
بسم الله الرحمن الرحيم

ISCISC 2025

بیست و دومین کنفرانس بین المللی انجمن رمز ایران

بیست و دومین کنفرانس بین المللی انجمن رمز ایران
در امنیت اطلاعات و فرشتاسی

Shahid Beheshti University
Cyberspace Research Institute

Iranian Society of Cryptology

سیستم‌های ارتباطات امن کوانتومی: مبانی، کاربردها و مسیرهای پیش رو

خلاصه:

با رشد سریع فناوری‌های کوانتومی، طراحی و پیاده‌سازی سیستم‌های مخابراتی امن بر پایه اصول مکانیک کوانتومی به یکی از حوزه‌های راهبردی در علم و صنعت تبدیل شده است. این کارگاه با هدف ارائه‌ی مروری جامع بر مبانی علمی و کاربردی ارتباطات کوانتومی، تلاش دارد مخاطبان را با مفاهیم پایه، ابزارهای نظری و فناوری‌های روز در این حوزه آشنا سازد. در بخش اول کارگاه، مفاهیم کلیدی مکانیک کوانتومی نظیر برهم‌نهی، درهم‌تنیدگی و نمایش برداری حالت‌ها مرور می‌شود. سپس ساختار سیستم‌های مخابرات کوانتومی، اجزای اصلی آن‌ها، مفاهیم اندازه‌گیری و تئوری اطلاعات کوانتومی معرفی می‌گردند. در ادامه، کاربردهای درهم تنیدگی در ارتباطات نظیر فرابرد کوانتومی و توزیع کلید کوانتومی مطرح می‌شوند. بخش دوم کارگاه بر رمزنگاری با استفاده از توزیع کلید کوانتومی تمرکز دارد. سپس ساختار و چالش‌های طراحی شبکه‌های کوانتومی در مقیاس‌های مختلف بررسی می‌شود. در پایان نیز مفاهیم نوظهوری چون اینترنت کوانتومی، اینترنت اشیای کوانتومی و حسگری کوانتومی بیان خواهد شد. این کارگاه علاوه بر جنبه‌های علمی، مسیرهای پژوهشی و مراکز فعال در این حوزه در کشور را نیز معرفی می‌کند و فرصتی برای علاقه‌مندان جهت ورود و فعالیت در مرزهای دانش فناوری‌های کوانتومی فراهم می‌آورد.

ارائه دهنده:

دنیا سادات رضائی شاد

اساتید مشاور:

دکتر حسین بهرامگیری

دکتر مهدی خواجه

دانشگاه صنعتی مالک اشتر

دوشنبه ۱۴ مهرماه

۸:۳۰-۱۲:۰۰

مرکز همایش‌های بین المللی دانشگاه شهید بهشتی

http://iscisc2025.sbu.ac.ir/

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6


1
مقدمه
مفاهیم مکانیک کوانتومی
2
کاربردهای درهم‌تنیدگی
3
توزیع کلید کوانتومی
4
شبکه و اینترنت کوانتومی
5
سیستم‌های مخابرات کوانتومی
6

پیشینه‌ی رمزنگاری

- از حدود ۱۹۰۰سال قبل از میلاد مسیح (در مجسمه‌های مصری) تا شروع قرن بیستم (طراحی الگوریتم‌های دستی)

Plaintext	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext	ZYXWVUTSRQPONMLKJIHGFEDCBA

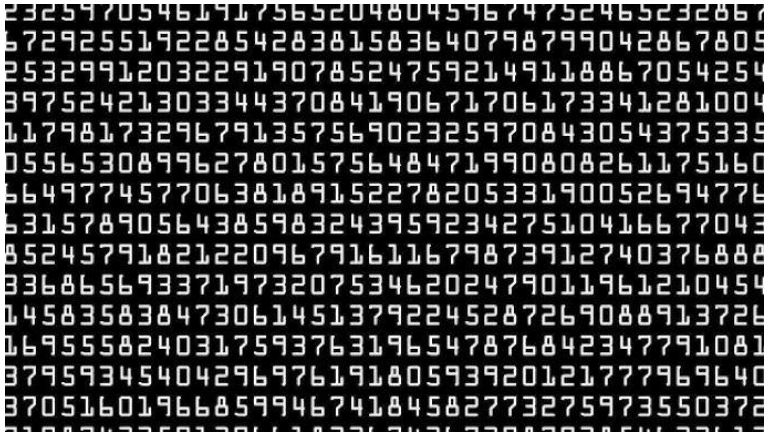
پیشینه‌ی رمزنگاری

- از حدود ۱۹۰۰سال قبل از میلاد مسیح (در مجسمه‌های مصری) تا شروع قرن بیستم (طراحی الگوریتم‌های دستی)

- حدود زمان جنگ جهانی دوم (با استفاده از ماشین‌های الکترومکانیکی)

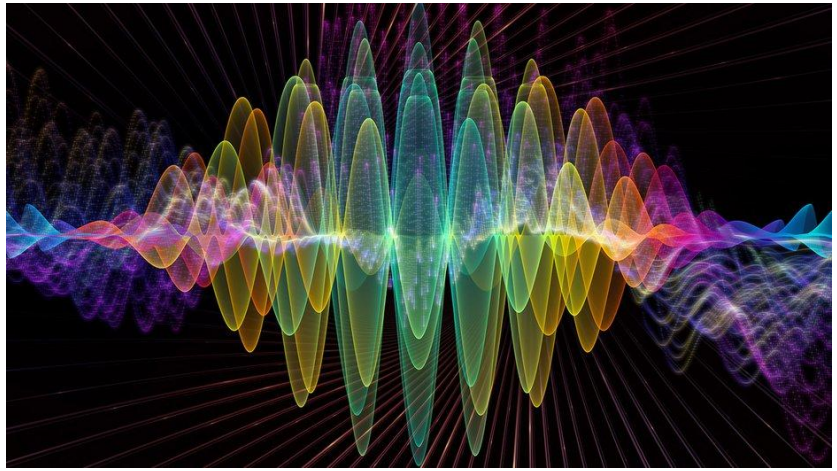
پیشینه‌ی رمزنگاری

- از حدود ۱۹۰۰سال قبل از میلاد مسیح (در مجسمه‌های مصری) تا شروع قرن بیستم (طراحی الگوریتم‌های دستی)
- حدود زمان جنگ جهانی دوم (با استفاده از ماشین‌های الکترومکانیکی)
- در پنجاه سال گذشته (استفاده‌ی گسترده از کامپیوترها برای محاسبات ریاضی)



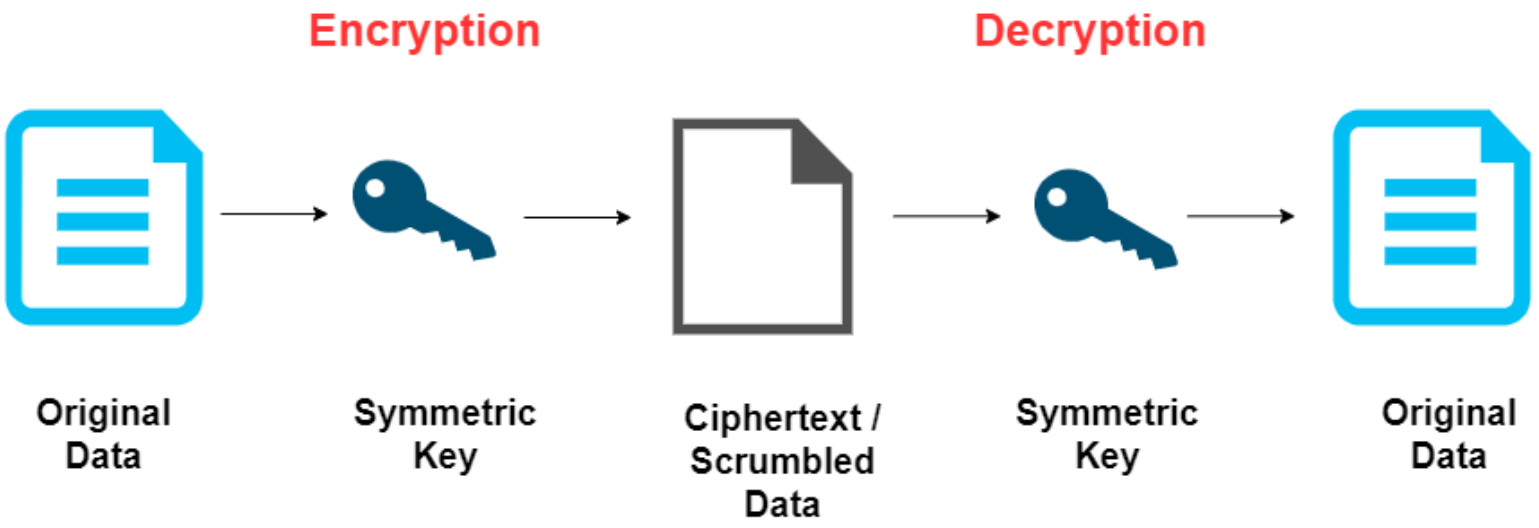
پیشینه‌ی رمزنگاری

- از حدود ۱۹۰۰سال قبل از میلاد مسیح (در مجسمه‌های مصری) تا شروع قرن بیستم (طراحی الگوریتم‌های دستی)
- حدود زمان جنگ جهانی دوم (با استفاده از ماشین‌های الکترومکانیکی)
- در پنجاه سال گذشته (استفاده‌ی گسترده از کامپیوترها برای محاسبات ریاضی)
- دوره‌ی جدید رمزنگاری (با استفاده از مکانیک کوانتومی)



رمزنگاری متقارن

- کلید یکسان در فرستنده و گیرنده

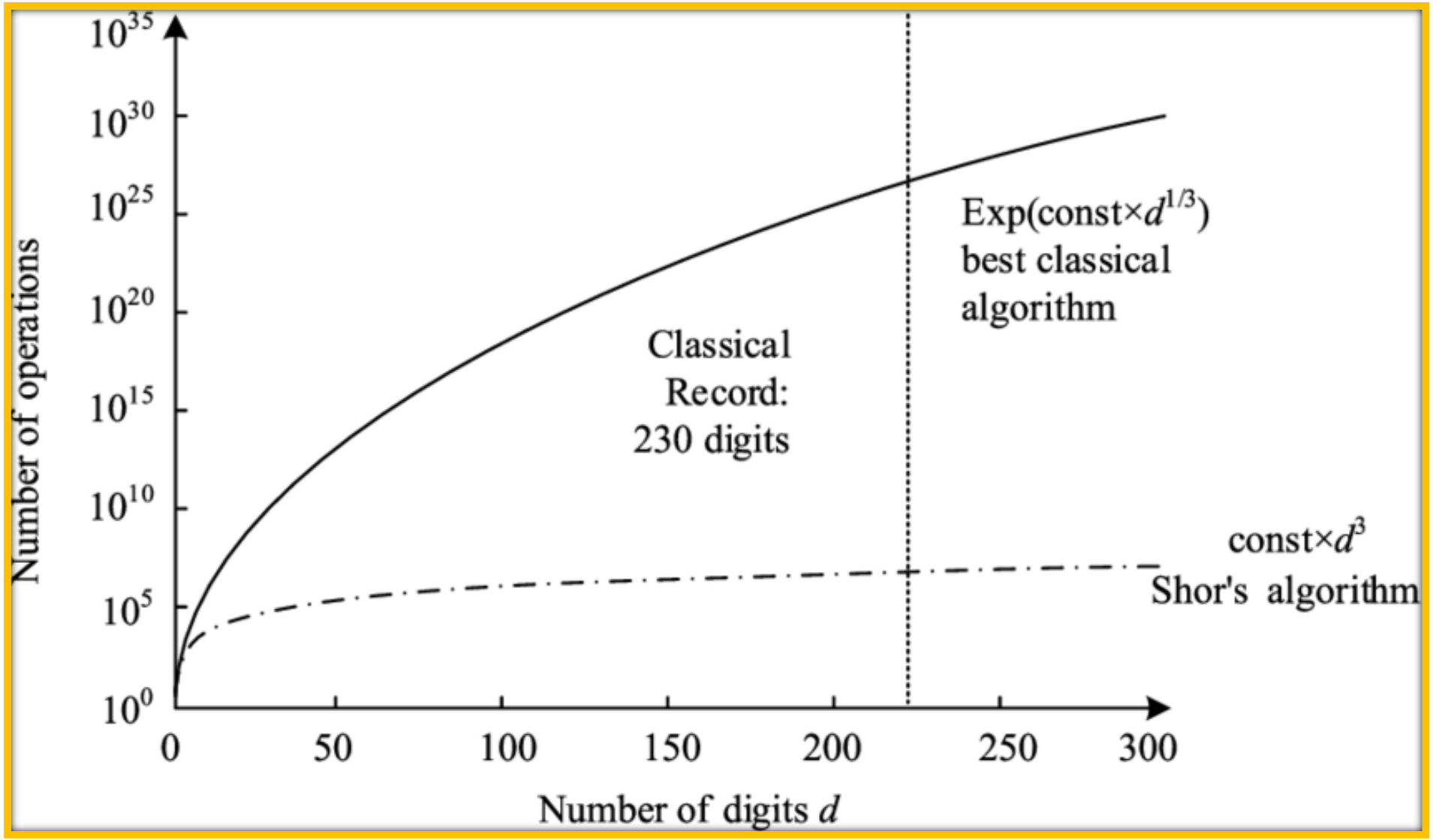


- مهم‌ترین چالش: مدیریت توزیع کلید
- رشد سریع تعداد کلیدهای لازم با بزرگ شدن شبکه‌ی کاربران
- عدم تضمین اشتراک گذاری امن کلید

رمزنگاری نامتقارن

- توزیع کلید از طریق رمزنگاری نامتقارن
- استفاده از یک کلید عمومی برای فرستنده و یک کلید خصوصی برای گیرنده
- امنیت بر اساس توابع یک طرفه
- سختی یک الگوریتم: رشد نمایی زمان اجرای الگوریتم با افزایش تعداد متغیرها
  - ✓ مثال: رمزنگاری RSA (۱۹۷۸) بر اساس سختی محاسبات ریاضی در تجزیه‌ی عدد بزرگ به عوامل اول
- امنیت وابسته به قدرت پردازش
- الگوریتم کوانتومی شر (۱۹۹۴): تجزیه ی عدد به عوامل اول در زمان چند جمله‌ای

رمزنگاری نامتقارن

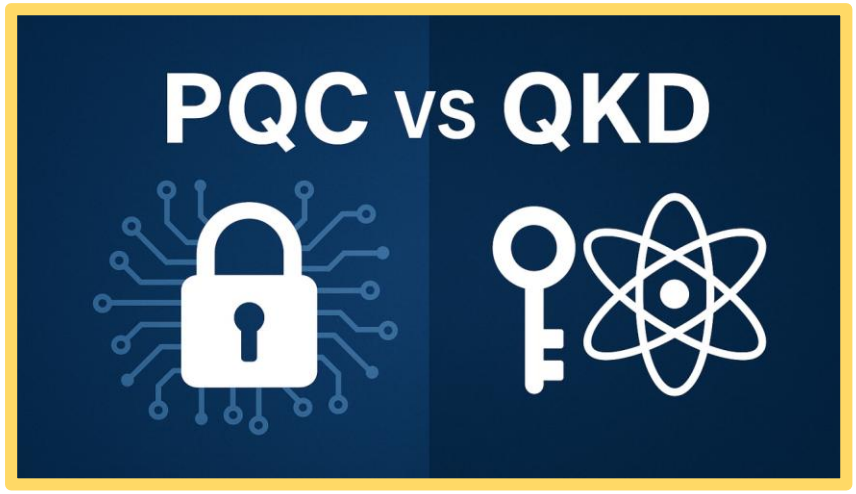


امنیت مطلق در ارتباطات

اگر دشمن، قدرت نامحدود پردازشی داشته باشد، چه راهی برای امن نگه داشتن ارتباطات وجود دارد؟

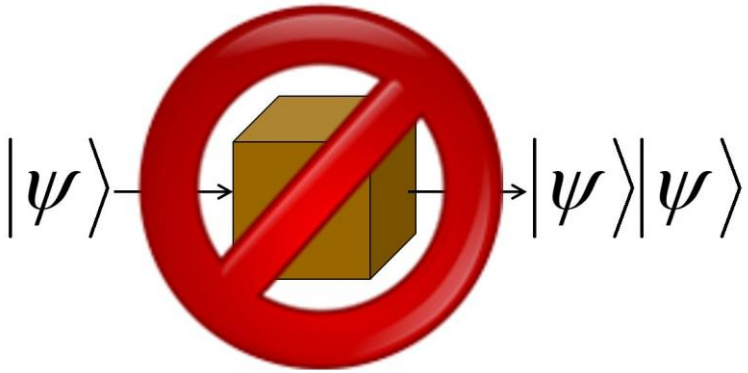
رمزنگاری کوانتومی

- رمزنگاری پسا کوانتومی
  - ✓ رمزنگاری کلاسیک اما مقاوم در برابر حملات فعلی کامپیوتر کوانتومی
  - ✓ عدم نیاز به سخت‌افزار جدید
- توزیع کلید کوانتومی (QKD)
  - ✓ استفاده از مکانیک کوانتومی برای تضمین امنیت کلید (مبتنی بر قوانین فیزیکی طبیعت)
  - ✓ رمزنگاری متقارن بر اساس کلید تولید شده (+ امکان اطلاع از شنود)



جمع‌بندی: چرا ارتباطات امن کوانتومی؟

- ✓ رمزنگاری کلاسیک بر پایه‌ی فرض‌های ریاضیات (مثل سختی تجزیه اعداد اول)
- ✓ به چالش کشیده شدن این فرض‌ها با ظهور رایانه‌های کوانتومی
- ✓ امنیت کوانتومی بر قوانین فیزیک بنا شده است، نه صرفاً محاسبات
- ✓ امکان تشخیص نفوذ با استفاده از ویژگی‌هایی مانند عدم تکثیر و اختلال در اثر اندازه‌گیری



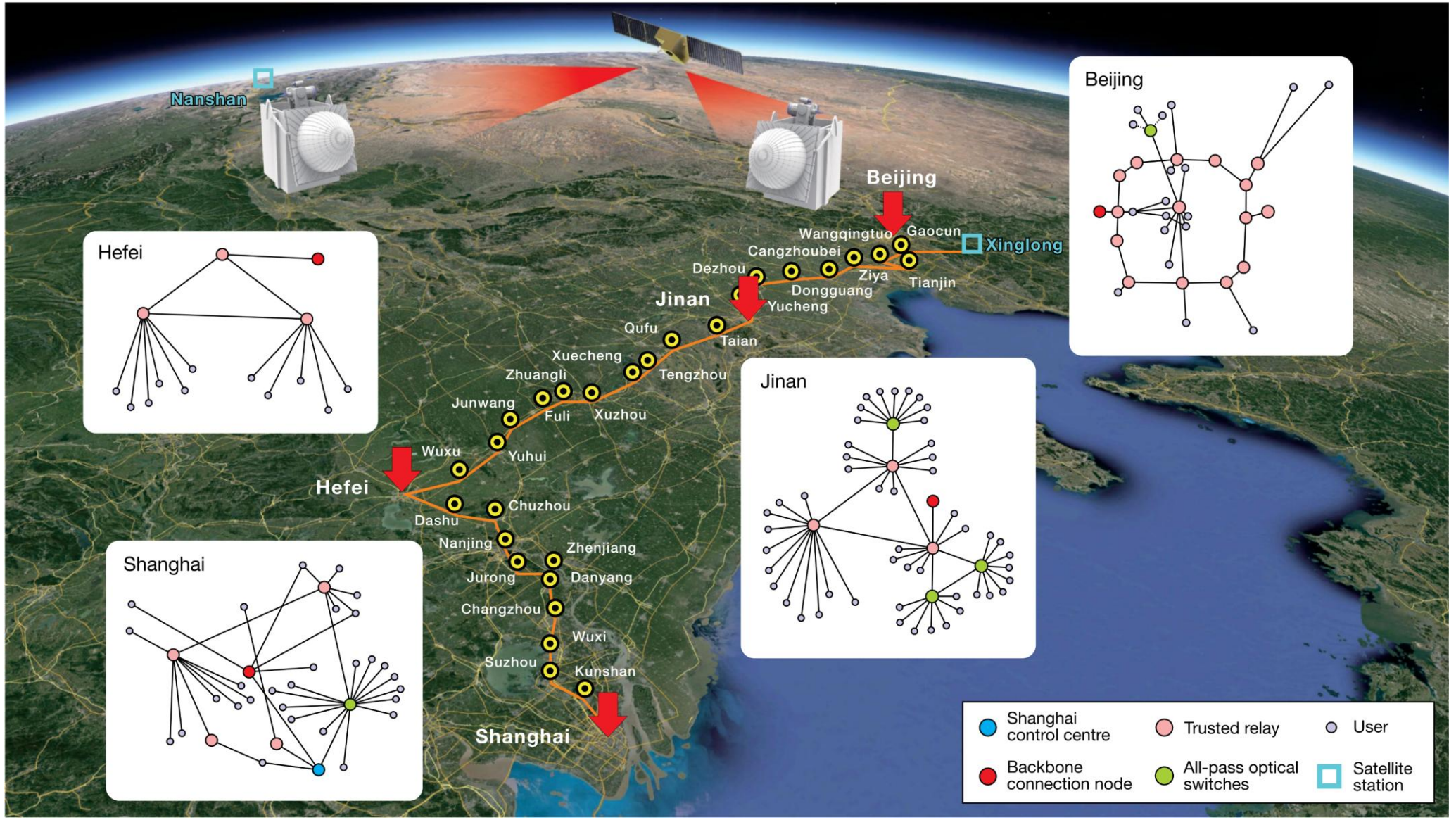
No-Cloning Theorem

Quantum Measurement and Collapse

توزیع کلید کوانتومی

- ورود فناوری توزیع کلید کوانتومی از آزمایشگاه به دنیای واقعی
- سرمایه‌گذاری عظیم کشورها و شرکت‌ها در توسعه‌ی شبکه‌های امن کوانتومی
  - ✓ چین، اتحادیه اروپا، امریکا و ...
  - ✓ صنایع مالی خصوصی و دولتی
  - ✓ شرکت‌های بزرگی مانند IBM، Toshiba، ID Quantique
  - ✓ توسعه‌ی دستگاه‌های تجاری QKD
- شکل‌گیری زیرساخت‌ها
  - ✓ شبکه‌های شهری
  - ✓ QKD مبتنی بر ماهواره

توزیع کلید کوانتومی



Chen et al., 2021, *An integrated space-to-ground quantum communication network over 4,600 kilometres*, Nature

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

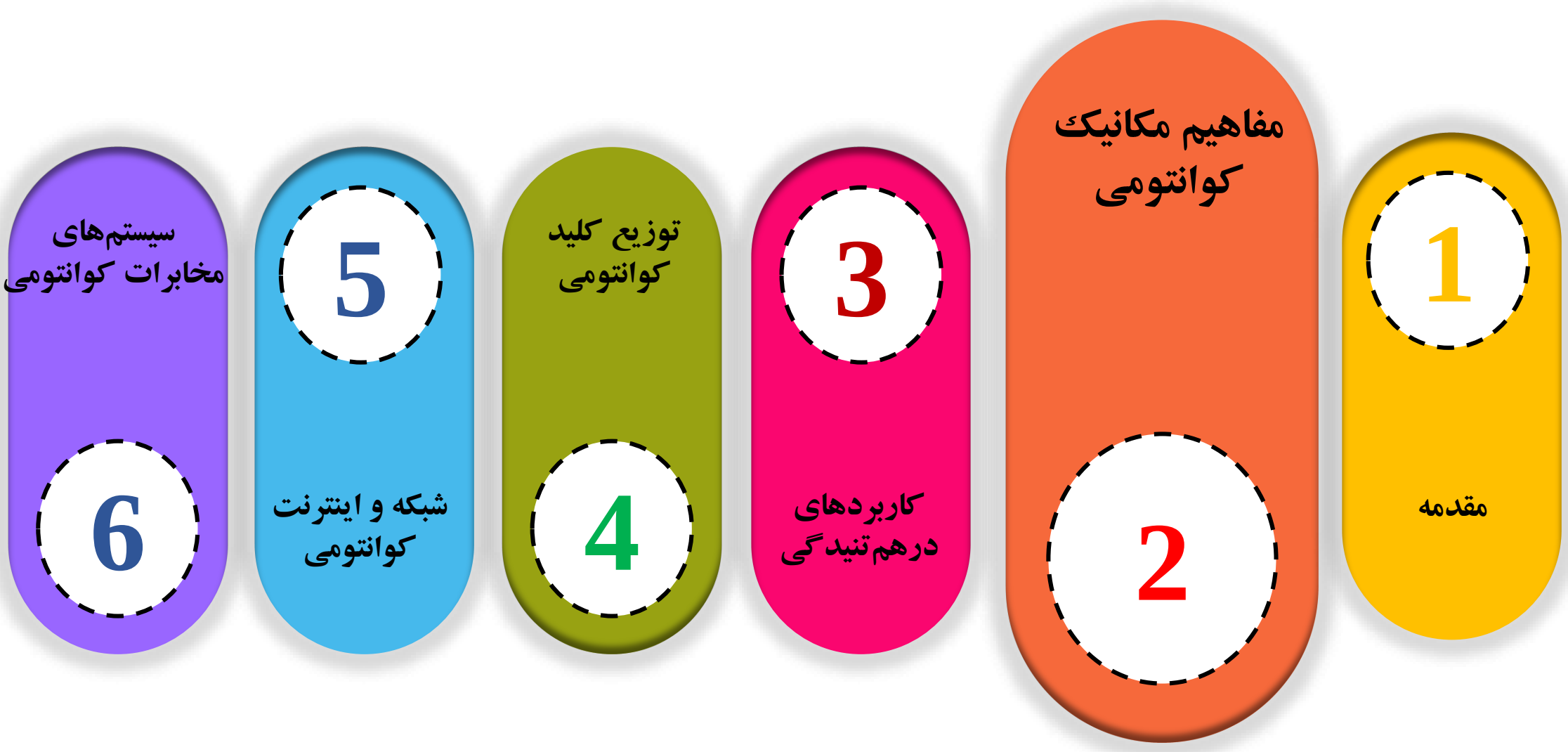
4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

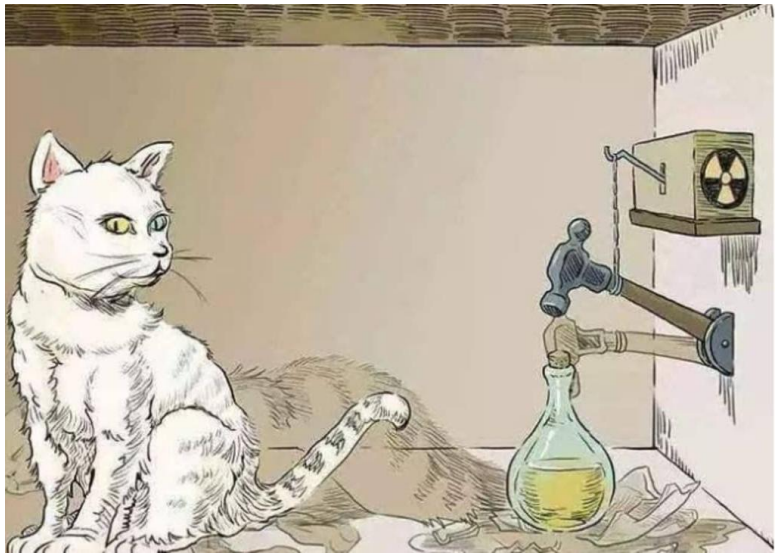

1
مقدمه
مفاهیم مکانیک کوانتومی
2
3
کاربردهای درهم‌تنیدگی
توزیع کلید کوانتومی
4
5
شبکه و اینترنت کوانتومی
سیستم‌های مخابرات کوانتومی
6

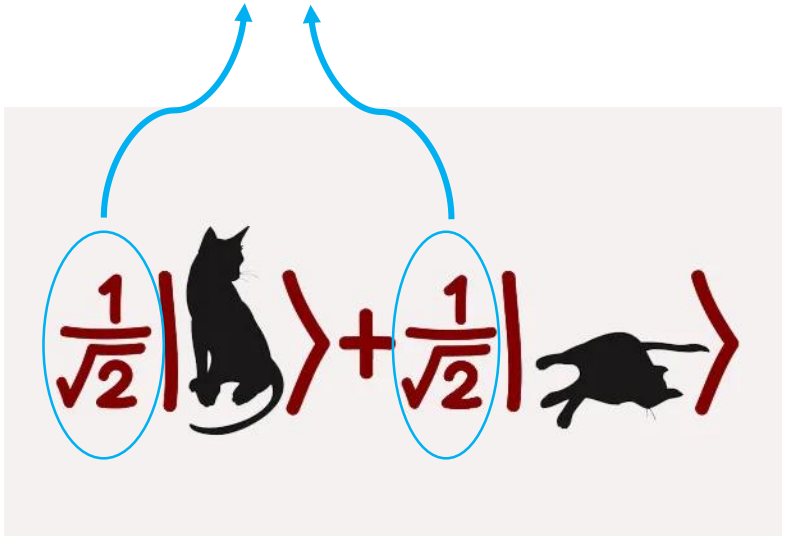
سرفصل مطالب این بخش

- بر هم نهی و دامنه‌ی احتمال
- تداخل
- تداخل تک فوتونی
- آزمایش دو شکاف
- کیوبیت
- عملگرهای کوانتومی
- نمایش دیراک
- اصول موضوعه مکانیک کوانتومی
- ضرب تانسوری
- در هم تنیدگی

برهم نهی و دامنه‌ی احتمال

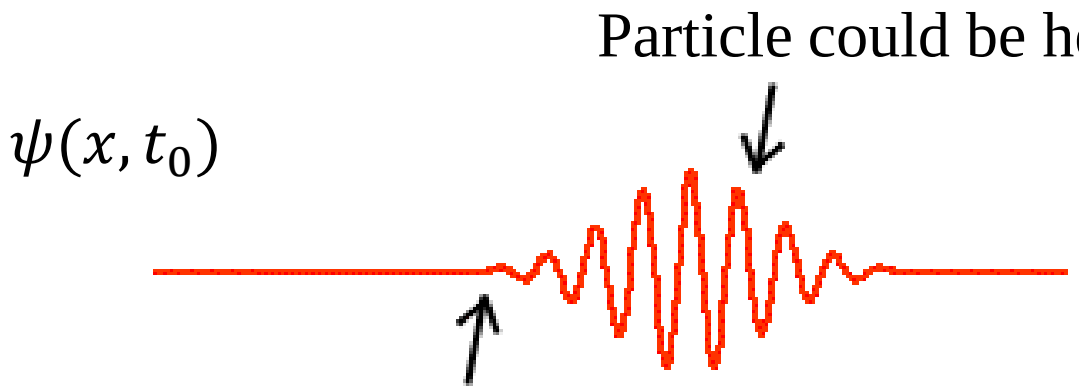
Probability amplitude





- دامنه‌ی احتمال: یک عدد مختلط
- اندازه‌ی مجذور آن برابر با احتمال حضور ذره در یک حالت کوانتومی پس از اندازه گیری (فروپاشی حالت کوانتومی)
- تا قبل از اندازه‌گیری، ذره در برهم‌نهی حالت‌ها

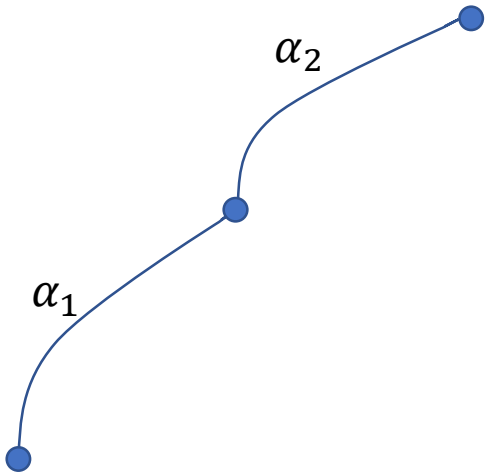
برهم نهی و دامنه‌ی احتمال



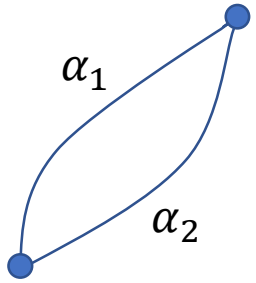
- $\psi(x,t)$: دامنه‌ی احتمال در (x,t)
- $|\psi(x,t)|^2$: احتمال یافتن ذره (پس از مشاهده) در (x,t)

برهم نهی و دامنه‌ی احتمال

$$p = |\alpha|^2$$



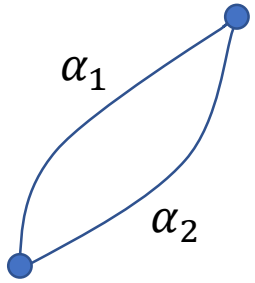
$$\alpha = \alpha_1 \alpha_2$$



$$\alpha = \alpha_1 + \alpha_2$$

تداخل

$$p = |\alpha|^2 = |\alpha_1 + \alpha_2|^2 = |\alpha_1|^2 + |\alpha_2|^2 + \alpha_1\alpha_2^* + \alpha_1^*\alpha_2$$
$$= |\alpha_1|^2 + |\alpha_2|^2 + 2|\alpha_1||\alpha_2|\cos(\phi_2 - \phi_1)$$
$$= p_1 + p_2 + 2\sqrt{p_1 p_2}\cos(\phi_2 - \phi_1)$$

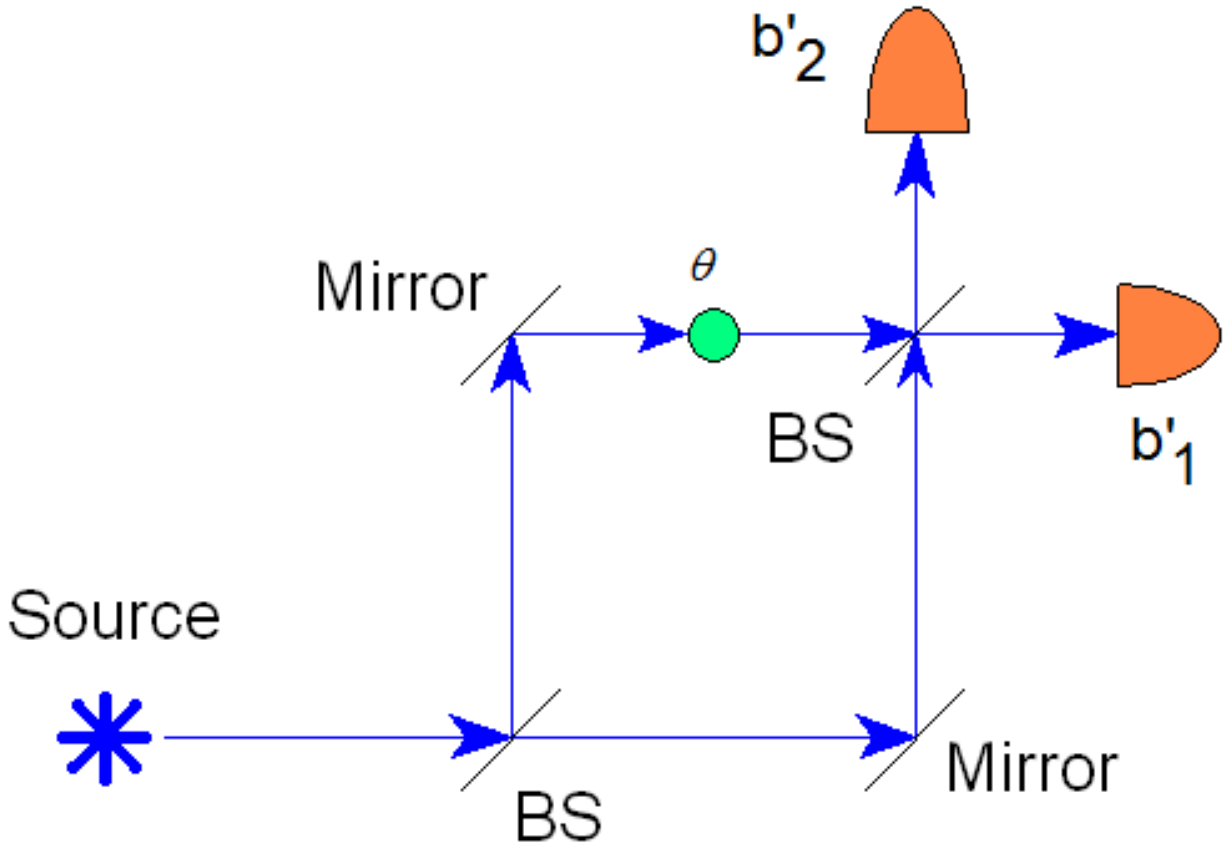


که در آن، $\alpha_1 = |\alpha_1|e^{i\phi_1}$ و $\alpha_2 = |\alpha_2|e^{i\phi_2}$.

نتیجه: وابستگی احتمال گذار از یک نقطه به نقطه‌ی دیگر، به اختلاف فاز بین دامنه‌ی احتمال دو مسیر

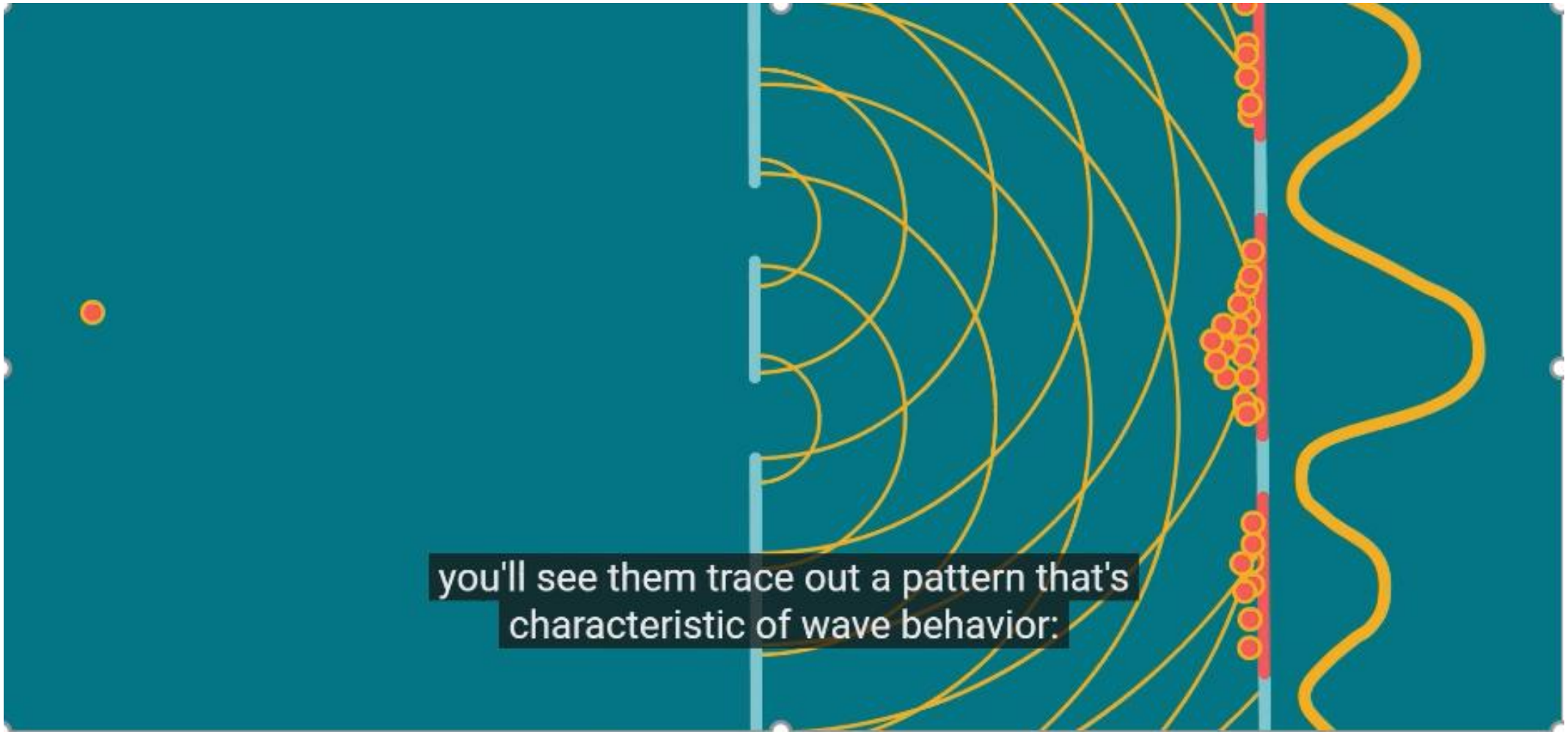
تداخل تک فوتونی

$$p_2 = \frac{1+\cos(\theta)}{2} = \cos^2(\frac{\theta}{2})$$



$$p_1 = \frac{1-\cos(\theta)}{2} = \sin^2(\frac{\theta}{2})$$

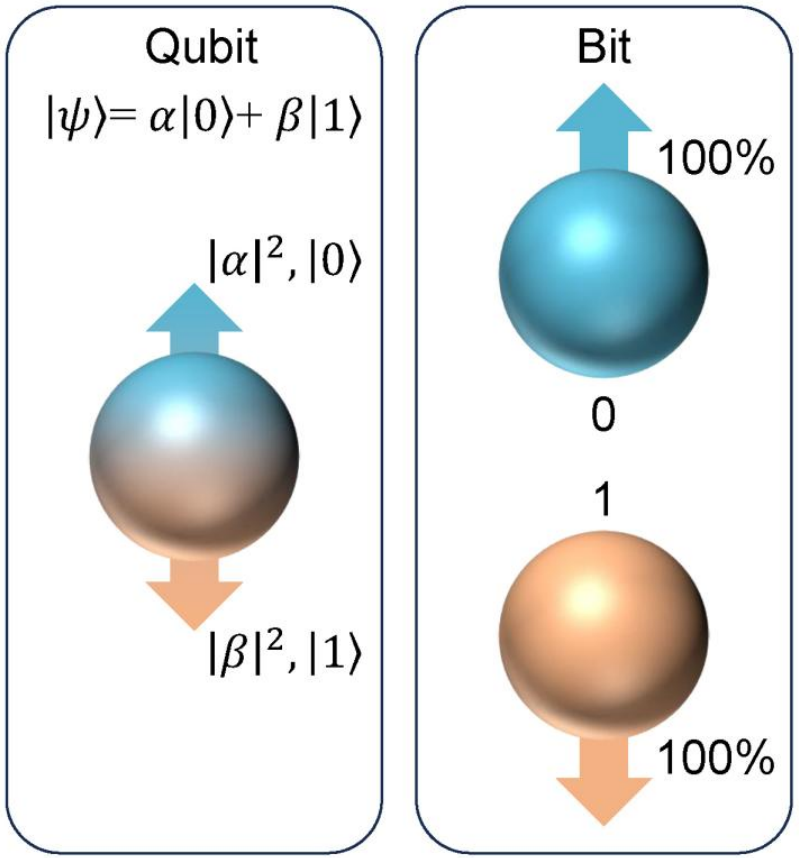
آزمایش دو شکاف



https://ed.ted.com/lessons/schrodinger-s-cat-a-thought-experiment-in-quantum-mechanics-chad-orzel

کیوبیت

- کیوبیت (بیت کوانتومی): واحد اطلاعات کوانتومی
- توصیف یک سیستم دو ترازه، مانند قطبش عمودی یا افقی یک فوتون



Pan et al., 2024, *The Evolution of Quantum Secure Direct Communication*, IEEE Commun. Surv. Tutor

کیوبیت

- کیوبیت (بیت کوانتومی): واحد اطلاعات کوانتومی
- توصیف یک سیستم دو ترازه، مانند قطبش عمودی یا افقی یک فوتون
- فرض کنید یک سیستم در برهم‌نهی دو رنگ متفاوت (آبی یا قرمز) با دامنه احتمال یکسان قرار دارد.
- اگر رنگ آبی را با بردار $\begin{bmatrix}1\\0\end{bmatrix}$ و رنگ قرمز را با بردار $\begin{bmatrix}0\\1\end{bmatrix}$ نشان دهیم:

$$\text{System state} : \quad \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}$$

- نگاه کردن ما به سیستم، معادل اندازه‌گیری رنگ آن است. تا قبل از نگاه کردن، سیستم کوانتومی در برهم نهی دو رنگ مختلف است. پس از نگاه به سیستم، حالت آن به یک رنگ مشخص تقلیل می‌یابد (فروپاشی می‌کند).

عملگرهای کوانتومی

- مفهوم
- ابعاد ماتریس متناظر
- عملگرهای یکانی
- عملگرهای مهم تک کیوبیتی کوانتومی:

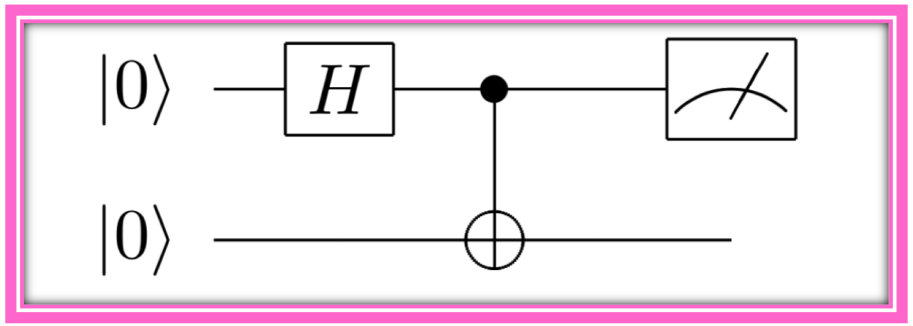
$$\hat{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\hat{X} = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\hat{Y} = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\hat{Z} = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



نمایش دیراک

	Standard Notation	Dirac Notation
Column Vector	$\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$	$\|x\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ Ket
Row Vector	$\vec{x}^{*T} = [x_1^* x_2^* \dots x_n^*]$	$\langle x\| = (\|x\rangle)^\dagger = [x_1^* x_2^* \dots x_n^*]$ Bra $(\dagger: dagger \triangleq Complex\ Conjugate\ Transpose)$
Inner Product	$(\vec{x}, \vec{y}) = \vec{y}^{*T}\vec{x}$ $= y_1^* x_1 + y_2^* x_2 + \cdots + y_n^* x_n$	$\langle y\|x\rangle = y_1^* x_1 + y_2^* x_2 + \cdots + y_n^* x_n$ Braket
norm	$\|\|\vec{x}\|\| = \sqrt{(\vec{x}, \vec{x})}$	$\|\|x\|\| = \sqrt{\langle x\|x\rangle}$
linear combination	$\vec{x} = a_1\overrightarrow{b_1} + a_2\overrightarrow{b_2} + \cdots + a_n\overrightarrow{b_n}$ $B = \{\overrightarrow{b_i}, i \in I\}, a_i = (\overrightarrow{b_i}, \vec{x})$	$\|x\rangle = a_1\|b_1\rangle + a_2\|b_2\rangle + \cdots + a_n\|b_n\rangle$ $B = \{\|b_i\rangle, i \in I\}, a_i \triangleq \langle b_i\|x\rangle$

ضرب تانسوری

$$|\psi_A\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix}$$

$$|\psi_B\rangle = \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}$$

$$|\psi_A\rangle \otimes |\psi_B\rangle = |\psi_A\rangle|\psi_B\rangle = \begin{bmatrix}\alpha_0|\psi_B\rangle\\ \alpha_1|\psi_B\rangle\end{bmatrix} = \begin{bmatrix}\alpha_0\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\\ \alpha_1\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{bmatrix}$$

$$\hat{A} = \begin{bmatrix}\alpha_{00} & \alpha_{01}\\ \alpha_{10} & \alpha_{11}\end{bmatrix}$$

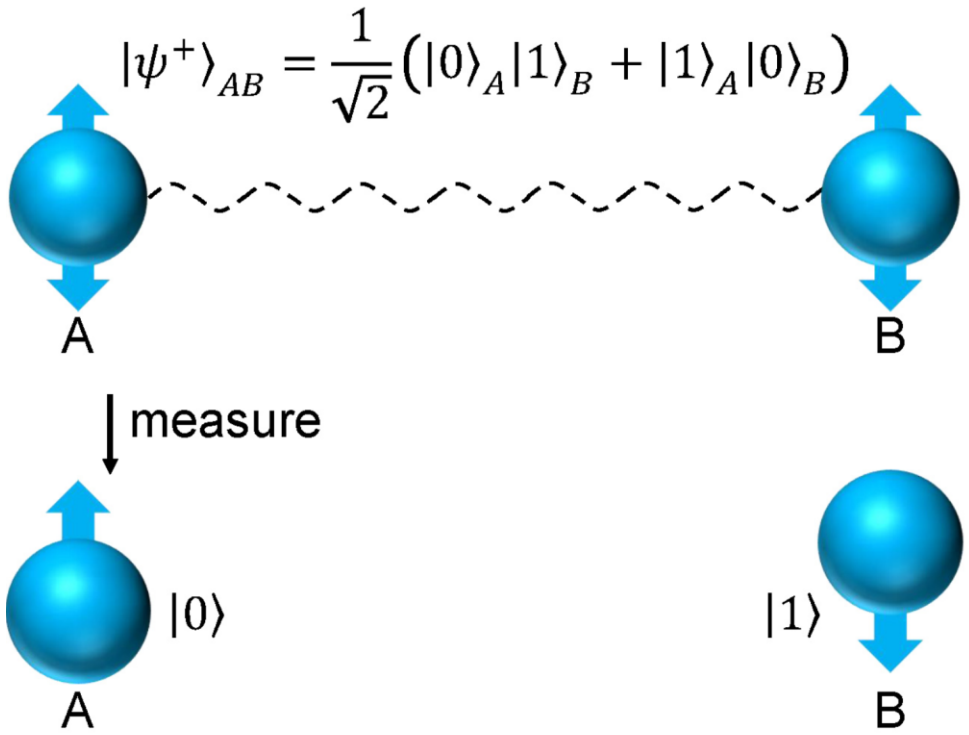
$$\hat{B} = \begin{bmatrix}\beta_{00} & \beta_{01}\\ \beta_{10} & \beta_{11}\end{bmatrix}$$

$$\hat{A} \otimes \hat{B} = \begin{bmatrix}\alpha_{00}\hat{B} & \alpha_{01}\hat{B}\\ \alpha_{10}\hat{B} & \alpha_{11}\hat{B}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\beta_{00} & \alpha_{00}\beta_{01} & \alpha_{01}\beta_{00} & \alpha_{01}\beta_{01}\\ \alpha_{00}\beta_{10} & \alpha_{00}\beta_{11} & \alpha_{01}\beta_{10} & \alpha_{01}\beta_{11}\\ \alpha_{10}\beta_{00} & \alpha_{10}\beta_{01} & \alpha_{11}\beta_{00} & \alpha_{11}\beta_{01}\\ \alpha_{10}\beta_{10} & \alpha_{10}\beta_{11} & \alpha_{11}\beta_{10} & \alpha_{11}\beta_{11}\end{bmatrix}$$

در هم تنیدگی

- تعامل بین دو حالت کوانتومی (دو زیرسیستم مجزا) و عدم امکان توصیف مستقل دو حالت کوانتومی
- وابستگی کامل حالت‌ها در سیستم‌های درهم‌تنیده

✓اندازه‌گیری یکی، وضعیت دیگری را تعیین می‌کند(تقلیل فوری به حالت پایه)



Pan et al., 2024, *The Evolution of Quantum Secure Direct Communication*, IEEE Commun. Surv. Tutor

در هم تنیدگی

- تعامل بین دو حالت کوانتومی (دو زیرسیستم مجزا) و عدم امکان توصیف مستقل دو حالت کوانتومی
- وابستگی کامل حالت‌ها در سیستم‌های درهم‌تنیده
  ✓اندازه‌گیری یکی، وضعیت دیگری را تعیین می‌کند(تقلیل فوری به حالت پایه)

- در هم تنیدگی روی فوتون‌ها، الکترون‌ها، مولکول‌ها و حتی الماس‌های کوچک
- غیرقابل نوشتن به صورت ضرب تانسوری

- مثال سیستم در هم تنیده:

$$\frac{1}{\sqrt{2}}(|1\rangle|0\rangle + |0\rangle|1\rangle) \quad \text{or} \quad \frac{1}{\sqrt{2}}(|1\rangle|1\rangle + |0\rangle|0\rangle)$$

- مثال سیستم غیردر هم تنیده:

$$|\psi_A\rangle = a|0\rangle + b|1\rangle \quad |\psi_B\rangle = c|0\rangle + d|1\rangle$$

$$|\psi_A\rangle \otimes |\psi_B\rangle = ac|0\rangle|0\rangle + ad|0\rangle|1\rangle + bc|1\rangle|0\rangle + bd|1\rangle|1\rangle$$

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

سرفصل مطالب این بخش

- فرابرد کوانتومی
- کدگذاری چگال
- ارتباط مستقیم امن کوانتومی
- توزیع کلید کوانتومی

فرابرد کوانتومی

$$|\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$$
$$|\psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

- هدف: انتقال حالت کوانتومی با مخابره‌ی بیت(های) کلاسیک
- عدم اطلاع فرستنده از حالت کوانتومی خود
- مثال:

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

1. اشتراک یک حالت در هم تنیده بل بین فرستنده و گیرنده

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{ab}$$

2. بازنویسی دو حالت کوانتومی

$$\begin{aligned} |\Psi\rangle = |\phi\rangle|\phi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle)_a \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{ab} \\ &= \frac{1}{\sqrt{2}}(\alpha|0,0,0\rangle + \beta|1,0,0\rangle + \alpha|0,1,1\rangle + \beta|1,1,1\rangle) \end{aligned}$$

3. اندازه‌گیری در پایه‌ی بل و ارسال نتیجه برای گیرنده

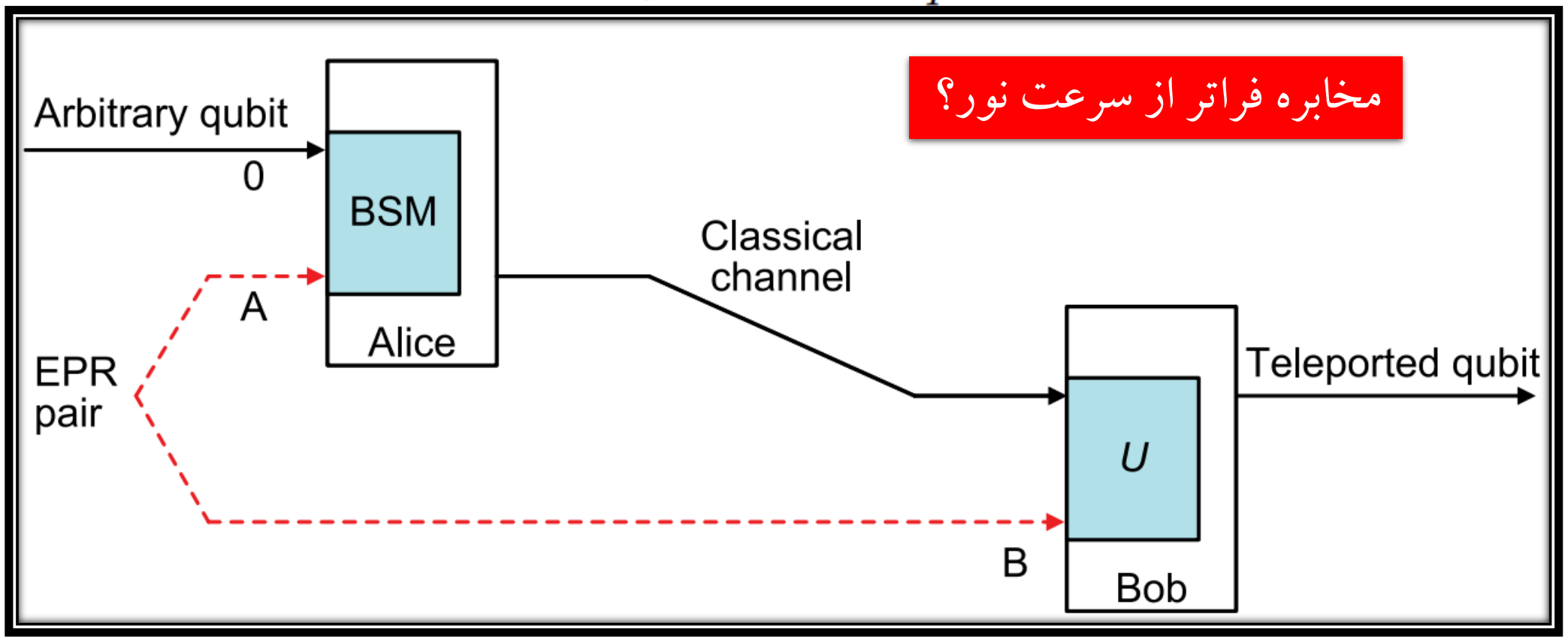
$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}(|\phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) \\ &+ |\psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle)) \end{aligned}$$

I	$\alpha\|0\rangle + \beta\|1\rangle$	$\|\phi^+\rangle$
Z	$\alpha\|0\rangle - \beta\|1\rangle$	$\|\phi^-\rangle$
X	$\beta\|0\rangle + \alpha\|1\rangle$	$\|\psi^+\rangle$
Y	$-\beta\|0\rangle + \alpha\|1\rangle$	$\|\phi^+\rangle$

فرابرد کوانتومی

- هدف: انتقال حالت کوانتومی با مخابره‌ی بیت(های) کلاسیک
- عدم اطلاع فرستنده از حالت کوانتومی خود

$$1 \text{ ebit} + 2\ bit \longrightarrow 1\ qubit$$



Pan et al., 2024, *The Evolution of Quantum Secure Direct Communication*, IEEE Commun. Surv. Tutor

کاربرد فرابرد کوانتومی؟

- محاسبات کوانتومی توزیع‌شده (Distributed Quantum Computing)
  - ✓ انتقال کیوبیت بین دو کامپیوتر کوانتومی در فاصله‌ی زیاد برای محاسبه‌ی همزمان
- شبکه کوانتومی (Quantum Network)
  - ✓ تکرار کننده‌ی کوانتومی
- حافظه‌های کوانتومی (Quantum Memories)
  - ✓ بازیابی و انتقال حالت کوانتومی از یک حافظه به حافظه دیگر
- انتقال حالت بین انواع مختلف سیستم‌ها
  - ✓ انتقال اطلاعات کوانتومی بین سیستم‌های ناهمگن (مثلاً بین یک یون و یک فوتون)
- ارتباط کوانتومی ماهواره‌ای
  - ✓ در پروژه‌های ماهواره‌ای (مثل Micius) برای انتقال حالت فوتون‌ها از زمین به ماهواره یا بالعکس

کدگذاری چگال (فشرده)

هدف: انتقال دو بیت اطلاعات با مبادله‌ی یک کیوبیت (معکوس فرابرد کوانتومی)

1. اشتراک گذاشتن یک زوج در هم تنیده EPR $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. اعمال یکی از عملگرهای پائولی وابسته به دو بیت اطلاعات روی کیوبیت فرستنده و ارسال آن برای گیرنده
3. اندازه‌گیری بل روی دو کیوبیت در هم تنیده در گیرنده

$$00 \longrightarrow I \longrightarrow |\phi^+\rangle,$$

$$01 \longrightarrow X \longrightarrow |\psi^+\rangle,$$

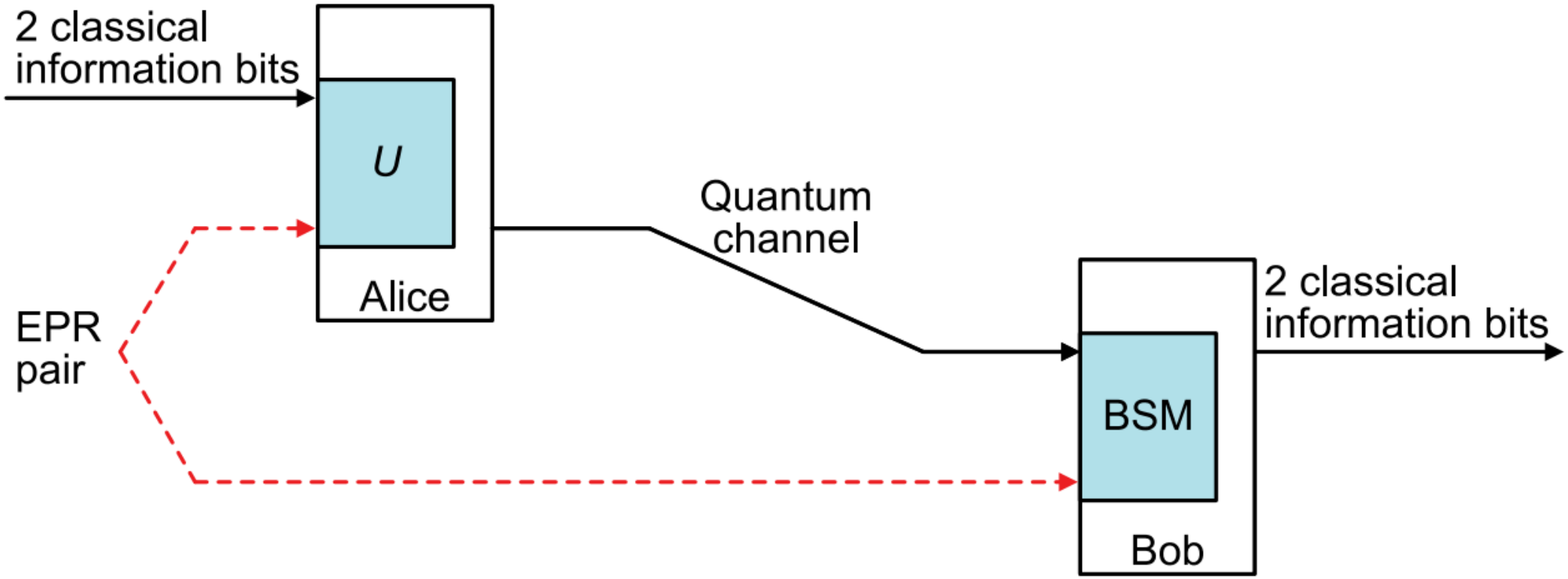
$$10 \longrightarrow Z \longrightarrow |\phi^-\rangle,$$

$$11 \longrightarrow Y \longrightarrow |\psi^-\rangle.$$

کدگذاری چگال (فشرده)

هدف: انتقال دو بیت اطلاعات با مبادله‌ی یک کیوبیت (معکوس فرابرد کوانتومی)

$$1\ ebit + 1\ qubit \longrightarrow 2\ bits$$



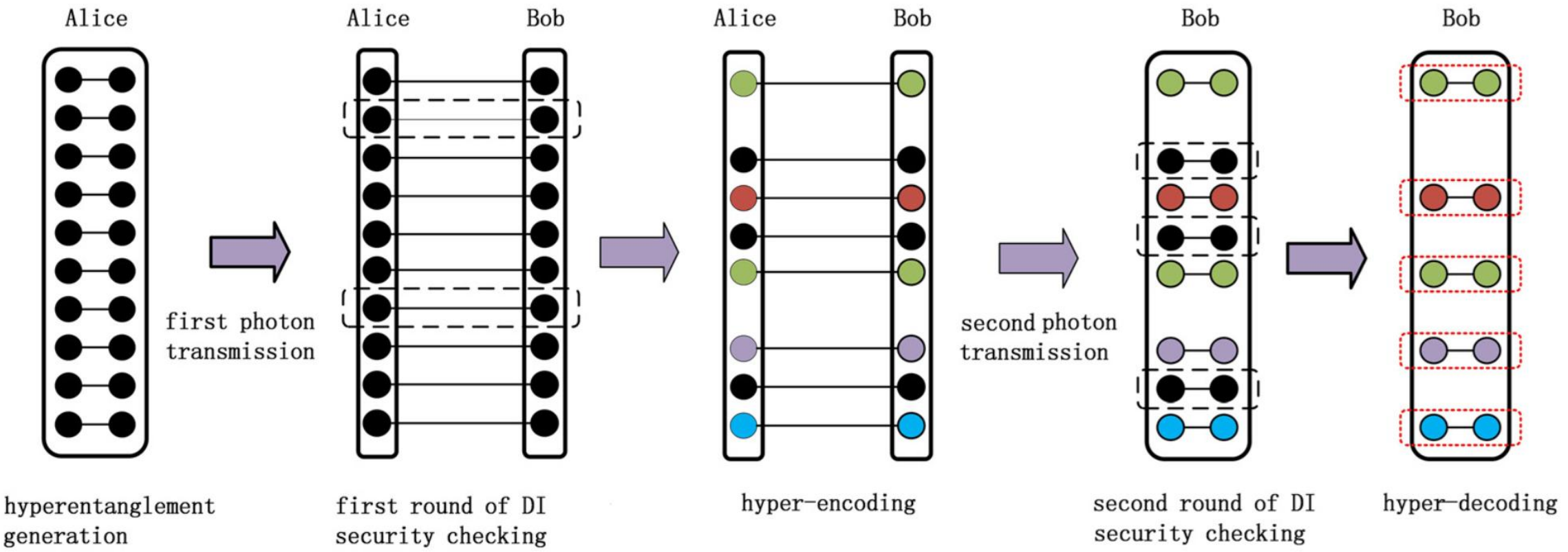
Pan et al., 2024, *The Evolution of Quantum Secure Direct Communication*, IEEE Commun. Surv. Tutor

کاربرد کدگذاری چگال؟

- افزایش ظرفیت کانال کلاسیک تا دو برابر
  - ✓ توزیع زوج‌های در هم تنیده پیش از شروع مخابره

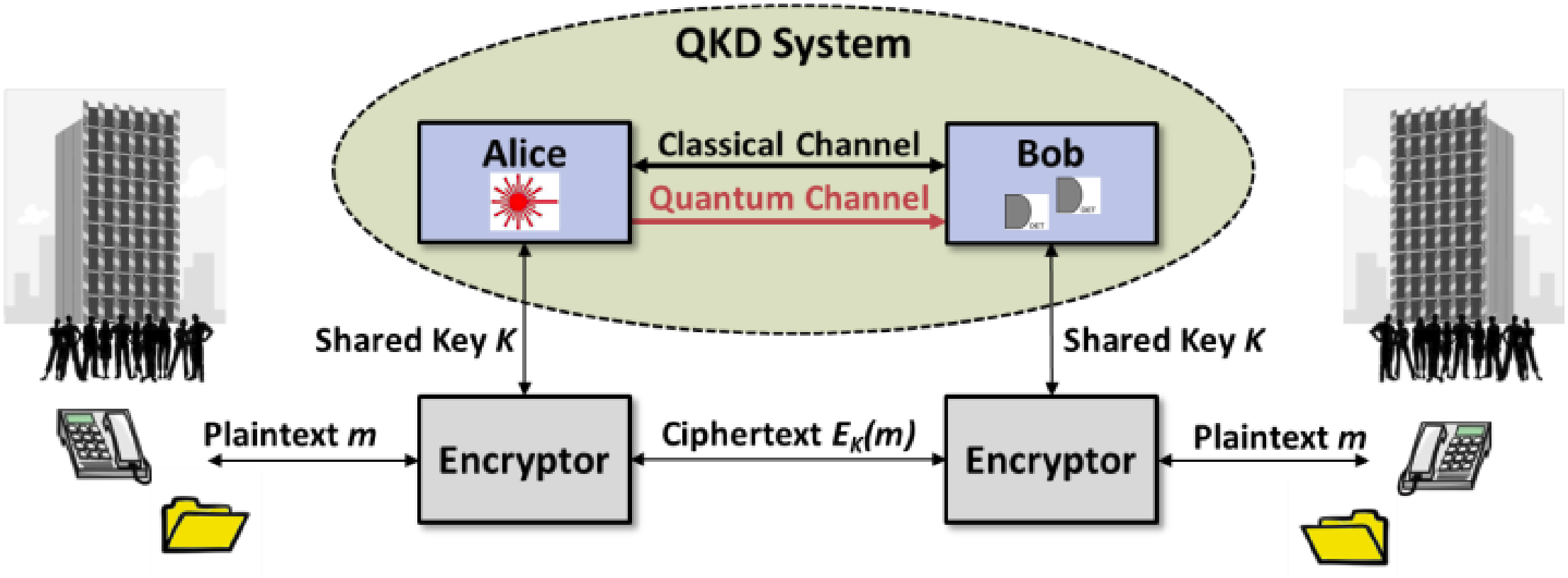
- روان کردن ترافیک شبکه
  - ✓ توزیع زوج‌های در هم تنیده در زمان کم بار بودن شبکه و استفاده از آن در زمان‌های اوج ترافیک شبکه

ارتباط مستقیم امن کوانتومی (QSDC)



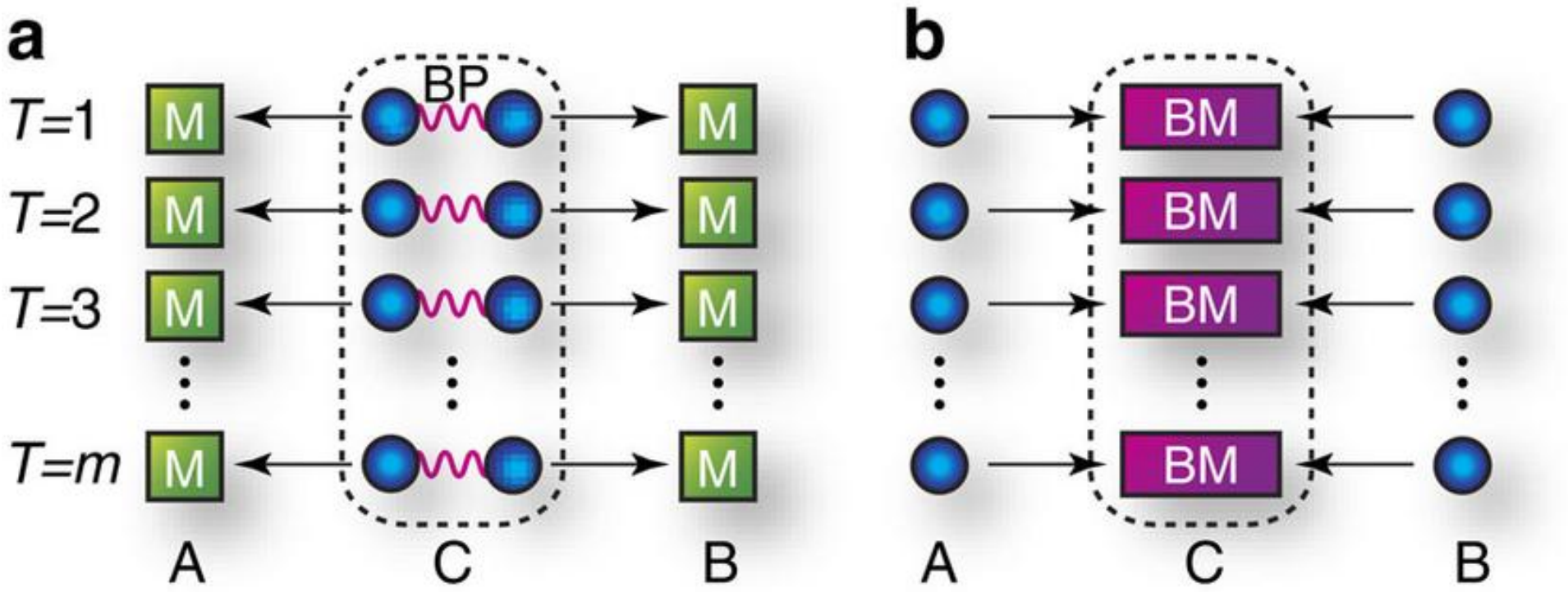
Zeng et al., 2024, *High-capacity device-independent quantum secure direct communication based on hyper-encoding*, Fund Res.

توزیع کلید کوانتومی (QKD)



Gawali et al., 2023, *QKD and Blockchain Based Secure Authentication in Medical Cyber-Physical Systems*, ICT Spr.

توزیع کلید کوانتومی (QKD)



Azuma et al., 2015, *All-photonic intercity quantum key distribution*, Nature.

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

سرفصل مطالب این بخش

- دسته‌بندی پروتکل‌های QKD
- دو قانون مهم مکانیک کوانتومی در QKD
- پروتکل BB84
- اشاره‌ای به حالت در هم تنیده پروتکل BB84
- پروتکل‌های DPS و COW
- پروتکل MDI
- معیارهای ارزیابی سیستم QKD
- حملات کوانتومی
- سیستم‌های QKD تجاری

دسته‌بندی پروتکل‌های QKD

- QKD Approach:
  1. Prepare and measure
  2. Entanglement-based
     - more robust to environmental impairments
     - technologically less mature than P&M
  3. Measurement Device Independent

- QKD type
  1. Discrete-variable (DV)
  2. Continues-variable (CV)
  3. Distributed-Phase Reference (DPR)

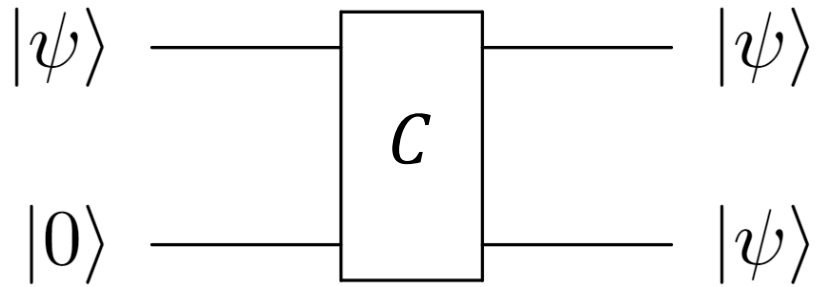
دسته‌بندی پروتکل‌های QKD

Protocol	Type	Approach	Year
BB84	DV	Prepare-and-measure	1984
E91	DV	Entanglement-based	1991
BBM92	DV	Entanglement-based	1992
GG02	CV	Prepare-and-measure	2002
DPS	DV	Prepare-and-measure	2002
Decoy-state	DV	Prepare-and-measure	2003–2005
SARG04	DV	Prepare-and-measure	2004
COW	DV	Prepare-and-measure	2005
MDI	DV/CV	Prepare-and-measure	2012
TF	DV	Prepare-and-measure	2018
PM	DV	Prepare-and-measure	2018

Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

دو قانون مهم مکانیک کوانتومی در QKD

- قضیه‌ی عدم تکثیر حالت کوانتومی



- Let $|\psi\rangle = a|x\rangle + \mathrm{b}|y\rangle$ and C be a cloner.
- It is not possible to have $C|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$

در تضاد با خطی و یونیتاری بودن مکانیک کوانتومی

- Simple proof:

$$C|\psi\rangle|0\rangle = \mathrm{C}[(a|x\rangle + \mathrm{b}|y\rangle)|0\rangle] = (a|x\rangle + \mathrm{b}|y\rangle)\,(a|x\rangle + \mathrm{b}|y\rangle)$$

$$\mathrm{C}[(a|x\rangle + \mathrm{b}|y\rangle)|0\rangle] = \mathrm{C}(a|x\rangle|0\rangle) + \mathrm{C}(b|y\rangle|0\rangle) = a|x\rangle|x\rangle + \mathrm{b}|y\rangle|y\rangle$$

دو قانون مهم مکانیک کوانتومی در QKD

- عدم قطعیت در تفکیک بدون ابهام دو حالت کوانتومی نامتعامد
- مثال:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

- تولید یکی از این دو حالت با احتمال یکسان
- هدف: تشخیص حالت با اندازه‌گیری در پایه‌ی مناسب

- اندازه‌گیری در پایه‌ی محاسباتی $\{|0\rangle,|1\rangle\}$:
  - اگر $|0\rangle$ تولید شده باشد، با احتمال صد درصد، $|0\rangle$ اندازه‌گیری می‌شود.
  - اگر $|+\rangle$ تولید شده باشد، با احتمال ۵۰ درصد $|0\rangle$ و با احتمال ۵۰ درصد $|1\rangle$ اندازه‌گیری می‌شود.

- دلیل عدم قطعیت: نامتعامد بودن دو حالت کوانتومی $|0\rangle$ و $|+\rangle$

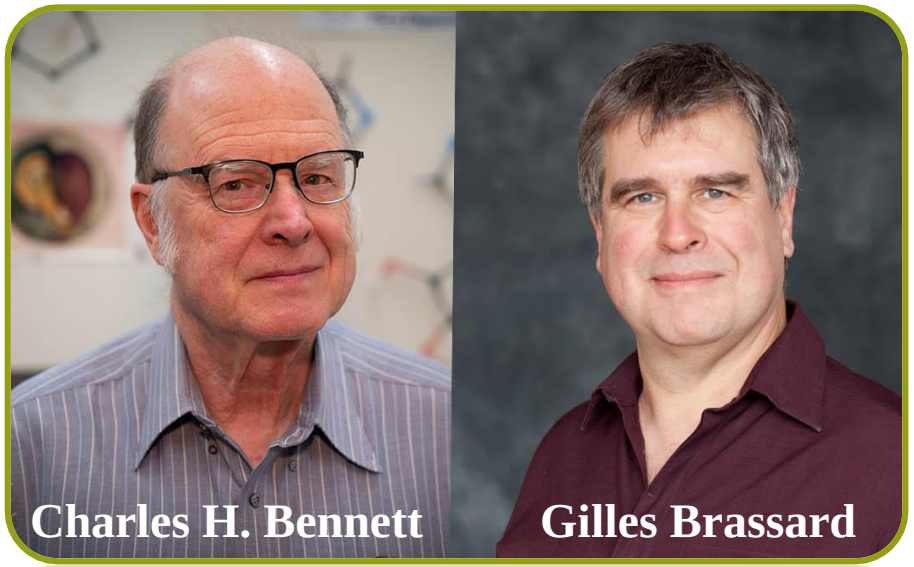
$$\langle 0|+\rangle = \frac{\langle 0|0\rangle + \langle 0|1\rangle}{\sqrt{2}} = \frac{1+0}{\sqrt{2}} \neq 0$$

- اندازه‌گیری دو حالت متعامد $|0\rangle$ و $|1\rangle$ چنین ابهامی ندارد.

$$\langle 0|1\rangle = 0$$

پروتکل BB84: مقدمه

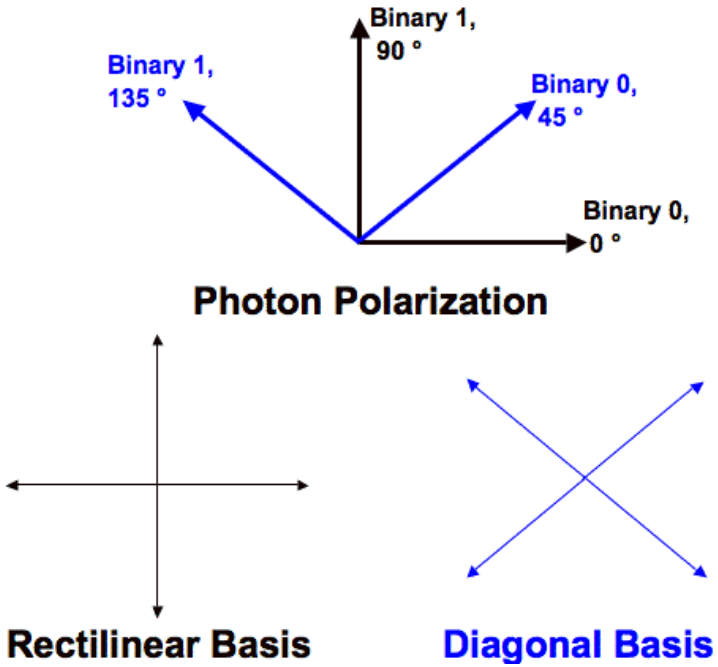
- اولین و معروف‌ترین پروتکل QKD در سال ۱۹۸۴ توسط بنت و براسارد



- نمایش قطبش عمودی را با $|V\rangle$ (معادل $|0\rangle$) و قطبش افقی را را با $|H\rangle$ (معادل $|1\rangle$)
- در این‌صورت قطبش‌های قطری $|D\rangle$ (معادل $|+\rangle$) و پادقطری $|A\rangle$ (معادل $|-\rangle$)

$$|D\rangle = \frac{|V\rangle + |H\rangle}{\sqrt{2}} \qquad |A\rangle = \frac{|V\rangle - |H\rangle}{\sqrt{2}}$$

پروتکل BB84: مقدمه



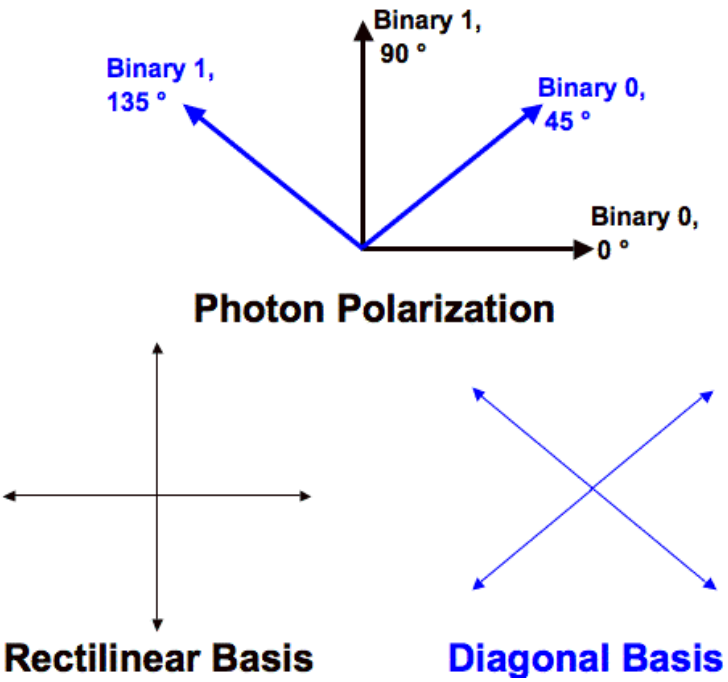
$$|D\rangle = \frac{|V\rangle + |H\rangle}{\sqrt{2}} \qquad |A\rangle = \frac{|V\rangle - |H\rangle}{\sqrt{2}}$$

- دو بیت تصادفی x و y

x	Key value
0	Binary 0
1	Binary 1

y	Chosen basis
0	Rectilinear Basis
1	Diagonal Basis

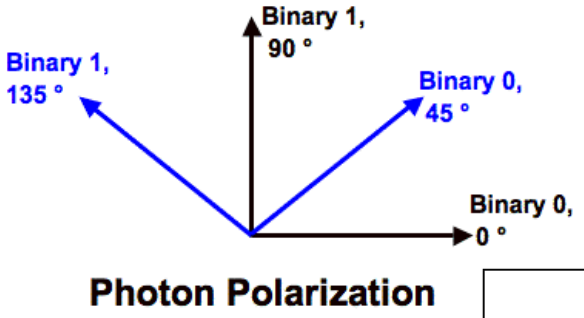
پروتکل BB84



- فاز کوانتومی:

1. تولید دو رشته بیت تصادفی x و y (احتمال برابر تولید ۰ و ۱ در هر رشته)
2. کدگذاری کیوبیت‌ها مطابق روش ذکر شده و ارسال آن‌ها از طریق کانال کوانتومی
3. دریافت حالت کوانتومی در گیرنده و کدبرداری در پایه‌ی خطی یا قطری با توجه به رشته بیت تصادفی y'
4. اندازه‌گیری حالت کوانتومی و دریافت رشته کلید خام x^{raw}

پروتکل BB84: مثال



Photon Polarization

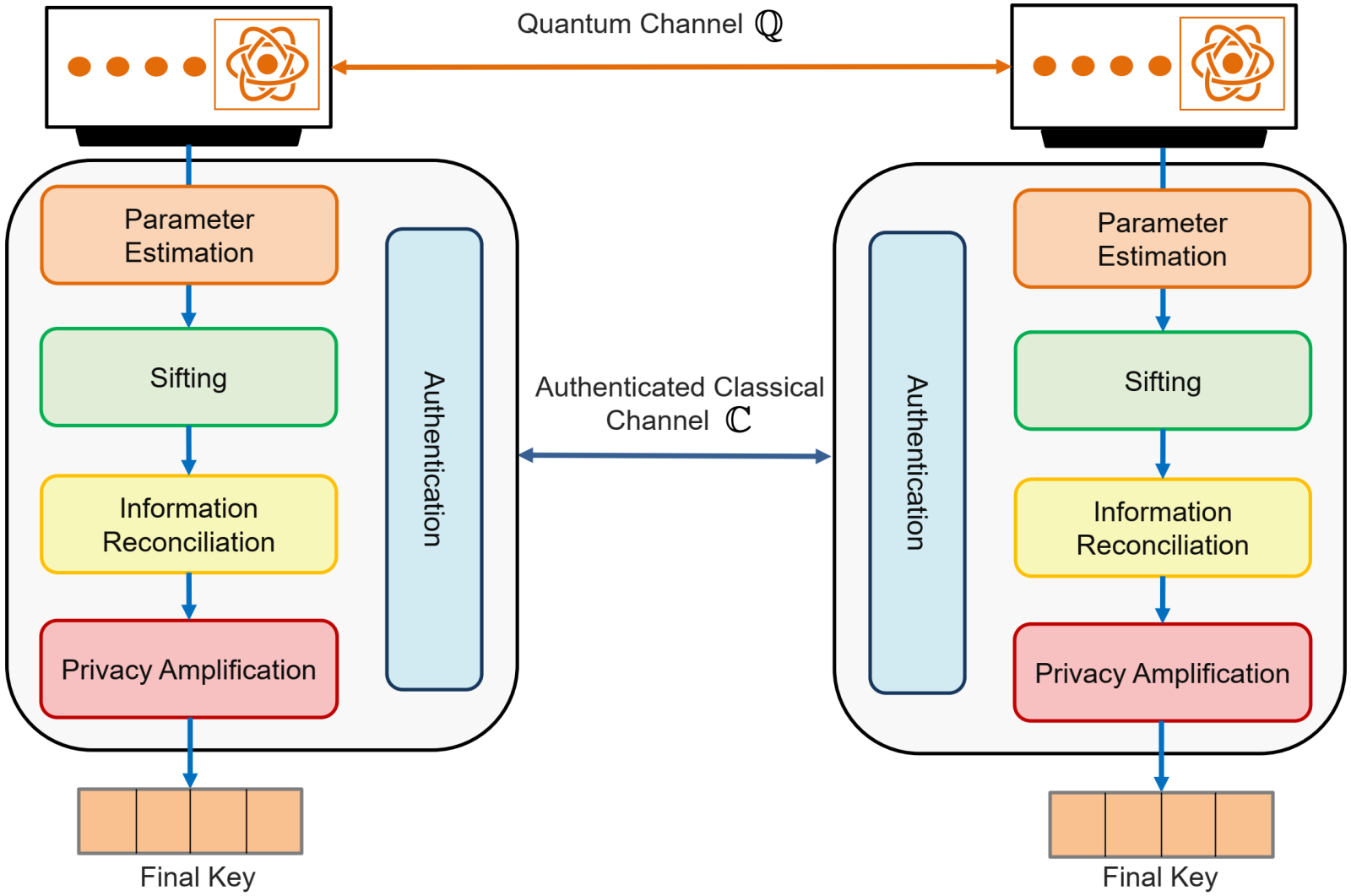
Alice	Transmission									Bob
Key sequence x	1	1	0	0	1	0	1	0	1	
Basis sequence y	1	0	0	0	0	1	1	1	1	
Preparation basis	×	+	+	+	+	×	×	×	×	
Qubit sequence	↖	↑	→	→	↑	↗	↖	↗	↖	
	1	1	0	1	0	0	1	1	0	Basis sequence y'
	×	×	+	×	+	+	×	×	+	Measurement basis
	1	1	0	1	1	1	1	0	1	Measured bit values x^{raw}
Basis matching	✓	✗	✓	✗	✓	✗	✓	✓	✗	Basis matching
Sifted key	1	-	0	-	1	-	1	0	-	Sifted key

پروتکل BB84

- فاز کلاسیک:

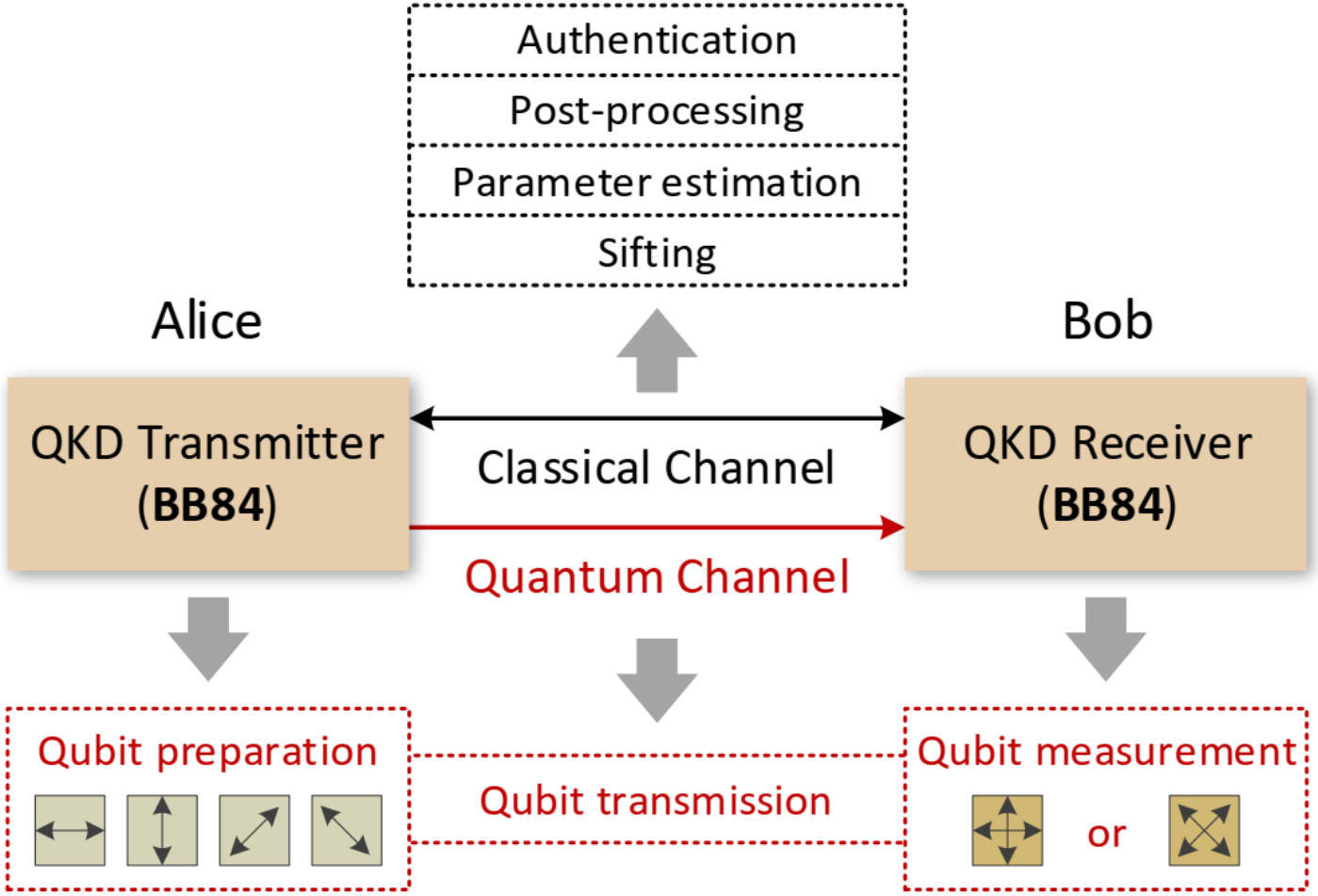
1. اعلام عمومی پایه‌ها و غربال کلید
2. تخمین پارامتر: اعلام عمومی بخشی از کلید
3. تصحیح خطا
4. تقویت امنیت

پروتکل BB84



Luo et al., 2024, An Overview of Postprocessing in QKD, Math. (MDPI)

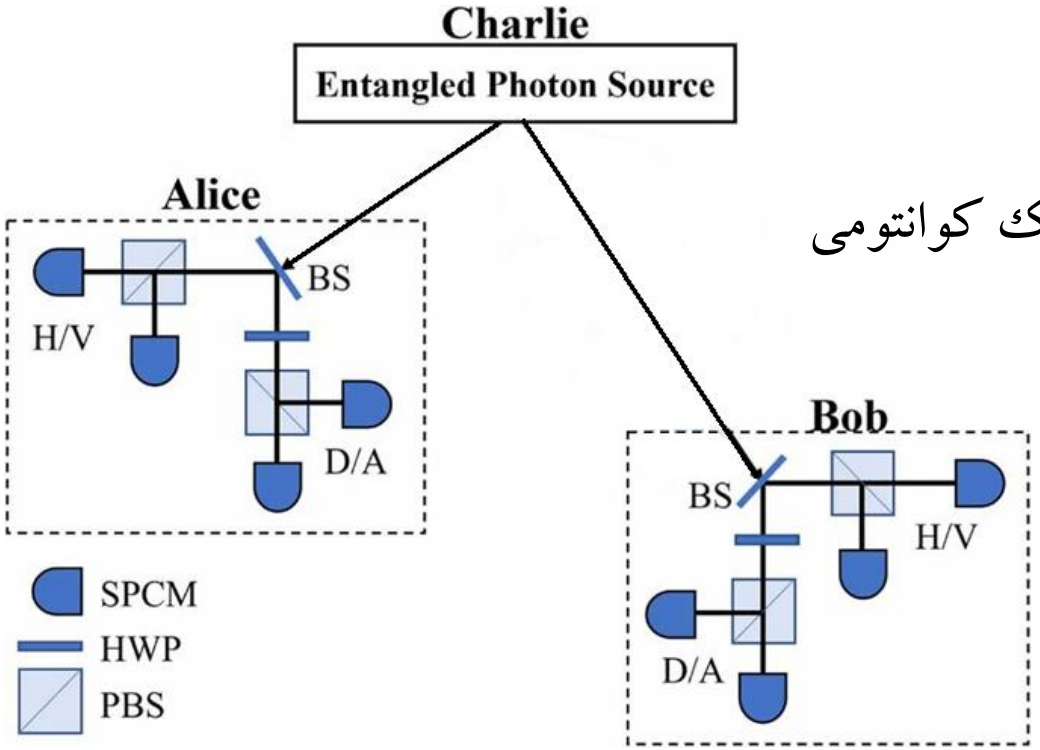
پروتکل BB84



Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

اشاره‌ای به حالت در هم تنیده پروتکل BB84

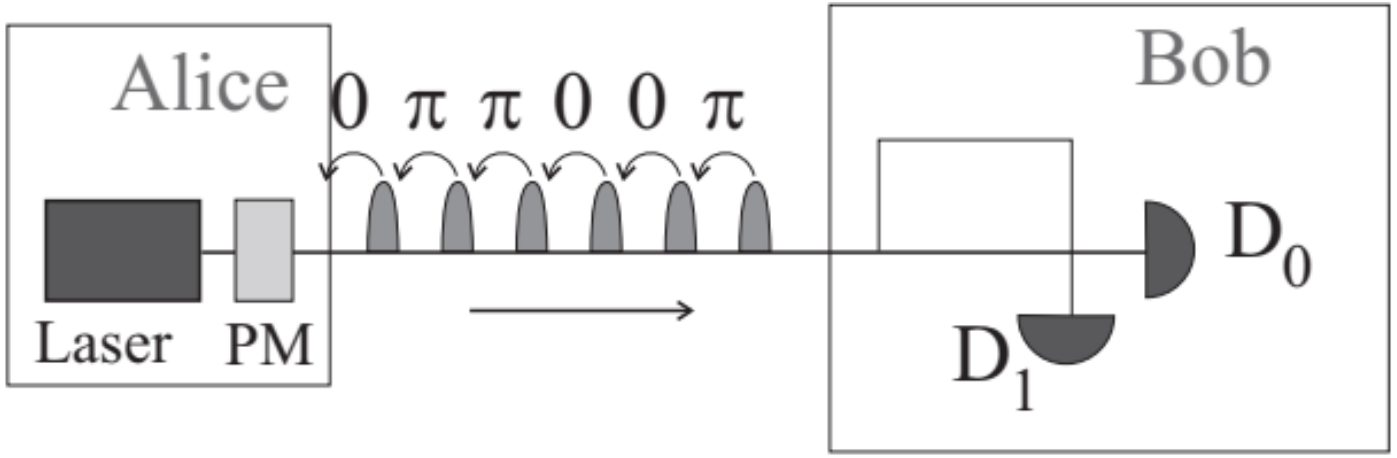
- اشتراک حالت در هم تنیده‌ی $\frac{1}{\sqrt{2}}(|V\rangle|V\rangle + |H\rangle|H\rangle)$ بین فرستنده و گیرنده
- پایه‌های فرستنده و گیرنده یکسان: بیت کلید یکسان (در صورت عدم حضور شنودگر)
- پایه‌های فرستنده و گیرنده متفاوت: به احتمال 50% بیت کلید یکسان
- ردیابی و تشخیص حضور شنودگر
- تضمین امنیت به اشتراک گذاری کلید بر اساس قوانین مکانیک کوانتومی



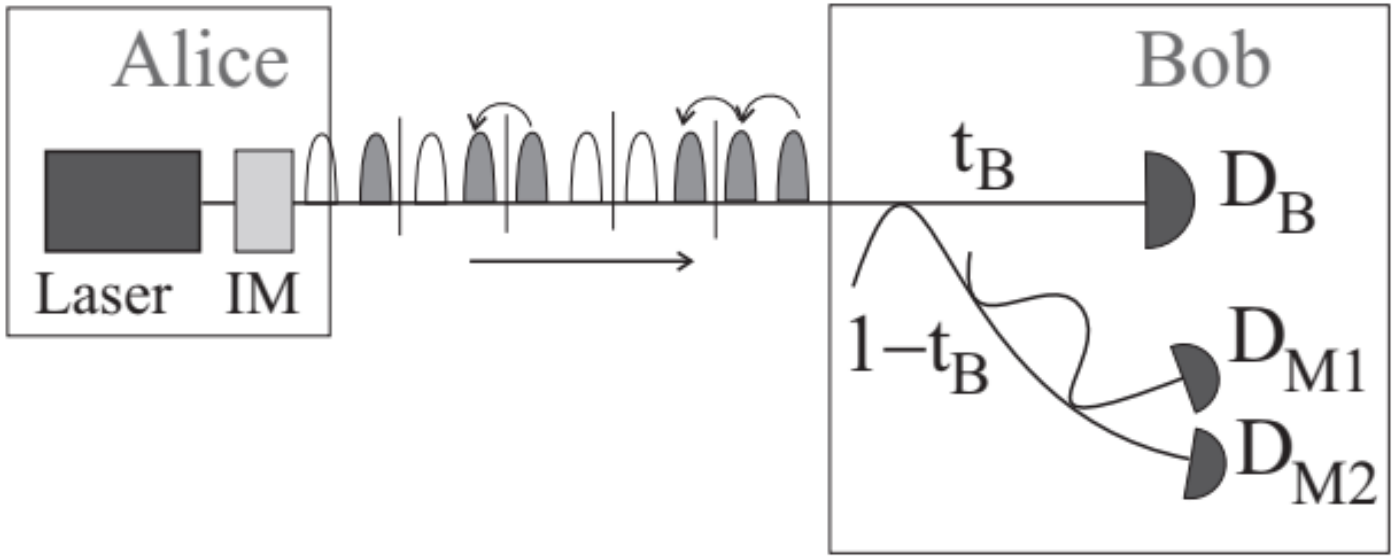
Mishra et al., 2022, *BBM92 QKD over a free space dusty channel of 200 meters*, J. Opt.

پروتکل‌های DPS و COW

DPS

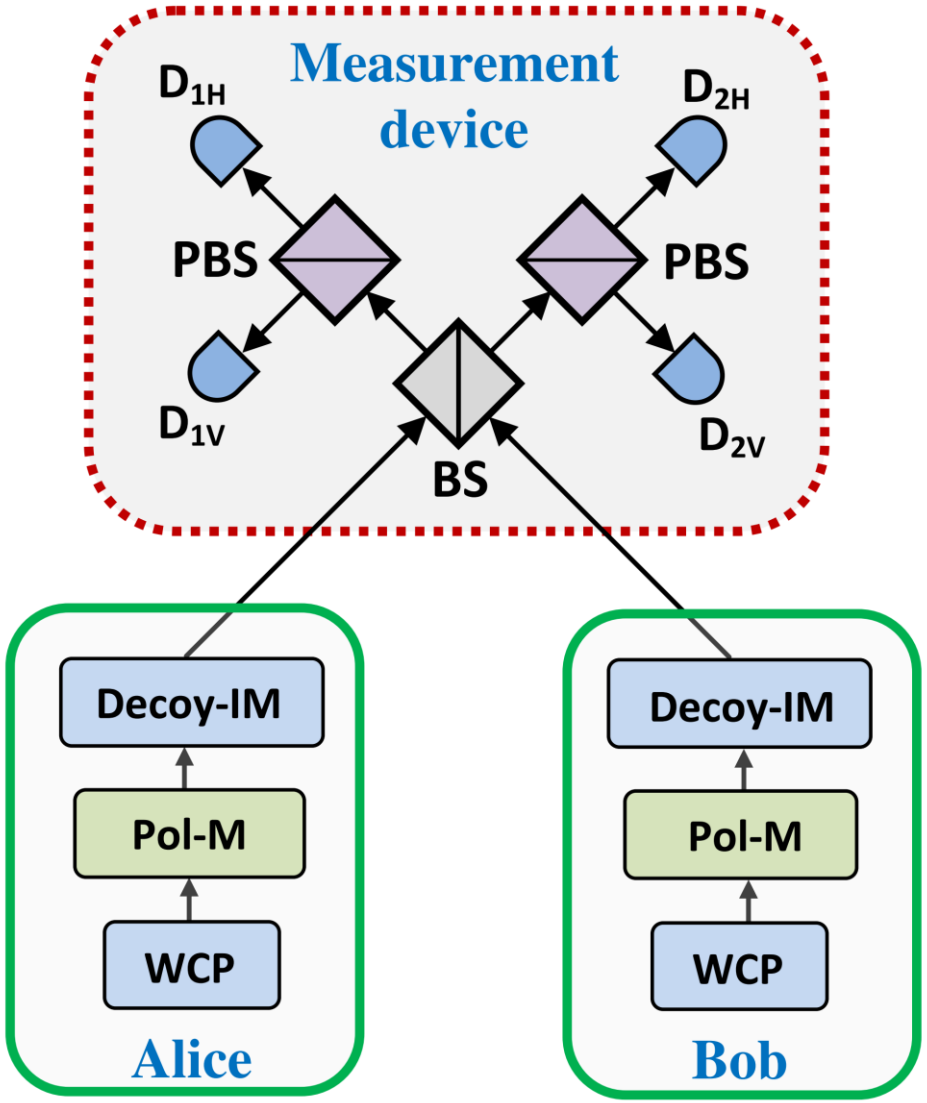


COW



Scarani et al., 2009, *The security of practical quantum key distribution*, Rev. Mod. Phys.

پروتکل MDI

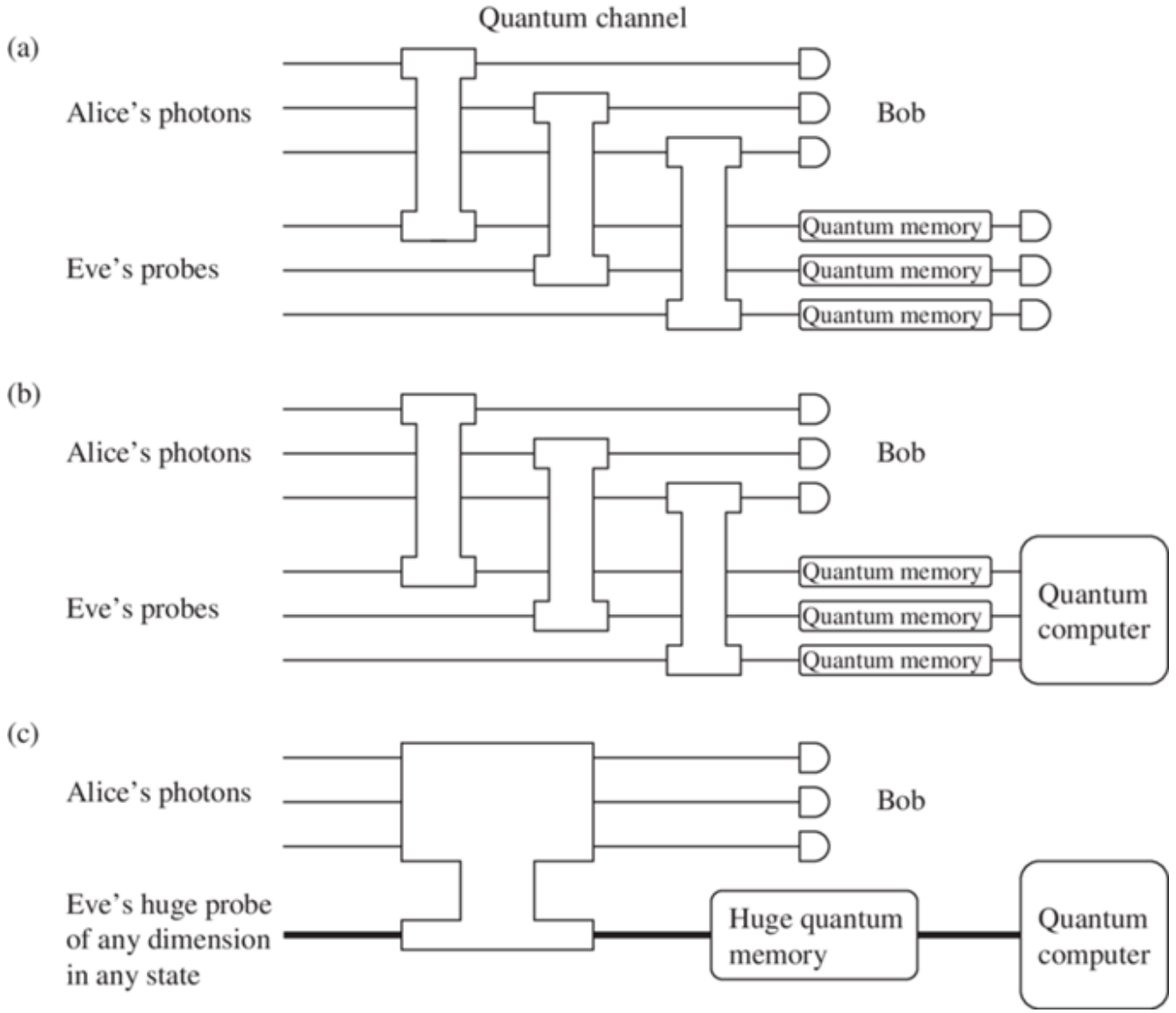


Lo et al., 2012, *Measurement-Device-Independent QKD*, PRL.

معیارهای ارزیابی سیستم QKD

- نرخ کلید امن (SKR) و نرخ خطای بیت کوانتومی (QBER)
- طول کانال
- مقاومت در برابر حملات
- هزینه‌ی پیاده‌سازی
- احتمال شکست کلید (شنودگر حداقل یک بیت از کلید را به دست آورد)
- طول موج سیگنال‌های کوانتوم و کنترلی
- نرخ پالس ساعت مورد نیاز
- نوع کانال

حملات کوانتومی



Diamanti, 2006, *Stanford University*, PhD Thesis.

حملات کوانتومی

Attack	Source/Detection	Target component	Manner	Year
Photon-number-splitting (Brassard *et al.*, 2000; Lütkenhaus, 2000)	Source	WCP (multi-photons)	Theory	2000
Detector fluorescence (Kurtsiefer *et al.*, 2001)	Detection	Detector	Theory	2001
Faked-state (Makarov *et al.*, 2006; Makarov and Hjelme, 2005)	Detection	Detector	Theory	2005
Trojan horse (Gisin *et al.*, 2006; Vakhitov *et al.*, 2001)	Source&Detection	Backflection light	Theory	2006
Time shift (Qi *et al.*, 2007a; Zhao *et al.*, 2008)	Detection	Detector	Experiment*	2007
Time side-channel (Lamas-Linares and Kurtsiefer, 2007)	Detection	Timing information	Experiment	2007
Phase remapping (Fung *et al.*, 2007; Xu *et al.*, 2010)	Source	Phase modulator	Experiment*	2010
Detector blinding (Lydersen *et al.*, 2010; Makarov, 2009)	Detection	Detector	Experiment*	2010
Detector blinding (Gerhardt *et al.*, 2011a,b)	Detection	Detector	Experiment	2011
Detector control (Lydersen *et al.*, 2011a; Wiechers *et al.*, 2011)	Detection	Detector	Experiments	2011
Faraday mirror (Sun *et al.*, 2011)	Source	Faraday mirror	Theory	2011
Wavelength (Huang *et al.*, 2013; Li *et al.*, 2011)	Detection	Beam-splitter	Experiment	2011
Dead-time (Henning *et al.*, 2011)	Detection	Detector	Experiment	2011
Channel calibration (Jain *et al.*, 2011)	Detection	Detector	Experiment*	2011
Intensity (Jiang *et al.*, 2012; Sajeed *et al.*, 2015b)	Source	Intensity modulator	Experiment	2012
Phase information (Sun *et al.*, 2012, 2015; Tang *et al.*, 2013)	Source	Phase randomization	Experiment	2012
Memory attacks (Barrett *et al.*, 2013)	Detection	Classical memory	Theory	2013
Local oscillator (Jouguet *et al.*, 2013a; Ma *et al.*, 2013b)**	Detection	Local oscillator	Experiment	2013
Trojan horse (Jain *et al.*, 2014, 2015)	Source&Detection	Backflection light	Experiment	2014
Laser damage (Bugge *et al.*, 2014; Makarov *et al.*, 2016)	Detection	Detector	Experiment	2014
Laser seeding (Sun *et al.*, 2015)	Source	Laser phase/intensity	Experiment	2015
Spatial mismatch (Chaiwongkhot *et al.*, 2019; Sajeed *et al.*, 2015a)	Detection	Detector	Experiment	2015

Xu et al., 2020, *Secure QKD with realistic devices*, Rev. Mod. Phys.

سیستم‌های QKD تجاری

Model	Company	Protocol	Secret Key rate	Max. Distance	Other specefication
Clavis XG	IDQ	Decoy BB84 (Time-bin)	995 bps @24dB	150 km	Key security parameter =4e-9
Cerberis XG	IDQ	COW (Time-bin)	1991bps @12dB 995bps @18dB	90 km	Key security parameter =4e-9
Multiplexed System	Toshiba	Decoy BB84 (Time-bin)	300 kbps @10dB	+90 km	Key failure probability <1e-10
Long Distance System	Toshiba	Decoy BB84 (Time-bin)	300 kbps @10dB	+150 km	Key failure probability <1e-10
QKD-PHA300	Quantum CTek	Decoy BB84 (Time-bin)	50kbps @ 10dB 1kbps @ 22dB	+100km	Quantum safe: Against attacks such as photon beam separation, light blinding, double counting and facility calibration attack
QKD-POL100	Quantum CTek	Decoy BB84 (Polarization)	1kbps@18dB	-	Quantum security: Against attacks such as photon beam separation, light blinding, double counting, Trojan light and seed light attack

سیستم‌های QKD تجاری

سیستم‌های QKD تجاری

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

1

مقدمه

2

مفاهیم مکانیک کوانتومی

3

کاربردهای درهم‌تنیدگی

4

توزیع کلید کوانتومی

5

شبکه و اینترنت کوانتومی

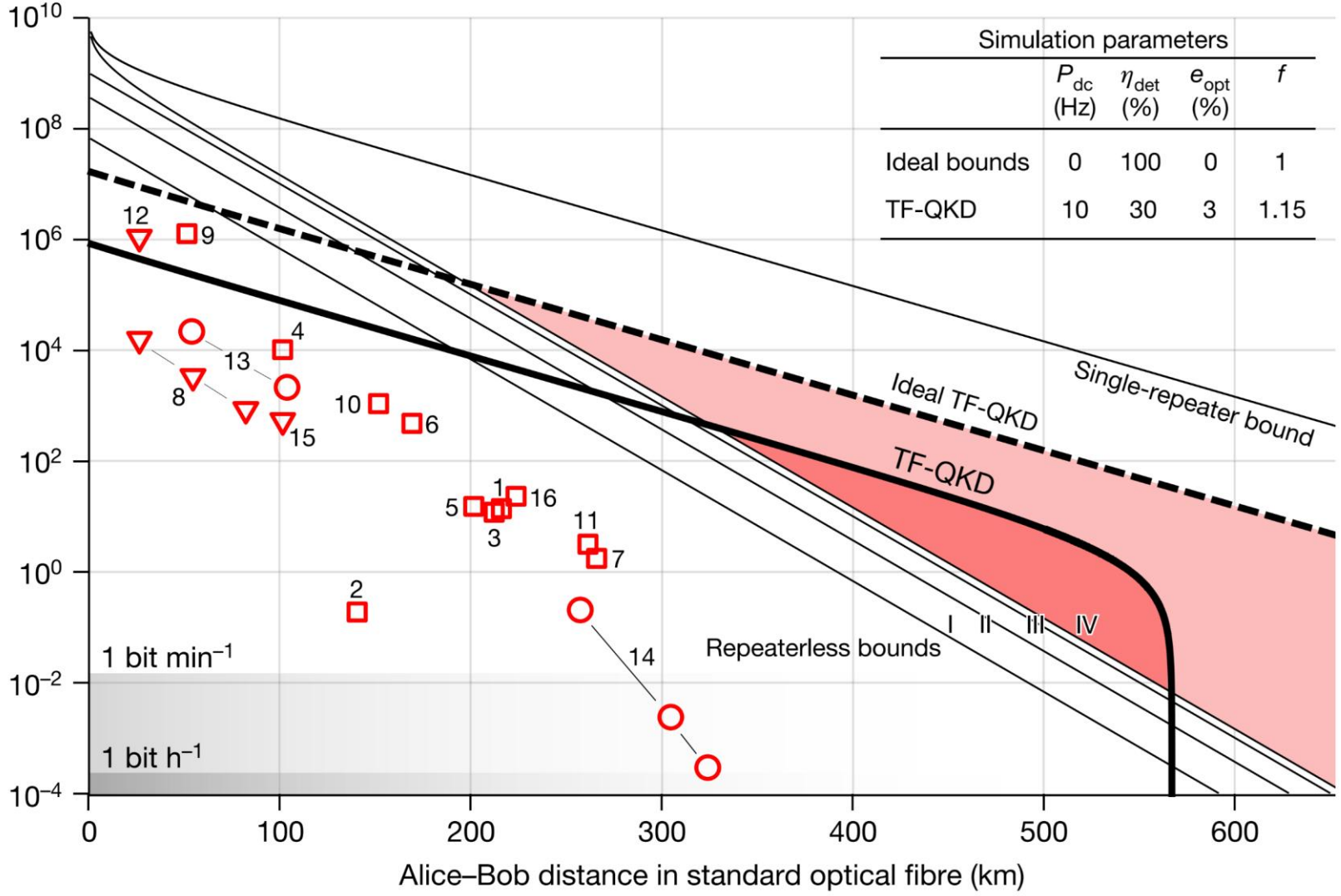
6

سیستم‌های مخابرات کوانتومی

سرفصل مطالب این بخش

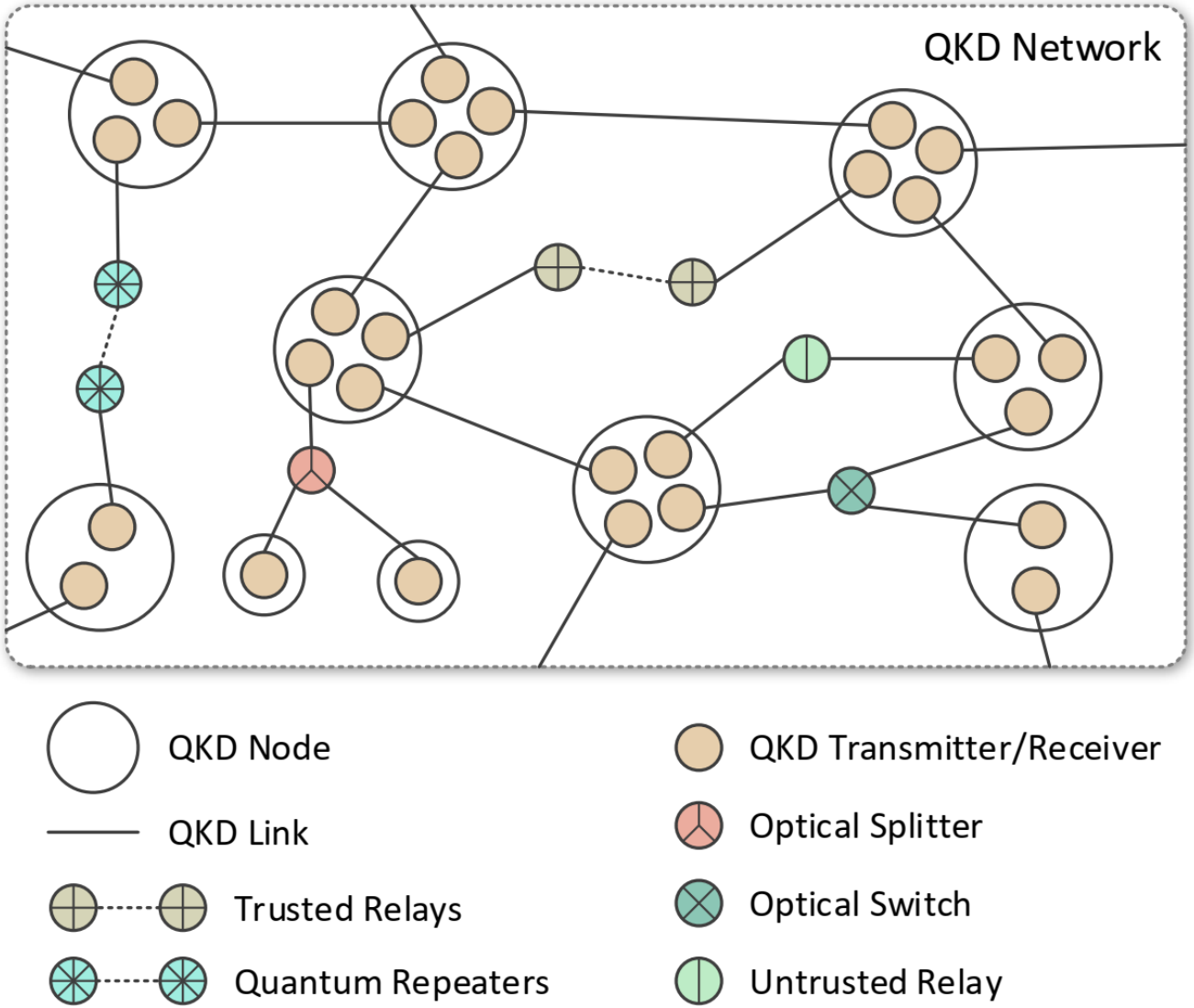
- محدودیت نرخ–فاصله
- روش‌های اتصال نودهای شبکه
- شبکه‌های توزیع کلید کوانتومی در سطح جهان
- شبکه‌های شهری
- شبکه‌های بلندبرد
- لایه‌های شبکه
- مالتی‌پلکسینگ کانال
- چالش‌های طراحی شبکه‌ی QKD
- طرح‌های سازگار با شبکه
- سازگاری بین مودهای مختلف: نگاشت مود
- استانداردهای کوانتومی
- مسیر پیش رو
- اینترنت کوانتومی
- IoT کوانتومی

محدودیت نرخ-فاصله



Lucamarini et al., 2018, *Overcoming the rate–distance limit of QKD without quantum repeaters*, Res. Let.

روش‌های اتصال نودهای شبکه



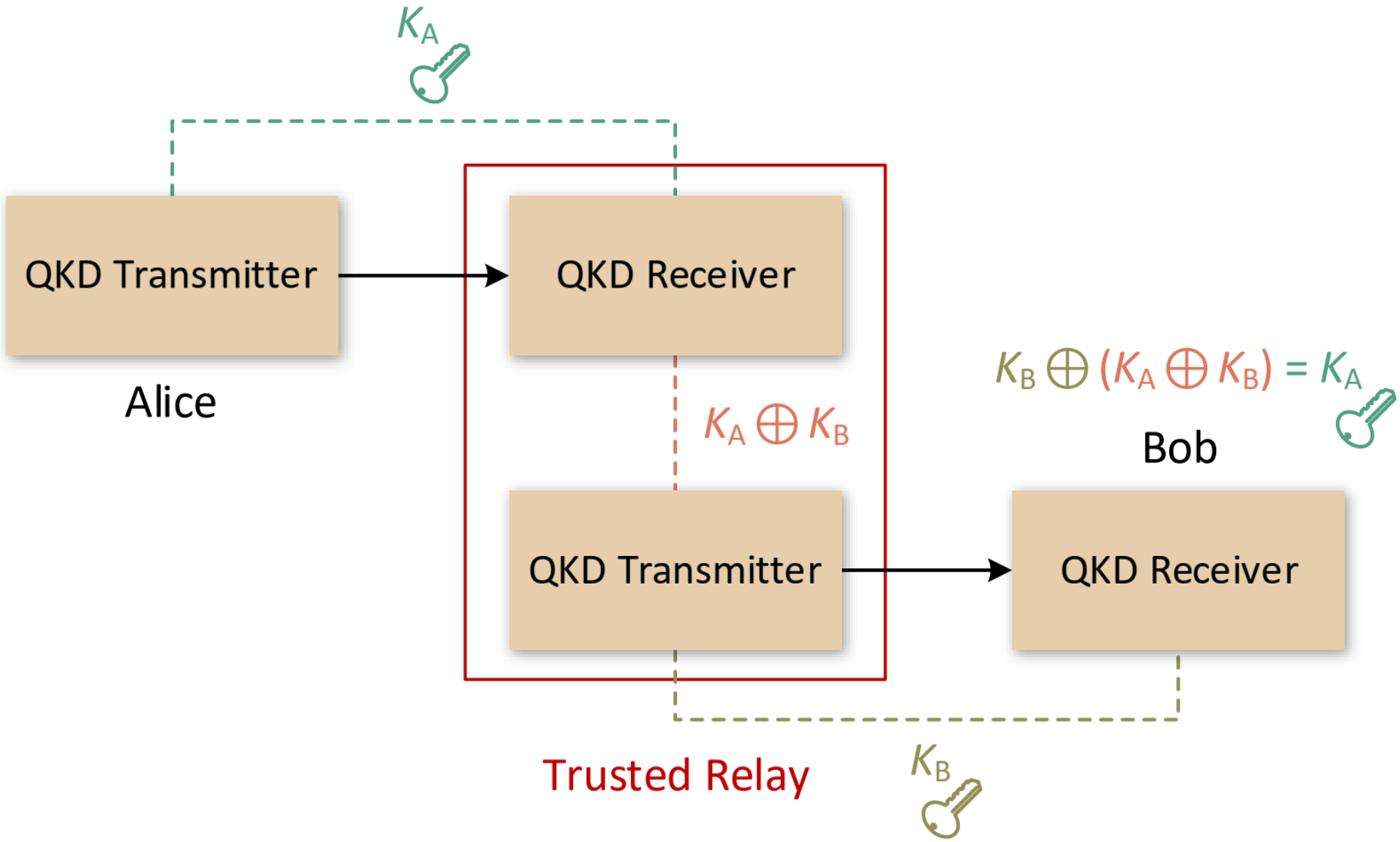
Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

روش‌های اتصال نودهای شبکه

	Optical switching	**Trusted relay-based**	**Untrusted relay-based**	**Quantum repeater**
Achievable distance	Relatively short	Arbitrary	Relatively long	Arbitrary
Scalability	Relatively low	High	Relatively low	High
Applicability	Limited	Wide	Limited	Wide
Security	High	Relatively low	High	High
Maturity	High	High	Relatively low	Low
Field trial	Available	Available	Available	Unavailable

Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

روش‌های اتصال نودهای شبکه: رله‌ی مطمئن



Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

شبکه‌های توزیع کلید کوانتومی در سطح جهان

USA
- Boston (DARPA, 2004)
- Washington, DC (2006)
- NIST local network (2006/2007/2019)
- Columbus, Ohio (2013)
- Cambridge-Lexington (2018)
- Boston-Washington, DC
- Boston-Georgia-California

UK
- Access network in lab (1997/2013)
- Cambridge (2019)
- Cambridge-Ipswich (2019)
- Bristol (2019/2020)
- Cambridge-London-Bristol

Russia
- Kazan (2016)
- Moscow (2017)
- Moscow-St. Petersburg
- Nationwide network

China
- Beijing-Tianjin (2005)
- Beijing (2007)
- Hefei (2008/2009/2012/2016)
- Wuhu (2009/2010)
- Hefei-Chaohu-Wuhu (2011)
- Jinan (2013)
- Shanghai (2016)
- Beijing-Shanghai (2017)
- Wuhan (2017)
- Zhucheng-Huangshan (2018)
- Wuhan-Hefei (2018)
- China-Austria (Xinglong-Graz, 2018)
- Xi'an/Guangzhou (2019)
- Integr. space-to-ground (2021)
- Jinan-Qingdao (2021)
- Nationwide network

Canada
- Calgary (2013)

Europe
- Vienna, Austria (SECOQC, 2008)
- Geneva, Switzerland (SwissQuantum, 2009)
- Madrid, Spain (2009/2014/2018/2020)
- Paris, France (2010)
- Austria-China (Graz-Xinglong, 2018)
- Eindhoven, Netherlands (2019)
- Florence, Italy (2019)
- European Union Network (OpenQKD)

South Africa
- Durban (2009/2010)

Japan
- Tokyo (2010/2013/2015)
- Nationwide network

South Korea
- Seongsu-Bundang (2016)
- Metropolitan network (2016)
- Nationwide network

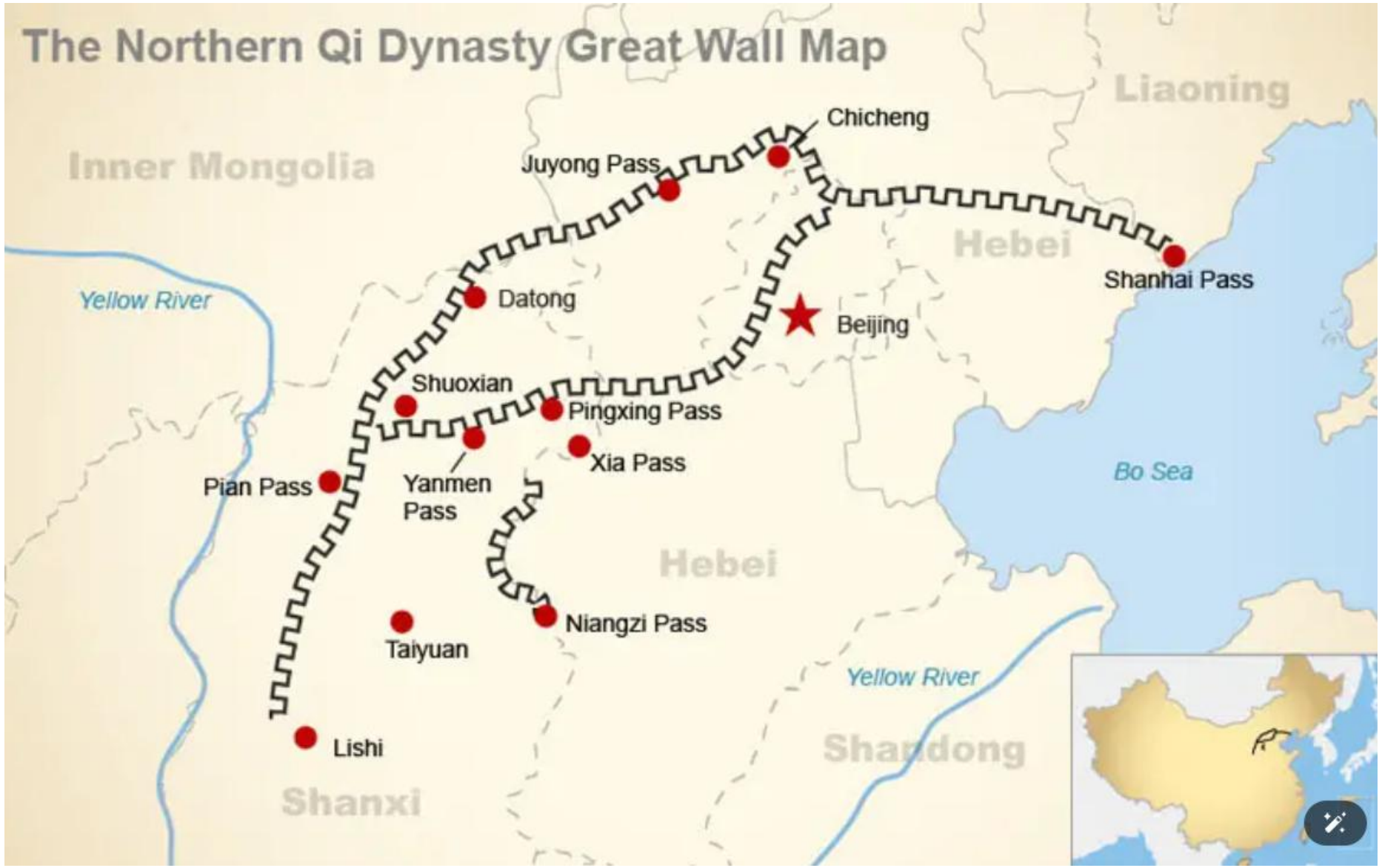
Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

شبکه‌های شهری

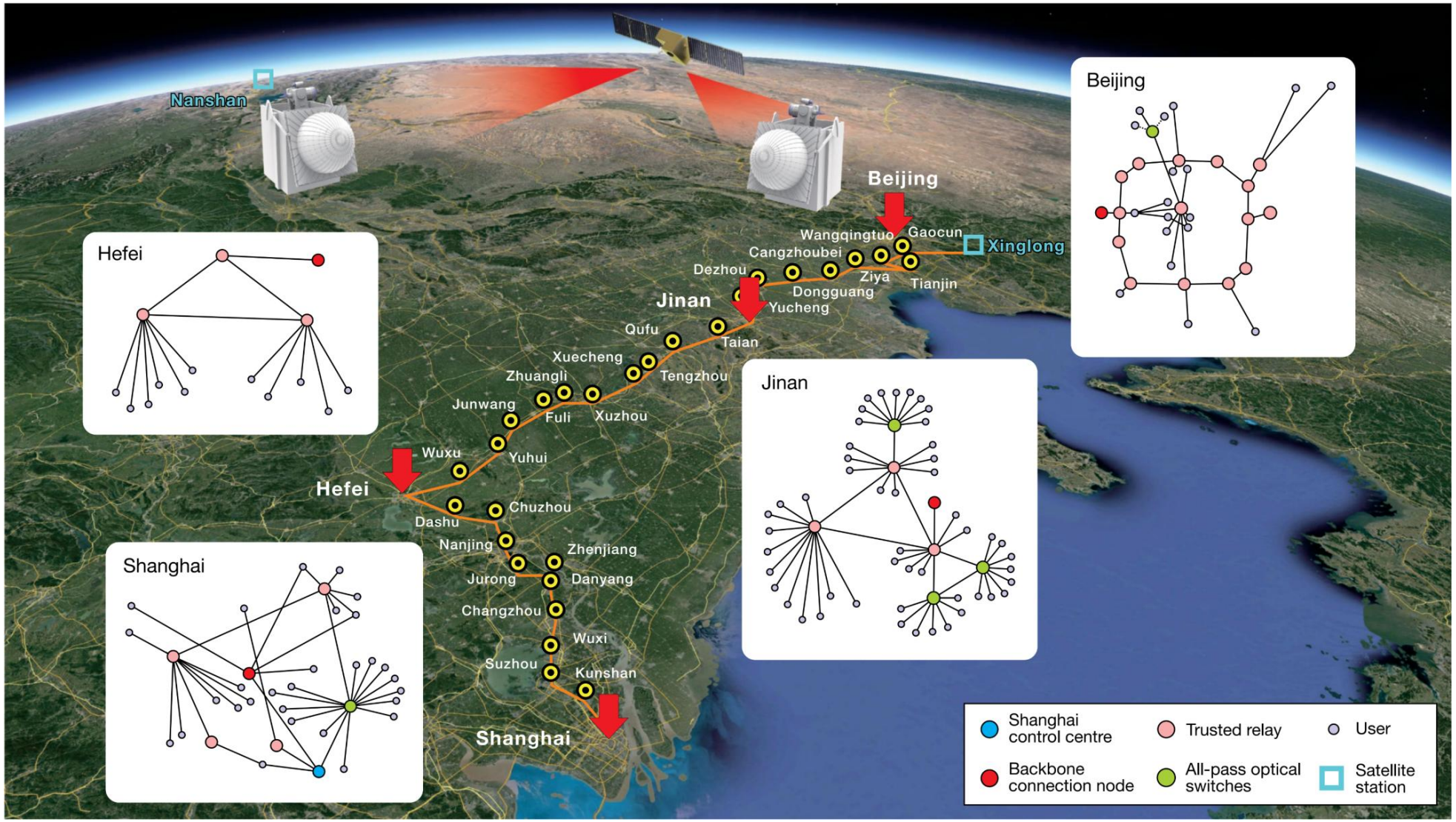
Metropolitan area	Optical switching	Trusted relay	Number of nodes	Link type	Longest link		Maximum secret-key rate	QKD type	Year	
					Length	Loss				
Boston	✓	✓	10	Optical fiber Free space	29.8 km	16.6 dB	10 kbps	DV	2004	
Beijing	✓	×	4	Optical fiber	42.6 km	16.4 dB	N/A	DV	2007	BB84/ Decoy BB84
Vienna	×	✓	6	Optical fiber Free space	85 km	20.4 dB	17 kbps	DV CV	2008	BB84/ Decoy BB84/ COW /SARG04/BBM92/CV
Hefei	×	✓	3	Optical fiber	20 km	5.6 dB	1.6 kbps	DV	2008	Decoy BB84
Geneva	×	✓	3	Optical fiber	17.1 km	–5.3 dB	2.4 kbps	DV	2009	SARG04
Durban	✓	✓	4	Optical fiber	27 km	N/A	891 bps	DV	2009	
Wuhu	✓	✓	7	Optical fiber	10 km	6.23 dB	2.53 kbps	DV	2009	
Hefei	✓	✓	5	Optical fiber	60 km	17 dB	4.5 kbps	DV	2009	
Madrid	✓	×	3	Optical fiber	N/A	N/A	N/A	DV	2009	
Wuhu	✓	×	5	Optical fiber	N/A	14.77 dB	4.91 kbps	DV	2010	
Tokyo	×	✓	6	Optical fiber	90 km	27 dB	304 kbps	DV	2010	Decoy BB84/ /SARG04 /BBM92/DPS
Hefei	✓	✓	46	Optical fiber	N/A	N/A	N/A	DV	2012	
Columbus	×	✓	4	Optical fiber	N/A	N/A	N/A	DV	2013	
Jinan	✓	✓	56	Optical fiber	N/A	N/A	N/A	DV	2013	
Madrid	✓	×	3	Optical fiber	16 km	5.12 dB	N/A	DV	2014	
Hefei	✓	×	4	Optical fiber	55 km	17.3 dB	38.8 bps	DV	2016	MDI
Shanghai	×	×	4	Optical fiber	19.92 km	15.1 dB	10 kbps	CV	2016	GG02
Kazan	×	✓	4	Optical fiber	12.4 km	6.8 dB	19.6 kbps	DV	2016	
South Korea	×	×	5	Optical fiber	107 km	N/A	N/A	DV	2016	
Moscow	×	✓	3	Optical fiber	30 km	13 dB	0.1 kbps	DV	2017	
Wuhan	✓	✓	>60	Optical fiber	N/A	N/A	N/A	DV	2017	
Madrid	×	✓	3	Optical fiber	26.4 km	11 dB	70 kbps	CV	2018	
Bristol	✓	×	4	Optical fiber	2.7 km	N/A	3.17 kbps	DV	2019	
Cambridge	×	✓	3	Optical fiber	10.6 km	3.9 dB	2.58 Mbps	DV	2019	Modified Decoy BB84 (T12)
Madrid	✓	✓	11	Optical fiber	55 km	12 dB	N/A	CV	2020	
Bristol	×	×	8	Optical fiber	16.9 km	29 dB	83.9 kbps	DV	2020	BBM92
Hefei	✓	✓	46	Optical fiber	18 km	N/A	60.5 kbps	DV	2021	

Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

شبکه‌های شهری



شبکه‌های شهری



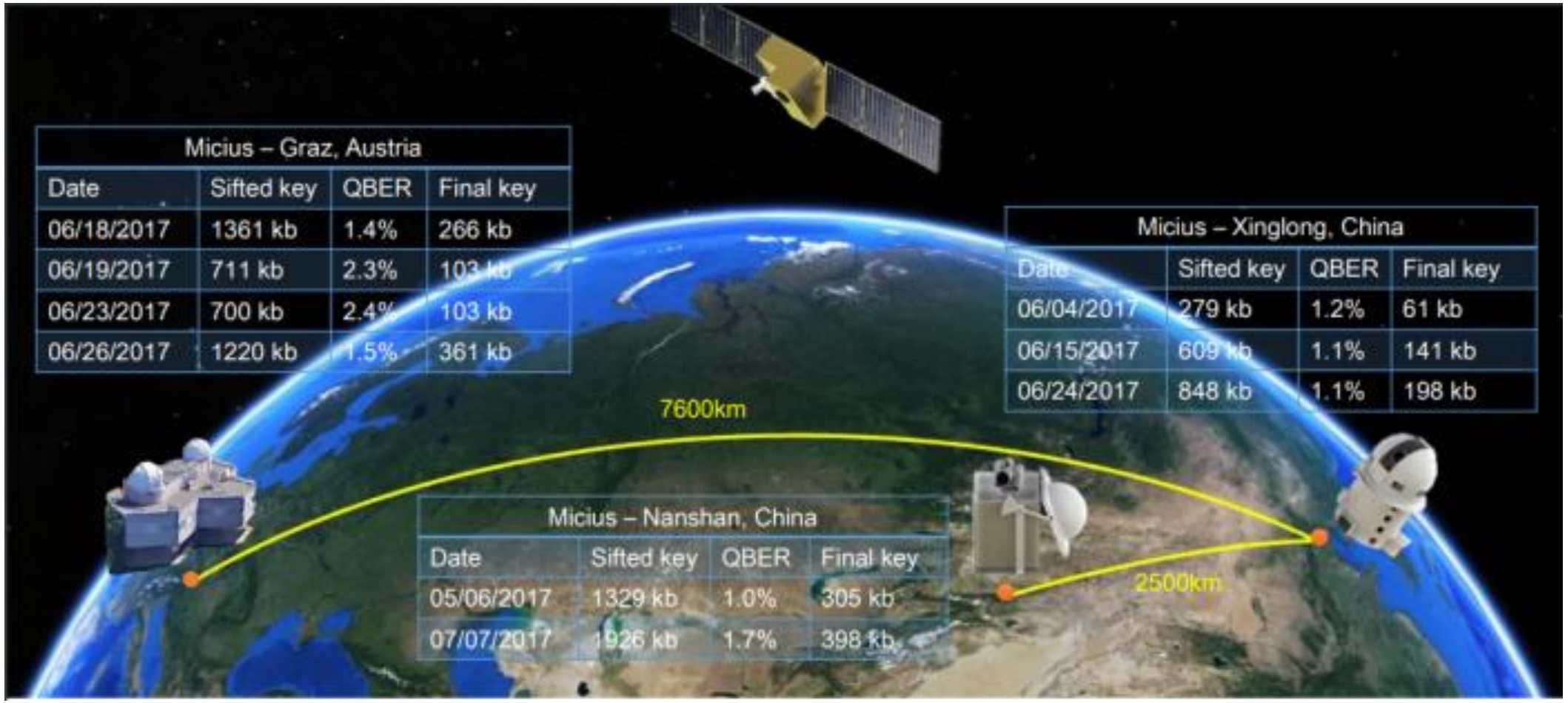
Chen et al., 2021, *An integrated space-to-ground quantum communication network over 4,600 kilometres*, Nature

شبکه‌های بلندبرد

Long-haul network	Trusted relay	Number of nodes	Number of links	Link type	Link span	QKD type	Year	Reference	Remark
Hefei-Chaohu-Wuhu	✓	9	8	Optical fiber	199 km	DV	2011	[180]	Long-term demonstration
Beijing-Shanghai	✓	32	31	Optical fiber	2,000 km	DV	2017	[46], [181]	Ultra-long QKD network Real-world applications
Zhucheng-Huangshan	×	2	1	Optical fiber	66 km	DV	2018	[182]	QKD integration with a commercial backbone network
Wuhan-Hefei	✓	11	10	Optical fiber	609 km	DV	2018	[183]	Real-world applications
China-Austria	✓	3	2	Free space	7,600 km	DV	2018	[48]	First satellite-relayed intercontinental QKD network
Cambridge-Ipswich	✓	5	4	Optical fiber	121 km	DV	2019	[128]	Co-fiber transmission of quantum and classical traffic
Integrated Space-to-Ground (China)	✓	Multiple	>702	Optical fiber Free space	4,600 km	DV	2021	[49]	Large-scale integrated space-to-ground QKD network
Jinan-Qingdao	×	3	2	Optical fiber	511 km	DV	2021	[184]	Field deployment of TF-QKD

Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

شبکه‌های بلندبرد

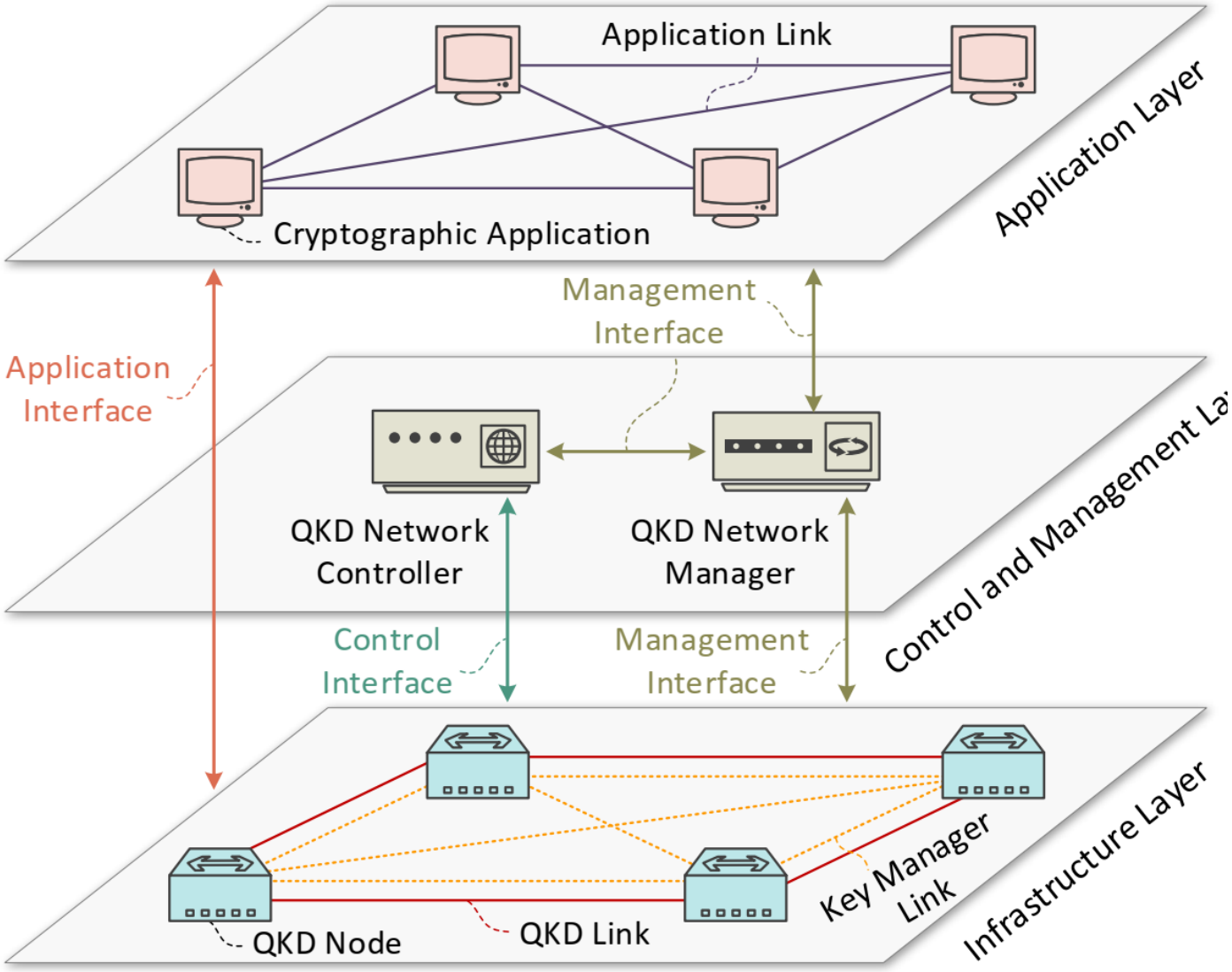


Liao et al., 2018, *Satellite-relayed intercontinental quantum network*, PRL.

Architecture	Feature (from bottom to top layers)	Manner	Year
Three-layer architecture	Quantum layer, Secret's layer, Data layer	Field trial	2008
	Quantum layer, Key management layer, Application layer	Field trial	2009
	Quantum layer, Key management layer, Communication layer	Field trial	2010
	Quantum layer, Key management layer, Application layer	Field trial	2010
	Physical layer, Quantum key management layer, Application layer	Experiment	2013
	Infrastructure layer, Control and management layer, Application layer	Theory	2016
	Quantum layer, Network key delivery layer, Application layer	Field trial	2019
	QKD layer, Control layer, Application layer	Theory	2019
	Infrastructure layer, Control layer, Application layer	Experiment	2019
	QKD layer, Control layer, Application layer	Experiment	2019
Four-layer architecture	Data layer, Key generation layer, Connection layer, Key management layer	Experiment	2009
	Optical layer, QKD layer, Control layer, Application layer	Theory	2017
	Data layer, QKD layer, Control layer, Application layer	Theory	2017
	Quantum layer, Key management layer, Key supply layer, Application layer	Experiment	2017
	Data layer, QKD layer, Control layer, Application layer	Theory	2018
	Optical layer, QKD layer, Control layer, Application layer	Theory	2019
Five-layer architecture	Quantum physical layer, Quantum logical layer, Classical physical layer, Classical logical layer, Application layer	Field trial	2021
Six-layer architecture	Quantum layer, Key management layer, QKD network control layer, QKD network management layer, Service layer, User network management layer	Recommendation	2019

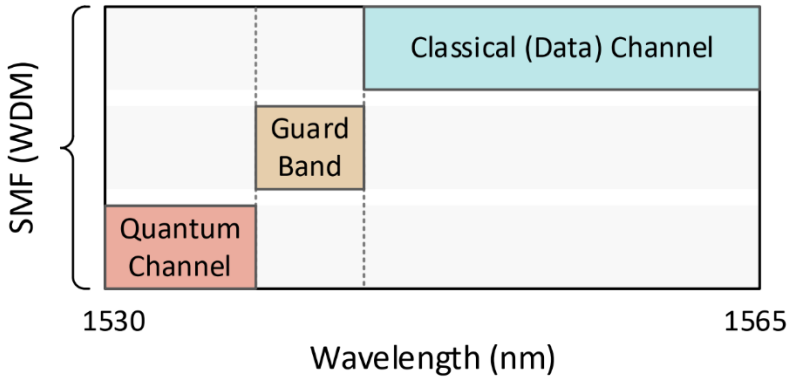
Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

لایه‌های شبکه

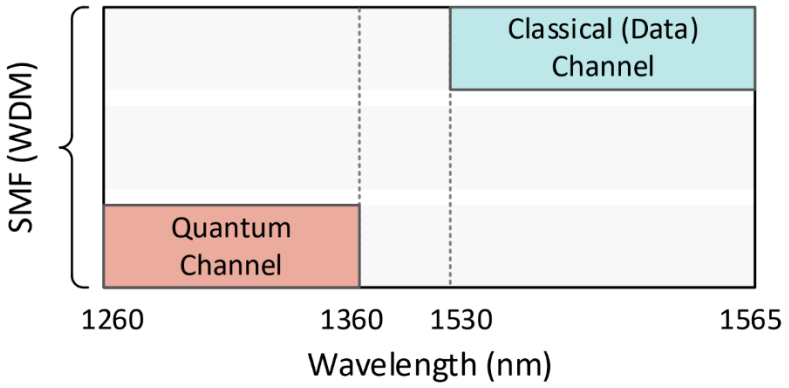


Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

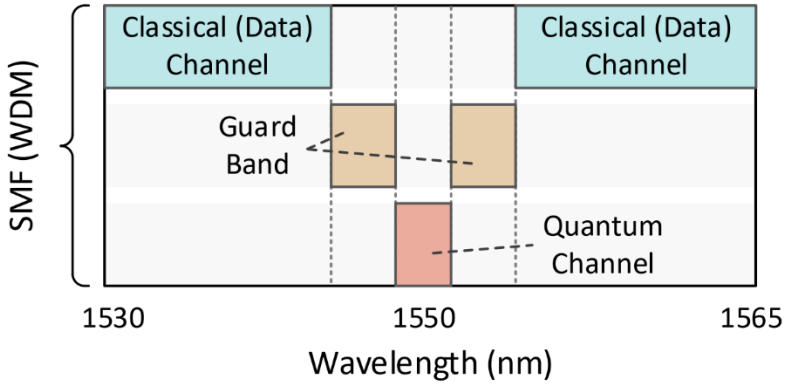
مالتی‌پلکسینگ کانال



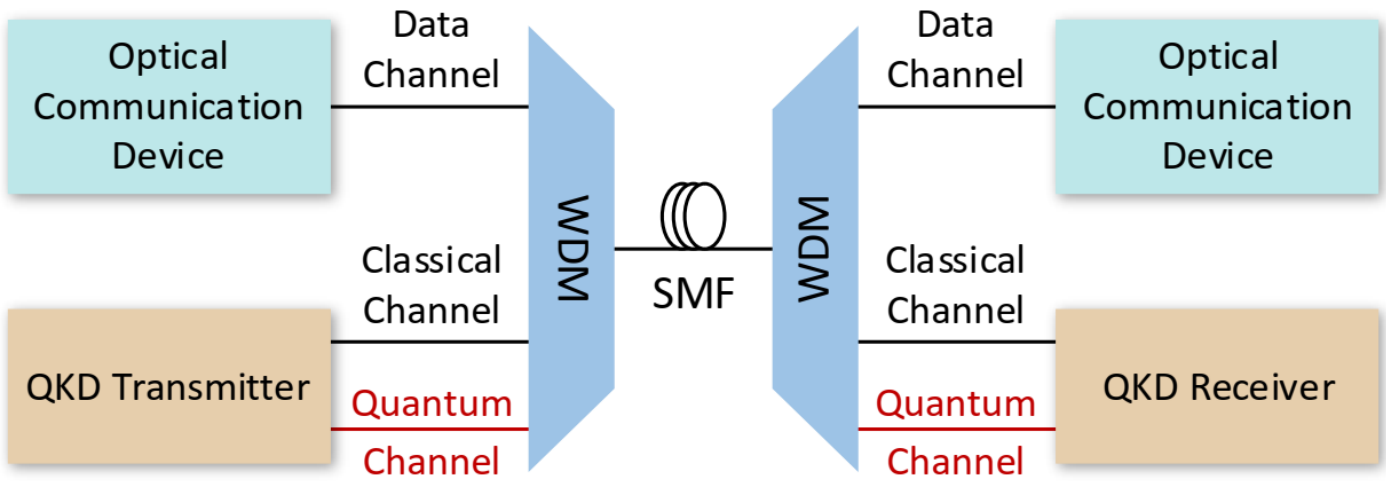
(a)



(b)



(c)

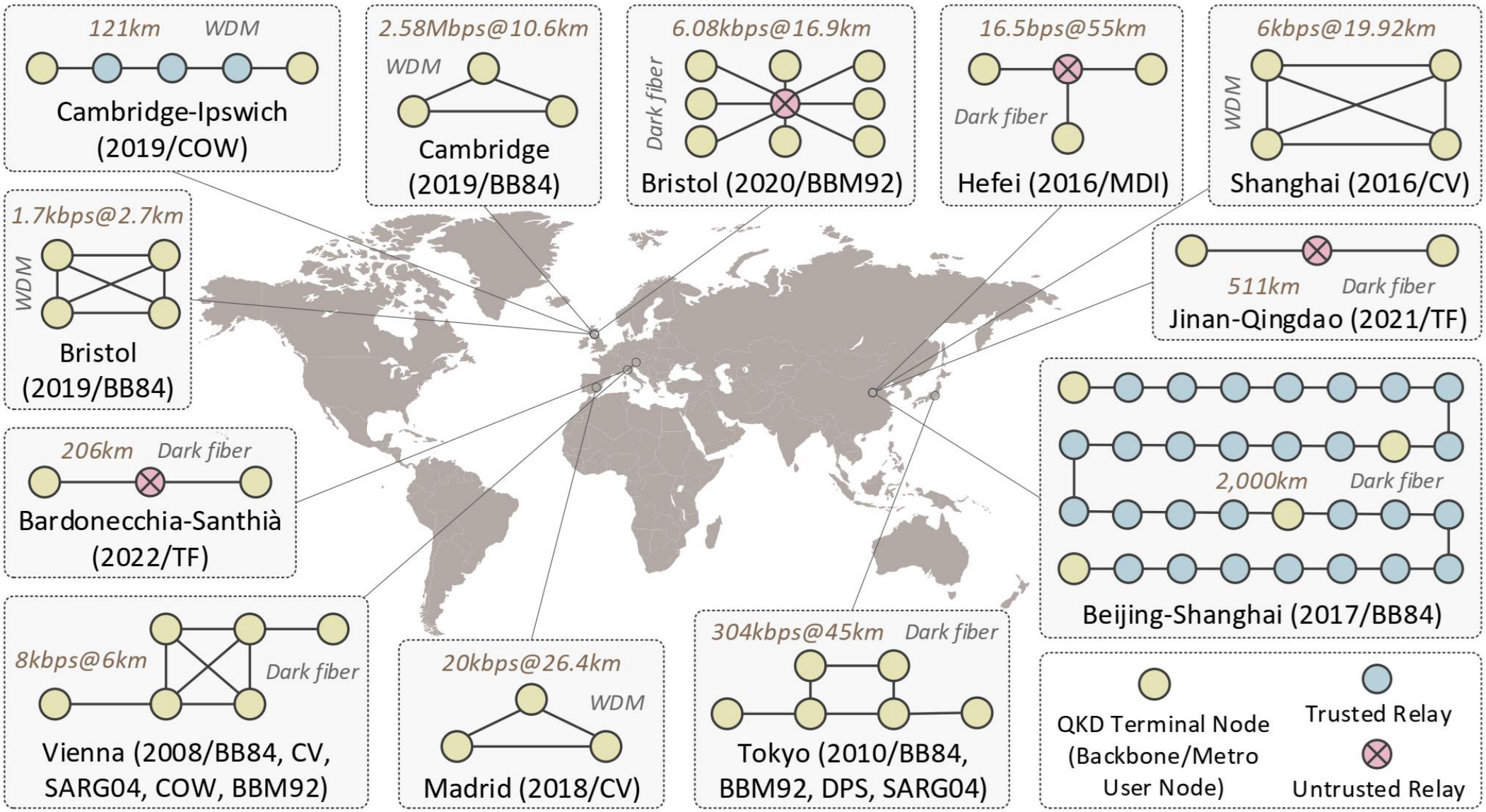


Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

چالش‌های طراحی شبکه‌ی QKD

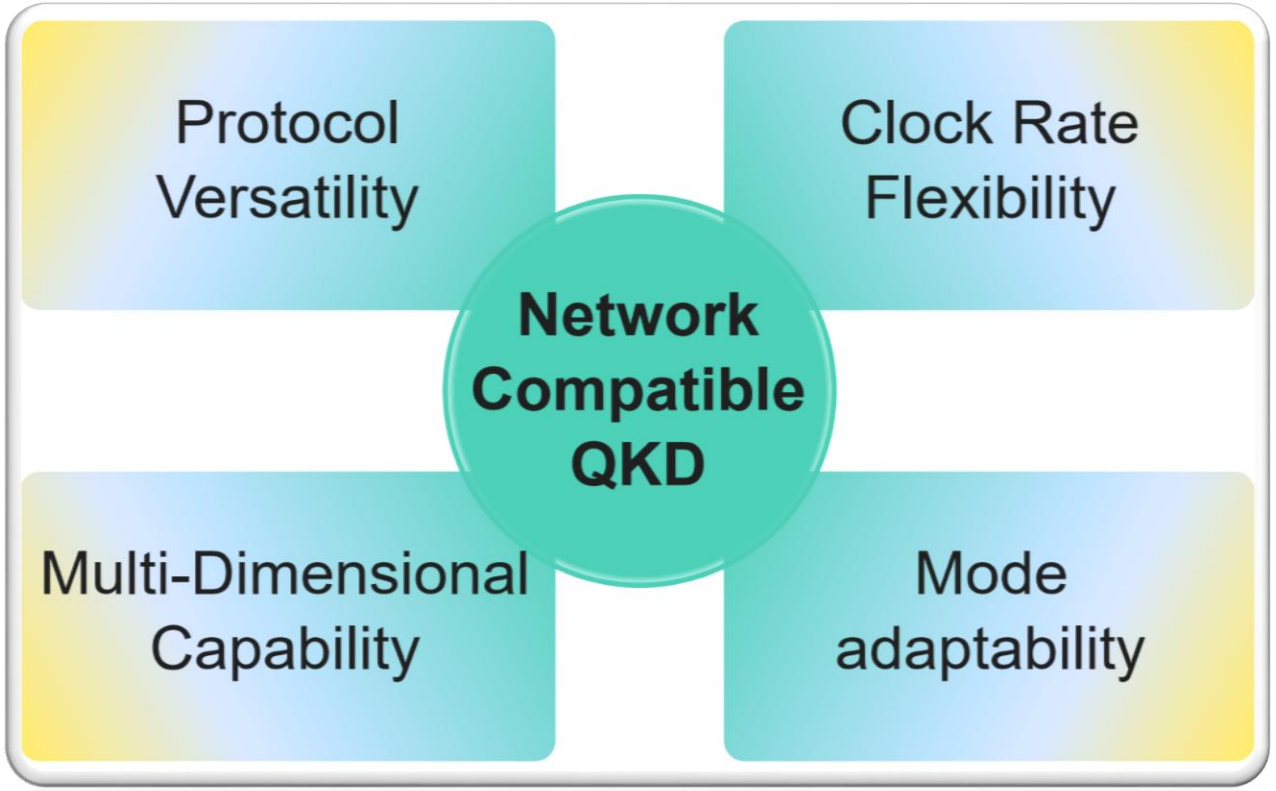
Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

طرح‌های سازگار با شبکه



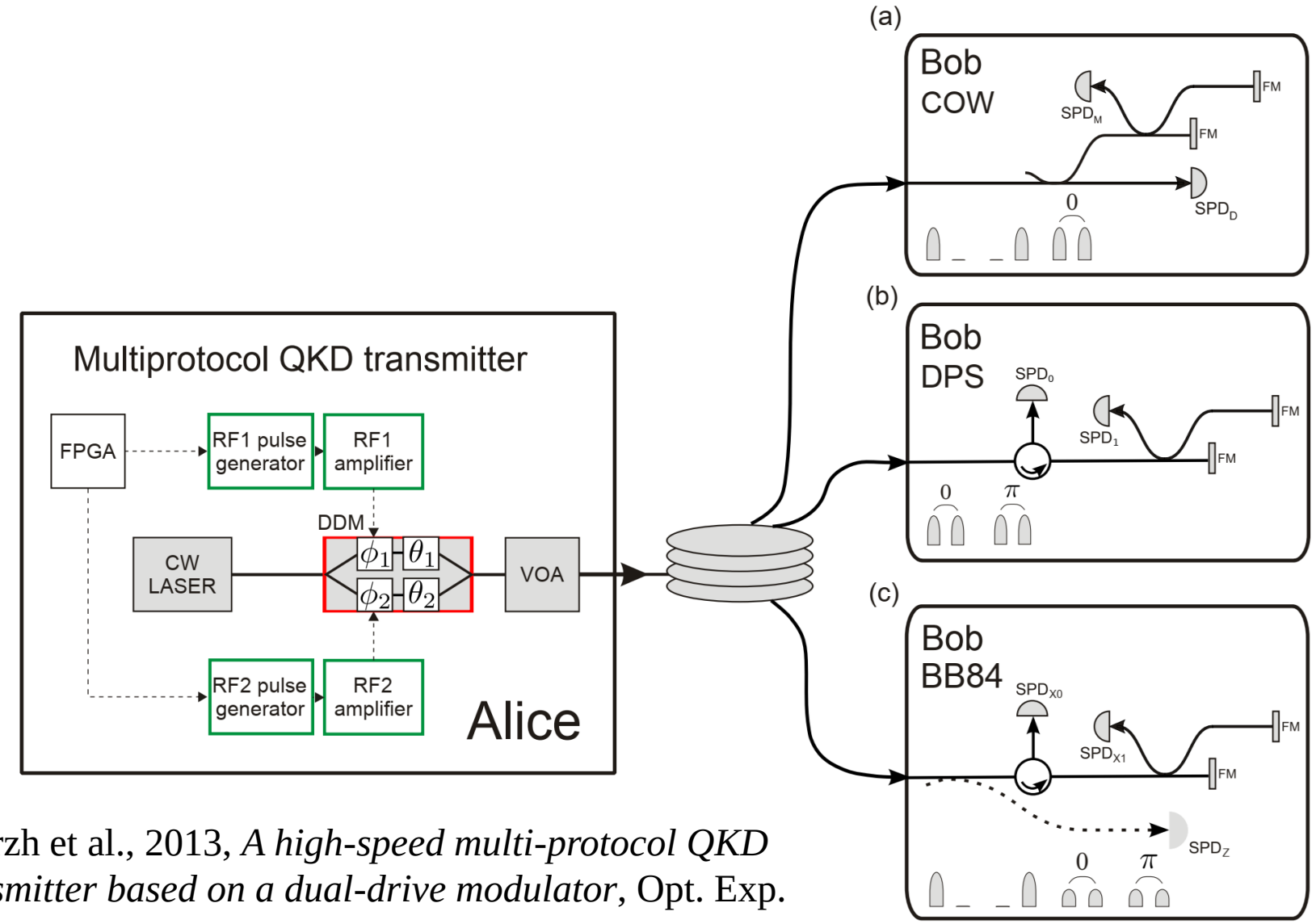
Cao et al., 2022, *From Single-Protocol to Large-Scale Multi-Protocol Quantum Networks*, IEEE Netw.

طرح‌های سازگار با شبکه



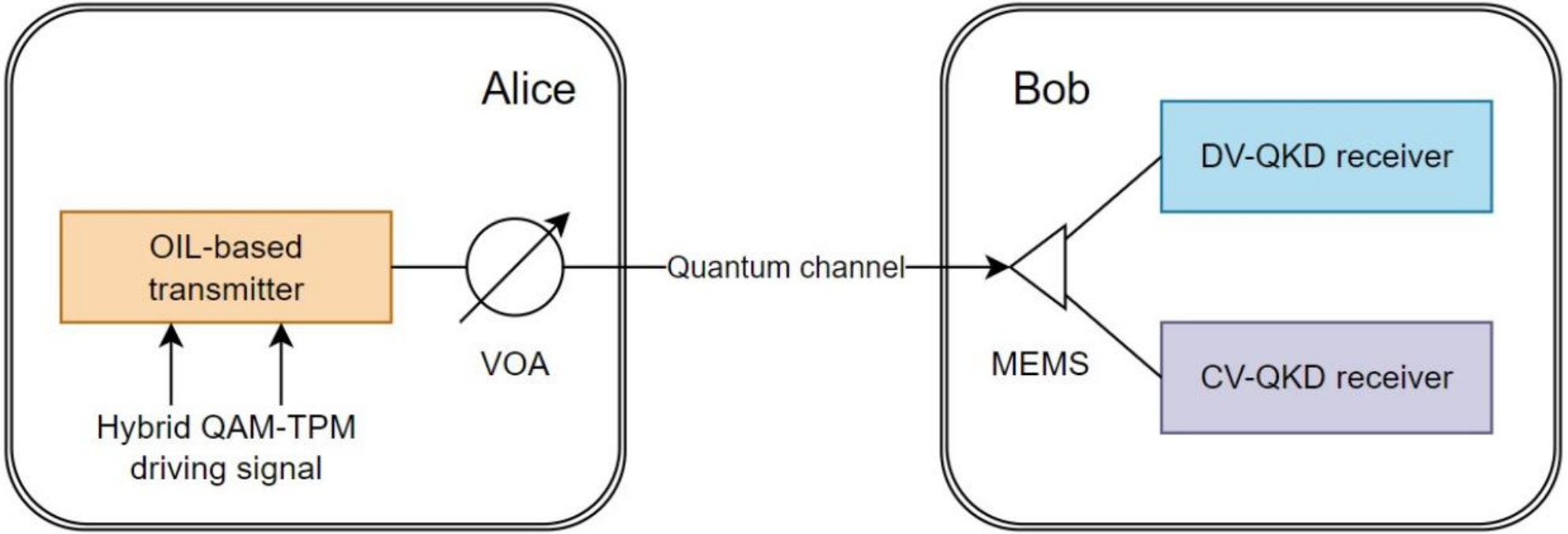
Rezaeishad et al., *Network Compatible QKD Transceiver*, in preparation.

طرح‌های سازگار با شبکه



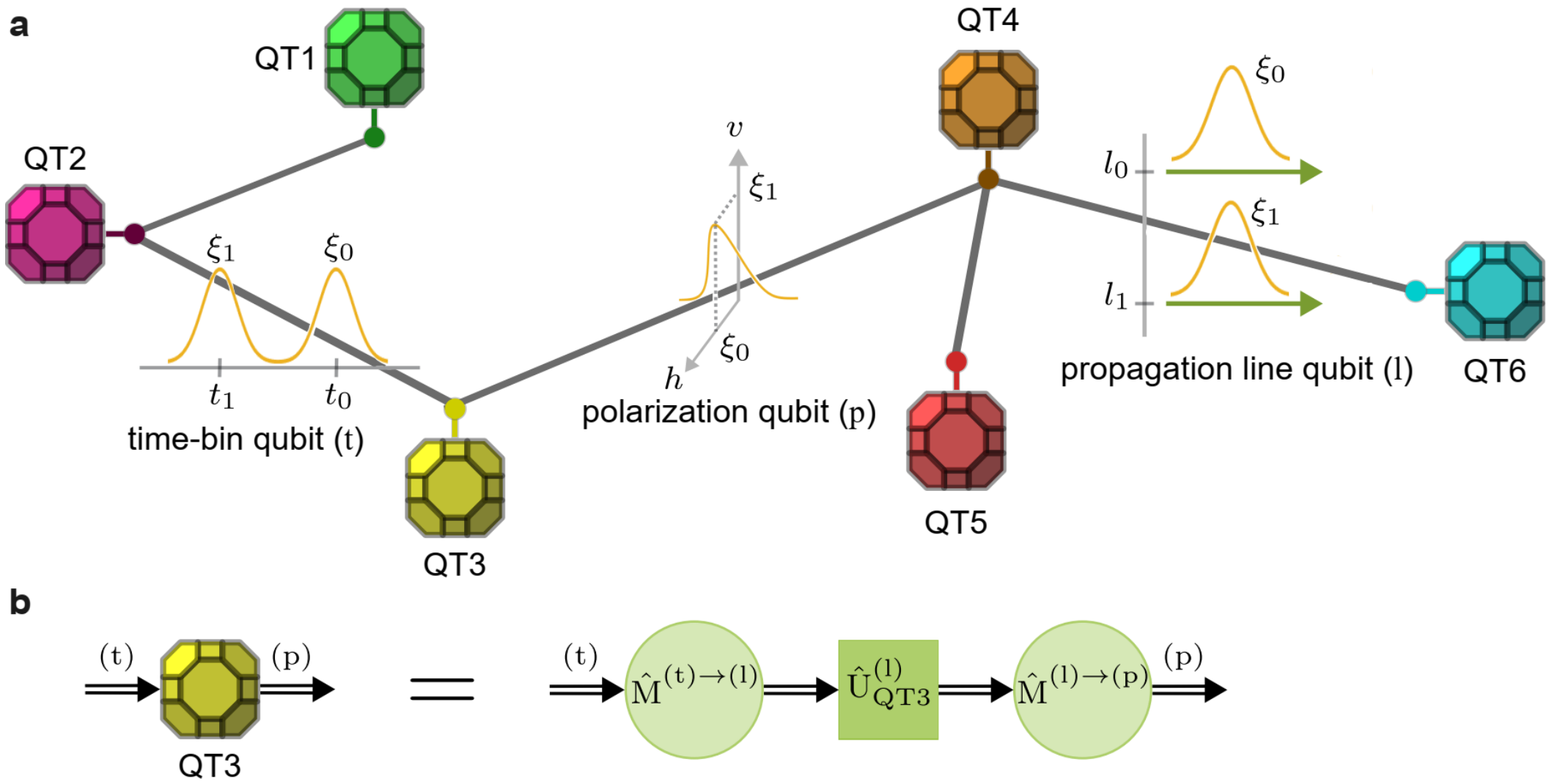
Korzh et al., 2013, *A high-speed multi-protocol QKD transmitter based on a dual-drive modulator*, Opt. Exp.

طرح‌های سازگار با شبکه



Grebenchukov1 et al., 2023, *Prospects of chip-based multi-protocol quantum key distribution transceivers*, ICTON.

سازگاری بین مودهای مختلف: نگاشت مود



Rezaeishad et al., 2025, *All-quantum mode-adaptable communication processors: mathematical frameworks*, Opt. Exp.

استانداردهای کوانتومی

Group	Serial Number	Subject	Type	Year/ Status	Ref.
ETSI	GS QKD 002	QKD use cases	Group specification	2010	[451]
	GR QKD 003	QKD components and internal interfaces	Group report	2018	[213]
	GS QKD 004	QKD application interface	Group specification	2020	[221]
	GS QKD 005	QKD security proofs	Group specification	2010	[452]
	GR QKD 007	QKD vocabulary	Group report	2018	[453]
	GS QKD 008	QKD module security specification	Group specification	2010	[454]
	GS QKD 011	Optical component characterization for QKD systems	Group specification	2016	[455]
	GS QKD 012	Device and communication channel parameters for QKD deployment	Group specification	2019	[66]
	GS QKD 014	Protocol and data format of REST-based key delivery API	Group specification	2019	[222]
	GS QKD 015	QKD control interface for SDN	Group specification	2021	[217]
	GS QKD 010	Protection against Trojan horse attacks in one-way QKD systems	Group specification	Drafting	[456]
	GS QKD 013	Characterization of optical output of QKD transmitter modules	Group specification	Drafting	[457]
	GS QKD 016	Common criteria protection profile for QKD	Group specification	Drafting	[458]
	GR QKD 017	QKD network architectures	Group report	Drafting	[459]
	GS QKD 018	QKD orchestration interface of SDN	Group specification	Drafting	[460]
	GR QKD 019	Design of QKD interfaces with authentication	Group report	Drafting	[461]

Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

Group	Serial Number	Subject	Type	Year/ Status	Ref.
ITU-T	Y.3800	Overview on networks supporting QKD	Recommendation	2019	[65]
	Y.3801	Functional requirements for QKD networks	Recommendation	2020	[462]
	Y.3802	QKD networks - Functional architecture	Recommendation	2020	[463]
	Y.3803	QKD networks - Key management	Recommendation	2020	[297]
	Y.3804	QKD networks - Control and management	Recommendation	2020	[464]
	Y.3805	QKD networks - SDN control	Recommendation	2021	[218]
	Y.3806	QKD networks - Requirements for QoS assurance	Recommendation	2021	[465]
	X.1702	Quantum noise random number generator architecture	Recommendation	2019	[466]
	X.1710	Security framework for QKD networks	Recommendation	2020	[467]
	X.1712	Security requirements and measures for QKD networks - Key management	Recommendation	2021	[468]
	X.1714	Key combination and confidential key supply for QKD networks	Recommendation	2020	[469]
	Y.3807	QKD networks - QoS parameters	Recommendation	Drafting	[470]
	Y.3808	Framework for integration of QKD network and secure storage network	Recommendation	Drafting	[471]
	Y.3809	QKD networks - Business role-based models	Recommendation	Drafting	[472]
	Y.QKDN-qos-fa	Functional architecture of QoS assurance for QKD networks	Recommendation	Drafting	[473]
	X.sec-QKDN-tn	Security requirements and designs for QKD networks - Trusted node	Recommendation	Drafting	[474]
	X.sec_QKDN_intrq	Security requirements for integration of QKD networks and secure network infrastructures	Recommendation	Drafting	[475]
	X.sec_QKDN_CM	Security requirements for QKD networks - Control and management	Recommendation	Drafting	[476]
	X.sec_QKDN_AA	Authentication and authorization in QKD networks using quantum safe cryptography	Recommendation	Drafting	[477]

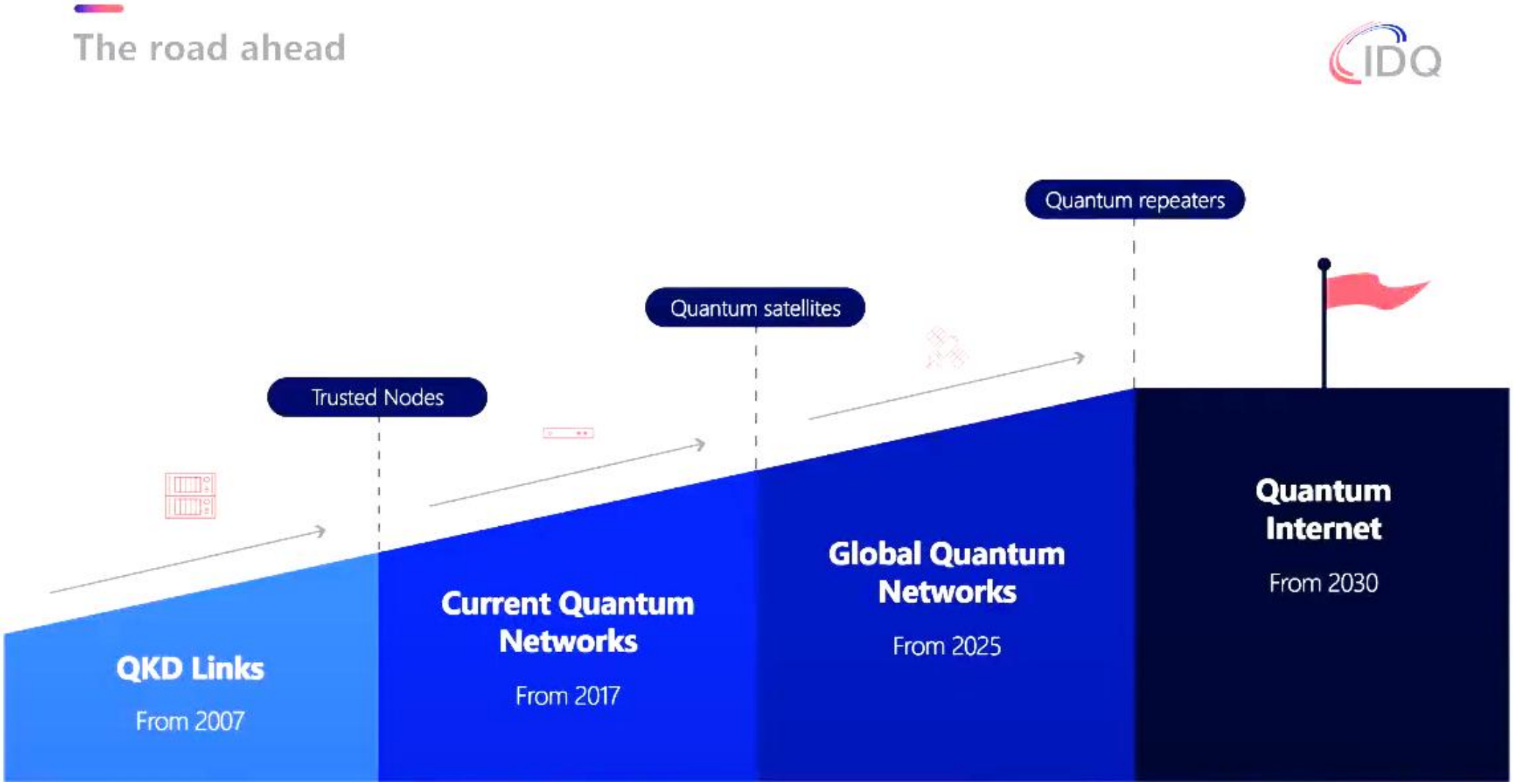
Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

استانداردهای کوانتومی

Group	Serial Number	Subject	Type	Year/ Status	Ref.
ISO/IEC	CD 23837-1	Security requirements, test and evaluation methods for QKD – Part 1: Requirements	Standard	Drafting	[478]
	CD 23837-2	Security requirements, test and evaluation methods for QKD – Part 2: Evaluation and testing methods	Standard	Drafting	[479]
IETF	draft-irtf-qirg-prin..	Architectural principles for a Qinternet	Internet-draft	2021	[480]
	draft-irtf-qirg-qua..	Applications and use cases for the Qinternet	Internet-draft	2021	[481]
IEEE	P1913	Software-defined quantum communication	Standard	Drafting	[482]
CSA	N/A	Introduction to QKD	Research artifact	2015	[483]

Cao et al., 2022, *The Evolution of QKD Networks: On the Road to the Qinternet* , IEEE Commun. Surv. Tutor.

مسیر پیش رو


The road ahead
IDQ
Quantum repeaters
Quantum satellites
Trusted Nodes
QKD Links
From 2007
Current Quantum Networks
From 2017
Global Quantum Networks
From 2025
Quantum Internet
From 2030

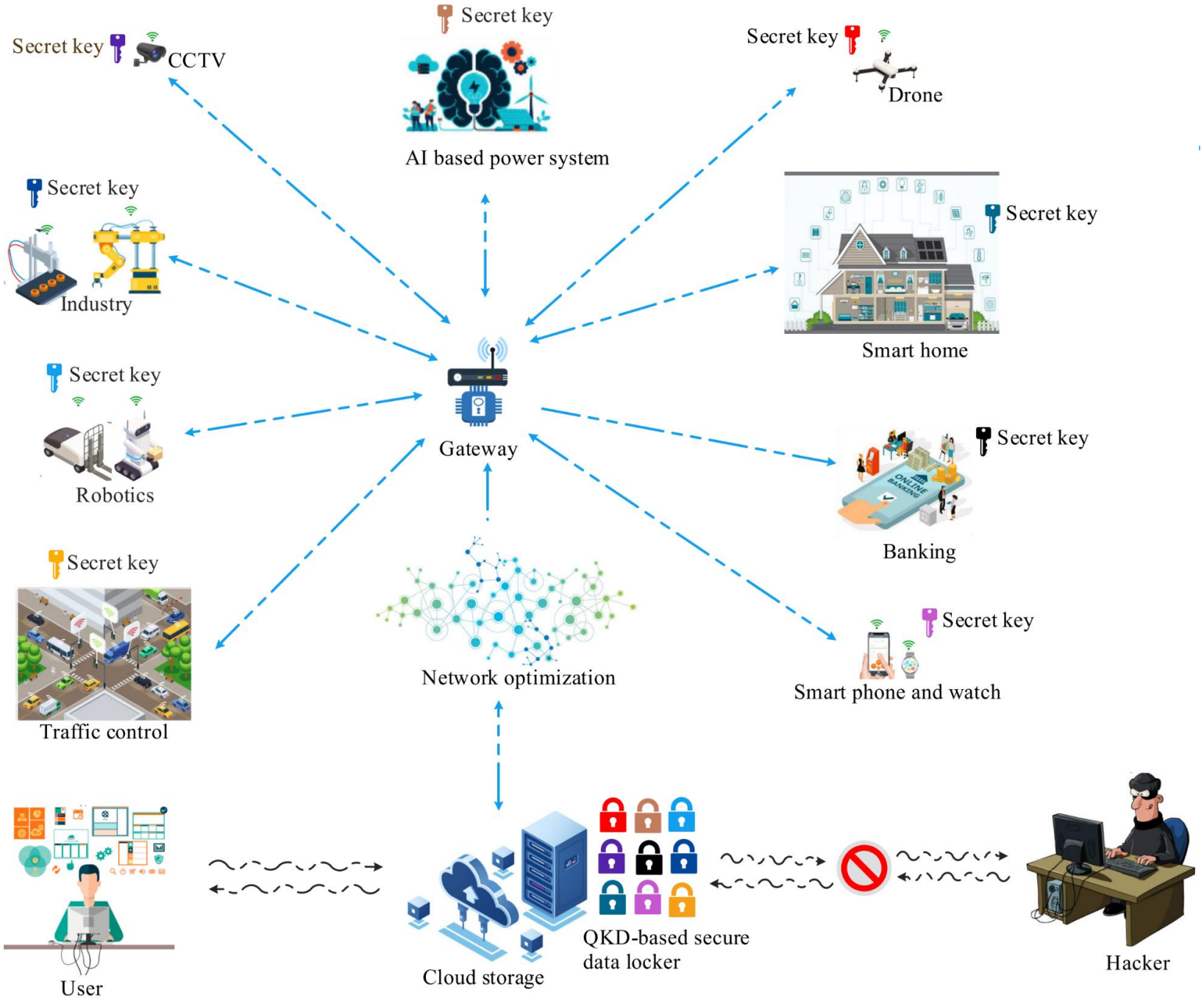
NATURE|Vol 453|19 June 2008|doi:10.1038/nature07127

The quantum internet

H. J. Kimble[1]

Quantum networks provide opportunities and challenges across a range of intellectual and technical frontiers, including quantum computation, communication and metrology. The realization of quantum networks composed of many nodes and channels requires new scientific capabilities for generating and characterizing quantum coherence and entanglement. Fundamental to this endeavour are quantum interconnects, which convert quantum states from one physical system to those of another in a reversible manner. Such quantum connectivity in networks can be achieved by the optical interactions of single photons and atoms, allowing the distribution of entanglement across the network and the teleportation of quantum states between nodes.

IoT کوانتومی



Hasan et al., 2023, *Quantum Communication Systems: Vision, Protocols, Applications, and Challenges*, IEEE Access.

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

سیستم‌های مخابرات کوانتومی

6

1

مقدمه

مفاهیم مکانیک کوانتومی

2

3

کاربردهای درهم‌تنیدگی

توزیع کلید کوانتومی

4

5

شبکه و اینترنت کوانتومی

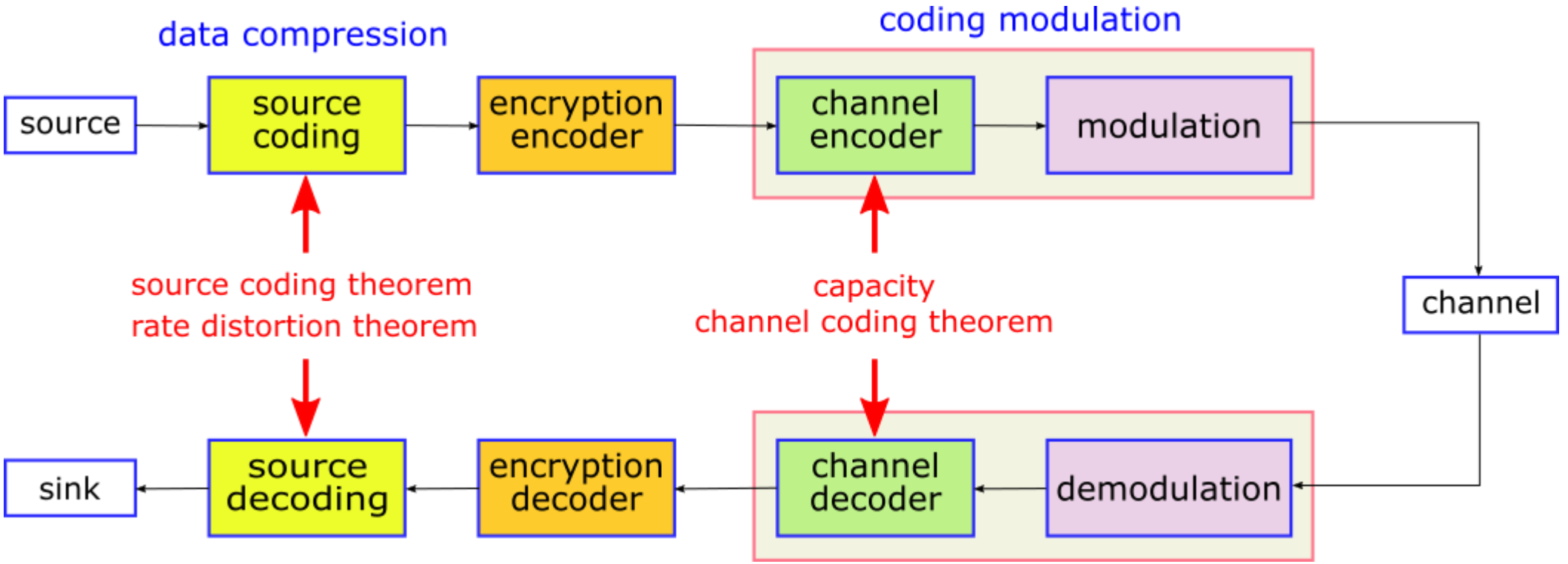
سیستم‌های مخابرات کوانتومی

6

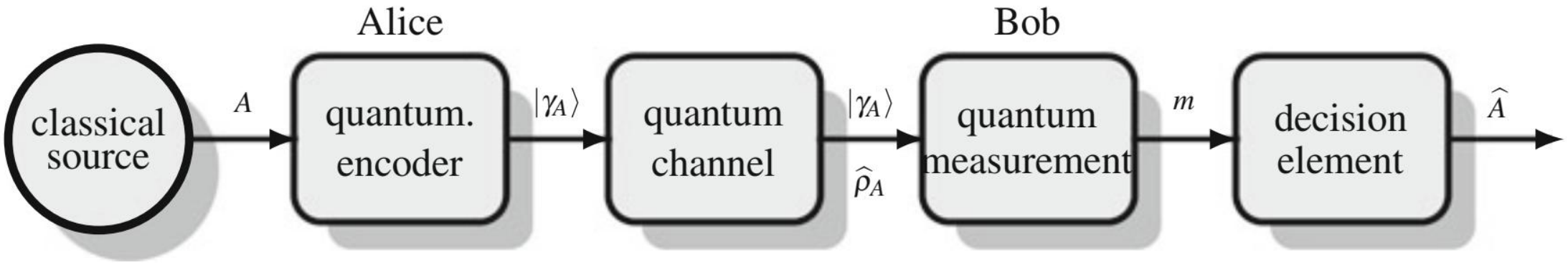
سرفصل مطالب این بخش

- اجزای اصلی سیستم مخابراتی دیجیتال
- سیستم مخابرات کوانتومی
- گیرنده‌ی بهینه کوانتومی
- مدولاسیون کوانتومی BPSK و شبیه‌سازی نرخ خطا
- مدولاسیون کوانتومی PPM و شبیه‌سازی نرخ خطا

اجزای اصلی سیستم مخابراتی دیجیتال



سیستم مخابرات کوانتومی



Cariolaro, 2015, *Quantum Communications*, Springer.

- یک منبع کلاسیک با K سمبل $\{0,1,\ldots,K-1\}$

$$q_i := P[A = i], \qquad i \in \mathcal{A}$$

- فرستنده (آلیس) هر سمبل A را به یک حالت کوانتومی در فضای هیلبرت کد می‌کند.

$$A \to |\gamma_A\rangle$$

- مثال: سیستم با سه سمبل

$$0 \to |\gamma_0\rangle \ , \ 1 \to |\gamma_1\rangle \ , \ 2 \to |\gamma_2\rangle$$

سیستم مخابرات کوانتومی

- اندازه‌گیری کوانتومی روی حالت دریافتی توسط گیرنده
- تصمیم‌گیری در مورد سمبل ارسال یشده بر اساس نتیجه‌ی اندازه‌گیری
- سیستم عملگر اندازه‌گیری گیرنده $\{P_k, k \in \mathcal{M}\}$
- به منظور تشخیص سمبل‌های فرستنده از یکدیگر باید $|\mathcal{M}| \geq |\mathcal{A}|$
- طبق فرضیه‌ی سوم مکانیک کوانتومی:

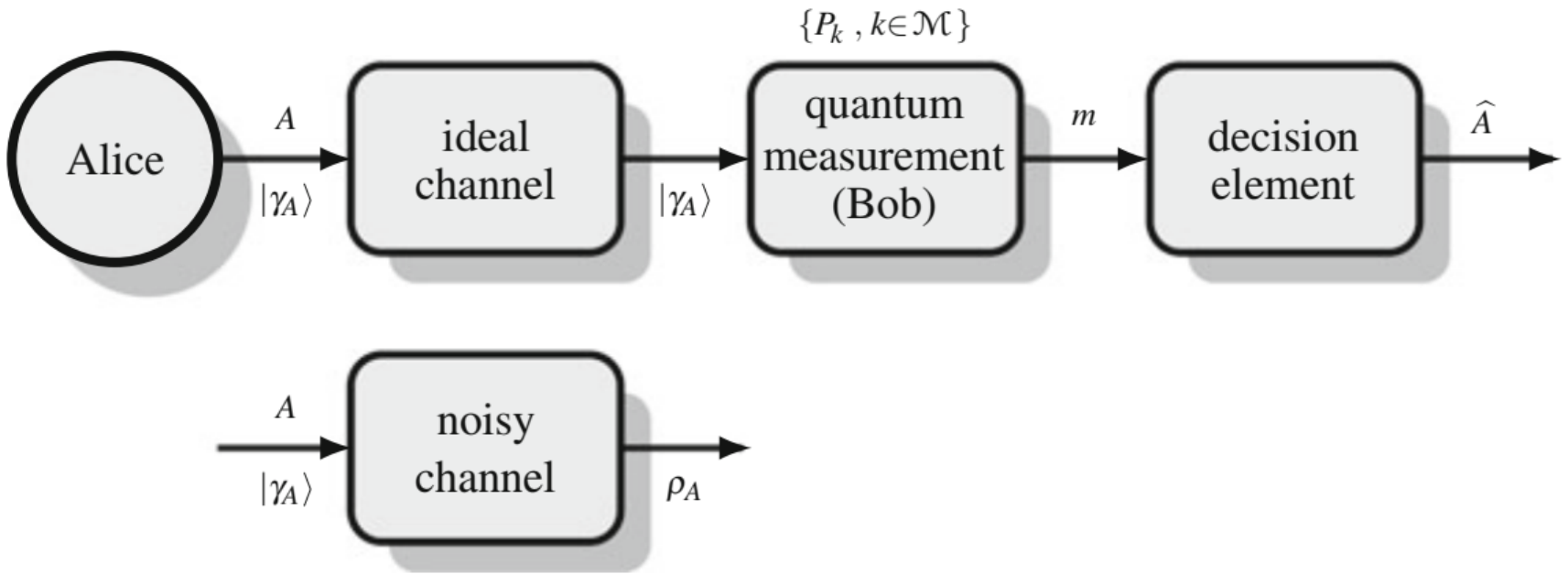
✓ اگر حالت دریافتی در گیرنده $|\gamma_A\rangle$ باشد، احتمال نتیجه‌ی اندازه‌گیری $m = k \in \mathcal{M}$ برابر است با

$$\mathrm{P}[m = k \mid \gamma_A] = \langle \gamma_A | P_k | \gamma_A \rangle, \qquad k \in \mathcal{M}$$

✓ در کانال نویزی که حالت دریافتی در گیرنده ρ_A است:

$$\mathrm{P}[m = k \mid \rho_A] = \mathrm{Tr}[\rho_A P_k], \qquad k \in \mathcal{M}$$

سیستم مخابرات کوانتومی

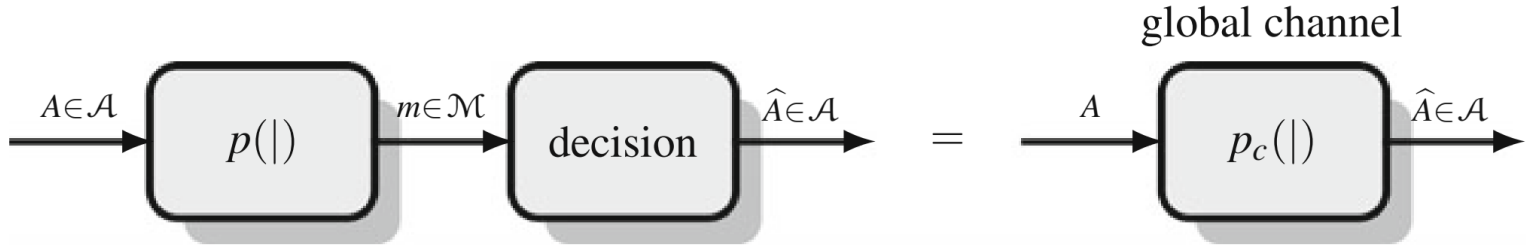


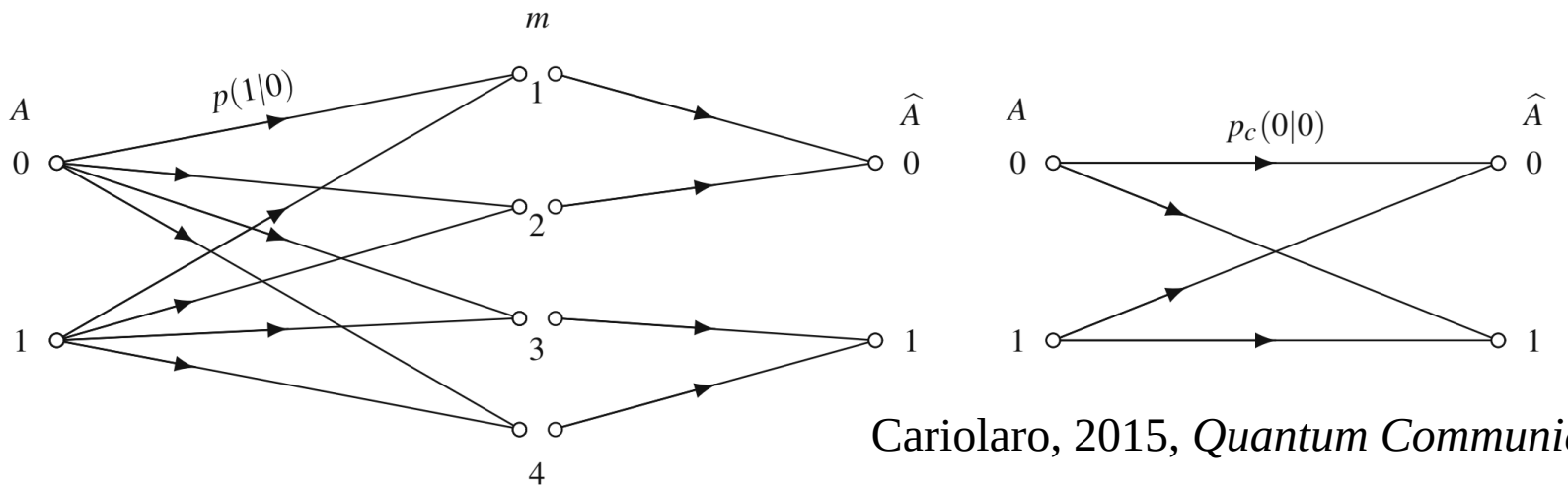
Cariolaro, 2015, *Quantum Communications*, Springer.

$$\mathrm{P}[m = k \mid \gamma_A] = \langle \gamma_A | P_k | \gamma_A \rangle, \qquad k \in \mathcal{M}$$

$$\mathrm{P}[m = k \mid \rho_A] = \mathrm{Tr}[\rho_A P_k], \qquad k \in \mathcal{M}$$

گیرنده بهینه کوانتومی





Cariolaro, 2015, *Quantum Communications*, Springer.

$$p_c(j|i) = P[\hat{A} = j|A = i] = P[m \in \mathcal{M}_j|A = i] = \sum_{m\in\mathcal{M}_j} P[m = k|A = i]$$

$$\Rightarrow p_c(j|i) = \sum_{m\in\mathcal{M}_j} \mathrm{Tr}\{\rho_i P_k\}.$$

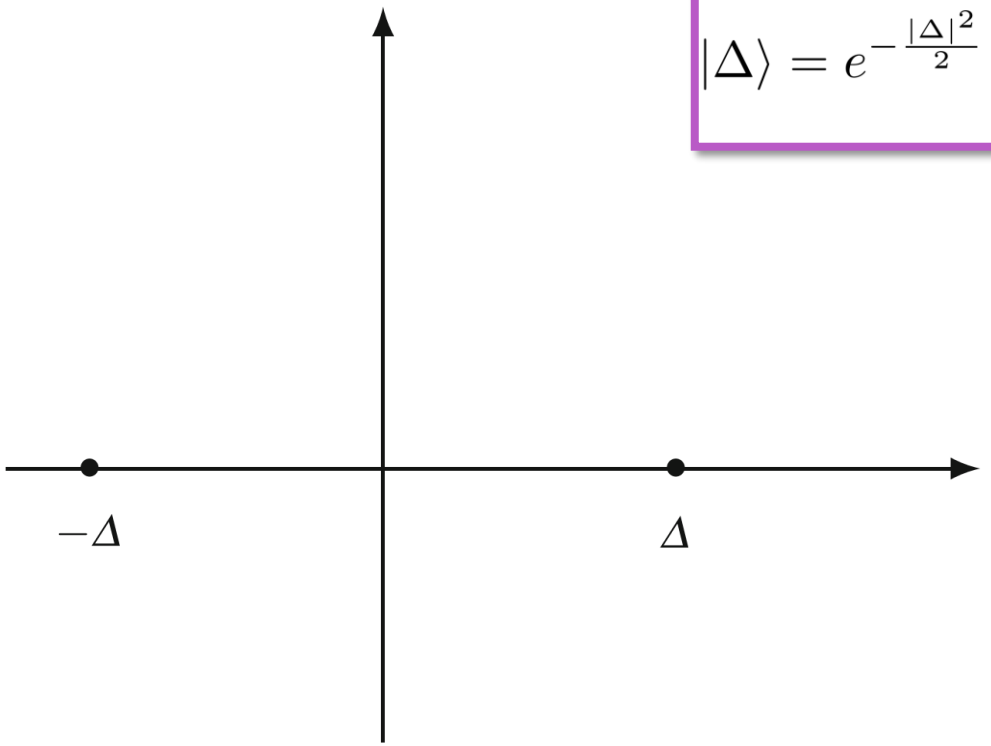
$$P_c = P[\hat{A} = A] = \sum_{i\in\mathcal{A}} q_i p_c(i|i)$$

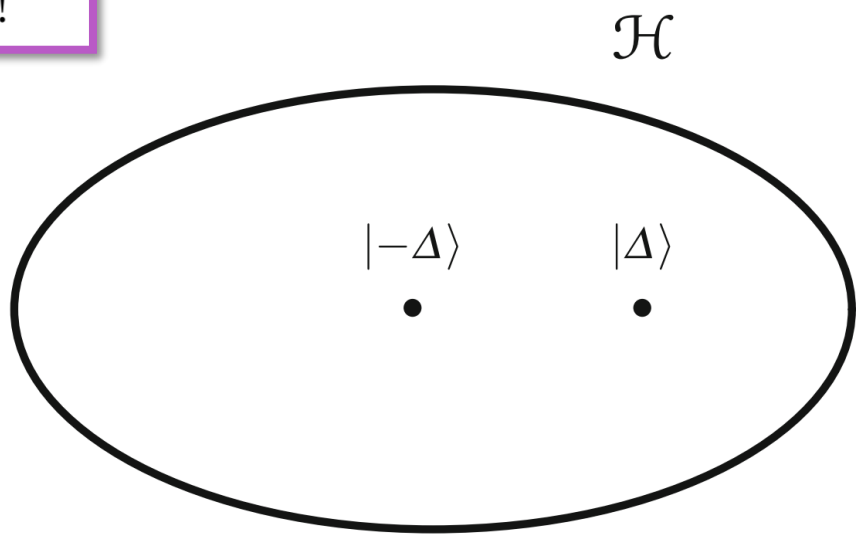
معیار گیرنده بهینه: بیشینه‌ی احتمال صحت

مدولاسیون کوانتومی BPSK

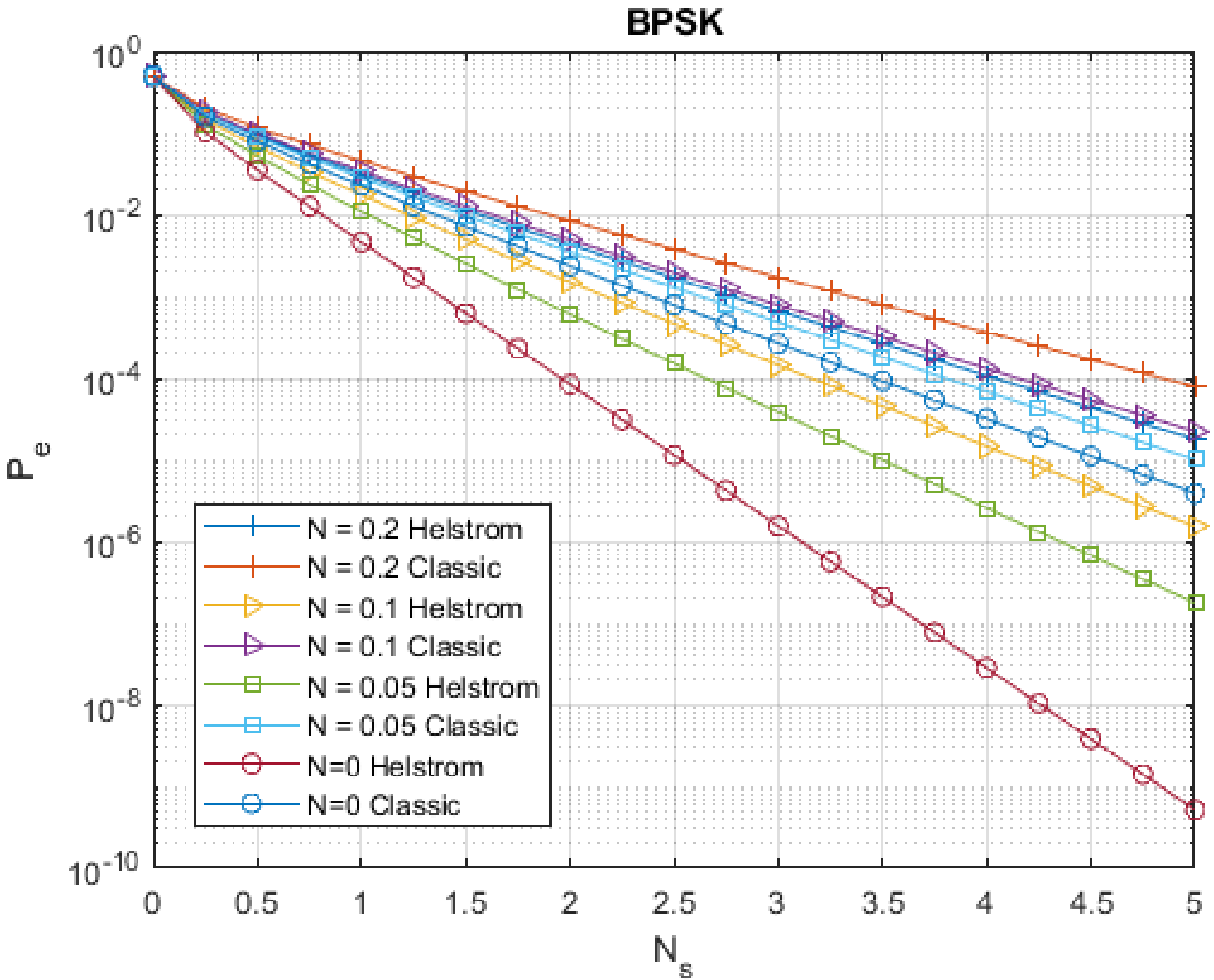
$$|\gamma_0\rangle = |\Delta\rangle \ , \ |\gamma_1\rangle = |-\Delta\rangle \ \in \mathcal{G}.$$

$$|\Delta\rangle = e^{-\frac{|\Delta|^2}{2}} \sum_{n=0}^{\infty} \frac{\Delta^n}{\sqrt{n!}} |n\rangle$$





مدولاسیون کوانتومی BPSK



N : average number of thermal photons associated with the mode

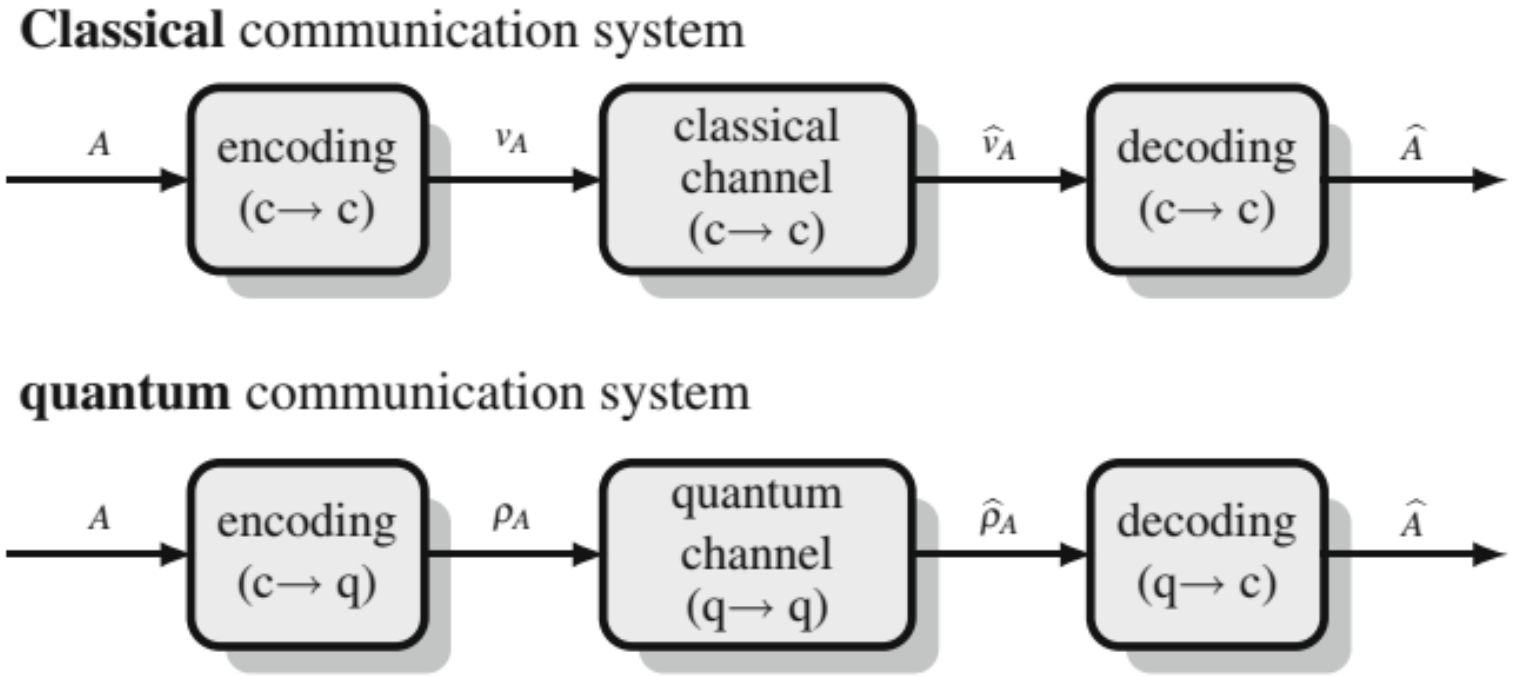
N_S : average number of signal photons per symbol

تفاوت سیستم کلاسیک و کوانتوم

- تفاوت اصلی: ماهیت فیزیکی حامل اطلاعات

- کلاسیک: حمل اطلاعات روی کمیت‌های قابل اندازه‌گیری (مثل دامنه یا فاز ولتاژ سیگنال نوری)

- کوانتوم: قرار گرفتن اطلاعات روی حالات کونتومی که قابل کپی کردن نیستند و اندازه‌گیری آن‌ها باعث اختلال می‌شود.



Cariolaro, 2015, *Quantum Communications*, Springer.

مدولاسیون کوانتومی PPM

$$|\beta_i\rangle = |\beta_{i,K-1}\rangle \otimes \ldots \otimes |\beta_{i,1}\rangle \otimes |\beta_{i,0}\rangle \quad , \quad i = 0, 1, \ldots, K-1$$

$$|\beta_{i,j}\rangle = |\Delta\rangle \text{ for } i = j \text{ and } |\beta_{i,j}\rangle = |0\rangle \text{ for } i \neq j$$

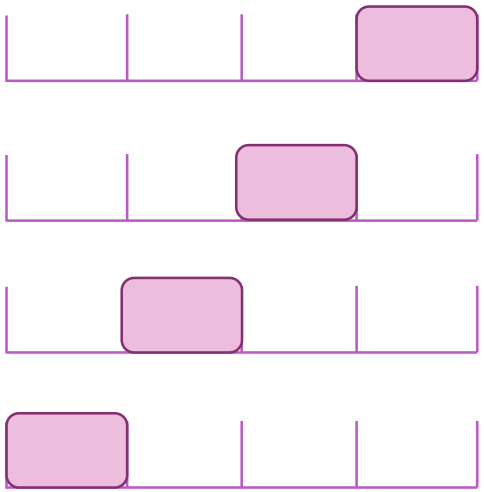
- مثال: مدولاسیون 4PPM

$$|\gamma_0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |\Delta\rangle$$

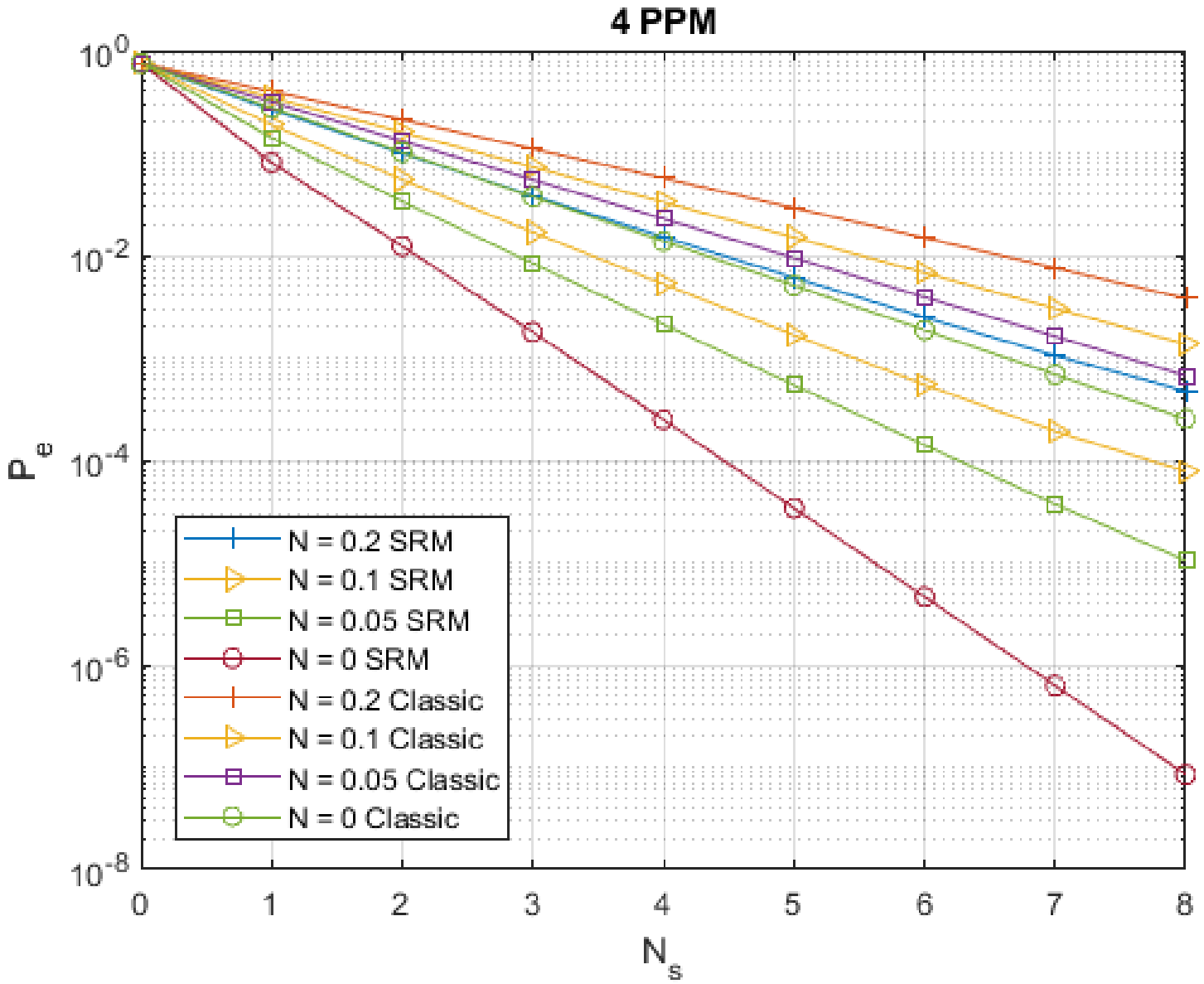
$$|\gamma_1\rangle = |0\rangle| \otimes 0\rangle \otimes |\Delta\rangle \otimes |0\rangle$$

$$|\gamma_2\rangle = |0\rangle \otimes |\Delta\rangle \otimes |0\rangle \otimes |0\rangle$$

$$|\gamma_3\rangle = |\Delta\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle$$



مدولاسیون کوانتومی 4 PPM



از توجه شما متشکرم

ds.rezaeishad@gmail.com

ds.rezaeishad@iut.ac.ir