Politechnika Śląska

UCZELNIA BADAWCZA
INICJATYWA DOSKONAŁOŚCI

# Quantum Secure Direct Communication

Piotr ZAWADZKI

Celem bezpośredniej komunikacji kwantowej (QSDC) jest realizacja poufnej komunikacji.

Bezpośrednia komunikacja kwantowa to odpowiednik szyfru.

Brak kluczy kryptograficznych – bezpieczeństwo wynika z praw fizyki.

# Agenda

Wprowadzenie

Formalizm

Idea kwantowego utajniania informacji

Analiza wybranych protokołów

Realizacje praktyczne

# Łatwą czy trudną mechanika kwantowa jest?

Quantum mechanics is astonishingly simple—once you take the physics out of it! In fact, QM isn't even "physics" in the usual sense: it's more like an operating system that the rest of physics runs on as application software. It's a certain generalization of the laws of probability. It says nothing directly about electrons, photons, or anything like that. It just talks about lists of complex numbers called amplitudes: how these amplitudes change as a physical system evolves, and how to convert them into the probability of seeing this or that result when you measure the system. And everything you've ever heard about the "weirdness of the quantum world," is simply different logical consequences of this one change to the rules of probability.
This makes QM, as a subject, possibly more computer-science friendly than any other part of physics.

Scott Aaronson (wywiad dla Scientific American)

Mechanika kwantowa jest uznawana za dziedzinę trudną. Niektórzy z wykładowców w celu zachęcenia studentów do nauki na wstępie wykładu zaprzeczają tej obiegowej opinii. Ja jednak nie zgadzam się z takim podejściem, uważam bowiem, że nie ma nic bardziej demoralizującego dla studenta usiłującego zrozumieć określone zagadnienie jak zakomunikowanie mu, że jest ono łatwe. Dlatego powiedzmy sobie otwarcie na wstępie – mechanika kwantowa jest trudną dziedziną ze względu na przewidywania sprzeczne z naszą intuicją i bardzo abstrakcyjne sformułowanie. Podstawowa trudność tkwi w oderwaniu się od naszej intuicji i przyzwyczajeń nabytych podczas obcowania ze światem makroskopowym. Mechanika kwantowa jest trudna – jednak nie ma drogi na skróty umożliwiającej ogarnięcie jej pojęć bez wysiłku umysłowego.

Piotr Zawadzki, *Mechanika kwantowa dla studentów Teleinformatyki*

# Aksjomaty mechaniki kwantowej

## Aksjomat 1. Stany

Stany układu kwantowego opisane są przez unormowane elementy przestrzeni Hilberta.

## Notacja Diraca

ket – elementy przestrzeni – wektory kolumnowe – $|\cdot\rangle$,

bra – wektory wierszowe – $\langle\cdot| = |\cdot\rangle^H$,

bracket – iloczyn skalarny wektorów $\langle\psi|\phi\rangle = \overline{\langle\phi|\psi\rangle}$.

## Aksjomat 2. Ewolucja

Ewolucję układu **izolowanego** opisuje operator unitarny.

## Operatory unitarne

$[U]^H = [U]^{-1}$

Chodzi o zachowanie kątów: $|\psi'\rangle = [U]\,|\psi\rangle$, $|\phi'\rangle = [U]\,|\phi\rangle$, $\langle\psi'|\phi'\rangle = \langle\phi|\,[U]^H[U]\,|\psi\rangle = \langle\psi|\phi\rangle$.

**Ewolucje** izolowanych układów kwantowych są opisane przez **obroty** w przestrzeni Hilberta.
**Stany** to po prostu **wersory** różnych kierunków.

# Aksjomaty mechaniki kwantowej

## Aksjomat 3. Pomiar

Mierzalnym wielkościom fizycznym (obserwablom) odpowiadają operatory hermitowskie. Wynikiem pomiaru jest jedna z wartości własnych wybrana losowo z prawdopodobieństwem równym długości rzutu odpowiadającego jej wektora własnego na wektor opisujący stan układu mierzonego. Układ mierzony po pomiarze pozostaje w stanie własnym odpowiadającym uzyskanemu wynikowi pomiaru.

## Operatory hermitowskie $[A]^H = [A]$

- zagadnienie własne $[A] |\lambda_k\rangle = \lambda_k |\lambda_k\rangle$, zatem $[A] = \sum_k \lambda_k |\lambda_k\rangle\langle\lambda_k|$,
- rzeczywiste wartości własne $\lambda_k$,
- wektory własne $|\lambda_k\rangle$ rozpinają przestrzeń stanów,
- rozkład spektralny $|\psi\rangle = c_0 |\lambda_0\rangle + c_1 |\lambda_1\rangle + \ldots c_D |\lambda_D\rangle$, $c_k = \langle\lambda_k|\psi\rangle$,
- pomiar – **losowy** wybór jednego z wektorów rozkładu spektralnego jako stanu końcowego, prawdopodobieństwo wyboru wynosi $p_k = |c_k|^2$, wynikiem pomiaru jest $\lambda_k$.

- Rachunek prawdopodobieństwa jest wbudowany w mechanikę kwantową,
- Pomiar kwantowy ma charakter niszczący – historia stanu zostaje zamazana.
- Stan układu nie jest modyfikowany gdy układ znajduje się w stanie własnym mierzonej obserwabli.

Uzasadnienie słuszności tego idealistycznego modelu na gruncie fizyki jest trudne – należy jednocześnie analizować obiekty mikro- i makroskopowe.

Allahverdyan, Armen E. et al. "A sub-ensemble theory of ideal quantum measurement processes." Annals of Physics 376 (2017): 324-352.

# Aksjomaty mechaniki kwantowej

## Aksjomat 4. Składanie/kompozycja układów

Przestrzeń stanów układu złożonego z podukładów $\mathrm{A}$ i $\mathrm{B}$ budujemy jako iloczyn tensorowy (Kroneckera) przestrzeni opisujących podukłady tj. $\mathcal{H}_{\mathrm{AB}} = \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$.

## Baza przestrzeni stanów układu złożonego

Operacyjnie oznacza to, że baza nowej przestrzeni jest zbudowana jako iloczyn Kroneckera wektorów bazowych przestrzeni składowych na zasadzie każdy z każdym. Zatem wymiar $|\mathcal{H}_{\mathrm{AB}}| = |\mathcal{H}_{\mathrm{A}}||\mathcal{H}_{\mathrm{B}}|$.

## Splątanie stanów

Niektóre ze stanów układu złożonego da się przedstawić jako iloczyn Kroneckera stanów zdefiniowanych w podukładach

$$|\psi_{\mathrm{AB}}\rangle = |\alpha_{\mathrm{A}}\rangle\, |\beta_{\mathrm{B}}\rangle$$

Stany takie nazywamy **separowalnymi**. Pozostałe to stany **splątane**.

- ☛ Liczba stopni swobody układu kwantowego rośnie wykładniczo z liczbą stopni swobody elementów składowych.
- ✗ Możliwości obliczeniowe dostępnego obecnie sprzętu są niewystarczające do analizy już stosunkowo prostych układów kwantowych.

# Interpretacje mechaniki kwantowej

## Model matematyczny działa znakomicie, niestety filozofowie mają problem

- Copenhagen,
- Hidden variables theory applied to subsystems,
- Hidden variables theory applied to entire universe,
- Many worlds,
- Collapse theories,
- Consistent histories,
- QBism,
- Relational quantum mechanics,
- CSM (contexts, systems, and modalities) approach,
- ETH approach.

Frauchiger, D., Renner, R. Nature Communications 9, 3711 doi:10.1038/s41467-018-05739-8, 2018

# Formalizm

# Operatory jedno-qubitowe

## Qubit — element dwuwymiarowej przestrzeni Hilberta

$\mathcal{H}_2$ – $|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$, $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$, $\langle a|b\rangle = 0$.

## Baza obliczeniowa

Niech wektory $\{|0\rangle, |1\rangle\}$ stanowią pewną bazę $\mathcal{H}_2$. WLOG $|0\rangle = [1, 0]^T$, $|1\rangle = [0, 1]^T$.

## Bramki, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

identyczność $[Id] = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $[Id]|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

zmiana fazy $[Z] = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $[Z]|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$,

odwrócenie bitu $[X] = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $[X]|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$,

? $j[Y] = [Z][X] = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $j[Y]|\psi\rangle = -\alpha|1\rangle + \beta|0\rangle$

# Operatory jedno-qubitowe

## Baza dualna

Wektory własne $[X]$: $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, rozkład spektralny: $[X] = |+\rangle\langle+| - |-\rangle\langle-|$

## Bramka Hadamarda $\quad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

Konwersja qubitów pomiędzy bazą obliczeniową i dualną: $[H] = |+\rangle\langle 0| + |-\rangle\langle 1|$, $[H]\,|\psi\rangle = \alpha\,|+\rangle + \beta\,|0\rangle$, $[H][H] = [Id]$,
$[H] = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$,

## Pomiar w niekompatybilnej bazie

Niech $|\psi\rangle = |-\rangle$ i mierzymy $[Z] = |0\rangle\langle 0| - |1\rangle\langle 1|$, zatem $\lambda_0 = +1$, $\lambda_1 = -1$, $|\lambda_0\rangle = |0\rangle$, $|\lambda_1\rangle = |1\rangle$. Mamy $|\psi\rangle = \frac{1}{\sqrt{2}}\,|\lambda_0\rangle + \frac{1}{\sqrt{2}}\,|\lambda_1\rangle$ i $|c_0|^2 = \frac{1}{2}$, $|c_1|^2 = \frac{1}{2}$. Zatem z $p = \frac{1}{2}$ wynikiem będzie $+1$ a stan qubitu po pomiarze pozostanie w stanie $|\lambda_0\rangle = |0\rangle$ lub $p = \frac{1}{2}$ wynikiem będzie $-1$ a stan qubitu po pomiarze pozostanie w stanie $|\lambda_1\rangle = |1\rangle$.
Dokładnie tak samo gdy $|\psi\rangle = |0\rangle$ lub $|\psi\rangle = |1\rangle$ i mierzymy $[X]$ to $p(+1) = p(-1) = \frac{1}{2}$.
Prawdopodobieństwo można wyliczyć bo znamy stan układu przed pomiarem.

# Operatory dwu-qubitowe

## Bramka $[CX]$ (Kontrolowane $[X]$)

Działa na dwóch qubitach: kontrolnym i docelowym $[CX_{\mathrm{ct}}] = |0\rangle\langle 0|_{\mathrm{c}} \otimes [Id]_{\mathrm{t}} + |1\rangle\langle 1|_{\mathrm{c}} \otimes [X]_{\mathrm{t}}$

## Generacja splątania

$$[CX_{\mathrm{AB}}][H]_{\mathrm{A}} |0_{\mathrm{A}}\rangle |0_{\mathrm{B}}\rangle = [CX_{\mathrm{AB}}] |+_{\mathrm{A}}\rangle |0_{\mathrm{B}}\rangle = \frac{1}{\sqrt{2}}[CX_{\mathrm{AB}}] \left(|0_{\mathrm{A}}\rangle |0_{\mathrm{B}}\rangle + |1_{\mathrm{A}}\rangle |0_{\mathrm{B}}\rangle\right) = \frac{1}{\sqrt{2}} \left(|0_{\mathrm{A}}\rangle |0_{\mathrm{B}}\rangle + |1_{\mathrm{A}}\rangle |1_{\mathrm{B}}\rangle\right) = |\beta_{00}\rangle_{\mathrm{AB}}$$

## Właściwości

Ogólnie mamy 4 pary EPR tworzące bazę w przestrzeni rozpiętej na dwóch qubitach

$$[CX_{\mathrm{AB}}][H]_{\mathrm{A}} \left|\mu_{\mathrm{A}}\right\rangle \left|\nu_{\mathrm{B}}\right\rangle = \left|\beta_{\mu\nu}\right\rangle_{\mathrm{AB}}$$

Pomiar Bella to zabieg służący do identyfikacji pary – urządzenie do generacji jest odwracalne

$$[H]_{\mathrm{A}}[CX_{\mathrm{AB}}] \left|\beta_{\mu\nu}\right\rangle_{\mathrm{AB}} = \left|\mu_{\mathrm{A}}\right\rangle \left|\nu_{\mathrm{B}}\right\rangle$$

Dostęp do jednego qubitu pary umożliwia jej konwersję na dowolną inną

$$[Z]_{\mathrm{A}}^{m}[X]_{\mathrm{A}}^{n} \left|\beta_{\mu\nu}\right\rangle_{\mathrm{AB}} = (-1)^{\mu n} \left|\beta_{\mu\oplus m,\nu\oplus n}\right\rangle_{\mathrm{AB}}$$

# Lokalne pomiary współdzielonej pary Bella

## Pomiary w zgodnych bazach

Para $|\beta_{00}\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle + |1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle)$, mierzymy $[Z]_{\mathrm{A}}$, a potem $[Z]_{\mathrm{B}}$.

Wynikiem pierwszego pomiaru jest z $p = \frac{1}{2}$:

- "$+1_{\mathrm{A}}$" i stan po pomiarze $|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle$ lub,
- "$-1_{\mathrm{A}}$" i stan po pomiarze $|1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle$.
- Jeżeli wynikiem pierwszego pomiaru jest "$+1_{\mathrm{A}}$" to wynikiem drugiego **musi** być "$+1_{\mathrm{B}}$".
- Jeżeli wynikiem pierwszego pomiaru jest "$-1_{\mathrm{A}}$" to wynikiem drugiego **musi** być "$-1_{\mathrm{B}}$".

**Pełna korelacja wyników pomiarów**.

## Pomiary w niekompatybilnych bazach

Para $|\beta_{00}\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle + |1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle)$, mierzymy $[Z]_{\mathrm{A}}$ a potem $[X]_{\mathrm{B}}$.

Wynikiem pierwszego pomiaru jest z $p = \frac{1}{2}$:

- sytuacja po pierwszym pomiarze jest taka sama,
- Jeżeli wynikiem pierwszego pomiaru jest "$+1_{\mathrm{A}}$" to wynikiem drugiego **może** być "$\pm 1$" z $p = \frac{1}{2}$,
- Jeżeli wynikiem pierwszego pomiaru jest "$-1_{\mathrm{A}}$" to wynikiem drugiego **może** być "$\pm 1$" z $p = \frac{1}{2}$,

**Całkowity brak korelacji wyników pomiarów**.

# Operator gęstości stanów

## Wartość oczekiwana pomiaru obserwabli

- stan czysty: $\langle\psi|[A]|\psi\rangle = \sum_k \lambda_k |\langle\lambda_k|\psi\rangle|^2 = \langle[A]\rangle$.
- Mieszanina stanów $\left\{\left|\psi^{(k)}\right\rangle\right\}$, suma udziałów $\sum r_k = 1$.

## Operator gęstości stanów: $[\rho] = \sum_k r_k \left|\psi^{(k)}\right\rangle\!\left\langle\psi^{(k)}\right|$

Wartość oczekiwana obserwabli

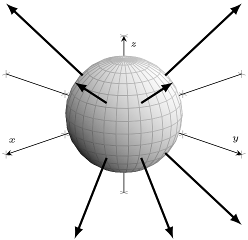
$$\langle[A]\rangle = \mathrm{Tr}\left\{[\rho][A]\right\}$$

Właściwości:

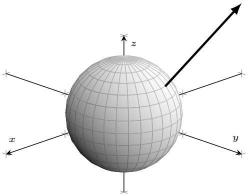
- hermitowski,
- dodatnio określony,
- $\mathrm{Tr}\left\{[\rho]\right\} = 1$.

# Klasyczne analogi operatora gęstości stanów

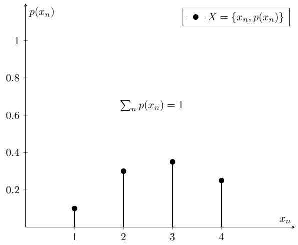
Operator gęstości stanów:



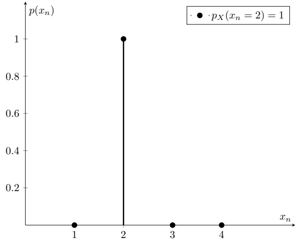

Wektor stanu:




Klasyczna zmienna losowa




Zmienna dyskretna



# Entropia von Neumanna

## Obliczanie funkcji dla operatorów hermitowskich

Zagadnienie własne $[A]|\lambda_k\rangle = \lambda_k|\lambda_k\rangle$. Mamy

$$[A]^2|\lambda_k\rangle = \lambda_k^2|\lambda_k\rangle$$

$$(a_N[A]^N + \ldots + a_1[A] + a_0)|\lambda_k\rangle = (a_N\lambda_k^N + \ldots + a_1\lambda_k + a_0)|\lambda_k\rangle$$

$$f([A])|\lambda_k\rangle = f(\lambda_k)|\lambda_k\rangle$$

## Entropia von Neumanna

$$S([\rho]) = -\operatorname{Tr}\{[\rho]\ln[\rho]\} = \langle -\ln[\rho]\rangle = -\sum_k \lambda_k \ln \lambda_k$$

## Entropia stanu czystego

$[\rho] = |\psi\rangle\langle\psi|$, $k = 1$, $|\lambda_1\rangle = |\psi\rangle$, $\lambda_1 = 1$, $S([\rho]) = 0$.

## Ślad częściowy

Niech $[\rho]_{\mathrm{AB}}$ będzie operatorem gęstości układu dwuskładnikowego. Układ $B$ jest niedostępny pomiarowo. Chcemy znaleźć operator $[\rho]_{\mathrm{A}}$, który dla wszystkich obserwabli określonych w "A" da tą samą wartość oczekiwaną co $\mathrm{Tr}\left\{[\rho]_{\mathrm{AB}}\left([A]_{\mathrm{A}}\otimes[Id]_{\mathrm{B}}\right)\right\}$.
Jedyną taką operacją jest ślad częściowy zdefiniowany jako $[\rho]_{\mathrm{A}}=\mathrm{Tr}_{\mathrm{B}}\left\{[\rho]_{\mathrm{AB}}\right\}=\sum_k \langle k_{\mathrm{B}}|[\rho]_{\mathrm{AB}}|k_{\mathrm{B}}\rangle$.

- Operator gęstości czystego qubitu $[\rho]=|0\rangle\langle 0|$. Mamy $\langle[Z]\rangle=1$, $\langle[X]\rangle=0$.
- Operator gęstości mieszaniny qubitów $[\rho]=\frac{1}{2}|0\rangle\langle 0|+\frac{1}{2}|1\rangle\langle 1|$. Niezależnie od obserwabli mamy $\langle[Z]\rangle=\langle[X]\rangle=0$.
- Niech $[\rho]_{\mathrm{AB}}=|\beta_{00}\rangle\langle\beta_{00}|_{\mathrm{AB}}$. **Układ jest w stanie czystym**. Niech system "B" będzie niedostępny pomiarowo. Wtedy

$$[\rho]_{\mathrm{A}}=\sum_{k=0}^{1}\langle k_{\mathrm{B}}||\beta_{00}\rangle\langle\beta_{00}|_{\mathrm{AB}}|k_{\mathrm{B}}\rangle=\frac{1}{2}|0\rangle\langle 0|_{\mathrm{A}}+\frac{1}{2}|1\rangle\langle 1|_{\mathrm{A}}$$

  Dla obserwatora **w układzie "A" para EPR** wygląda jak **statystyczna mieszanina** qubitów.
- entropia von Neumana ($S([\rho_{\mathrm{A}}])=1$) jest równa entropii Shannona losowego bitu.

# Idea kwantowego utajniania informacji

# Trochę historii

## Najpierw była kryptografia kwantowa ...

- połowa lat 70-tych – Wiesner usiłuje opublikować system Quantum Money - odrzucone przez czasopisma,
- 1982 – Feynmann postuluje konieczność konstrukcji komputerów kwantowych,
- 1983 – Benioff proponuje kwantowy odpowiednik maszyny Turinga,
- 1983 – reprint pracy Wiesnera,
- 1984 – Bennet, Brassard – BB84 – pierwszy protokół QKD,
- ...kryptografia kwantowa to interesująca nisza badawcza.
- 1994 – Shor – probabilistyczny algorytm faktoryzacji liczb w czasie wielomianowym.
- ... – od tego czasu obserwuje się lawinowy wzrost zainteresowania możliwościami zastosowania kwantowych metod przetwarzania informacji do różnych celów – głównie **Kryptografia** i **Obliczenia kwantowe**.

# Kamienie milowe QSDC

**TABLE 1.** Timeline of important milestones in QSDC's theoretical and experimental contributions.

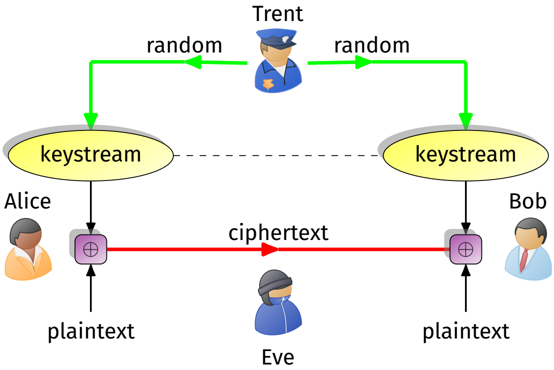
**TABLE 1.** Timeline of important milestones in QSDC's theoretical and experimental contributions.

| Theoretical proposals | | Experimental demonstrations |
|---|---|---|
| Long *et al.* [36] proposed a high-capacity QSDC protocol. | 2000 | |
| Deng *et al.* [37] proposed a two-step QSDC protocol. | 2003 | |
| Deng *et al.* [38] created a QSDC protocol using single photons (DL04). Yan and Zhang [52] proposed a QSDC protocol using teleportation. | 2004 | |
| Wang *et al.* [53] conceived a high-dimensional two-step QSDC protocol. | 2005 | |
| Murakami *et al.* [54] proposed a QSDC scheme based on singe-qubit. | 2007 | |
| Lin *et al.* [55] designed a QSDC protocol using $\chi$-state. | 2008 | |
| Shi *et al.* [56] proposed a QSDC scheme based on three-dimensional hyperentanglement. | 2011 | |
| Yoon *et al.* [57] used QSDC to design quantum signature. | 2014 | |
| Naseri *et al.* [58] proposed a N-users QSDC network. Cao *et al.* [59] provided a quantum secure direct communication scheme in the non-symmetric channel. | 2015 | |
| Zawadzki [60] studied the attack strategies in QSDC. Zarmehi and Houshmand [61] constructed a bidirectional QSDC network. | 2016 | Hu *et al.* [47] created a DL04 QSDC testbed relying on single-photon frequency coding. Lum *et al.* [62] used quantum data locking for high speed QSDC. |
| | 2017 | Zhang *et al.* [48] realized a two-step QSDC protocol with the aid of quantum memory. Zhang *et al.* [49] achieved long-distance transmission using this two-step QSDC protocol. |
| Zhou *et al.* [63] designed a measurement-device-independent DL04 QSDC protocol. Niu *et al.* designed a measurement-device-independent two-step QSDC protocol. Huang *et al.* [64] studies implementation vulnerabilities of QSDC. | 2018 | Sun *et al.* [50] reported the quantum-memory-free DL04 QSDC protocol. |
| Zhou *et al.* [65] proposed a device-independent two-step QSDC protocol. | 2019 | Qi *et al.* [51] constructed a practical QSDC system for intra-city applications. Shapiro *et al.* [66] used quantum low probability of intercept for high-rate QSDC. Massa *et al.* [67] realized a bi-directional QSDC. |
| | 2020 | Pan *et al.* [68] reported an experimental free-space QSDC. |

D. Pan, K. Li, D. Ruan, S. X. Ng and L. Hanzo, IEEE Access, vol. 8, pp. 121146-121161, 2020, doi: 10.1109/ACCESS.2020.3006136.

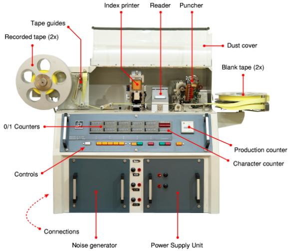
# Utajnienie informacji klasycznie

## One Time Pad



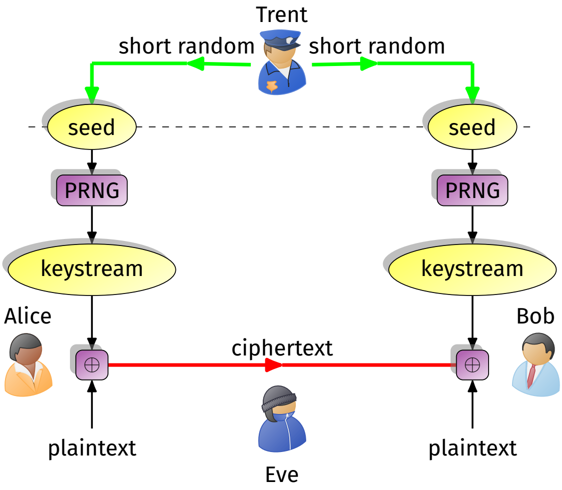

Vernam (1917), Shannon (1949)

- Izolacja informacyjna Eve oparta na kluczu współdzielonym: $I(A;E) = 0$ gdy $H(M) = H(M|C)$, i $H(M|CK) = 0$.
- ✓ Bezwarunkowe bezpieczeństwo,
- Klucz musi być losowy, zatem $H(keystream) = \mathrm{Length}(keystream)$,
- ✗ Klucz dłuższy niż tekst jawny,
- ✗ klucz może być użyty jednokrotnie.




cryptomuseum.com

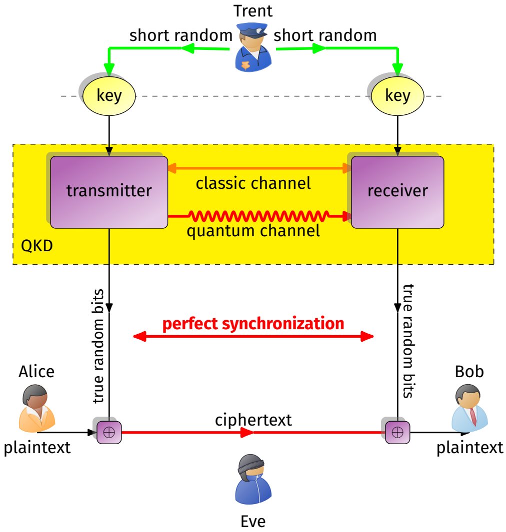
# Utajnienie informacji klasycznie
## Szyfry strumieniowe




- ✓ Klucz inicjujący PRNG jest znacznie krótszy niż tekst jawny,
- ☛ ale musi być odnawiany co pewien czas,
- ✗ $H(keystream) = H(seed)$,
- ✗ Warunkowe bezpieczeństwo.

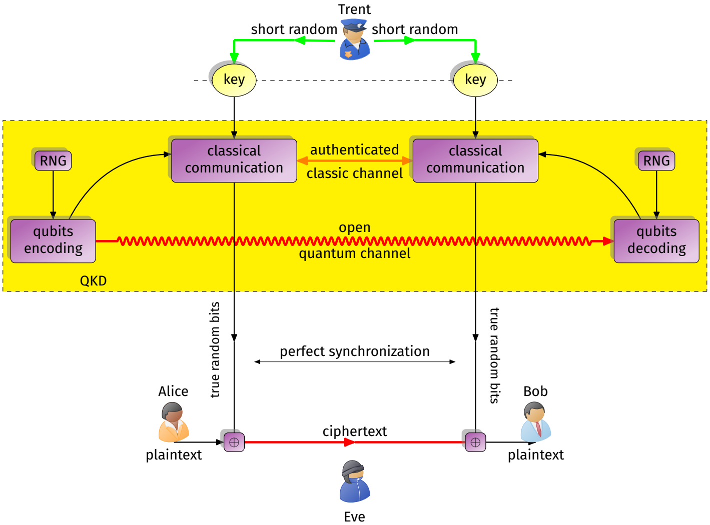
# Wspomagane kwantowo utajnianie informacji

## Kwantowa dystrybucja klucza




- ✓ Klucz inicjujący jest krótki,
- ☛ i **NIE** musi być odnawiany co pewien czas,
- ✓ $H(\mathit{keystream}) = \mathrm{Length}(\mathit{keystream})$,
- ✓ Bezwarunkowe bezpieczeństwo,
- ☛ przy założeniu, że sprzęt realizuje model matematyczny,
- ☛ i uwierzytelnienie kanału klasycznego jest bezwarunkowo bezpieczne.

# Wspomagane kwantowo utajnianie informacji
## Kwantowa dystrybucja klucza




### Komunikacja kwantowa wymaga klasycznego postprocessingu

sifting – odrzucenie cykli które nie mogły się udać,

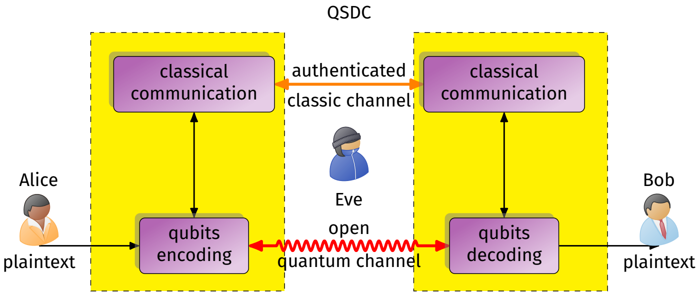
error detection and correction – estymacja stopy błędów i ich korekcja,

privacy amplification – redukcja informacji Eve o wyjściowym ciągu bitów do zera.

### Nieklasyczny prymityw kryptograficzny

QKD to sposób na synchronizację generatorów liczb losowych.

# Wspomagane kwantowo utajnianie informacji
## Poufna komunikacja kwantowa



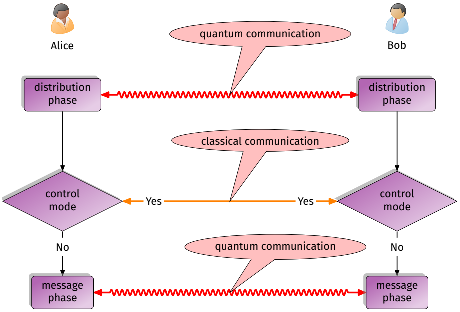

### Założenia

- Kanał klasyczny służy tylko do wymiany danych kontrolnych,
- Informacja wrażliwa przesyłana jest wyłącznie w kanale kwantowym,
- Uwierzytelnienie kanału klasycznego musi być zapewnione przez zewnętrzny prymityw.

### Nieklasyczny prymityw kryptograficzny

- ✓ Brak odwołań do szyfrów klasycznych.
- ✓ Poufność informacji wynika ze sposobu jej zakodowania w stanach kwantowych.

# Ogólna struktura protokołów




## Etapy komunikacji

1. Dystrybucja kwantowych nośników,
2. Kodowanie i transmisja informacji wrażliwej,
3. Dekodowanie.

## Najbardziej zaawansowane protokoły

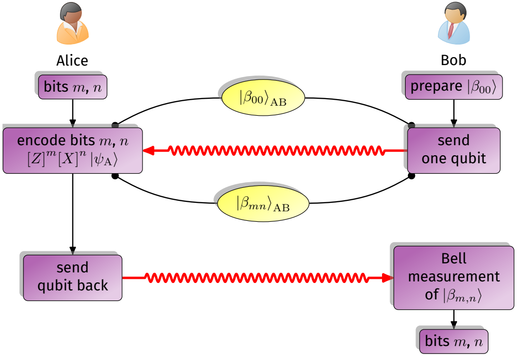
- Ping-Pong (PP) Boström, Felbinger 2002,
- Two-Step (TS) Deng, Long, Liu, 2003,
- Deng-Long (DL) Deng, Long, 2004.

Przedstawione dalej schematy nie są tożsame z oryginalnymi propozycjami i uwzględniają modyfikacje wprowadzone na dalszych etapach rozwoju oraz redukcje pozwalające na przejrzystą ilustrację różnic.

| PP | TS | DL |
|---|---|---|
| Bob przygotowuje | Alice przygotowuje | Bob losuje bity $b$ i $v$ i przygotowuje |
| $\|\Phi_{\mathrm{AB}}\rangle = \frac{\|0_{\mathrm{A}}\rangle\|0_{\mathrm{B}}\rangle+\|1_{\mathrm{A}}\rangle\|1_{\mathrm{B}}\rangle}{\sqrt{2}}$ | $\|\Phi_{\mathrm{AB}}\rangle = \frac{\|0_{\mathrm{A}}\rangle\|0_{\mathrm{B}}\rangle+\|1_{\mathrm{A}}\rangle\|1_{\mathrm{B}}\rangle}{\sqrt{2}}$ | $\|\psi_{\mathrm{B}}\rangle = [H]^b \|v\rangle$ |
| Bob $\xrightarrow{\text{qubit A}}$ Alice | Alice $\xrightarrow{\text{qubit B}}$ Bob | Bob $\xrightarrow{\|\psi_{\mathrm{B}}\rangle}$ Alice |
| Alice koduje dwa bity | Alice koduje dwa bity | Alice koduje jeden bit |

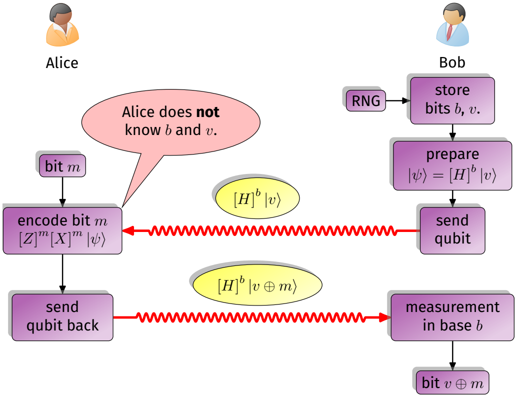
# Idea poufnego kodowania informacji w stanach kwantowych

Protokół PP




Ewa widzi: $[\rho]_{\mathrm{E}} = \mathrm{Tr}_{\mathrm{B}} \left\{ |\beta_{m,n}\rangle\langle\beta_{m,n}|_{\mathrm{AB}} \right\} = \frac{1}{2}[Id]$

Protokół DL

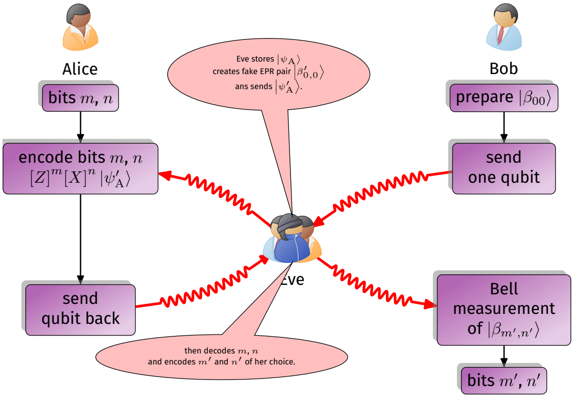



Ewa widzi:

$$[\rho]_{\mathrm{E}} = \frac{1}{4}(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|) = \frac{1}{2}[Id]$$

**Podsłuch nie ma sensu!**

# Atak MITM (intercept-resend)



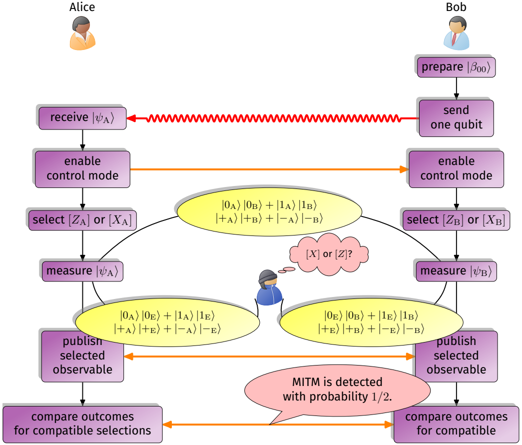

## Jednak Eve może atakować fazę dystrybucji nośników i fazę komunikacji łącznie

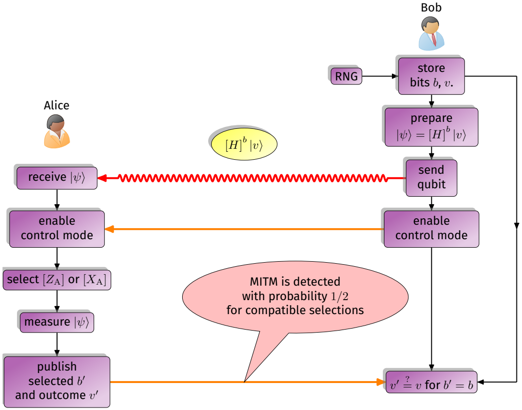
Kanał kwantowy jest **otwarty**, więc jest podatny na MITM.

# Cykle kontrolne

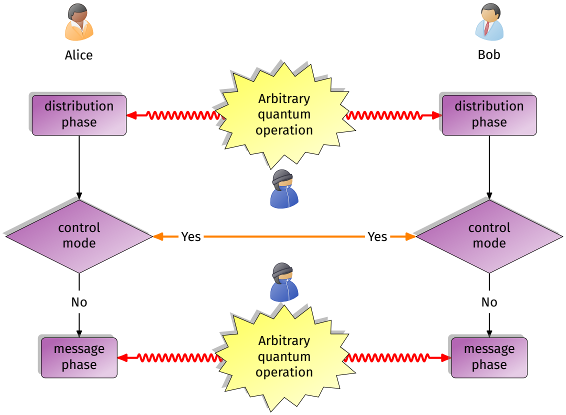
## służą do statystycznego sprawdzenia autentyczności nośników

Strony korzystają z **uwierzytelnionego** kanału klasycznego.



# Atak niekoherentny




- Eve ograniczona jest jedynie przez prawa mechaniki kwantowej, zatem na qubitach *en-route* może wykonywać dowolne operacje.
- Qubit nie jest izolowany zatem jego przekształcenia nie muszą być unitarne.
- Czy takie działania mogą dać Eve dodatkowe korzyści?

# Opis układów oddziałujących z otoczeniem

## Mapy CPTP — perspektywa lokalna

to odwzorowania w przestrzeni operatorów gęstości $[\rho] \overset{M_{\mathrm{CPTP}}}{\longrightarrow} [\rho']$:

PTP – obraz przekształcenia jest nadal operatorem gęstości,

C – można dołożyć dowolną ilość izolowanych qubitów i mapa $M$ nadal zachowa swoje właściwości.

## Operatory Krauss — perspektywa lokalna

Mapę CPTP można przedstawić jako przekształcenie postaci $[\rho'] = \sum_m [K_m][\rho][K_m]^H$.

- warunki CPTP są spełnione gdy $\sum_m [K_m]^H[K_m] = [Id]$,
- operatory $[K_m]$ są obrazem operatorów rzutowych (pomiaru) zdefiniowanych w rozszerzonej przestrzeni obejmującej otoczenie,
- otoczenie bezustannie mierzy badany układ a wyniki pomiaru są zapominane,

# Opis układów oddziałujących z otoczeniem

## Obraz Stinespringa — perspektywa globalna

Układ qubit plus otoczenie jest izolowany, zatem nieunitarne operacje na qubicie można opisać jako operacje unitarne na układzie qubit plus otoczenie

$$[\rho'] = \mathrm{Tr}_{\mathrm{Env}} \left\{ [U] \left( [\rho] \otimes [\rho_{\mathrm{Env}}] \right) [U]^H \right\}$$

## Jak bardzo należy rozszerzyć przestrzeń/perspektywę aby taki opis obejmował **wszystkie** możliwe operacje na qubicie?

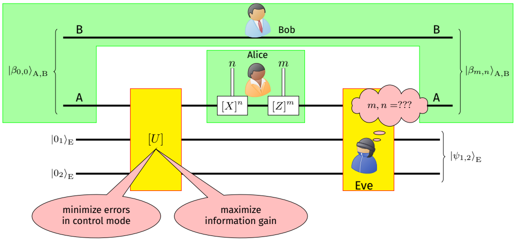
Liczba stopni swobody dodanego rozszerzenia musi być co najmniej **dwa** razy większa od wymiaru rozważanego układu.

## Bezpośrednie zastosowanie w kryptografii

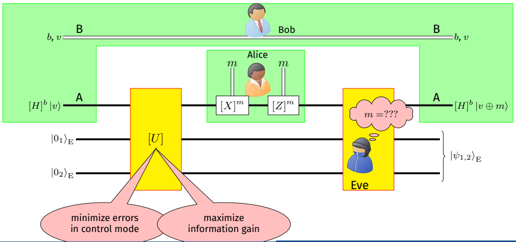
Opis wszystkich możliwych operacji na **qubicie** uzyskamy badając wszystkie operacje unitarne na układzie uzupełnionym o **dwa qubity**. Rozważanie większych układów nie ma sensu.

# Ataki niekoherentne (indywidualne)

Protokół PP




Protokół DL




## Przebieg ataku

- Eve splątuje kontrolowany przez siebie układ z dystrybuowanym qubitem,
- Alice kodując informację wpływa również na układ Eve,
- Eve badając stan dostępnego dla niej układu usiłuje odgadnąć operację wykonaną przez Alice.

## Właściwości

- dobrze dobrany tryb kontrolny wykrywa z niezerowym prawdopodobieństwem splątanie z układem Eve,
- maksymalny zysk informacyjny Eve $\max\{I(A;E)\}$ zależy monotonicznie od stopy *BER* w trybie kontrolnym,
- dla tzw. odpornych protokołów

$$\max\{I(A;E)\} \overset{BER\to 0}{=} 0,$$

tj. nie istnieje niewykrywalna operacja Eve umożliwiająca wyciek informacji.

## Oszacowanie (od góry) informacji uzyskanej przez Eve

- początkowy stan systemu $\left[\rho^{(0)}\right]_{\mathrm{BAE}} = |\beta_{00}\rangle\langle\beta_{00}|_{\mathrm{AB}} \otimes |00\rangle\langle 00|_{\mathrm{E}}$,
- stan systemu po splątaniu z systemem Eve: $\left[\rho^{(1)}\right]_{\mathrm{BAE}} = \left([Id]_{\mathrm{B}} \otimes [U]_{\mathrm{AE}}\right)\left[\rho^{(0)}\right]_{\mathrm{BAE}}\left([Id]_{\mathrm{B}} \otimes [U]^{H}_{\mathrm{AE}}\right)$,
- stan dostępny pomiarowo w trybie kontrolnym: $\left[\rho^{(2)}\right]_{\mathrm{AB}} = \mathrm{Tr}_{\mathrm{E}}\left\{\left[\rho^{(1)}\right]_{\mathrm{BAE}}\right\}$,
- stany systemu po kodowaniu Alice

$$[\rho_{m,n}]_{\mathrm{BAE}} = \left([Id]_{\mathrm{B}} \otimes [Z]^{m}_{\mathrm{A}} \otimes [Id]_{\mathrm{E}}\right)\left([Id]_{\mathrm{B}} \otimes [X]^{n}_{\mathrm{A}} \otimes [Id]_{\mathrm{E}}\right)\left[\rho^{(1)}\right]_{\mathrm{BAE}}\left([Id]_{\mathrm{B}} \otimes [X]^{n}_{\mathrm{A}} \otimes [Id]_{\mathrm{E}}\right)\left([Id]_{\mathrm{B}} \otimes [Z]^{m}_{\mathrm{A}} \otimes [Id]_{\mathrm{E}}\right)$$

- stany dostępne pomiarowo dla Eve:

$$[\rho_{m,n}]_{\mathrm{AE}} = \mathrm{Tr}_{\mathrm{B}}\left\{[\rho_{m,n}]_{\mathrm{BAE}}\right\}$$

- kres górny informacji dostępnej dla Eve (przy ustalonej transformacji $[U]_{\mathrm{AE}}$ określa kres Holevo

$$\max\left\{I(A;E)\right\} = S\left(\sum_{m,n} p_{m,n}[\rho_{m,n}]_{\mathrm{AE}}\right) - \sum_{m,n} p_{m,n} S\left([\rho_{m,n}]_{\mathrm{AE}}\right)$$

gdzie $S([\rho])$ oznacza entropię von Neumanna, a $p_{m,n}$ są prawdopodobieństwami pojawienia się symboli na wejściu kanału.

### Cel obliczeń

- Należy oszacować od góry informację dostępną dla Eve ($\max\left\{I(A;E)\right\}$) uwzględniając wszystkie możliwe ataki ($[U]_{\mathrm{AE}}$).
- Dla każdej transformacji należy wyznaczyć indukowany *BER* w trybie kontrolnym.

Analiza wybranych protokołów

# Model idealny

## Założenia

- Kanał kwantowy jest bezszumny i bezstratny,
- Jedynym źródłem błędów transmisji jest aktywność Eve.

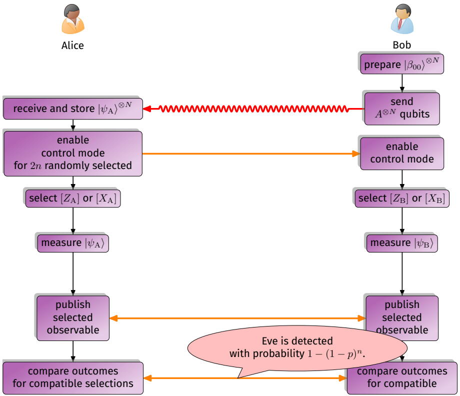
## Protokoły sekwencyjne

- Alice i Bob przesyłają informacje sekwencyjnie, bit po bicie,
- Alice i Bob wplatają losowo cykle kontrolne pomiędzy cykle informacyjne,
- dla każdego cyklu kontrolnego istnieje skończone prawdopodobieństwo $p$, że Eve zostanie wykryta,
- Eve pozostanie **ukryta** po $n$ cyklach z prawdopodobieństwem $(1-p)^n$,
- zatem, zostanie **wykryta** z prawdopodobieństwem $d(n) = 1-(1-p)^n$, $\lim_{n\to\infty} d(n) = 1$,

## Protokoły sekwencyjne są pseudo bezpieczne

- prawdopodobieństwo wykrycia rośnie z numerem cyklu,
- początkowy fragment informacji wrażliwej jest słabo zabezpieczony i może być przechwycony ze stosunkowo dużym prawdopodobieństwem.

# Protokoły blokowe




## Usunięcie quasi security jest możliwe

- Alice i Bob przesyłają qubity w blokach po $N$,
- Po dystrybucji każdego bloku na $2n$ losowo wybranych qubitach wykonywane są cykle kontrolne,
- średnio $n$ cykli ma zgodne bazy pomiarowe,
- Eve zostanie **wykryta** z prawdopodobieństwem $d(n) = 1 - (1-p)^n$, bo wystarczy jeden błąd transmisji aby przerwać transakcję,
- Alice koduje informację wrażliwą na pozostałych $(N - 2n)$ qubitach **tylko** gdy **nie wykryto** Eve,

## Przetwarzanie w blokach umożliwia dowolne podniesienie marginesu bezpieczeństwa

- ✗ Wadą jest konieczność wyposażenia stron w rejestry kwantowe przechowujące przetwarzane bloki – awykonalne przy obecnym stanie technologii.
- ✗ Uwzględnienie szumów jeszcze bardziej komplikuje powyższy scenariusz.

# QSDC w kanałach nieidealnych

## Założenia

- Kanał kwantowy wprowadza błędy i straty,
- Błędy i straty wywołane niedoskonałościami medium są **nieodróżnialne** od błędów i strat wywołanych aktywnością Eve.

## Dylematy Alice i Boba

- pesymistyczne założenie – błędy i straty należy traktować jak gdyby pochodziły od Eve, bowiem może ona zastąpić używany kanał kwantowy lepszym (w granicy idealnym) kanałem kwantowym,
- błędy są immanentną cechą transmisji kwantowej zatem nie mogą one powodować przerwania protokołu,
- Alice i Bob muszą po prostu pogodzić się z faktem, że część qubitów może być bezkarnie zaatakowana i tolerować związany z tym potencjalny wyciek części przesyłanej informacji.

## Model

Jak w ramach tego modelu zapewnić poufność przesyłanej informacji?

- Alice i Bob komunikują się korzystając z kanałów idealnych,
- Eve podsłuchuje komunikację a jej aktywność indukuje błędy zarówno na etapie dystrybucji nośników jak i transferu informacji,
- Alice i Bob tolerują błędy w trybie kontrolnym o ile ich stopa nie przekracza pewnej wartości maksymalnej $e_{\max}$,
- degradacja nośników związana z atakiem Eve powoduje również zmniejszenie informacji wzajemnej pomiędzy Alice i Bobem.

# Wykorzystanie splątania

## Kryptografia symetryczna — Shannon, 1949

Alice i Bob współdzielą ten sam **tajny** klucz. Eve jest statystycznie niezależna od informacji współdzielonej prze Alice i Boba.

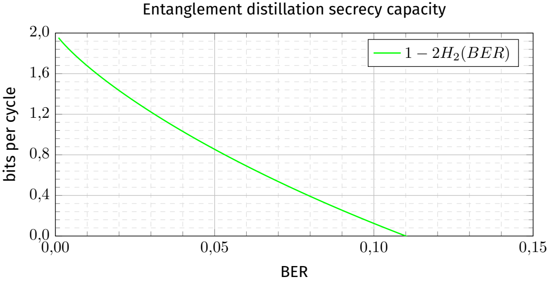
## Kwantowa odmiana paradygmatu Shannona

Alice i Bob są w stanie wymieniać informację w sposób poufny gdy współdzielą pary EPR.
Splątanie zastępuje współdzielony klucz. Para EPR jest równoważna dwóm bitom informacji poufnej.

## Destylacja splątania

From Wikipedia, the free encyclopedia
Entanglement distillation (also called entanglement purification) is the transformation of $N$ copies of an arbitrary entangled state $[\rho]$ into some number of approximately pure Bell pairs, using only local operations and classical communication (LOCC).

# Wykorzystanie splątania




## Pomysł na izolację Eve

Z bloku $N$ współdzielonych (i być może splatanych z systemem Eve) należy wydestylować $n$ **czystych** par EPR. Transmisji za pomocą czystych par Eve **nie może** podsłuchać.

Górny kres sprawności protokołu destylacji

$$\frac{n}{N} = 1 - H_2(BER_x) - H_2(BER_z)$$

$H_2(\cdot)$ – entropia Shannona, $BER$ – stopa błędów w trybie kontrolnym

Wu, J, Lin, Z, Yin, L, Long, G-L. "Security of quantum secure direct communication based on Wyner's wiretap channel theory." Quantum Engineering. 2019; doi:10.1002/que2.26

## Niestety realizacja praktyczna poza zasięgiem obecnej technologii

- ✗ Strony muszą być wyposażone w pamięci $N$-qubitowe,
- ✗ Lokalne operacje wymagają *de facto* komputera kwantowego.

# Inne paradygmaty poufności informacji

**Kryptografia asymetryczna** — Diffie, Hellman, 1976

Eve nie jest w stanie rozwiązać pewnego złożonego obliczeniowo problemu.

**Prawa fizyki** — Wyner, 1975

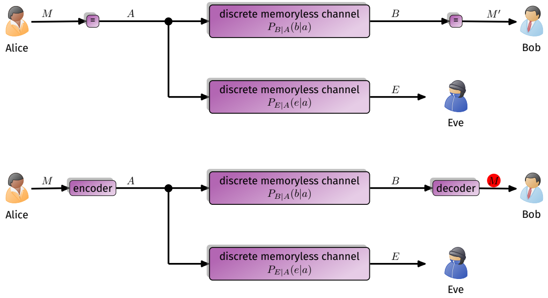
Szum może służyć do zapewnienia poufności. Eve ma częściową wiedzę o informacji przesyłanej pomiędzy Alice i Bobem.

**Rezultaty Wyner'a pasują wprost do komunikacji kwantowej**

- klasyczny post-processing wykorzystuje się w QKD,
- klasyczny pre-processing umożliwia realizacje protokołów QSDC.

# Wiretap channel

## Odrzucenie żądania całkowitej informacyjnej izolacji Eve.




### Model komunikacji

- Alice i Bob komunikują za pomocą kanału wprowadzającego błędy,
- Podsłuch Eve jest również niedoskonały.

### Twierdzenie Wynera

Secrecy capacity: $C_s = I(A;B) - I(A;E)$.
Istnieje kod nadmiarowy umożliwiający **wierną i** bezwarunkowo bezpieczną **poufną** komunikację gdy $C_s > 0$.

### Physical Layer Security

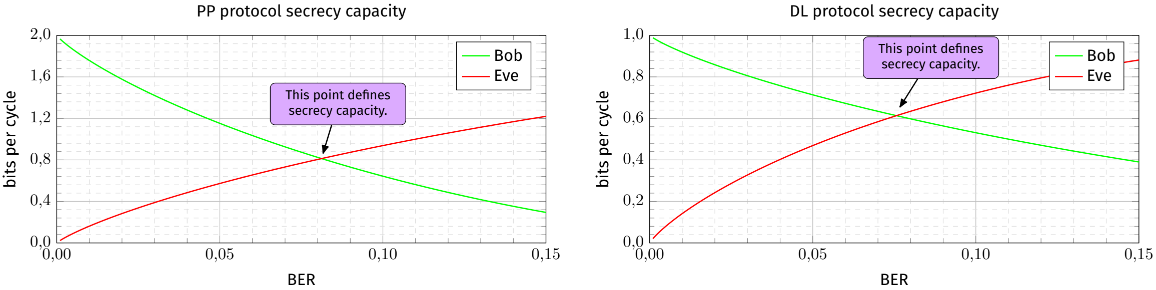
Twierdzenie ma zastosowanie nie tylko do komunikacji kwantowej

W przeciwieństwie do modelu Shannona bezwarunkowe bezpieczeństwo może być osiągnięte nawet gdy napastnik **nie** jest informacyjnie odizolowany od systemu Alice i Boba.

# Model Wynera idealnie pasuje do protokołów QSDC!

## Bezwarunkowe bezpieczeństwo można osiągnąć

przez **klasyczny preprocessing wiadomości** dla protokołów kwantowych zapewniających $C_s > 0$.




Wykresy uzyskano dla kanałów bezstratnych i przy założeniach upraszczających estymację $I(A;B)$.

# Optymalny kod namiarowy dla modelu Wynera

## Analiza Wynera i wyniki pochodne

**nie** określają jak skonstruować kod spełniający warunki twierdzenia.

## Właściwości zastosowanego kodu są kluczowe

- W omawianych dalej realizacjach praktycznych zastosowane kody nadmiarowe nie są opisane.
- Zastosowanie wprost istniejących kodów nadmiarowych nie prowadzi do bezpiecznego systemu.

## Zawadzki, 2015

Zastosowanie transformacji All-Or-Nothing do wiadomości przed wysłaniem.

# Realizacje praktyczne

# Pierwsze realizacje praktyczne

## Chinese scientists implement the world's first quantum secure direct communication system

Source: Global Times Published: 2020/9/20 13:57:20


photo: web

https://www.globaltimes.cn/content/1201420.shtml

# Pierwsze realizacje praktyczne

Light | Science & Applications

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature › light: science & applications › articles › article

Article | Open Access | Published: 14 September 2021

## A 15-user quantum secure direct communication network

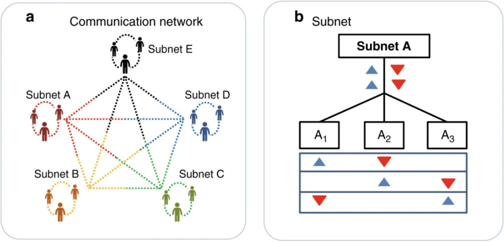
Zhantong Qi, Yuanhua Li, Yiwen Huang, Juan Feng, Yuanlin Zheng & Xianfeng Chen

*Light: Science & Applications* **10**, Article number: 183 (2021) | Cite this article

**2171** Accesses | **7** Citations | **32** Altmetric | Metrics

**Fig. 1: Composition of a quantum network.**

From: A 15-user quantum secure direct communication network




**a** The quantum network is fully connected by five subnets (A, B, C, D, and E are represented by red, orange, green, blue, and black, respectively). The dotted lines between the subnets (ten links with different colors) are the correlated time–energy photon pairs between the subnets. **b** Every subnet (such as subnet A) is equipped with a 1 × 3 BS and a delay controlling module, which splits a frequency-correlated entangled photon pair (red and blue signs) and sends them to three users randomly.

# Zamiast zakończenia

## Chiny są nabardziej zaawansowane w rozwoju kyptografii kwantowej

i Stany Zjednoczone się tego obawiają.

SEPTEMBER 12, 2018

Image credit: Getty Images

**Quantum Hegemony?**

China's Ambitions and the Challenge to U.S. Innovation Leadership

By Elsa B. Kania and John Costello

f | in | Print | Download PDF

https://www.cnas.org/publications/reports/quantum-hegemony