Marcin Pawłowski

Autoreferat

Gdańsk 2017

I. IMIĘ I NAZWISKO

Marcin Pawłowski

II. POSIADANE DYPLOMY, STOPNIE NAUKOWE/ARTYSTYCZNE – Z PODANIEM NAZWY, MIEJSCA I ROKU ICH UZYSKANIA ORAZ TYTUŁU ROZPRAWY DOKTORSKIEJ

Stopień doktora nauk fizycznych nadany przez Radę Wydziału Matematyki, Fizyki i Informatyki Uniwersytetu Gdańskiego w dniu 18.11.2010.

Tytuł rozprawy doktorskiej: "Fizyczna teoria informacji".

III. INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH/ARTYSTYCZNYCH

- 05.05.2010 - 31.12.2010: asystent techniczny, Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański
- 01.11.2010 - 30.04.2014: asystent, School of Mathematics, University of Bristol
- 16.07.2012 - 30.04.2013: asystent techniczny, Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański
- 01.05.2013 - 30.06.2015: scpecjalista naukowo-badawczy, Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański
- since 01.07.2015: adjunkt, Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański

IV. WSKAZANIE OSIĄGNIĘCIA WYNIKAJĄCEGO Z ART. 16 UST. 2 USTAWY Z DNIA 14 MARCA 2003 R. O STOPNIACH NAUKOWYCH I TYTULE NAUKOWYM ORAZ O STOPNIACH I TYTULE W ZAKRESIE SZTUKI (DZ. U. NR 65, POZ. 595 ZE ZM.)

A. Tytuł osiągnięcia naukowego/artystycznego

Jednotematyczny cykl publikacji pt. *Kody swobodnego dostępu w informatyce kwantowej.*

B. Lista publikacji

1. M. Pawłowski, N. Brunner, Śemi-device-independent security of one-way quantum key distribution", Phys. Rev. A **84**, 010302(R) (2011).

2. M. Pawłowski, A. Winter, "Hyperbits: the information quasiparticles", Phys. Rev. A **85**, 022331 (2012).

3. H-W. Li, M. Pawłowski, Z-Q. Yin, G-C. Guo, Z-F. Han, Śemi-device independent random number expansion protocol with n to 1 quantum random access codes"Phys. Rev. A **85**, 052308 (2012).

4. H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, Z.-F. Han, Żelationship between semi- and fully-device-independent protocols", Phys. Rev. A **87**, 020302(R) (2013).

5. J. Ahrens, P. Badziąg, M. Pawłowski, M. Żukowski, M. Bourennane, Experimental Tests of Classical and Quantum Dimensions", Phys. Rev. Lett. **112**, 140401 (2014).

6. P. Mironowicz, H.-W. Li, M. Pawłowski, "Properties of dimension witnesses and their semi-definite programming relaxations", Phys. Rev. A **90**, 022322 (2014).

7. A. Grudka, K. Horodecki, M. Horodecki, W. Kłobus, M. Pawłowski, "When Are Popescu-Rohrlich Boxes and Random Access Codes Equivalent?", Phys. Rev. Lett. **113**, 100401 (2014).

8. S. Muhammad, A. Tavakoli, M. Kurant, M. Pawłowski, M. Żukowski, M. Bourennane, "Quantum bidding in Bridge", Phys. Rev. X **4**, 021047 (2014).

9. M. Dall'Arno, E. Passaro, R. Gallego, M. Pawłowski, A. Acín, Ątacks on semi-device independent quantum protocols", QIC **15**, 0037 (2015).

10. H.-W. Li, Z.-Q. Yin, M. Pawłowski, G.-C. Guo, Z.-F. Han, "Detection efficiency and noise in a semi-device-independent randomness-extraction protocol", Phys. Rev. A **91**, 032305 (2015).

C. Omówienie celu naukowego/artystycznego ww. pracy/prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

Osiągnięcie naukowe jest częścią prac zbiorowych. Mój wkład opisany jest w pkt. IB załącznika *Wykaz opublikowanych prac naukowych lub twórczych prac zawodowych oraz informacja o osiągnięciach dydaktycznych, współpracy naukowej i popularyzacji nauki.* Wkład współautorów jest przedstawiony na załączonych oświadczeniach.

W dalszej części auroreferatu referencje oznaczone literami, np. [A], odnoszą się do prac stanowiących cykl publikacji, na którym opiera się niniejszy wniosek habilitacyjny. Referencje oznaczone liczbami, np. [1], wskazują na prace wnioskodawcy nie wchodzące w skład jednotematycznego cyklu publikacji. Pozostałe referencje oznaczone pierwszymi literami z nazwisk autorów i rokiem publikacji, np. [BB84] odnoszą się do publikacji innych osób i zostały włączone celem osadzenia autoreferatu we właściwym kontekście.

1. Wstęp

Kwantowe przetwarzanie informacji, jako jego uogólnienie, jest silniejsze od jego klasycznego odpowienika. Pozwala na zwiększoną efektywność niektórych zadań, np. przyspieszenie obliczeń [S97], i pozwala na inne, niemożliwe do wykonania w klasycznym świecie, np. kryptografia zabezpieczona przed wrogami mającymi dostęp do nieograniczonej mocy obliczeniowej [BB84]. Szczerólnie interesujący jest w tej dziedzinie obszar zajmujący się rozproszonym przetwarzaniem informacji. Jest tak z wielu powodów, z których najważniejsze to: (a) duża różnorodność zadań, np. wspomniana już kwantowa dystrybucja klucza [BB84], generacja liczb losowych [LYW11], redukcja złożoności komunikacyjnej [BCD01], certyfikacja wymiaru przestrzeni Hilberta [GBHA10] lub powiększanie bezbłędnej pojemności informacyjnej (ang. *zero-error channel capacity*)[CLMW10]; (b) silne związki z podstawowymi pojęciami jak: nierówności Bella [BZPZ04], zasada nieoznaczoności [OW10] czy nielokalność [15, BBLMTU06]; (c) względna łatwość implementacji w porównaniu z zadaniami wykonywanymi w jednej lokacji, które wymagają znacznie bardziej skomplikowanych układów aby wykazać wyższość nad klasycznymi zasobami.

Kwantowe kody swobodnego dostępu okazały się potężnym narzędziem w wielu aspektach obliczeń rozproszonych. Ich dwoma podstawowymi zaletami są wszechstronność oraz mała ilość wymaganej komunikacji. Pierwsza z nich wynika z ich podatności na uogólnienia, która pozwala na zastosowanie ich w wielu różnych scenariuszach. Druga pozwala na ich eksperymentalne realizacje przy wykorzystaniu dzisiejszej technologii, co czyni je interesującymi z eksperymentalnego punktu widzenia oraz potencjalnymi kandydatami na przyszłe, praktyczne aplikacje.

Celami serii prac, które składają się na to osiągnięcie są: badanie podstawowych właściwości kwantowych kodów swobodnego dostępu, znalezienie nowych protokołów komunikacyjnych wykorzystujących te kody oraz nowych zastosowań dla już istniejących, eksperymentalne przetestowanie tych protokołów, stworzenie metod efektywnej analizy eksperymentalnych rezultatów i zbadanie ich związku z fundamentalnymi pojęciami.

2. *Kody swobodnego dostępu*

Kod Swobodnego Dostępu (KSD) jest zadaniem dla dwóch współpracujących stron. Jedna z nich zwyczajowo nazywana jest Alicją a druga Bobem. Alicja pełni rolę nadawcy a Bob odbiorcy. W niektórych przypadkach występuje także ich przeciwnik - ktoś kto chce podsłuchać ich klucz kryptograficzny lub odkryć ich tajne liczby losowe. Ta strona nazywana jest Ewą. Wszystkie strony mogą otrzymywać liczby całkowite jako dane wejściowe oraz produkować całkowite dane wyjściowe. Te pierwsze oznaczane są małymi literami a, b lub e a drugie wielkimi A, B lub E odpowiednio dla Alicji, Boba lub Ewy. Będziemy używać tego samego oznaczenia zarówno dla zmiennej losowej jak i jej wartości jednak w taki sposób aby znaczenie wynikało jasno z kontekstu.

W najbardziej ogólnym KSD wejście Alicji a składa się z wielu liczb $a_0, ..., a_{n-1}$ a Boba b jest podzbiorem k liczb całkowitych $b_0, ..., b_{r-1}$ od 0 do $n-1$. Wartości danych wejściowych wybrane są zgodnie ze wcześniej ustalonym rozkładem prawdopodobieństwa $P(a, b)$. Następnie Alicja ma możliwość wysłania wiadomości o wymiarze d do Boba, który powinien zwrócić $B = (a_{b_0}, ..., a_{b_{r-1}})$. Jeśli to mu się uda mówimy, że zadanie zakończyło się sukcesem.

Możemy wyróżnić trzy podstawowe typy KSD ze względu na zasoby dostępne dla stron:

1. Klasyczne KSD. Strony mogę korzystać tylko z zasobów klasycznej teorii informacji, czyli dzielić klasyczne korelacje oraz wysyłać klasyczną inforamcję. W takim przypadku przez wymiar wiadomości równy d rozumiemy, że Alicja może wysłać do Boba jeden z d różnych sygnałów (innymi słowy: przekazać mu $\log d$ bitów informacji).

2. KSD wspomagane splątaniem. Komunikacja pozostaje klasyczna, ale strony mogą dzielić stany splątane.

3. Kwantowe KSD (KKSD). Strony mogą na początku dzielić wyłącznie klasyczne korelacje, ale Alicja może wysyłać do Boba systemy kwantowe opisywane przestrzenią Hilberta o wymiarze d.

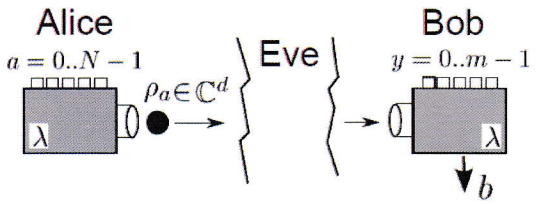
Rozważanie najbardziej ogólnej postaci KSD jest, w większości przypadków, niekonieczne ponieważ jego własności, którymi jesteśmy zainteresowani są obecne także w prostszych przypadkach. Dlatego ograniczymy się do przypadku kiedy Bob jest zainteresowany wyłącznie jedną z liczb Alicji, czyli $k = 1$. Dodatkowo założymy, że wszystkie zmienne $a_0, ..., a_{n-1}$ są binarne. Jeśli nie będzie wyraźnie zaznaczone, że jest inaczej, zakładać będziemy, że rozkład $P(a, b)$ jest jednorodny oraz, że $d = 2$. Kod tego typu oznaczać będziemy jako $n^{(d)} \to 1$ KSD. Dla wymiaru $d = 2$ będziemy pomijać górny indeks i pisać $n \to 1$ KSD.

Kwantowe kody swobodnego dostępu są obecne w informatyce kwantowej od długiego czasu. Zostały odkryte i formalnie zdefiniowane w [ANTV02]. W [CGS08] ich uogólnienie do innych niż binarne danych wejściowych Alicji zostało przedstawione. KSD wspomagane

splątaniem zostały zaproponowane w [18]. Później, do już znanych zastosowań w teorii informacji [ANTV02], inne zostały dodane: kryptografia [A], złożoność komunikacyjna [BCD01] podstawy mechaniki kwantowej [15, SBKTP09, OW10], i inne. Publikacje, które składają się na to osiągnięcie należą do właśnie tych dziedzin.

3. *Dystrybucja klucza częściowo niezależna od urządzeń*

W zadaniach, w których bezpieczeństwo jest ważne powinniśmy być niechętni do zaufania urządzeniom, które wykorzystujemy, gdyż ich dostawca mógł celowo umieścić w nich tylne wejścia do późniejszego wykorzystania. Ostatnio dużo uwagi skupiło się na amerykańskiej NSA, która zapłaciła firmie RSA Security żeby ta ustawiła generator liczb pseudolosowych Dual_EC_DRBG, którego wyniki NAS była w stanie przewidzieć, jako domyślny w swoich urządzeniach [M13]. Aby chronić się przed tego typu atakami protokoły Niezależne od Urządzeń (NU) (*ang. Device Independent*) zostały zaproponowane [MY98]. W protokołach tego typu jesteśmy w stanie oszacować pewne parametry, np. bezpieczeństwo komunikacji, bez żadnej wiedzy na temat zasad działania używanych urządzeń, bazując jedynie na oszacowanych rozkładach prawdopodobieństwa $P(A, B|a, b)$. To podejście zostało wykorzystane do Kwantowej Dystrybucji Klucza (KDK) [E91], Generacji Liczb Losowych (GLL) [PAM10] oraz ograniczaniu od dołu wymiaru przesyłanego systemu [GBHA10].



Rysunek 1: Schematyczne przedstawienie jednokierunkowego ND KDK. Źródło: [A].

W [A] zaprezentowaliśmy pierwszy protokół Częściowo Niezależny od Urządzeń (CNU) (*ang. Semi-Device Independent*). Słowo "Częściowo"pojawia się w nazwie dlatego, że, podobnie jak w przypadku NU, żadne założenia nie są powzięte jeśli chodzi o urządzenia. Zakładamy jednak górne ograniczenie na wymiar przestrzeni Hilberta przesyłanego systemu.

Protokół wykorzystany tam do dystrybucji klucza, schematycznie przedstawiony na Rys.1, jest $2 \rightarrow 1$ KKSD. W każdej rundzie Alicja koduje dwa bity a_0 i a_1 w systemie, który wysyła do Boba, który losowo wybiera jeden z nich do zdekodowania. Później ogłasza swój wybór, ale nie wartość otrzymaną, która zostaje użyta jako bit klucza.

Prawdopodobieństwo P_B, z którym Bob poprawnie odgaduje bit Alicji bezpośrednio przekłada się na efektywność generacji klucza. Pomysłem, na którym oparty jest dowód jest

własność KKSD ograniczająca prawdopodobieństwo zgadnięcia wartości a_0, a_1 i $a_0 \oplus a_1$ przez odbiorcę:

$$P(a_0) + P(a_1) + P(a_0 \oplus a_1) \leqslant \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right). \tag{1}$$

Jako pierwszy otrzymał ją R. K onig [K07] i pozostaje ona prawdziwa nawet jeśli Bob i Ewa współpracują. Skoro, w tym protokole, Ewa nie wie, który z bitów Bob stara się poznać ona może zgadywać inny. Załóżmy, że Bob stara się odkodować a_0 i ma prawdopodobieństwo sukcesu $P_B(a_0)$ aa Ewa zgaduje a_1 z $P_E(a_1)$. W takim wypadku, po połączeniu sił, mogą oni zgadnąć także $a_0 \oplus a_1$ z prawdopodobieństwem $P_{BE}(a_0 \oplus a_1) \geqslant P_B(a_0) + P_E(a_1) - 1$. Po podstawieniu tego do (1) otrzymujemy

$$P_B(a_0) + P_E(a_1) \leqslant \frac{5 + \sqrt{3}}{4} \tag{2}$$

i analogiczną nierówność z a_0 i a_1 zamienionymi rolami. To pokazuje, że jeśli Ewa próbuje zgadnąć inny bit niż Bob (innymi słowy: mierzy przechwycony system w złej bazie) zaowocuje to zaburzeniem prawdopodobieństwa sukcesu Boba. Z nierówności (2) i jej symetrii względem a_0 i a_1 otrzymujemy

$$P_B + P_E \leqslant \frac{5 + \sqrt{3}}{4}, \tag{3}$$

gdzie P_B jest uśrednionym prawdopodobieństwem $P_B = \frac{1}{2}(P_B(a_0) + P_B(a_1))$, które Alicja i Bob mogą oszacować poprzez wybranie losowego podzbioru rund protokołu i wymianę wszystkich danych z tych rund.

Wynik otrzymany przez Csiszara i Körnera [CK78] implikuje, że komunikacja w takim scenariuszu jest odporna na indywidualne ataki kiedy $P_B > P_E$. To jest zagwarantowane jeśli

$$P_B > \frac{5 + \sqrt{3}}{8} \approx 0.8415. \tag{4}$$

Dla optymalnego kodowania Alicji i pomiarów Boba mogą oni osiągnąć $P_B = \cos^2(\pi/8)) \approx 0.8536..$ Wtedy efektywność generacji klucza można otrzymać używając pracy [CK78]. Wynosi ona $r = I(A : B) - I(A : E) \approx 0.31$. Gdzie $I(X : Y)$ oznacza shannonowską informację wzajemną pomiędzy zmiennymi X i Y.

4. Generacja losowości częściowo niezależna od urządzeń

Protokół NU GLL [PAM10] jest oparty o ten sam eksperyment co KDK [E91]. Patrząc wstecz, wydaje się naturalnym założenie, że możliwe jest wygenerowanie liczb losowych w scenariuszu CNU używając tego samego układu jak ten do generacji bezpiecznego klucza.

Zostało to po raz pierwszy pokazane w [LYW11]. Protokół przedstawiony tam był oparty, tak jak nasz KDK z [A], na $2 \to 1$ KKSD i mógł produkować liczby losowe w tempie 0.2284 bita na rundę eksperymentu. W [C] postawiliśmy i udzieliliśmy odpowiedzi na pytanie: czy uogólnienie scenariusza do $n \to 1$ KKSD może spowodować zwiększenie tego tempa?

Powodem dla którego spodziewamy się zaobserwować losowość w każdym $n \to 1$ KKSD jest prawo przyczynowości informacji [15]. Mówi ono, że cała informacja niesiona przez system nie może przekroczyć jego całkowitej pojemności nawet jeśli nie cała informacja może być potem odkodowana. W $n \to 1$ KKSD układ o wymiarze 2 ma pojemność komunikacyjną jednego bitu. Jeśli ma nieść informację o n bitach to o żadnym z nich nie może być ona pełna i wynik pomiaru musi mieć pewną dozę niepewności. Standardowym narzędziem w teorii informacji używanym do mierzenia ilości niepewności (losowości) jest min-entropia definiowana przez

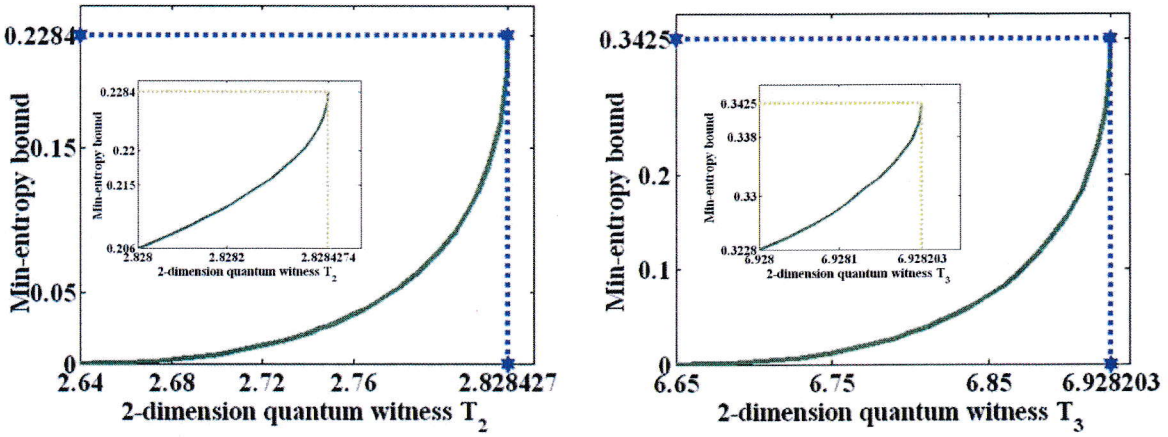
$$H_\infty(X) = -\log \max_{x,y} P(X = x|y), \tag{5}$$

gdzie X jest zmienną losową, której entropię mierzymy, x jej dopuszczalnymi wartościami, a y reprezentuje parametry, do których nie mamy dostępu ale zakładamy, że potencjalny przeciwnik może mieć. Dla binarnych obserwabli maksymalna wartość H_∞ to 1. Odpowiada ona idealnej losowości. Wartość 0 oznacza całkowitą przewidywalność przez osoby o dostępie do parametru y.

Rozważyliśmy $n \to 1$ KKSD dla $n = 2, 3, 4, 5$, dla których optymalne konstrukcje zostały znalezione a optymalne średnie prawdopodobieństwa sukcesu podane w [ALMO08]. Następie przeprowadziliśmy numeryczną minimalizację min-entropii ograniczoną przez określone średnie prawdopodobieństwo sukcesu KKSD. Wyniki dla $n = 2$ i 3 są przedstawione odpowiednio na Rys. 2 i 3. Zaobserwowaliśmy, że dla maksymalnych wartości prawdopodobieństwa sukcesu, które można otrzymać przy użyciu zasobów informatyki kwantowej $3 \to 1$ KKSD produkuje 0.3425 bitów losowości na rundę co stanowi o 0.1141 niż kod $2 \to 1$. To poprawa o prawie 50%.

Dla $n = 4$ i 5 obliczyliśmy wyłącznie ilość losowości otrzymywaną w przypadku kiedy maksymalne średnie prawdopodobieństwo sukcesu jest osiągnięte. Otrzymaliśmy wartości odpowiednio 0.1388 i 0.1024.

Powodem, dla którego dla $n = 3$ otrzymujemy więcej losowości niż dla 2 jest to, że jeśli kodujemy więcej bitów w pojedynczym układzie, z powodu jego ograniczonej pojemności, więcej informacji jest utracone o każdym z nich. Jednak, dla większych n do gry wchodzą wyniki z [HINRY06]. Pokazano tam, że dla każdej kwantowej strategii dla $n > 3$ prawdopodobieństwa sukcesu nie mogą być takie same dla każdego a, b i y jeśli prawdopodobieństwo sukcesu ma być większe od $\frac{1}{2}$. To oznacza, że dla pewnych kombinacji a, b i y otrzymamy mniej losowości niż dla innych. Ponieważ nie mamy dostępu do y musimy



Rysunek 2: Min-entropia jako funkcja średniego prawdopodobieństwa sukcesu KKSD. Świadki wymiaru T_2 i T_3 są liniowymi funkcjami średnich prawdopodobieństw sukcesu P_2 i P_3 odpowiadające kodom $2 \to 1$ i $3 \to 1$. Łącząca je relacja to $T_n = 2^n(2P_n - 1)$. Źródło: [C].

zawsze założyć najgorszy możliwy przypadek. Dlatego, chociaż ilość losowości *obecnej* w $n \to 1$ KKSD jest prawdopodobnie wysoka, ilość *certyfikowalnej* jest znacznie mniejsza. Podsumowując, $3 \to 1$ KKSD jest najlepszym protokołem CNU GLL w tej rodzinie.

5. *Świadki wymiaru*

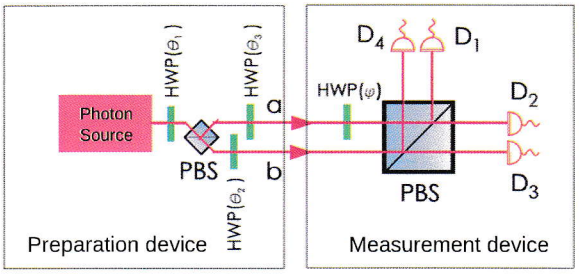
Rozważmy kombinacje liniowe o postaci:

$$W = \sum_{B,a,b} \omega_{B,a,b} P(B|a,b) \leqslant C_d, \tag{6}$$

gdzieω_{xty}^{bs} i C_d są liczbami rzeczywistymi. Mówimy, że nierówność w powyższej formie jest liniowym świadkiem wymiaru dla klasycznej komunikacji o wymiarze d jeśli: (i) jest ona prawdziwa dla każdego rozkładu prawdopodobieństwa $P(B|a,b)$, który można otrzymać przesyłając system o wymiarze d, i (ii) istnieje przynajmniej jeden rozkład $P(B|a,b)$ (wykorzystujący komunikację o wymiarze przynajmniej $d+1$), dla którego ta nierówność jest łamana. Jeśli analogiczne stwierdzenie jest prawdziwe dla $W \leqslant Q_d$ i kwantowej komunikacji of wymiarze d, wtedy nazywamy W świadkiem dla kwantowej komunikacji. Warto zauważyć, że w definicji nic nie zakładamy o tym jak wiadomość jest przygotowywana lub jakie pomiary wykonuje Bob, więc procedura ta jest NU.

Ograniczając się do układów o określonym wymiarze, kwantowa komunikacja może być bardziej efektywna od klasycznej. Ta przewaga może być uwidoczniona przy wykorzystaniu świadków wymiaru jeśli używając odpowiednio dobranej strategii wykorzystującej stany opisywane przestrzenią Hilberta o wymiarze d możliwe jest złamanie jakiegoś klasycznego

świadka splątania dla tego wymiaru. Bardziej formalnie, mówimy, że świadek wymiaru, dla którego $W \leqslant C_d \leqslant Q_d$ może być wykorzystany jako *test nieklasyczności* dla systemów o wymiarze d. Rozważmy eksperyment, w którym generowany jest rozkład prawdopodobieństwa $P(B|a,b)$ taki, że $W > C_d$. Oznacza to, ze w takim eksperymencie na pewno zastosowane zostały czysto kwantowe układy (jeśli przyjmiemy założenie, że miały one wymiar co najwyżej d). KSD są przypadkiem świadków wymiaru, które mogą być wykorzystane jako testy nieklasyczności. W [E] opisujemy eksperymentalną realizację takiego testu.



Rysunek 3: Eksperyment do testowania klasycznych i kwantowych wymiarów. Po lewej znajduje się źródło pojedynczych fotonów, emitujące poziomo spolaryzowane fotony, które, po przejściu przez trzy płytki półfalowe (HWP) ustawione pod kątami θ_i (gdzie $i = 1, 2, 3$), zostają przygotowane w odpowiednich stanach. Informacja zakodowana jest w polaryzacji i dwóch modach przestrzennych. Prawdopodobieństwa potrzebne do obliczenia świadka wymiaru D_{CHSH} otrzymywane są ze zliczeń w detektorach D_i, po odpowiednim dobraniu orientacji φ płytki półfalowej po lewej stronie urządzenia. PBS oznacza zwierciadło półprzepuszczalne. Źródło [E].

Nasz eksperyment jest schematycznie przedstawiony na Rys.3. Wykorzystaliśmy go do realizacji $2 \rightarrow 1$ KSD z komunikacją klasycznych i kwantowych systemów o wymirach 2,3 i 4. Nasze wyniki przedstawione są w tabeli I. Wartość D_{CHSH} używana w tabeli jest liniową funkcją P_2 - średniego prawdopodobieństwa sukcesu $2 \rightarrow 1$ KSD. Łączy je relacja $D_{CHSH} = 2^{n+1}(2P_n - 1)$. D_{CHSH} też równe $2T_2$ używanemu w poprzedniej sekcji. Wykorzystywanie różnych wyznaczników, które mogą być łatwo na siebie konwertowane, może wydawać się niepotrzebne, ale używamy go aby pokazać związek KSD z różnymi innymi obiektami i dowodzi ich wszechstronności (w kolejnej sekcji znajduje się dłuższe omówienie).

Warto zwrócić uwagę, że zarówno w teorii jak i w eksperymencie obserwujemy taką samą hierarchię zasobów: pojedynczy bit jest słabszy od kubita, który z kolei jest gorszy od klasycznego systemu o wymiarze 3, który jednak nie jest tak dobry jak jego kwantowy odpowiednik. Dla systemów o wymiarze 4 tylko jeden eksperyment został przeprowadzony gdyż tutaj zarówno klasyczne jak i kwantowe strategie pozwalają na osiągnięcie maksymalnej algebraicznej wartości D_{CHSH}. W tym punkcie $2 \rightarrow 1$ KSD przestaje być świadkiem wymiaru jak i testem nieklasyczności.

Skoro eksperymentalna realizacja 2 *to*1 KSD z użyciem kubitów może być wykorzystana do CNU KDK lub GLL przy użyciu protokołów z poprzednich sekcji, możemy określić jak dobry byłby nasz eksperyment gdyby został wykorzystany do powyższych zadań. Wartość D_{CHSH}

Ograniczenie nierówności	D_{th}	D_{exp}	D^b_{exp}	ΔD_p	ΔD_d	ΔD_T
D_{CHSH}(bit)	4	3.94	3.98	0.08	0.010	0.08
D_{CHSH}(qubit)	5.66	5.51	5.56	0.12	0.008	0.12
D_{CHSH}(trit)	6	5.90	5.96	0.13	0.010	0.13
D_{CHSH}(qutrit)	6.47	6.44	6.50	0.14	0.009	0.14
D_{CHSH}(quart)	8	7.88	7.94	0.16	0.010	0.16

Tablica I: **Eksperymentalne wyniki testów świadków wymiaru.** D_{th}, D_{exp} and D^b_{exp} reprezentują wartości teoretyczne, eksperymentalne oraz eksperymentalne po uwzględnieniu ciemnych zliczeń dla świadka wymiaru. ΔD_p, ΔD_d i ΔD_T są błędami pomiarów wynikającymi odpowiednio z ograniczonej precyzji ustawień płytek półfalowych i niedoskonałości rozdzielania polaryzacji, poissonowskiej statystyki oraz całkowitymi. Źródło: [E].

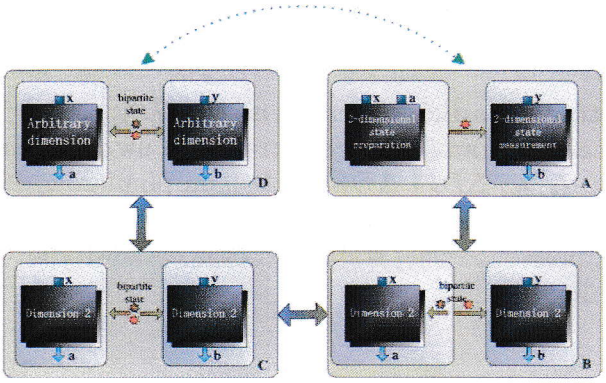
dla kubitów otrzymana w eksperymencie daje stosunek bitów klucza do rund eksperymentu równy 5.18% lub 6.67% jeśli założymy, że obserwowane ciemne zliczenia nie są kontrolowane przez Ewę (korzystając z wyników z [A]). Dla GLL otrzymalibyśmy 0.0595 bitów na rundę jeśli przyjmiemy $D_{CHSH} = 5.51$. Dla $D_{CHSH} = 5.56$ otrzymamy 0.0820 (korzystając z wyników z [C]). Są jednak dwa poważne problemy z tymi wartościami. Opisuję je i przedstawiam metody radzenia sobie z nimi w kolejnych dwóch sekcjach.

6. *Randomness estimation*

Wyniki z [C] zostały otrzymane przy wykorzystaniu algorytmu Levenberga-Marquardta do znalezienia minimalnej entropii konsystentnej z określoną wartością średniego prawdopodobieństwa sukcesu. Niestety, nie ma gwarancji, że minimum przez niego znajdowane jest globalne. Rozwiązaliśmy ten problem w [D] podając algorytm, który ma taką gwarancję. Nasz pomysł polegał na pokazaniu jak przejść z protokołu CNU (z komunikacją pojedynczego kubitu) do NU (wykorzystującego stany splątane bez komunikacji), dla których znamy algorytmy [NPA08] z gwarancją znalezienia globalnego minimum. Teraz opiszę w skrócie jak działa nasza metoda.

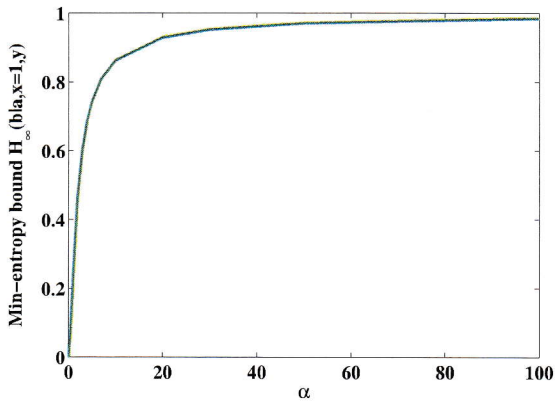
Każdy protokół CNU może być zrealizowany w następujący sposób. Alicja ma parę systemów w stanie singletowym. Jeśli chce przygotować stan $|\phi\rangle$ mierzy jeden układ w bazie $\{|\phi\rangle, |\phi^\perp\rangle\}$ a drugi skolapsuje do jednego z tych stanów. Opierając się na wyniku pomiaru wysyła ona ten układ do Boba bez zmian lub wykonuje transformację unitarną, która zamienia $|\phi^\perp\rangle$ na $|\phi\rangle$ przed wysłaniem. Jeśli wyniki pomiarów Boba są binarne Alicja nie musi nawet wykonywać tej transformacji. Może po prostu wysłać swój wynik pomiaru do Boba (0 oznacza $|\phi\rangle$ a 1 $|\phi^\perp\rangle$), który dodając go modulo 2 do swojego dostanie dokładnie taki sam rozkład prawdopodobieństwa jak w początkowym protokole CNU. Te dwa przypadki

oznaczone są literami (A) i (B) na Rys. 4.



Rysunek 4: Schemat metody znajdywania dolnego ograniczenia na entropię w protokołach CNU używając PPO. Dokładny opis w głównym tekście. Rysunek wzięty z citeM-divssdi gdzie x i y były użyte jako wejścia Alicji i Boba a a i b jako ich wyniki.

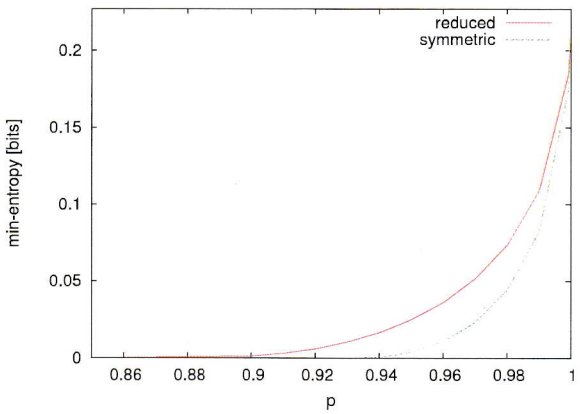
Oczywiście, nic nie ulegnie zmianie, jeśli źródło stanu singletowego znajdzie się poza laboratorium Alicji i będzie ona tylko odbiorcą jednego z podsystemów stanu splątanego, tak jak Bob. Ta sytuacja oznaczona jest literą (C). Wiele natomiast zmieni się, kiedy założymy, że strony otrzymują stan maksymalnie splątany o nieznanym wymiarze. To przedstawione jest w części oznaczonej (D). To jednak tylko zwiększa możliwe rozkłady prawdopodobieństwa więc każde dolne ograniczenie na entropię w (D) będzie też dolnym ograniczeniem w (A). (D) z kolei jest po prostu opisem scenariusza NU z pewnymi ograniczeniami na wykorzystywany stan kwantowy. Możemy oszacować od dołu entropię w takim przypadku korzystając z metod wykorzystujących Programowanie Pół-Określone (PPO) z [NPA08] a fakt, że stan jest maksymalnie splątany odzwierciedlony jest poprzez dodatkowe ograniczenia na rozkład wyników.



Rysunek 5: Maksymalna ilość losowości możliwa do otrzymania przy użyciu $2 \to 1$ KSD z ważonym prawdopodobieństwem sukcesu jako wyznacznikiem. Dla $b = 0$ waga wynosi 1 a dla $b = 1$ jest ona równa α. Przypadek rozważany w poprzednich sekcjach odpowiada $\alpha = 1$, który daje co najwyżej 0.23 bitów losowości. Źródło: [D].

Używając tej nowej techniki optymalizacyjnej byliśmy w stanie potwierdzić, że minima znalezione przy zastosowaniu algorytmu Levenberga-Marquardta w [C] były rzeczywiście globalne. Dodatkowo, poprzez znalezienie tego związku, byliśmy w stanie pokazać, że odpowiednik NU dla $2 \to 1$ KSD to słynna nierówność CHSH [CHSH69]. To właśnie jest powodem, dla którego indeks CHSH pojawia się w poprzedniej sekcji oraz dlaczego zamieniono P_2 na T_2 (dlatego, że zakres wartości osiąganych przez T_2 jest taki sam jak CHSH). Co więcej byliśmy w stanie przełożyć do scenariusza CNU rezultaty z [AMP12] gdzie pokazano, że drobna modyfikacja nierówności CHSH prowadzi do generacji znacznie większej

ilości losowości. Odkryliśmy, że dla $2 \to 1$ KSD ta modyfikacja przekłada się na używanie ważonego średniego prawdopodobieństwa sukcesu i przeanalizowaliśmy taki kod. Wyniki przedstawione są na Rys. 5.



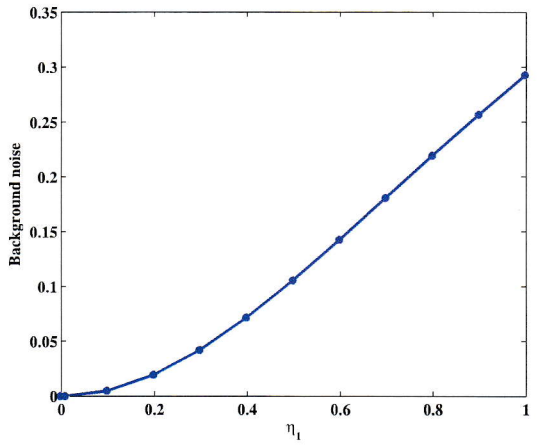
Rysunek 6: Ilość losowości otrzymywana przy użyciu $2 \to 1$ KSD opartego o symetryczne i zredukowane świadki wymiaru: $D_C HISH$ i T_2. p oznacza ułamek maksymalnej kwantowe wartości świadka. Źródło: [G].

Wyniki z [D] zostały uogólnione w [G] gdzie metoda z Rys. 4 została przystosowana dla dowolnej ilości komunikacji i formy testu nieklasyczności. Co więcej, zbadaliśmy tam ogólne właściwości świadków. Weźmy pod uwagę wzór (6). Nazwiemy go symetrycznym świadkiem jeśli $B = 0,1$ i istnieje takie bijektywne odwzorowanie dla danych wejściowych Alicji $\phi : a \to a$, że dla każdego a, b i B $\omega_{B,a,b} = -\omega_{B,\phi(a),b} = -\omega_{\bar{B},a,b}$, gdzie $\bar{B}$ to negacja B.

Jeśli świadek wymiaru jest symetryczny możemy zredukować ilość wejść Alicji o połowę. Robimy to poprzez wybranie dowolnego podzbioru $\bar{A}$ wartości a takiego, że zawiera on dokładnie połowę możliwych wartości i $\forall_{a \in \bar{A}} \phi(a) \notin \bar{A}$. Wtedy konstruujemy nowego świadka poprzez usunięcie wszystkich jego elementów zawierających $a \notin \bar{A}$. Takiego świadka nazywamy *zredukowanym*. T_2 z[C] jest zredukowanym świadkiem wymiaru odpowiadającym D_{CHSH} z [E]. Chociaż są bardzo zbliżone, te dwie miary sukcesu $2 \to 1$ KSD zachowują się inaczej kiedy wykorzystujemy je do certyfikacji losowości. W [G] dokonaliśmy ich porównania, które zamieszczam na Rys.6.

7. *Efektywność detektorów*

Drugi problem, na który napotykamy się przy szacowaniu losowości produkowanej w danym eksperymencie jest spowodowany przez nieefektywne detektory fotonów. Za każdym razem kiedy przeprowadzamy rundę kwantowego protokołu cząstka (zwykle foton) wysyłana jest od Alicji do Boba. Jednakże, w praktyce, często zdarza się, że jest ona zgubiona po drodze lub nie zarejestrowana przez odbiorcę. W [E] przyjęliśmy tak zwane założenie uczciwego próbkowania (*ang. fair sampling assumption*), które mówi, że przypadki, w których cząstka nie jest zarejestrowana zdarzają się losowo. Jednakże, nie musi mieć to miejsca w scenariuszach NU lub CNU gdzie spodziewamy się, że Ewa manipulowała naszymi urządzeniami w złej woli.



Rysunek 7: Maksymalny tolerowany szum jako funkcja efektywności detektorów (η_1). Źródło: [J].

Najprostszym i najbardziej efektywnym sposobem poradzenia sobie z tym problemem jest przypisanie wcześniej ustalonego wyniku dla wszystkich przypadków kiedy żaden nie jest wyprodukowany. Niestety, drastycznie obniża to średnią wartość prawdopodobieństwa sukcesu KSD (a także wszystkich innych wskaźników) i poniżej pewnej (zwykle dość wysokiej) wartości progowej żadna ilość losowości nie może być poświadczona. W [J] obliczyliśmy progową wartość efektywności detektorów dla $2 \to 1$ KSD, która wynosi $\frac{1}{\sqrt{2}} \approx 0.71$. Jednak jest to czysto teoretyczny wynik, który nie bierze pod uwagę, żadnych innych niedoskonałości eksperymentu. Jeśli zdecydujemy się modelować zakłócenia w kanale komunikacyjnym poprzez dodawanie białego szumu otrzymamy związek przedstawiony na Rys. 7. Ten wykres został wykonany przy założeniu, że jeśli stan ρ jest wysłany przez nadawcę, odbiorca otrzyma $(1-p)\rho + p\frac{\mathbb{1}}{2}$, gdzie p to ilość szumu.

Niestety, nawet 0.71 jest wartością efektywności detektorów bardzo trudną do uzyskania w eksperymentach przy obecnej technologii. Dlatego, podjęliśmy próby znalezienia metod obniżenia tego progu. W następnej sekcji pokażemy jak może być to uzyskane poprzez mierzenie prawdopodobieństwa sukcesu w inny sposób.

8. Prawdopodobieństwo sukcesu w najgorszym przypadku

Jeśli, w konkretnym przypadku, nie jesteśmy w stanie poświadczyć żadnej ilości losowości oznacza to, że istnieje klasyczny model odtwarzający obserwowany rozkład prawdopodobieństwa. Przyjmijmy teraz rolę adwersarza i spróbujmy wykorzystać nieefektywne detektory w taki sposób, żeby wyniki pomiarów były całkowicie deterministyczne podczas gdy wartość testu nieklasyczności sugeruje inaczej (przyjmując założenie uczciwego próbkowania) i znajdźmy strategię, która pozwala to uzyskać. Najprostsza, dla $2 \to 1$ KSD to nakazanie Alicji wysyłania zawsze a_0 do Boba, który dla $b = 0$ zwraca otrzymaną wartość, a dla $b = 1$ ogłasza, że nie doszło do detekcji cząstki. W przypadkach kiedy detekcja zostaje ogłoszona Bob ma zawsze poprawny wynik. Przyjęcie założenia uczciwego próbkowania oznacza założenie, że jego prawdopodobieństwo sukcesu byłoby takie samo, gdyby wykrył cząstkę też w pozostałych przypadkach. Dlatego otrzymujemy średnie prawdopodobieństwo sukcesu równe 1 w tym przypadku. To więcej

niż nawet kwantowa teoria pozwala. Będziemy nazywali takie zachowanie (czyli, używanie tylko klasycznych zasobów i założenia uczciwego próbkowania aby zwiększyć wartość testu nieklasyczności powyżej klasycznego limitu) *wykorzystywaniem luki efektywności detektorów.*

W [I] pokazaliśmy, że jeśli w $n \to 1$ KSD, klasyczne prawdopodobieństwo sukcesu w najgorszym przypadku równe jest $\frac{1}{2}$ to wykorzystywanie luki efektywności detektorów nie może zwiększyć tej wartości. To prawdopodobieństwo zdefiniowane jest jako $\min_{a,b} P(B = a_b|a,b)$. Tak szczęśliwie się składa, że klasyczne prawdopodobieństwo sukcesu w najgorszym przypadku dla każdego $n \to 1$ KSD równe jest $\frac{1}{2}$ jeśli strony nie mają dostępu do współdzielonej losowości [ANTV02]. To oznacza, że jeżeli założymy, że urządzenia Alicji i Boba działają niezależnie, to możliwe jest generowanie losowości przy dowolnie niskiej efektywności detektorów. Ten fakt został użyty przy eksperymentalnej demonstracji generacji losowości w [LBL15].

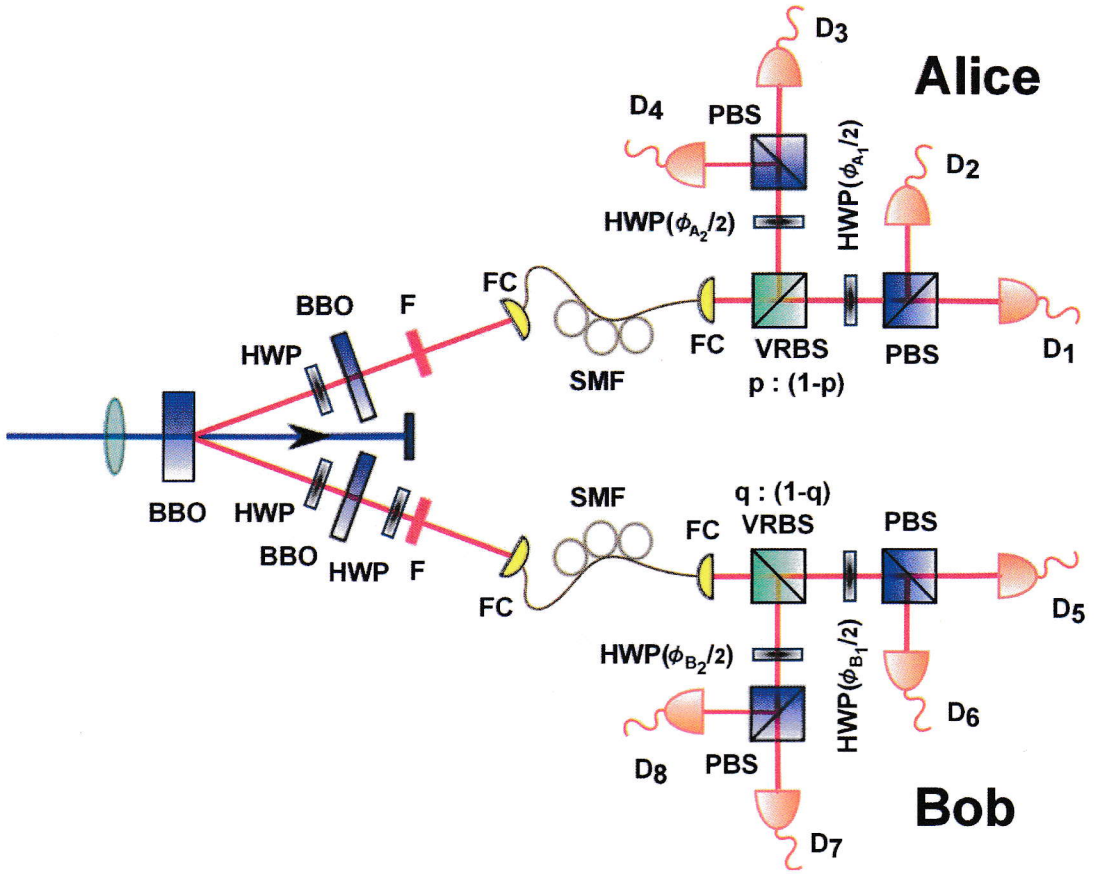
Naturalnym pytaniem jest: czy niezależność urządzeń jest wystarczająca aby zabezpieczyć się przed atakami z wykorzystywaniem luki efektywności detektorów bez dodatkowego założenia o klasycznym prawdopodobieństwu sukcesu w najgorszym przypadku równym $\frac{1}{2}$. W [I] podajemy przykład $3^{\log 6} \to 1$ KSD, który ma to prawdopodobieństwo większe od $\frac{1}{2}$ i pokazujemy, że może ono być zwiększone przy wykorzystaniu takich ataków.

Żądanie aby urządzenia nie były skorelowane może być trudne do uzasadnienia w niektórych przypadkach, jednak są inne metody radzenia sobie z nieefektywnymi detektorami co pokazuję w kolejnej sekcji.

9. Kwantowy Brydż

Niektóre praktyczne zastosowania mogą pozwolić na możliwość powtórzenia rundy protokołu jeśli cząstka nie zostanie wykryta, jednocześnie zabraniając tego kiedy będzie. Rozważmy przypadek Brydża Sportowego. Podczas licytacji każdy z graczy ogłasza swoje odzywki. W tych odzywkach gracze kodują informacje o swoich rękach ale ograniczona ilość możliwych odzywek nakłada ograniczenie na ilość informacji jaką mogą się podzielić. Całkowicie dozwoloną zagrywką jest poproszenie jakiegokolwiek gracza o powtórzenie odzywki jeśli nie jesteśmy pewni czy dobrze ją usłyszeliśmy. Jednak, zakazane jest wykorzystywanie tego to sekretnego przekazywania dodatkowych informacji. Jeśli pojawią się jakiekolwiek wątpliwości dotyczące uczciwości graczy muszą oni być w stanie logicznie wytłumaczyć wszystkie swoje zagrania w grze dowodząc tym że mogli podjąć decyzje, które podjęli bez dostępu do żadnych informacji, które nie zostały przekazane w sposób dozwolony.

W [F] pokazaliśmy, że możliwe jest wykorzystanie tej własności gry i skonstruowanie kwantowej strategii, która czyli licytację bardziej efektywną bez łamania jakichkolwiek zasad Światowej Federacji Brydża. Tą strategią jest $2 \to 1$ KSD. Byliśmy w stanie pokazać, że w pewnych szczególnych przypadkach prawdopodobieństwo wygrania w grze równe jest ważonemu średniemu prawdopodobieństwu sukcesu dla tego kodu. W tej samej



Rysunek 8: Schemat eksperymentalnej realizacji Kwantowego Brydża. Światło UV o długości 390 nm skupione zostaje na grubym na 2 mm nieliniowym krysztale BBO (β boran baru) w celu produkcji par fotonów. Płytki półfalowe (HWP) i dwa grube na 1 mm kryształy BBO wykorzystywane są do kompensacji podłużnych i poprzecznych dryfów. Wyemitowane fotony zostają wpuszczone w dwumetrowe jednomodowe światłowody (SMF) i przechodzą przez filtry interferencyjne o wąskiej przepustowości (F) ($\Delta\lambda = 1\,\text{nm}$). Alicja wykorzystuje zwierciadło półprzepuszczalne (VRBS) o regulowanej przepuszczalności $(p : 1-p)$ w celu wybrania bazy pomiaru z prawdopodobieństwami p i $1-p$ (odpowiadające jej danej wejściowej a). Jej obserwable A_1 i A_2 są realizowane poprzez płytki półfalowe obrócone o kąty ϕ_{A_1} i ϕ_{A_2}. Bob także wykorzystuje zwierciadło półprzepuszczalne (VRBS) o regulowanej przepuszczalności $(q : 1-q)$ w celu wybrania bazy pomiaru z prawdopodobieństwami q i $1-q$ (odpowiadające jego danej wejściowej b). Jego obserwable B_1 i B_2 są realizowane poprzez płytki półfalowe obrócone o kąty ϕ_{B_1} i ϕ_{B_2}. Pomiary polaryzacji dla obu stron zostały wykonane przy użyciu zwierciadeł półprzepuszczalnych wrażliwych na polaryzację (PBS) i detektorów fotonów (D). Źródło: [F].

pracy donieśliśmy o eksperymentalnej realizacji naszego protokołu, która przedstawiona jest na Rys. 8. Ponieważ zasady brydża nie pozwalają na komunikację kwantową byliśmy zmuszeni do wykorzystania klasycznej wspieranej splątaniem. Oprócz tego zastosowania KSD wspomagane splątaniem są też wygodnym narzędziem do badania podstaw mechaniki

kwantowej o czym traktują dwie kolejne sekcje.

10. Hiperbity

W [B] rozważaliśmy przypadek, w którym Bob zwraca binarny wynik B. Pokazaliśmy, że w takim przypadku bit klasycznej komunikacji wspomagany splątaniem tworzy informacyjną kwazicząstkę, którą nazwaliśmy *hiperbitem*. Rozważmy kubit przygotowany w konkretnym stanie, wysłany a następnie poddany pomiarowi rzutowemu. Taki scenariusz może być wygodnie przedstawiony w formalizmie sfery Blocha, gdzie każdy możliwy czysty stan kubitu leży na 3-wymiarowej sferze a pomiary odpowiadają wektorom w 3-wymiarowej przestrzeni. Stany mieszane leżą wewnątrz sfery a prawdopodobieństwo zaobserwowania konkretnego wyniku jest określone przez projekcję wektora odpowiadającego stanowi na ten, który odpowiada pomiarowi. Hiperbity są naturalnym uogólnieniem tego schematu. Jedyną różnicą jest to, że stany leżą na hipersferze o dowolnym wymiarze (a wektory odpowiadające pomiarom mają taki sam wymiar jak sfera).

Użyteczność hiperbitów wynika z ich prostoty oraz faktu że pozwalają łączyć scenariusze wykorzystujące kwantową komunikację z tymi, które wykorzystują klasyczną wspomaganą splątaniem. Jednym z ich zastosowań okazało się poprawienie rezultatów z [A]. Oparliśmy tam bezpieczeństwo na nierówności (1) i otrzymaliśmy progowe prawdopodobieństwo sukcesu Boba równe 0.8415, które jest bardzo blisko maksymalnemu dozwolonemu przez mechanikę kwantową. W [B]pokazaliśmy, że dla $2 \rightarrow 1$ KSD wspomaganego splątaniem zachodzi

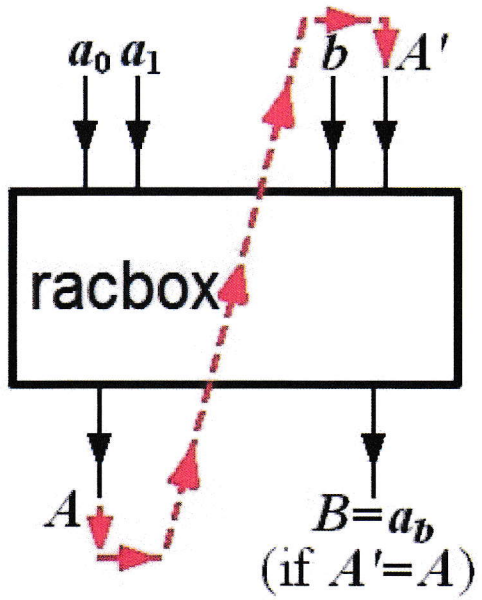
$$E(a_0)^2 + E(a_1)^2 + E(a_0 \oplus a_1)^2 \leqslant 1, \tag{7}$$

gdzie $E(a_i) = 2P(a_i) - 1$. To nierówność silniejsza od (1). Ponieważ hiperbit jest uogólnieniem kubitu, ta sama nierówność dotyczy też $2 \rightarrow 1$ KKSD, na którym bazuje protokół z [A]. Używając (7) zamiast (1) otrzymujemy niższe prawdopodobieństwo sukcesu wymagane do bezpiecznej komunikacji równe 0.8335.

11. Pudła KSD

KSD zostały wykorzystane w [15] do wyprowadzenia ograniczenia na łamanie nierówności CHSH. Dzięki temu byliśmy w stanie wykluczyć możliwość istnienia, tak zwanych, Pudeł-PR. Te hipotetyczne urządzenia, zaproponowane w [PR94] pozwalają na łamanie tej nierówności aż do jej algebraicznego maksimum. W [H] zaproponowaliśmy inny typ hipotetycznego urządzenia: Pudła-KSD. Tak jak Pudła-PR ich zasada działania nie jest znana. Jedyne co o nich zakładamy to to, że pozwalają na realizację $n \rightarrow 1$ KSD z 100% prawdopodobieństwem sukcesu przy zaledwie jednym bicie komunikacji pomiędzy stronami. Schematyczna reprezentacja $2 \rightarrow 1$ Pudła-KSD przedstawiona jest na Rys.9. a_0 i a_1 są danymi

wejściowymi Alicji, A to wiadomość, którą wysyła do Boba. Bob powinien użyć jej oraz swojej zmiennej b jako wejścia do jego części pudła, ale ponieważ może zdecydować się wprowadzić inną wartość dlatego ta część jego danych wejściowych oznaczona jest przez A'. Z definicji Pudła-KSD, jeśli $A = A'$ wynik B Boba musi być zawsze równy a_b.



Rysunek 9: Schematyczna reprezentacja $2 \rightarrow 1$ Pudła-KSD. Źródło: [H].

Następnie porównaliśmy oba typy pudeł. Już z [15] wynikało, że Pudło-PR może zostać wykorzystane do stworzenia $2 \rightarrow 1$ Pudła-KSD i, bardziej ogólnie, n Pudeł-PR wystarcza na zbudowanie jednego $n + 1 \rightarrow 1$ Pudła-KSD. W [H], że nie da się tego zrobić używając mniejszej ilości. Drugim pytaniem, które postawiliśmy w [H] było czy każde Pudło-KSD może symulować Pudło-PR. Otrzymaliśmy dość niespodziewany rezultat, że jest to prawda wyłącznie dla pudeł nie dopuszczających komunikacji szybszej od światła. Są to pudła, które stosują się do zasady, że żadna informacja nie może zostać przesłana bez komunikacji. W przypadku pudła z Rys. 9 ta zasada oznacza, że rozkład prawdopodobieństwa jednej ze stron nie może zależeć od danych wejściowych drugiej, czyli $P(A|a_0, a_1, A', b) = P(A|a_0, a_1)$ i $P(B|a_0, a_1, A', b) = P(B|A', b)$. Jeśli ta zasada nie jest spełniona możliwe są takie Pudła-KSD, które nie mogą symulować Pudeł-PR.

V. POZOSTAŁE OSIĄGNIĘCIA NAUKOWO-BADAWCZE

Dane bibliometryczne:

- Liczba publikacji: **52** (**41** po doktoracie)
- Sumaryczna ilość cytowań: **720** (**630** bez autocytowań)
- H-index: **12**
- Sumaryczny impact factor: **205,034**

A. Przed doktoratem

1. *Nierówności Bella wspomagane komunikacją*

Mój doktorat skupiał się na badaniach związku pomiędzy podstawowymi pojęciami fizycznymi a protokołami przetwarzania informacji i badania nierówności Bella

wspomaganych klasyczną komunikacją okazały się bardzo wszechstronnym narzędziem w tej dziedzinie. W [15] wyprowadziliśmy maksymalne łamanie nierówności CHSH korzystając wyłącznie z podstawowych założeni teorii informacji, które musza być spełniane przez wszystkie układy fizyczne. Kontynuowaliśmy tą pracę w [16] gdzie wyprowadziliśmy dodatkowe ograniczenia oraz w [18] gdzie uogólniliśmy narzędzia wykorzystane w [15] i [16]. Prace te przyciągnęły dość dużą uwagę więc opisaliśmy je w sposób popularnonaukowy w Świecie Nauki [20].

Podejście zastosowane w pracach z powyższego akapitu miało na celu dowiedzenie się więcej o maksymalnym kwantowym łamaniu nierówności Bella. W innych pracach badaliśmy jak dopuszczenie komunikacji wpływa na ograniczenie klasyczne. W [22] rozważaliśmy ilość i typ informacji jaki jest wymagany przez klasyczne modele wspomagane przez jednokierunkową komunikację pomiędzy stronami aby osiągnąć maksymalną kwantową wartość CHSH. Później, w [19] badaliśmy dowolne nierówności Bella i komunikację.

2. *Monogamia nierówności Bella*

Innym aspektem nierówności Bella poruszanym w moim doktoracie była ich monogamia. To określenie odnosi się do faktu, że jeśli pomiary jednej ze stron mogą zostać użyte do złamania nierówności Bella razem z pewną grupą innych stron, silniejsze ograniczenie nakładane jest na możliwość użycia tych samych pomiarów do złamania ich z inną grupą. W [14] wyprowadziliśmy ilościowe ograniczenie na monogamię każdej dwuosobowej nierówności Bella. W [21] udało mi się pokazać, że do wyprowadzenia bezpieczeństwa kryptografii kwantowej, używanie jej pełnego formalizmu jest zbędne, a założenie wyłącznie, że obowiązują ograniczenia monogamii wystarczające.

3. *Kryptografia w Mechanice Bohmowskiej*

Podejście zastosowane w [21] było NU, czyli nic nie zostało założone o działaniu urządzeń a bezpieczeństwo dowiedzione wyłącznie na podstawie obserwowanych korelacji wyników pomiarów. Jednak, takie podejście nie jest możliwe jeśli założymy, że Mechanika Bohmowska jest teorią, która poprawnie opisuje działanie naszych urządzeń [H93]. W [11] i [13] pokazaliśmy, że także w tej teorii bezpieczna kryptografia jest możliwa o ile dysponujemy dobrym opisem używanego sprzętu oraz poczynione są pewne modyfikacje w protokole dystrybucji klucza.

4. *Inne*

Podczas mojego doktoratu pracowałem także nad innymi zagadnieniami, nie związanymi z główną linią moich badań. Rezultatem tych prac były publikacje na temat: opisu splątania z próżnią w różnych reprezentacjach drugiej kwantyzacji [12]; porównania prędkości uczenia się rozwiązywania pewnego problemu przez klasyczne i kwantowe algorytmy[17]; oraz górnego ograniczenia na ilość baz wzajemnie bezstronnych, które można otrzymać korzystając z określonej metody [23].

B. Po doktoracie

1. *Nierówności Bella*

Po uzyskaniu tytułu doktorskiego kontynuowałem pracę nad podobnymi zagadnieniami i brałem udział w wielu projektach dotyczących nierówności Bella. W [24] dowiedliśmy kilku istotnych właściwości rodziny nierówności GYNI citegyni.

W [33] uogólniliśmy rezultaty z [14] i otrzymaliśmy bardziej precyzyjny opis relacji monogamii dla różnych nierówności. Wykorzystaliśmy także rezultaty z [21] w celu znalezienia jak te relacje wpływają na przewidywalność wyników pomiarów.

W [30] kontynuowaliśmy pracę z [19] i rozważaliśmy asymetryczne nierówności Bella oraz jak częściowa przewidywalność wyboru ustawienia wpływa na ich graniczenia.

W [36] wprowadziliśmy nowy typ nierówności Bella poprzez ograniczenie ich formy do takiej, która zawiera tylko jeden możliwy wynik dla każdego wejścia. Następnie zbadaliśmy ich właściwości i przedstawiliśmy możliwe przyszłe zastosowania.

W [37] badaliśmy trójstronne korelacje i przedstawiliśmy zestaw nierówności, które mogą być wykorzystane do rozróżnienia pomiędzy wieloma różnymi teoriami.

W [38] zbadaliśmy związek pomiędzy splątaniem a nielokalnością w przypadku nierówności CGLMP [CGLMP02].

W [39] otrzymaliśmy ścisłe ograniczenie na klasyczną wartość uogólnionych gier CHSH.

2. *Inne testy nieklasyczności*

Chociaż nierówności Bella są najbardziej znanymi przypadkiem testów, który może wykluczyć możliwość klasycznego opisu eksperymentu, nie są jedynymi. W moich badaniach rozważałem różne rodzaje takich testów. Jednym z nich jest, tak zwany, eksperyment PBR [PBR12], którego celem jest dowiedzenie optymalności opisu stanów kwantowych przez funkcję falową. W [40] dokonaliśmy jego analizy pod kontem podatności na nieefektywne detektory i znaleźliśmy wartość progową ich efektywności wymaganą aby test był rozstrzygający.

W [41] badaliśmy sieci komunikacyjne i pokazaliśmy, że zwiększanie ich złożoności zwiększa także różnicę pomiędzy efektywnością klasycznych i kwantowych zasobów.

W [42] zaproponowaliśmy nowy typ gry, w której gracze dysponujący kwantowymi zasobami mają przewagę nad ich klasycznymi odpowiednikami.

W [43] przeformułowaliśmy nierówności niekontekstualne tak aby miały znaczenie operacyjne.

3. Losowość

Większość z testów opisanych w dwóch poprzednich sekcjach może zostać wykorzystana w praktycznych aplikacjach. Jedną z nich jest generacja, ekspansja, amplifikacja oraz certyfikacja losowości. W [35] pokazaliśmy jak można amplifikować, innymi słowy: poprawić jakość, dowolnie słabej losowości.

W [31] badaliśmy problem amplifikacji losowości, bez zakładania poprawności pełnego formalizmu mechaniki kwantowej. Było już wcześniej wiadome, że jeśli komunikacja szybsza niż światło jest niemożliwa, to losowość może zostać wzmocniona [CR12]. Byliśmy w stanie poprawić wyniki z [CR12] poprzez obniżenie progowej jakości losowości powyżej, której amplifikacja jest możliwa.

W [27] badaliśmy potencjał wielu różnych testów nieklasyczności do produkcji losowości i określiliśmy ilość szumu jaką mogą one tolerować. Pokazaliśmy, że to jaki test jest optymalny do GLL zależy od ilości szumu oczekiwanej w eksperymencie.

Podczas kiedy w [35] i [31] zakładaliśmy, że dostępna losowość ma określoną formę, w [32] przedstawiliśmy protokół zdolny amplifikować dowolnie słabą losowość ze źródła dowolnego typu.

W [44] stworzyliśmy protokół generacji losowości oparty o paradoks Hardy'ego [H92]. Był to pierwszy protokół tego typu oparty o teście nieklasyczności nie wykorzystującym pojedynczej nierówności.

W [45] pokazaliśmy metodę certyfikacji większej ilości losowości bez żadnej zmiany w eksperymencie. Jedynym kosztem jest to, że czas potrzebny na obliczenie ilości otrzymanej losowości rośnie bardzo szybko. Wykonaliśmy także eksperyment i zademonstrowaliśmy naszą metodę na danych przez niego wyprodukowanych.

W [46] skupiliśmy się na bardziej ogólnym przypadku, w którym urządzenie używane do generacji losowości i to, które używane jest do jej amplifikacji są skorelowane. Pokazaliśmy, że nawet w takim przypadku amplifikacja jest możliwa.

4. *Kwantowa kryptografia*

Inną aplikacją testów nieklasyczności jest bezpieczna dystrybucja klucza i pracowałem także w tej dziedzinie. Moja wcześniejsza praca [21] przyciągnęła dużo uwagi i zainicjowała dalsze prace oraz komentarze. [25] jest odpowiedzią na jeden z nich.

Losowość jest uważana za niezbędny zasób do kwantowej kryptografii. Nasze wyniki opisane w poprzedniej sekcji pokazały, że amplifikacja jest dość trudna. Dlatego, zadaliśmy pytanie czy możliwe jest wykorzystanie słabej losowości. W [26] pokazaliśmy, że można znacząco obniżyć wymagania dotyczące jej jakości jeżeli zastosujemy protokoły KDK wykorzystujące stany splątane o dużym wymiarze przestrzeni Hilberta.

Typowe protokoły KDK wykorzystujące splątanie, używają wyników pomiarów jako klucza. Nie jest to jedyna możliwość, ponieważ w kryptografii opartej na kwantowej komunikacji istnieje protokół [SARG04], w którym to dane wejściowe są do tego używane. Nisetety, jest on wyjątkowo nieefektywny. W [47] pokazaliśmy, że w przypadku kryptografii opartej na splątaniu tak się nie dzieje i przedstawiliśmy protokół, który lepiej sobie radzi niż standardowe. Jego zalety wynikają z faktu, że źródła losowości używane do generacji wejść są pod kontrolą użytkownika inaczej niż wyniki pomiarów.

W [26] i [47] badaliśmy używanie losowości w KDK. W [48] pokazaliśmy, sprzeczny z intuicją wynik, że losowość wcale nie jest do kryptografii niezbędna. Bazuje on na fakcie, że z punktu widzenia Ewy, wiadomość, która ma zostać zaszyfrowana jest losowa i może zostać wykorzystana jako początkowe źródło losowości.

5. *Inne*

Po doktoracie kontynuowałem także badania niezwiązane z moimi głównymi zainteresowaniami. W [34] dokonaliśmy przeglądu wyników otrzymanych w [15] oraz pracach z dziedziny, którą [15] zapoczątkowała.

O ile w [17] badaliśmy prędkość z jaką kwantowy algorytm uczy się klasycznego zadania, o tyle w [29] skupiliśmy się na problemie znalezienia czysto kwantowego algorytmu.

Prace nad KSD wzbudziły we mnie zainteresowanie innymi protokołami komunikacyjnymi. W [28] przeanalizowaliśmy problem kwantowej teleportacji z niedoskonałym klasycznym kanałem komunikacyjnym i pokazaliśmy jak wpływa to na wierność procesu.

Innym rozważanym przez nas protokołem był problem złożoności komunikacyjnej oparty na nierówności CGLMP [CGLMP02]. Rozważyliśmy jego rozwiązanie przy użyciu dwóch typów zasobów: kwantowej komunikacji i splątania. W [49] odkryliśmy zaskakujący fakt: zasoby te są ekwiwalentne dla tego problemu, ale tylko do wymiaru 7. Powyżej tego kwantowa komunikacja staje się bardziej efektywna.

KSD są ciągle rozwijane i, razem ze współpracownikami, prowadzę wiele projektów z nimi związanych. W tej sekcji opisuję dwa projekty, które zaowocowały trzema pracami, a nie zostały włączone do dzieła, gdyż zostały opublikowane gdy przygotowania wniosku habilitacyjnego były już dość zaawansowane.

Pierwszy z nich zainspirowany został przez [49] gdzie odkryliśmy sprzeczne z intuicją właściwości ekwiwalencji kwantowej komunikacji i splątania jako zasobów. Zdecydowaliśmy się sprawdzić czy podobne efekty pojawiają się dla KKSD i stworzyliśmy nowy protokół specjalnie do tego celu. W nim trzy strony komunikują się sekwencyjnie. Pierwsze dwie kodują różne części danych wejściowych podczas gdy ostatnia jest odbiorcą tak jak w standardowym przypadku. Pokazaliśmy, że to samo prawdopodobieństwo sukcesu jak w przypadku 2 stron może być osiągnięte, ale tylko przy użyciu jednego z zasobów. To którego zależy od tego jak dane wejściowe rozdzielone są pomiędzy dwóch pierwszych użytkowników [51]. Z drugiej strony dla standardowych KSD sytuacja jest znacznie prostsza i dla każdego wymiaru większego niż 2 kwantowa komunikacja jest bardziej efektywnym zasobem [50].

Drugi projekt jest uogólnieniem [H]. W [52] rozwijaliśmy dalej idee z tamtej pracy badając związek pudeł PR z bardziej ogólnymi KSD. Oprócz badania przypadków pozwalających lub nie na komunikację szybszą niż światło badaliśmy także ilość Pudeł-PR potrzebna do symulacji Pudeł-KSD.

[A] M. Pawłowski, N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

[B] M. Pawłowski, A. Winter, Hyperbits: the information quasiparticles, Phys. Rev. A **85**, 022331 (2012).

[C] H-W. Li, M. Pawłowski, Z-Q. Yin, G-C. Guo, Z-F. Han, Semi-device independent random number expansion protocol with n to 1 quantum random access codes Phys. Rev. A **85**, 052308 (2012).

[D] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, Z.-F. Han, Relationship between semi- and fully-device-independent protocols, Phys. Rev. A **87**, 020302(R) (2013).

[E] J. Ahrens, P. Badziąg, M. Pawłowski, M. Żukowski, M. Bourennane, Experimental Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **112**, 140401 (2014).

[F] S. Muhammad, A. Tavakoli, M. Kurant, M. Pawłowski, M. Żukowski, M. Bourennane, Quantum bidding in Bridge, Phys. Rev. X **4**, 021047 (2014).

[G] P. Mironowicz, H.-W. Li, M. Pawłowski, Properties of dimension witnesses and their semi-definite programming relaxations, Phys. Rev. A **90**, 022322 (2014).

[H] A. Grudka, K. Horodecki, M. Horodecki, W. Kłobus, M. Pawłowski, When Are Popescu-Rohrlich Boxes and Random Access Codes Equivalent?, Phys. Rev. Lett. **113**, 100401 (2014).

[I] M. Dall'Arno, E. Passaro, R. Gallego, M. Pawłowski, A. Acin, Attacks on semi-device independent quantum protocols, QIC **15**, 0037 (2015).

[J] H.-W. Li, Z.-Q. Yin, M. Pawłowski, G.-C. Guo, Z.-F. Han, Detection efficiency and noise in a semi-device-independent randomness-extraction protocol, Phys. Rev. A **91**, 032305 (2015).

[11] D. Aerts, M. Czachor, M. Pawłowski, Entangled-state cryptographic protocol that remains secure even if nonlocal hidden variables exist and can be measured with arbitrary precision", Phys. Rev. A **73**, 034303 (2006).

[12] M. Pawłowski, M. Czachor, Degree of entanglement as a physically ill-posed problem: The case of entanglement with vacuum", Phys. Rev. A **73**, 042111 (2006).

[13] D. Aerts, M. Czachor, M. Pawłowski, Security in quantum cryptography vs. nonlocal hidden variables, AIP Conference Proceedings **889**, 71-78 (2007).

[14] M. Pawłowski, Č. Brukner, Monogamy of Bell's inequality violations in non-signaling theories , Phys. Rev. Lett. **102**, 030403 (2009).

[15] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Żukowski, Information Causality as a Physical Principle , Nature **461**, 1101 (2009).

[16] J. Allcock, N. Brunner, M. Pawłowski, V. Scarani, Recovering part of the quantum boundary from information causality, Phys. Rev. A **80**, 040103(R) (2009).

[17] D. Manzano, M. Pawłowski, Č. Brukner, The speed of quantum and classical learning for performing the k-th root of NOT, New J. Phys. **11**, 113018 (2009).

[18] M. Pawłowski, M. Żukowski, Entanglement assisted random access codes, Phys. Rev. A **81**, 042326 (2010).

[19] M. Pawłowski, K. Horodecki, P. Horodecki, R. Horodecki, Local bounds with reduced entropy, in: R. Horodecki, S. Kilin, J. Kowalik (Eds.), Quantum Cryptography and Computing, IOS Press, Amsterdam, (2010).

[20] M. Pawłowski, M. Żukowski, The depth of obviousness, Scientific American (Polish edition), **228**, 48 (2010).

[21] M. Pawłowski, Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations, Rev. A **82**, 032313 (2010).

[22] M. Pawłowski, J. Kofler, T. Paterek, M. Seevinck, Č. Brukner, Nonlocal setting and outcome information for violation of Bell's inequality , New J. Phys. **12**, 083051 (2010).

[23] T. Paterek, M. Pawłowski, M. Grassl, Č. Brukner, On the connection between mutually unbiased bases and orthogonal Latin squares, Phys. Scr. **T140**, 014031 (2010) .

[24] R. Augusiak, T. Fritz, M. Kotowski, M. Kotowski, M. Pawłowski, M. Lewenstein, A. Acín, Tight Bell inequalities with no quantum violation from qubit unextendible product bases, Phys. Rev. A **85**, 042113 (2012).

[25] M. Pawłowski, Reply to "Comment on 'Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations' ", Rev. A **82**, 032313 (2010).

[26] M. Huber, M. Pawłowski, Weak randomness in device independent quantum key distribution and the advantage of using high dimensional entanglement, Phys. Rev. A **88**, 032309 (2013).

[27] P. Mironowicz, M. Pawłowski, Robustness of quantum randomness expansion protocols in the presence of noise, Phys. Rev. A **88**, 032319 (2013).

[28] R. Weinar, W. Laskowski, M. Pawłowski, Activation of entanglement in teleportation, J. Phys. A **46**, 435301 (2013).

[29] J. Bang, J. Ryu, S. Yoo, M. Pawłowski, J. Lee, Strategy for quantum algorithm design assisted by machine learning, New Journal of Physics **16**, 073017 (2014).

[30] P. Horodecki, M. Pawłowski, R. Horodecki, Intrinsic asymmetry with respect to adversary: new feature of Bell inequalities, J. Phys. A: Math. Theor. **47**, 424016 (2014).

[31] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, R. Ramanathan, Free randomness amplification using bipartite chain correlations, Phys. Rev. A **90**, 032322 (2014).

[32] J. Bouda, M. Pawłowski, M. Pivoluska, M. Plesch, Device-independent randomness extraction for arbitrarily weak min-entropy source, Phys. Rev. A **90**, 032313 (2014).

[33] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, A. Acín, Elemental and tight monogamy relations in nonsignalling theories, Phys. Rev. A **90**, 052323 (2014).

[34] M. Pawłowski, V. Scarani, Information causality, *Quantum Theory: Informational Foundations and Foils* Chiribella, Spekkens Edts., Springer (2015).

[35] P. Mironowicz, R. Gallego, M. Pawłowski, Robust amplification of Santha-Vazirani sources with three devices, Phys. Rev. A **91**, 032317 (2015).

[36] Ł. Czekaj, M. Pawłowski, T. Vertesi, A. Grudka, M. Horodecki, R. Horodecki, Quantum advantage for distributed computing without communication, Phys. Rev. A **92**, 032122 (2015).

[37] D. Saha, M. Pawłowski, Structure of quantum and broadcasting nonlocal correlations, Phys. Rev. A **92** 062129 (2015).

[38] A. Tavakoli, S. Zohren, M. Pawłowski, Maximal Non-Classicality in Multi-Setting Bell Inequalities, J. Phys. A: Math. and Theor. **49**, 145301 (2016).

[39] M. Pivoluska, M. Pawłowski, M. Plesch, Tight bound on the classical value of generalized Clauser-Horne-Shimony-Holt games, Phys. Rev. A **94**, 022338 (2016).

[40] A. Dutta, M. Pawłowski, M. Żukowski, Detection-efficiency loophole and the Pusey-Barrett-Rudolph theorem, Phys. Rev. A **91**, 042125 (2015).

[41] J. Bowles, N. Brunner M. Pawłowski, Testing dimension and nonclassicality in communication networks, Phys. Rev. A **92**, 022351 (2015).

[42] J. Bang, J. Ryu, M. Pawłowski, B. S. Ham, J. Lee, Quantum-mechanical machinery for rational decision-making in classical guessing game, Scientific Reports **6**, 21424 (2016).

[43] Z.-P. Xu, D. Saha, H.-Y. Su, M. Pawłowski, J.-L. Chen, Reformulating noncontextuality

inequalities in an operational approach, Phys. Rev. A **94**, 062103 (2016).

[44] H.-W. Li, M. Pawłowski, R. Rahaman, G.-C. Guo, Z.-F. Han, Device and semi-device independent random numbers based on non-inequality paradox, Phys. Rev. A **92**, 022327 (2015).

[45] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski, M. Bourennane, Increased Certification of Semi-device Independent Random Numbers using Many Inputs and More Postprocessing, New J. Phys. **18**, 065004 (2016).

[46] H. Wojewodka, F.G.S.L. Brandao, A. Grudka, M. Horodecki, K. Horodecki, P. Horodecki, M. Pawłowski, R. Ramanathan, Amplifying the randomness of weak sources correlated with devices,IEEE Transactions on Information Theory, **63**, 7592 (2017).

[47] R. Rahaman, M. G. Parker, P. Mironowicz, M. Pawłowski, Dimensional discontinuity in quantum communication complexity at dimension seven, Phys. Rev. A **92**, 062304 (2015).

[48] E. A. Aguilar, R. Ramanathan, J. Kofler, M. Pawłowski, Completely Device Independent Quantum Key Distribution, Phys. Rev. A **94**, 022305 (2016).

[49] A. Tavakoli, M. Pawłowski, M. Żukowski, M. Bourennane The Magical Number Seven: An Unexpected Dimensional Threshold in Quantum Communication Complexity, Phys. Rev. A **95**, 020302R (2017).

[50] A. Tavakoli, B. Marques, M. Pawłowski, M. Bourennane, Spatial versus Sequential Correlations for Random Access Coding, Phys. Rev. A **93**, 032336 (2016).

[51] A. Hameedi, D. Saha, P. Mironowicz, M. Pawłowski, M. Bourennane Complementarity between entanglement-assisted and quantum distributed random access code, Phys. Rev. A 95, 052345 (2017).

[52] A. Chaturvedi, M. Pawłowski, K. Horodecki, Random access codes and non-local resources, Phys. Rev. A **96**, 022125 (2017).

[S97] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J.Sci.Statist.Comput., **41(2)**, 303 (1997).

[BB84] C. H. Bennett, G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, 175 (1984).

[LYW11] H-W Li, Z-Q Yin, Y-C Wu, X-B Zou, S. Wang, W. Chen, G-C Guo, Z-F Han, Phys. Rev. A **84**, 034301, (2011).

[BCD01] H. Buhrman, R. Cleve, W. van Dam, SIAM J.Comput. **30**, 1829-1841 (2001).

[GBHA10] R. Gallego, N. Brunner, C. Hadley, A. Acin, Phys. Rev. Lett. **105**, 230501, (2010).

[CLMW10] T. S. Cubitt, D. Leung, W. Matthews, A. Winter, Improving zero-error classical communication with entanglement, Phys. Rev. Lett. **104**, 230503 (2010).

[BZPZ04] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004).

[OW10] J. Oppenheim, S. Wehner, The uncertainty principle determines the non-locality of quantum mechanics, Science, **330**, 1072 (2010).

[BBLMTU06] G. Brassard, H. Buhrman, N. Linden, A.A. Méthot, A. Tapp, F. Unger, Phys. Rev. Lett. **96**, 250401 (2006).

[ANTV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Journal of the ACM **49**, 1 (2002).

[ALMO08] A. Ambainis, D. Leung, L. Mancinska, M. Ozols, arXiv:0810.2937, (2008).

[HINRY06] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond and S. Yamashita, N. J. Phys. **8**, 129, (2006).

[CGS08] A. Casaccino, E. F. Galvao, S. Severini, Phys. Rev. A **78**, 022310 (2008).

[SBKTP09] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, G. J. Pryde, Preparation contextuality powers parity-oblivious multiplexing, Phys. Rev. Lett. **102**, 010401 (2009).

[M13] Csiszar and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[MY98] D. Mayers, A. Yao, *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, p. 503 Washington DC, USA, (1998).

[E91] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., **67**, 661 (1991).

[PAM10] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Random numbers certified by Bell's theorem, Nature **464**, 1021, (2010).

[K07] R. König, *de Finetti theorems for Quantum States*, PhD thesis, University of Cambridge, (2007).

[CK78] I. Csiszar and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[NPA08] M. Navascues, S. Pironio, A. Acin, New Journal of Physics **10**, 073013 (2008).

[CHSH69] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[AMP12] A. Acin, S. Massar, and S. Pironio, Phys. Rev. Lett. 108, 100402 (2012).

[LBL15] T. Lunghi, J. Bohr Brask, C. Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, N. Brunner, *A self-testing quantum random number generator*, Phys. Rev. Lett. **114**, 150501 (2015).

[PR94] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[H93] P. R. Holland, *The Quantum Theory of Motion: An Account of the De Broglie–Bohm Causal Interpretation of Quantum Mechanics* Cambridge University Press, Cambridge (1993).

[ABBAGP10] M. Almeida, J.-D. Bancal, N. Brunner, A. Ac´in, N. Gisin, S. Pironio, Phys. Rev. Lett. **104**, 230404 (2010).

[CGLMP02] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).

[PBR12] M. F. Pusey, J. Barrett, T. Rudolph, Nature Physics **8**, 476 (2012).

[CR12] R. Colbeck, R. Renner, Nature Physics **8**, 450 (2012).

[H92] L. Hardy, Phys. Rev. Lett. **68**, 2981 (1992).

[SARG04] V. Scarani, A. Ac´in, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

Gdańsk, 13.11.2017