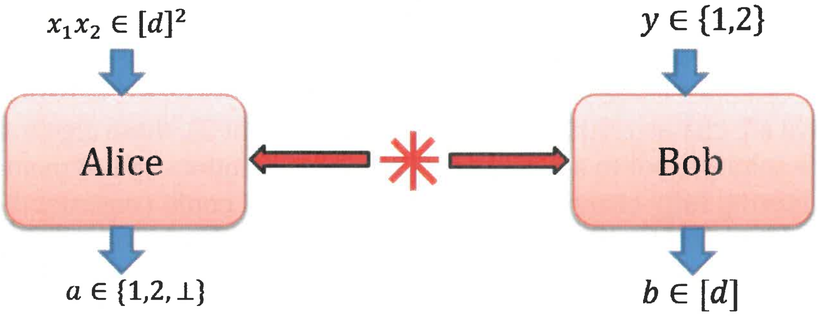

Figure 4: Bell scenario in which we have constructed a Bell inequality violated maximally by an arbitrary pair of mutually unbiased bases in dimension d.

5. Presentation of significant scientific or artistic activity carried out at more than one university, scientific or cultural institution, especially at foreign institutions

During my academic career I have conducted research at the following institutions:

- Center for Quantum Technologies, National University of Singapore (December 2011 to September 2014)
- Technical University in Delft, the Netherlands (October 2014 to December 2015)
- Center for the Mathematics of Quantum Theory QMATH, University of Copenhagen, Denmark (January 2016 to June 2018)
- Center for Theoretical Physics, Polish Academy of Sciences (July 2018 to June 2019)
- Faculty of Physics, University of Warsaw (since July 2019)

At each of these institutions I was an active member of the academic community and participated regularly in seminars or conferences and workshops organised locally (also as a presenter). Particularly important events are mentioned in the following section.

6. Presentation of teaching and organizational achievements as well as achievements in popularization of science or art

Teaching activities:

- In 2015 I acted as a teaching assistant for a "Quantum computing and communication" class at the Technical University in Delft taught by prof. Stephanie Wehner.
- In October lat 2016 and 2017 I gave a week-long LaTeX class at the University of Copenhagen for the first year students of mathematics.
- In academic year 2016/2017 I supervised two master's theses: Zabulon Bucumi (African Institute for Mathematical Sciences, Senegal, remote supervision) and Tim Coopmans (University of Amsterdam; supervised jointly with prof. Christian Schaffner). Both theses were successfully defended in 2017.
- In July 2018 I gave a graduate-level mini-course "Randomness and device independence" at the Quantum Information Science Summer School in Seul organised by the Korea Institute of Advanced Study.
- In the summer semester of the academic year 2019/2020 together with dr Alex Streltsov I taught a 30-hour class "Advanced quantum information: entanglement and nonlocality" for master's-level students at the Faculty of Physics of the University of Warsaw.
- In academic year 2019/2020 I supervised two bachelor's theses, which were defended in September 2020 and, moreover, I was a co-supervisor of the PhD these of Mate Farkas (University of Gdańsk). Currently, I act as a supervisor for two bachelor's theses, one master's thesis and, moreover, I am a co-supervisor of a PhD student (Gabriel Pereira Alves).

Organisational activities:

- In 2012 I was a member of the organising committee of QCrypt 2012, I was the only person responsible for organising the poster session.
- In 2018 I was on the program committee for CEQIP.

Outreach activities:

- In 2012 I performed experimental demonstrations for the attendees of the Alumni Open Day at the National University of Singapore.
- In 2012 I acted as a judge at the International Mathematical Challenge organised by NUS High School of Mathematics and Science (Singapore).
- In 2015 I was invited to deliver a talk at the annual event of the Christiaan Huygens student association at the Technical University in Delft.
- In October 2016 I was the organiser of the "Quantum corner" within the Culture Night at the University of Copenhagen.

7. Apart from information set out in 1-6 above, the applicant may include other information about his/her professional career, which he/she deems important.

Not applicable.

The habilitation cycle consists of the following works (chronological order):

[1] J. Kaniewski, Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities, Physical Review Letters **117**, 070402 (2016)

[2] J. Kaniewski, Self-testing of binary observables based on commutation, Physical Review A **95**, 062323 (2017)

[3] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, Physical Review A **98**, 062307 (2018)

[4] M. O. Renou, J. Kaniewski, N. Brunner, Self-testing entangled measurements in quantum networks, Physical Review Letters **121**, 250507 (2018)

[5] M. Farkas, J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Physical Review A **99**, 032316 (2019)

[6] T. Coopmans, J. Kaniewski, C. Schaffner, Robust self-testing of two-qubit states, Physical Review A **99**, 052123 (2019)

[7] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, R. Augusiak, Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems, Quantum **3**, 198 (2019)

[8] J. Kaniewski, A weak form of self-testing, Physical Review Research **2**, 033420 (2020)

[9] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments, Science Advances **7**, eabc3847 (2021)

Jędrzej Kaniewski
....
(signature)