



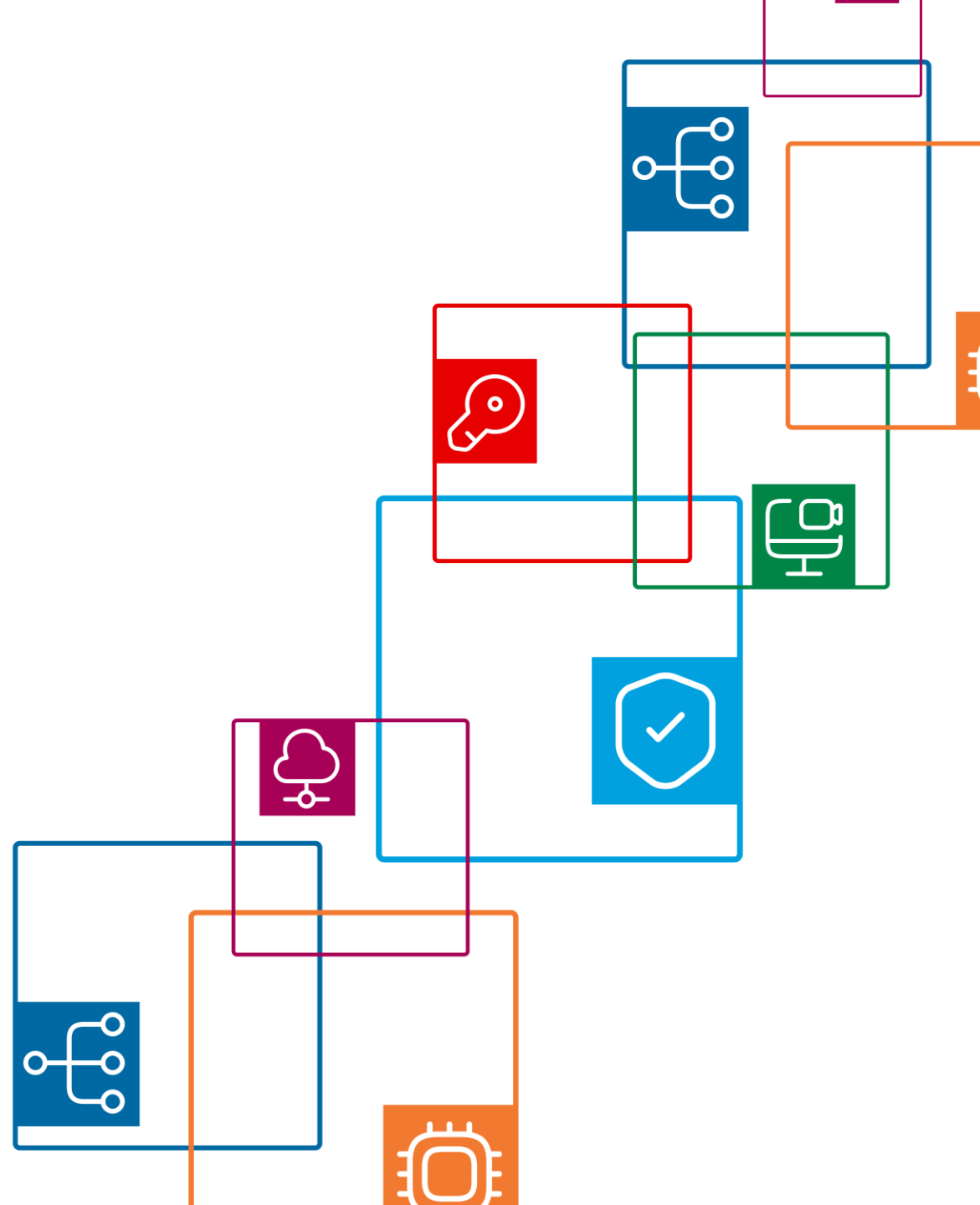
QKD a CESNET

Kvantová distribuce klíčů:
od principu k šifrovanému přenosu

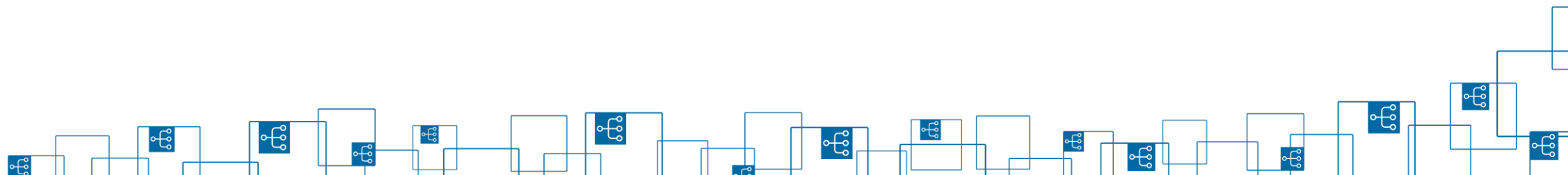
Ing. Tomáš Novák

CESNET • Oddělení optických sítí

Konference CESNET 2026

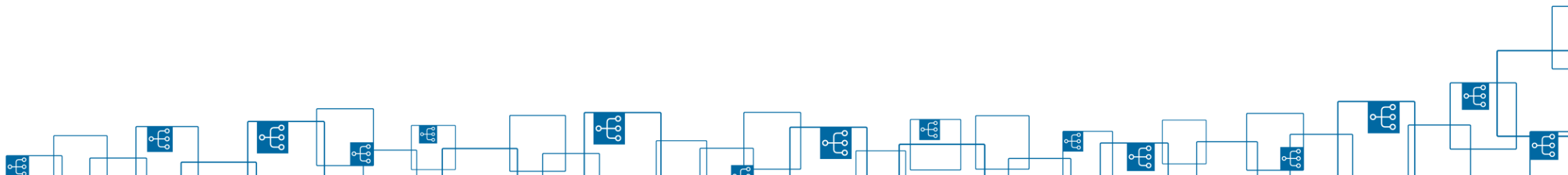


- Současná kryptografie
- Ohrožení kvantovými počítači
- QKD je částí řešení
- Ilustrace protokolu BBM92
- QDK projekty v CESNETu



Dvě základní role současné kryptografie:

- Šifrování dat
 - ochrana obsahu zprávy/dat
 - **symetrická kryptografie**



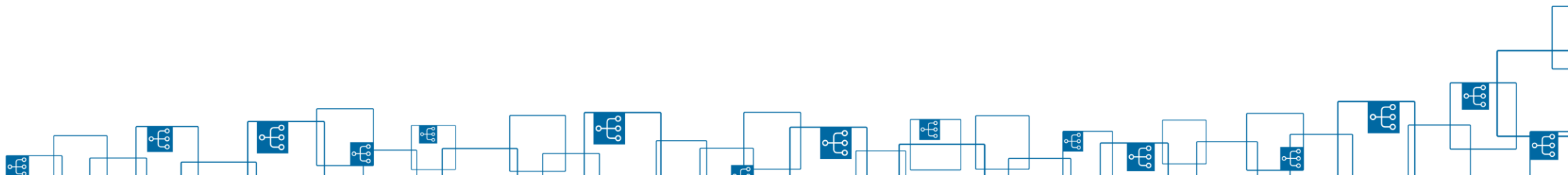
Dvě základní role současné kryptografie:

- Šifrování dat

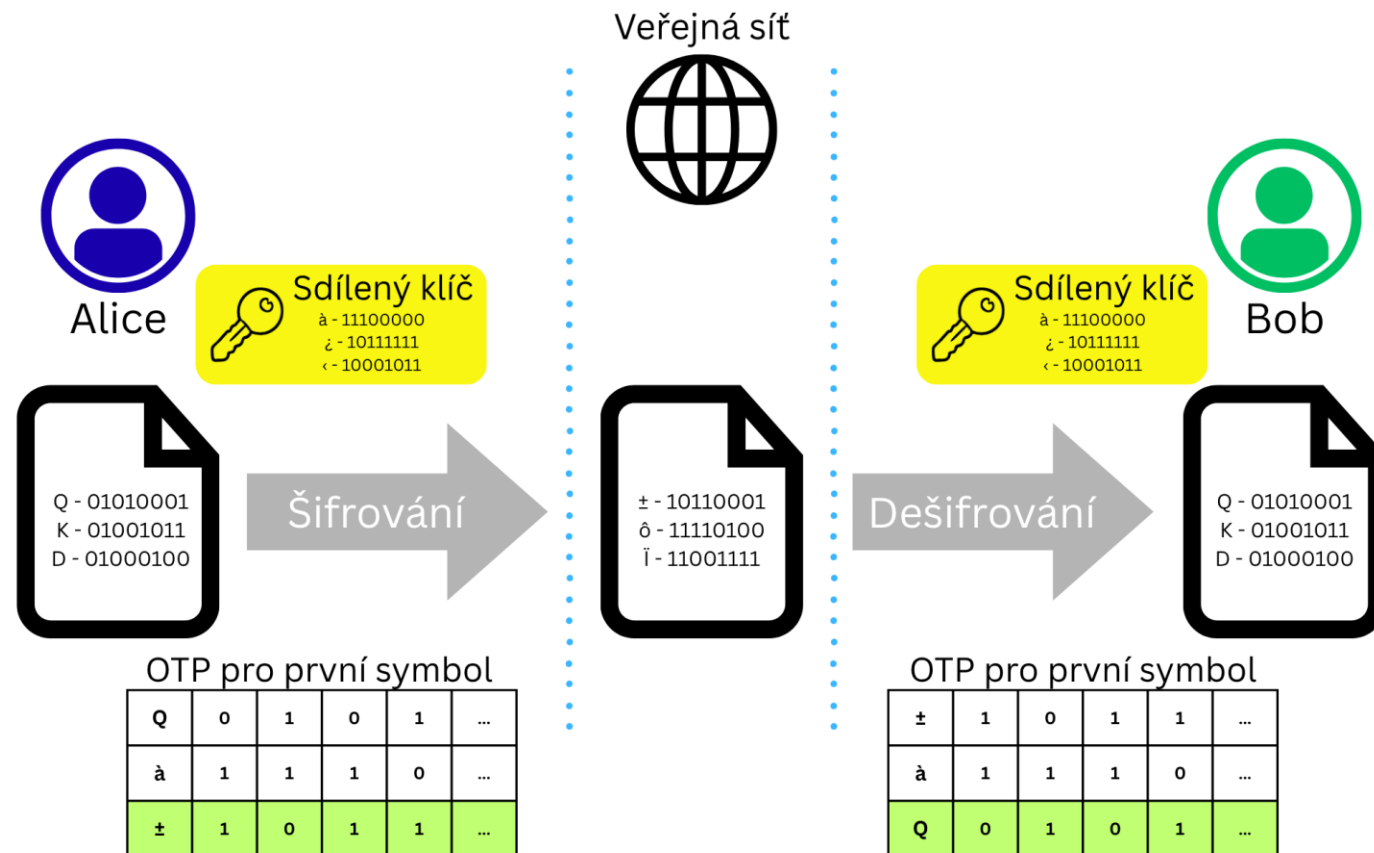
- ochrana obsahu zprávy/dat
- **symetrická kryptografie**

- Distribuce klíče a ověření identity

- bezpečné předání klíče a ověření protistrany
- **asymetrická kryptografie**

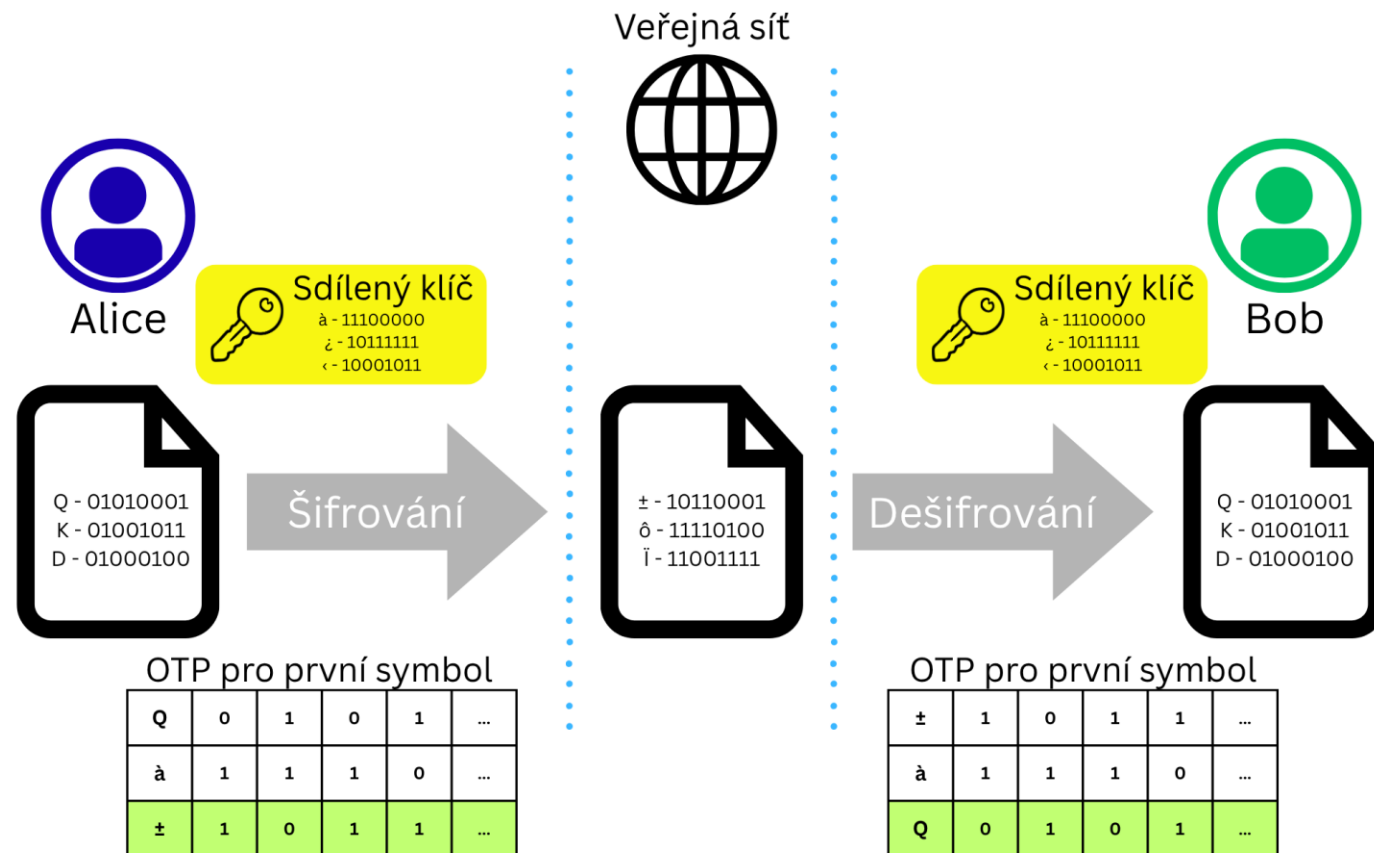


Symetrická kryptografie



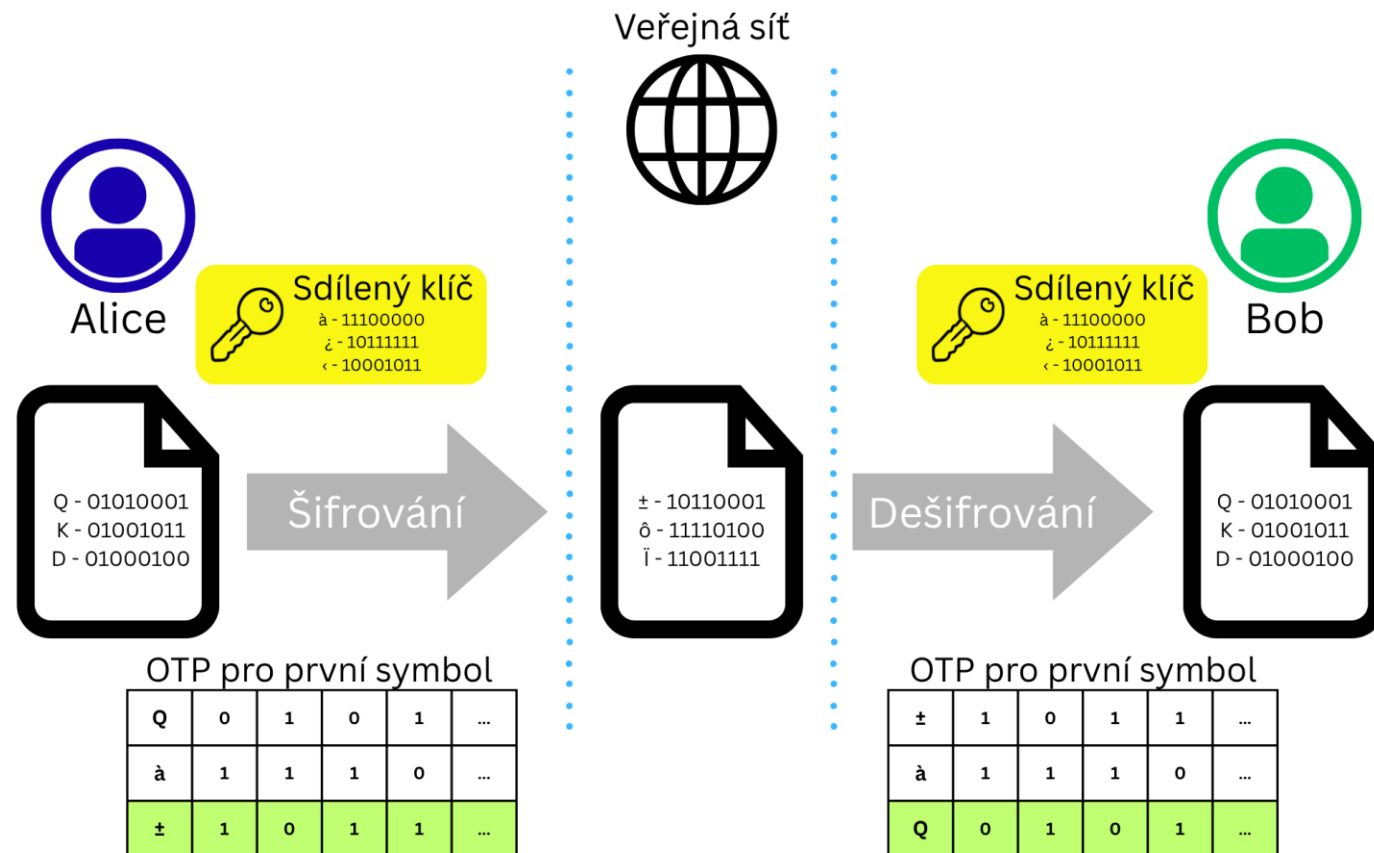
Symetrická kryptografie

- sdílený **náhodný** klíč pro šifrování i dešifrování



Symetrická kryptografie

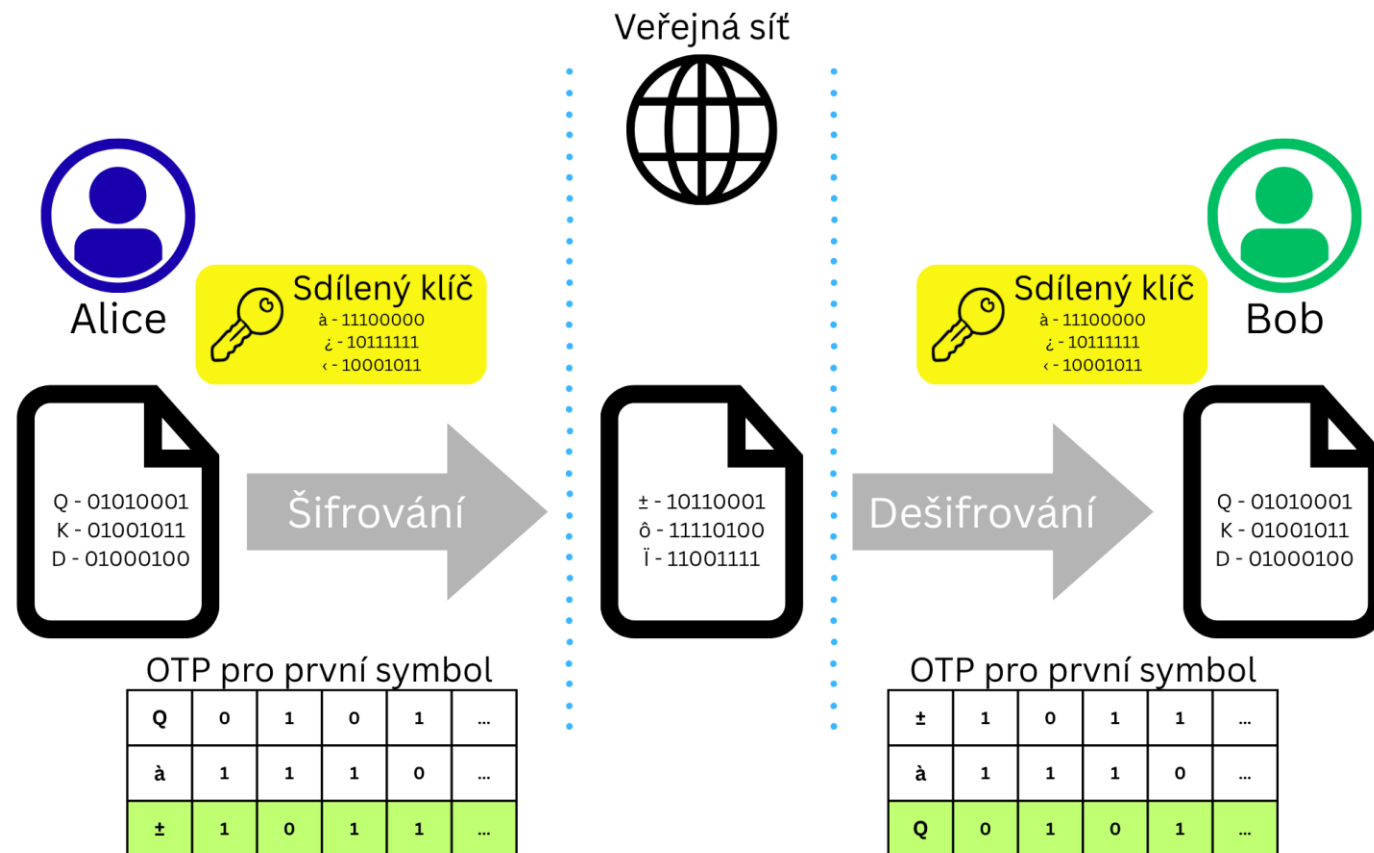
- sdílený **náhodný** klíč pro šifrování i dešifrování
- bezpečnost stojí na utajení a **bezpečném sdílení klíče**



Symetrická kryptografie

- sdílený **náhodný** klíč pro šifrování i dešifrování
- bezpečnost stojí na utajení a **bezpečném sdílení klíče**

Jak bezpečně sdílet tajný klíč?

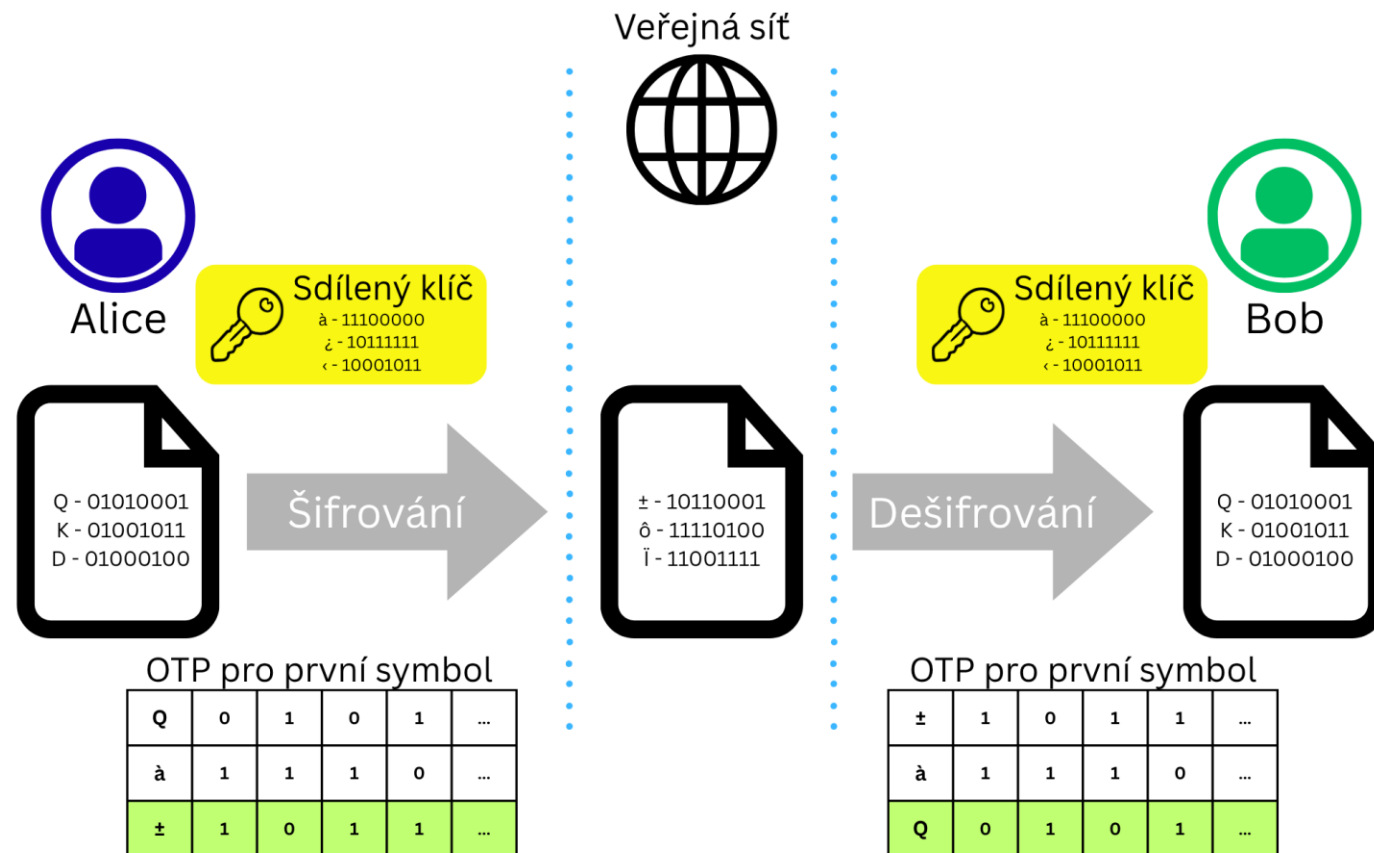


Symetrická kryptografie

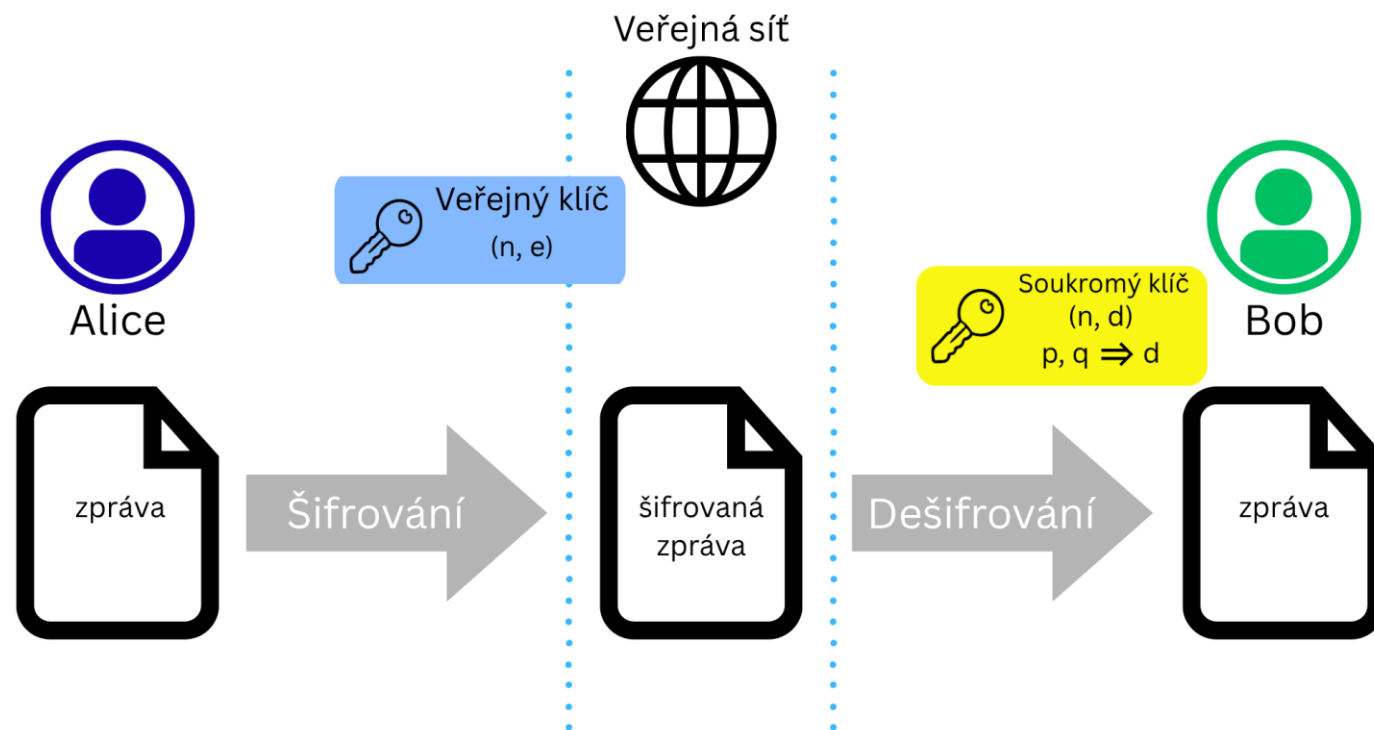
- sdílený **náhodný** klíč pro šifrování i dešifrování
- bezpečnost stojí na utajení a **bezpečném sdílení klíče**

Jak bezpečně sdílet tajný klíč?

One-Time-Pad vs. AES

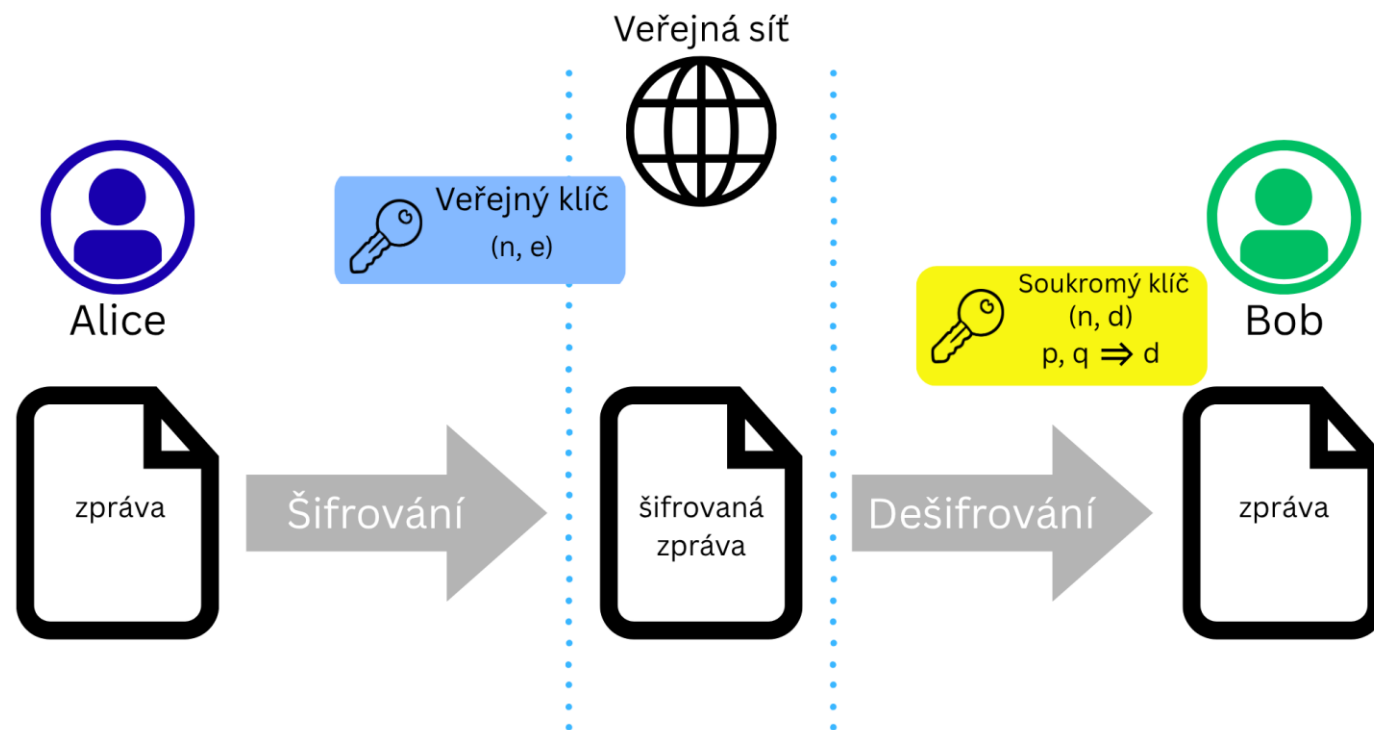


Asymetrická kryptografie



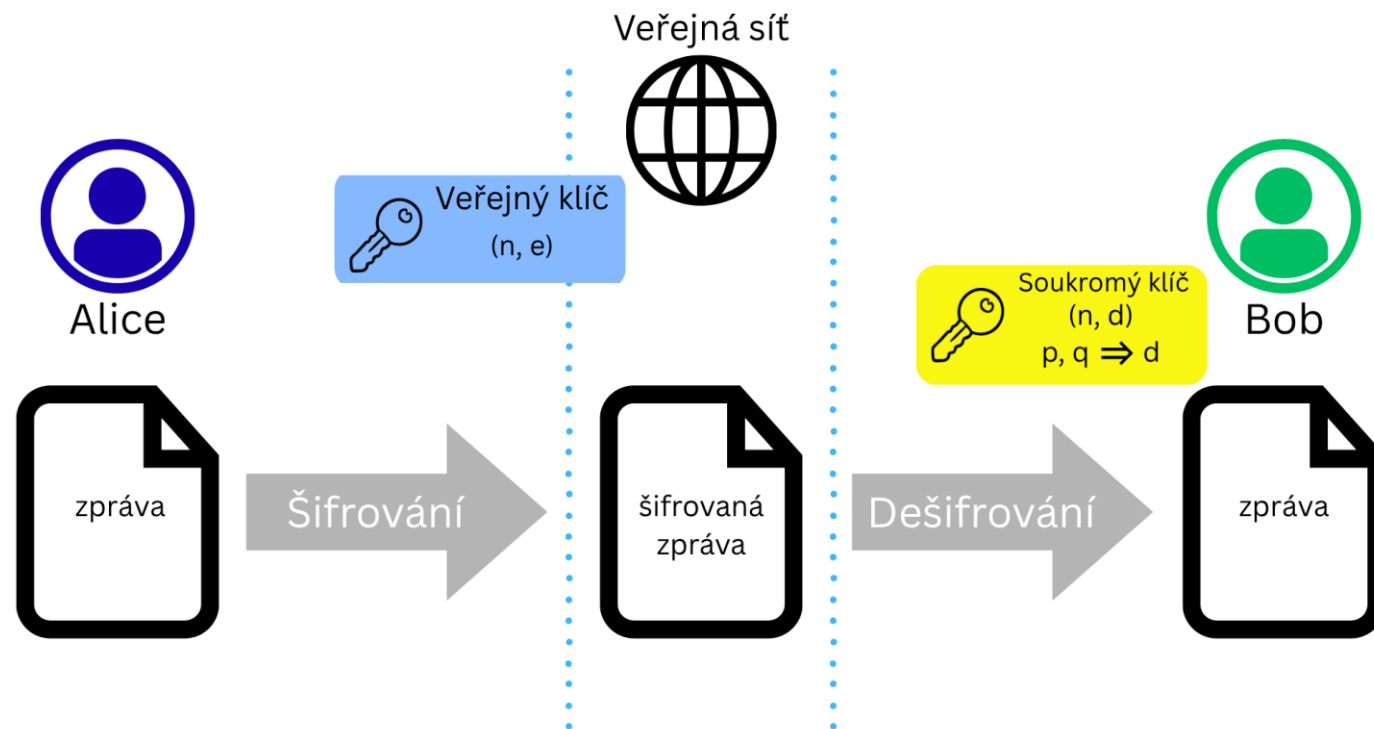
Asymetrická kryptografie

- veřejný klíč pro šifrování / ověření



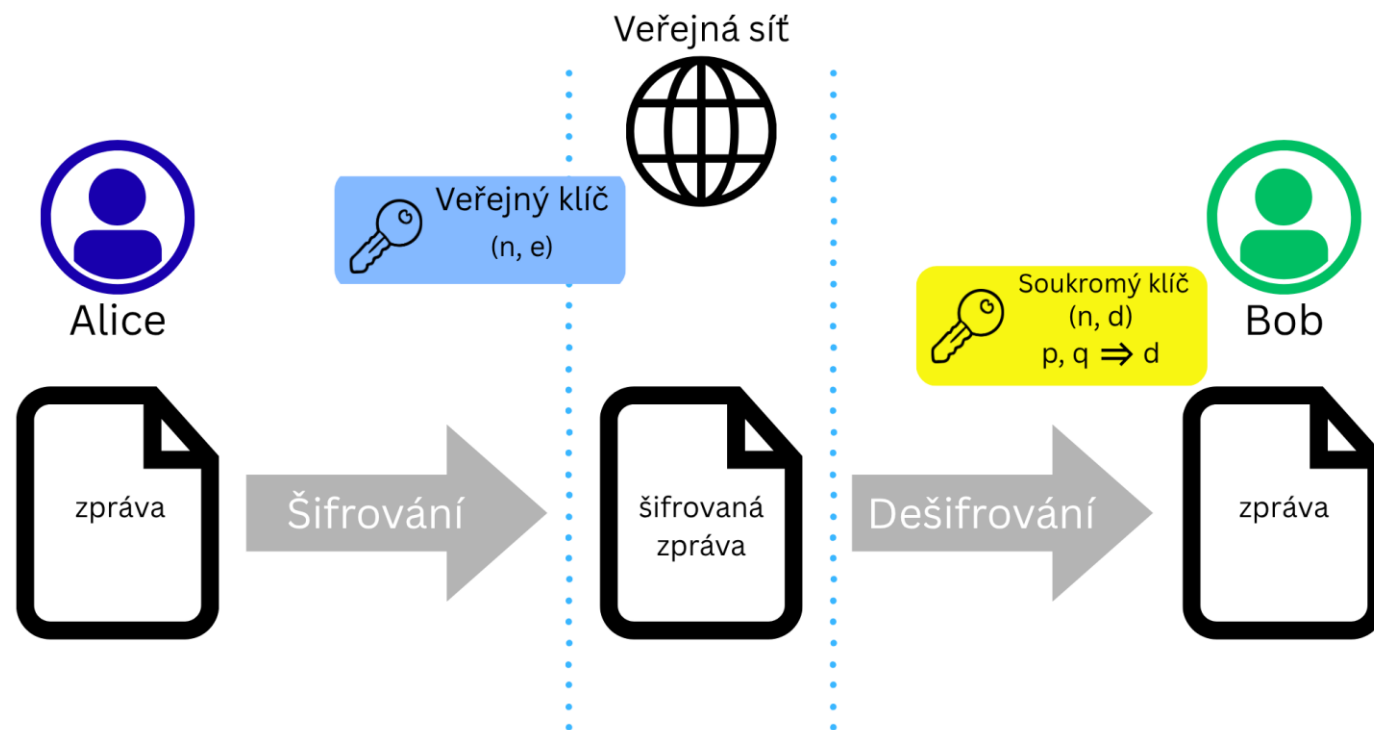
Asymetrická kryptografie

- **veřejný klíč** pro šifrování / ověření
- **soukromý klíč** pro dešifrování / podpis



Asymetrická kryptografie

- **veřejný klíč** pro šifrování / ověření
- **soukromý klíč** pro dešifrování / podpis
- bezpečnost stojí na výpočetně obtížných matematických úlohách

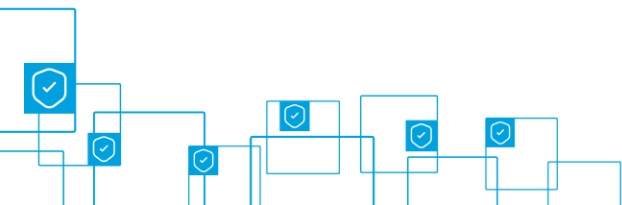


Asymetrická kryptografie

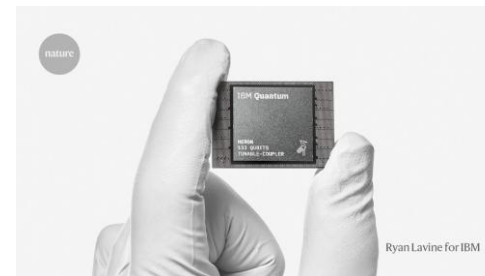
- **veřejný klíč** pro šifrování / ověření
- **soukromý klíč** pro dešifrování / podpis
- bezpečnost stojí na výpočetně obtížných matematických úlohách

součin: $p \cdot q \rightarrow n$, $61 \cdot 53 \rightarrow 3233$
faktORIZACE: $n \rightarrow p \cdot q$, $3233 \rightarrow 61 \cdot 53$

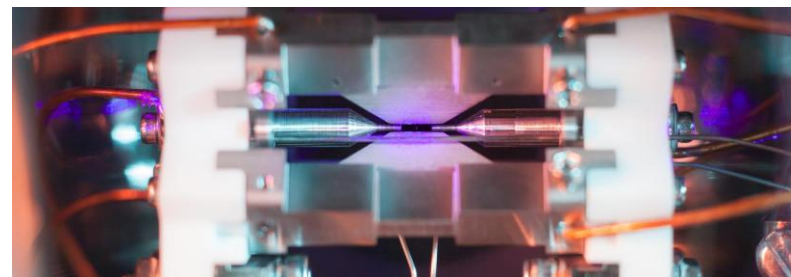
součin: $p \cdot q \rightarrow n$, $61 \cdot 53 \rightarrow 3233$
faktORIZACE: $n \rightarrow p \cdot q$, $3233 \rightarrow 61 \cdot 53$



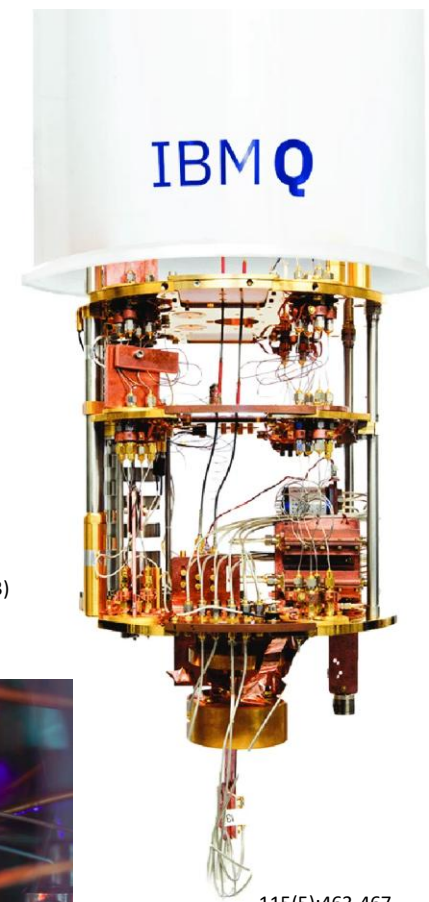
Kvantové počítače a dnešní kryptografie



Nature **624**, 238 (2023)



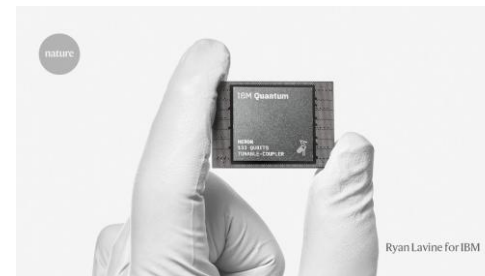
<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>



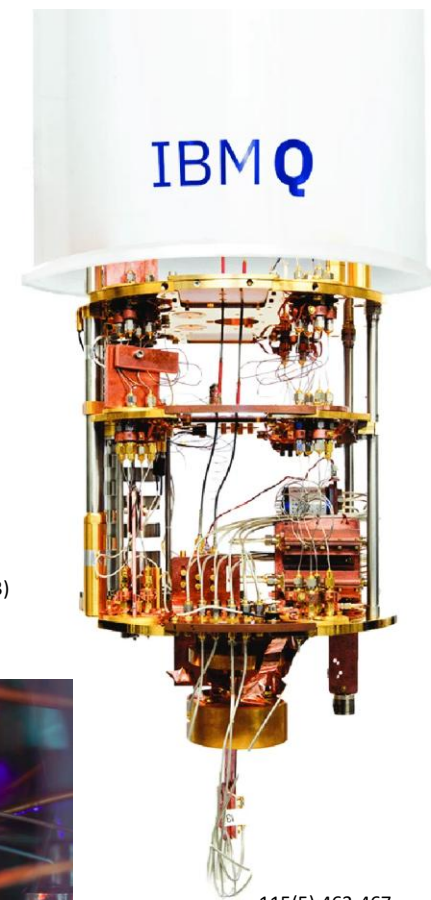
115(5):463-467

Kvantové počítače a dnešní kryptografie

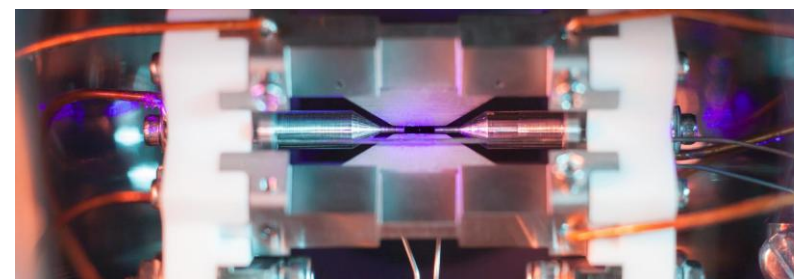
- Shorův algoritmus



Nature **624**, 238 (2023)



115(5):463-467



<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>

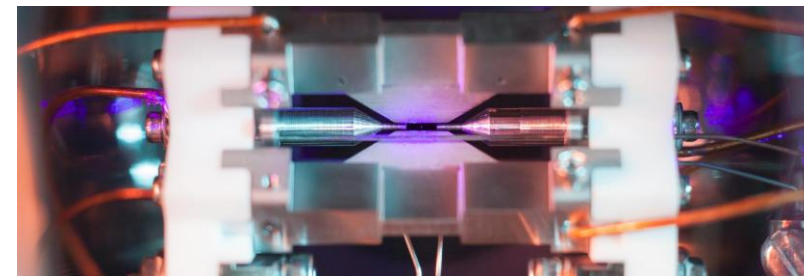
Kvantové počítače a dnešní kryptografie

▪ Shorův algoritmus

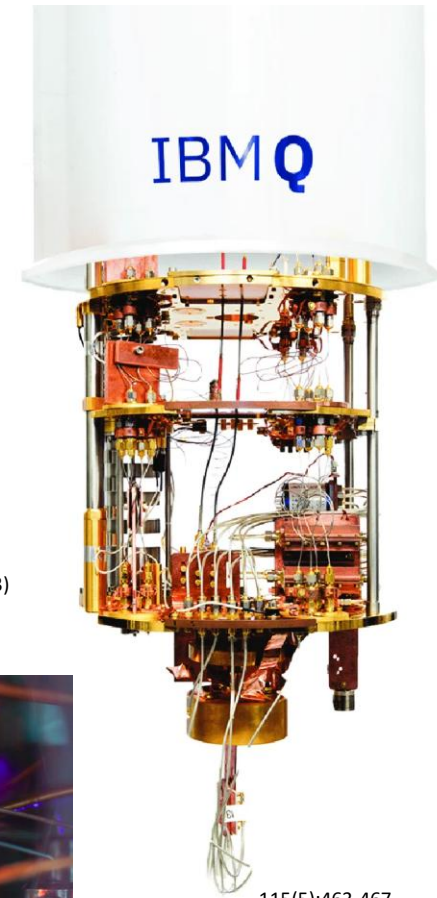
- ohrožuje RSA, Diffie-Hellman a ECC
- dopad: HTTPS / TLS, VPN, SSH, PKI, e-mail, IoT, ...



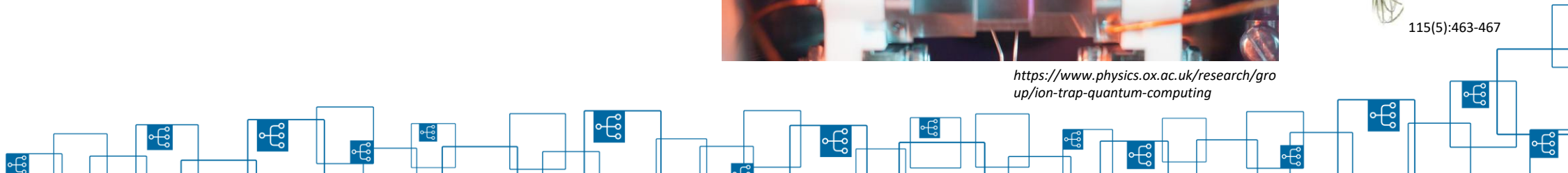
Nature **624**, 238 (2023)



<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>



115(5):463-467



Kvantové počítače a dnešní kryptografie

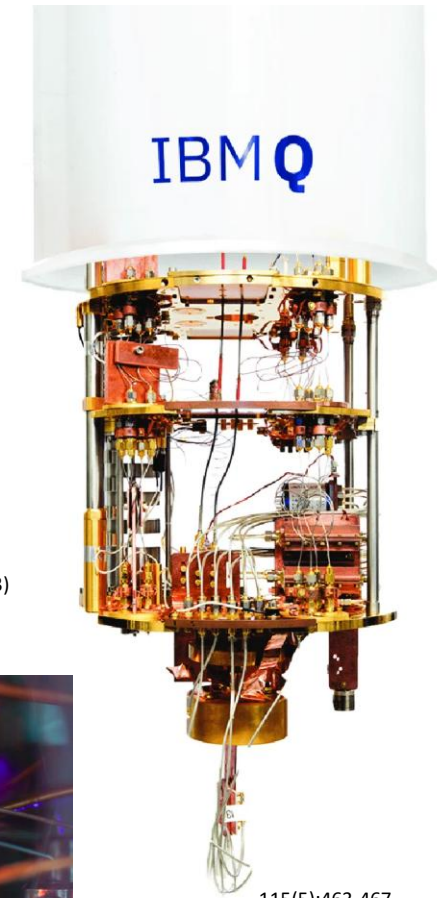
▪ Shorův algoritmus

- ohrožuje RSA, Diffie-Hellman a ECC
- dopad: HTTPS / TLS, VPN, SSH, PKI, e-mail, IoT, ...

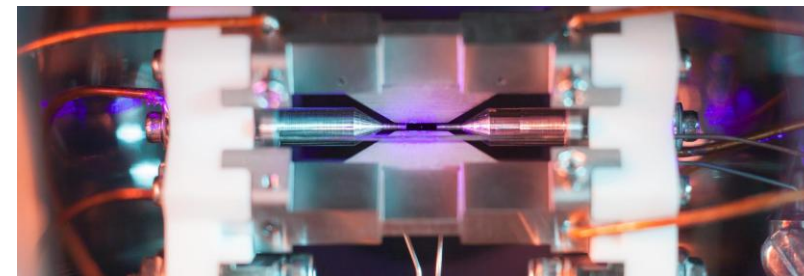
Řeší faktORIZACI a diskretní logaritmus v polynomiálním čase



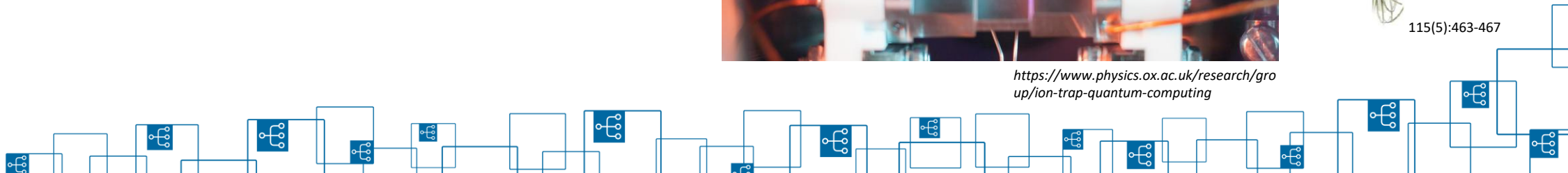
Nature **624**, 238 (2023)



115(5):463-467



<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>



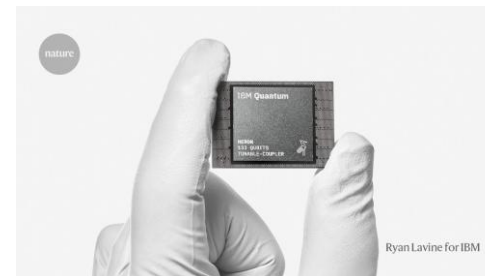
Kvantové počítače a dnešní kryptografie

■ Shorův algoritmus

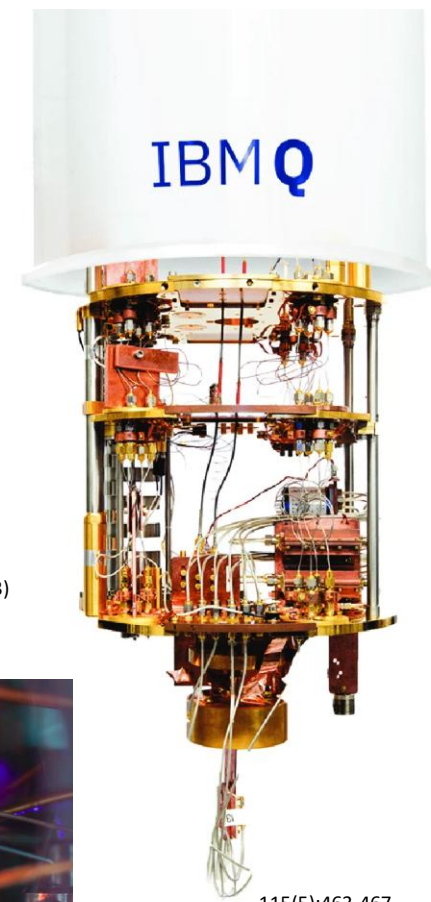
- ohrožuje RSA, Diffie-Hellman a ECC
- dopad: HTTPS / TLS, VPN, SSH, PKI, e-mail, IoT, ...

Řeší faktORIZACI a diskretní logaritmus v polynomiálním čase

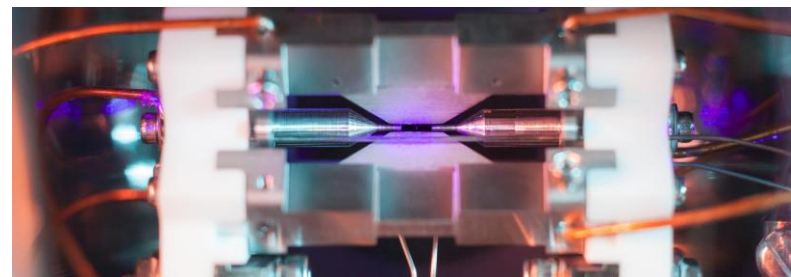
■ Groverův algoritmus



Nature **624**, 238 (2023)



115(5):463-467



<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>

Kvantové počítače a dnešní kryptografie

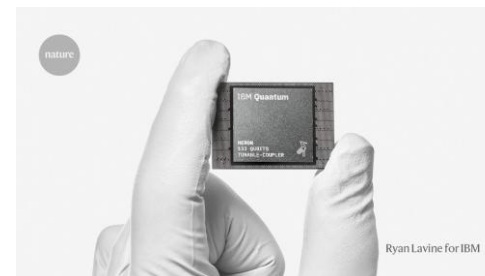
■ Shorův algoritmus

- ohrožuje RSA, Diffie-Hellman a ECC
- dopad: HTTPS / TLS, VPN, SSH, PKI, e-mail, IoT, ...

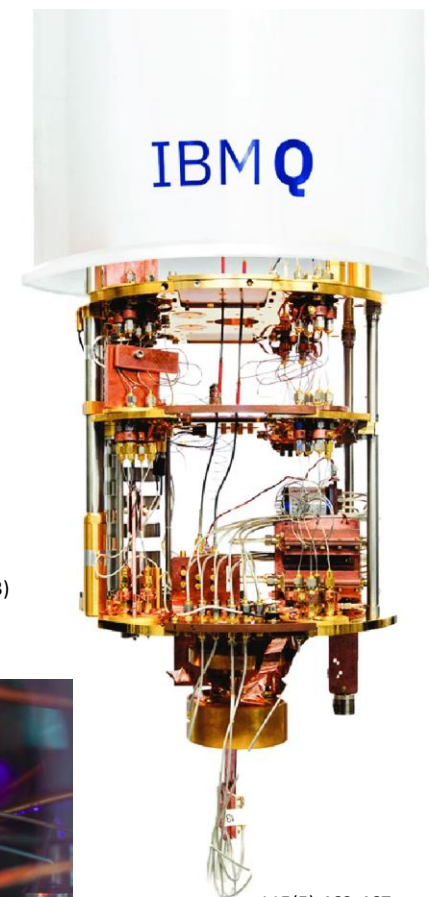
Řeší faktORIZACI a diskretní logaritmus v polynomiálním čase

■ Groverův algoritmus

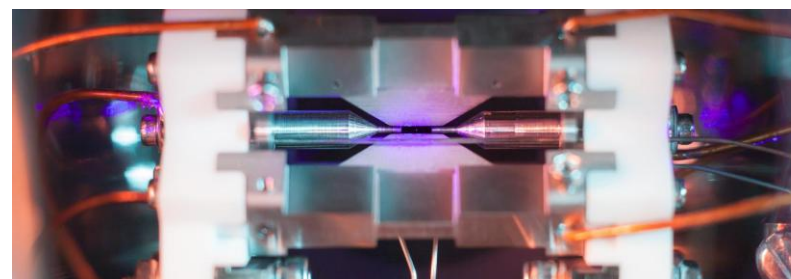
- urychluje hrubou sílu nad symetrickými klíči
- praktická obrana: delší klíče



Nature **624**, 238 (2023)



115(5):463-467



<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>

Kvantové počítače a dnešní kryptografie

▪ Shorův algoritmus

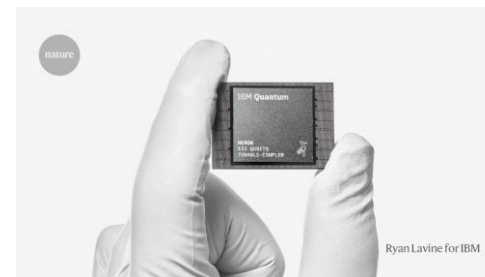
- ohrožuje RSA, Diffie-Hellman a ECC
- dopad: HTTPS / TLS, VPN, SSH, PKI, e-mail, IoT, ...

Řeší faktORIZACI a diskretní logaritmus v polynomiálním čase

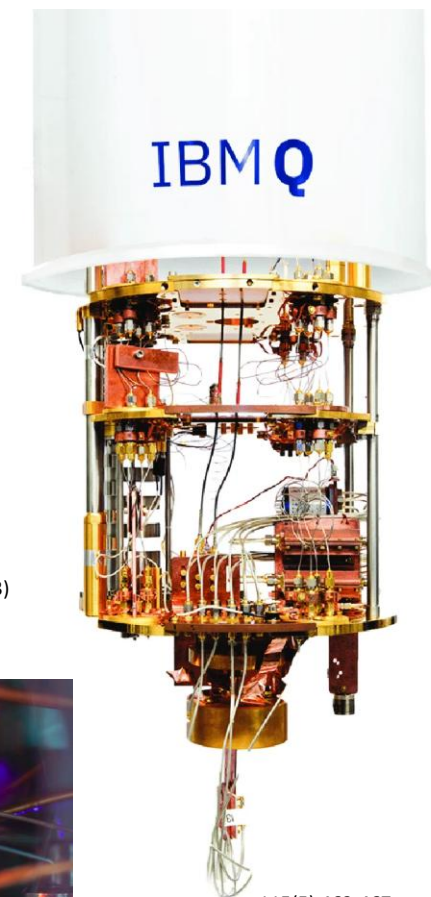
▪ Groverův algoritmus

- urychluje hrubou sílu nad symetrickými klíči
- praktická obrana: delší klíče

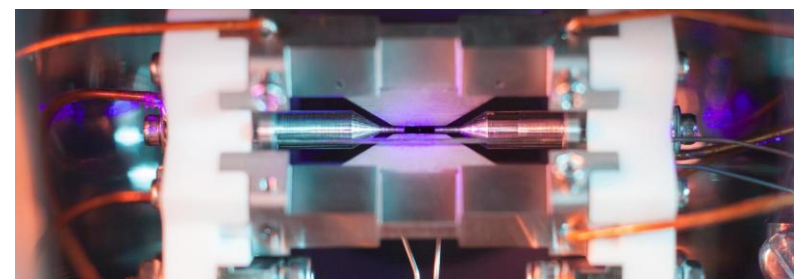
Hledání v seznamu v $O(\sqrt{N})$ čase oproti $O(N/2)$



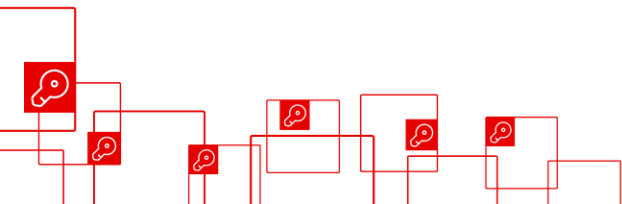
Nature **624**, 238 (2023)



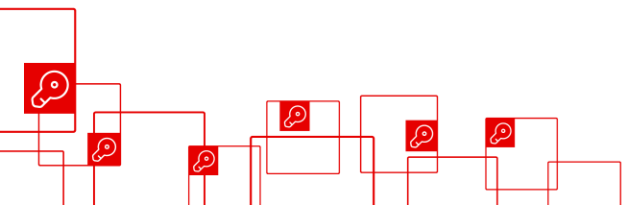
115(5):463-467



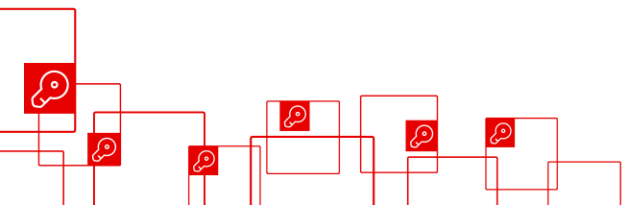
<https://www.physics.ox.ac.uk/research/group/ion-trap-quantum-computing>



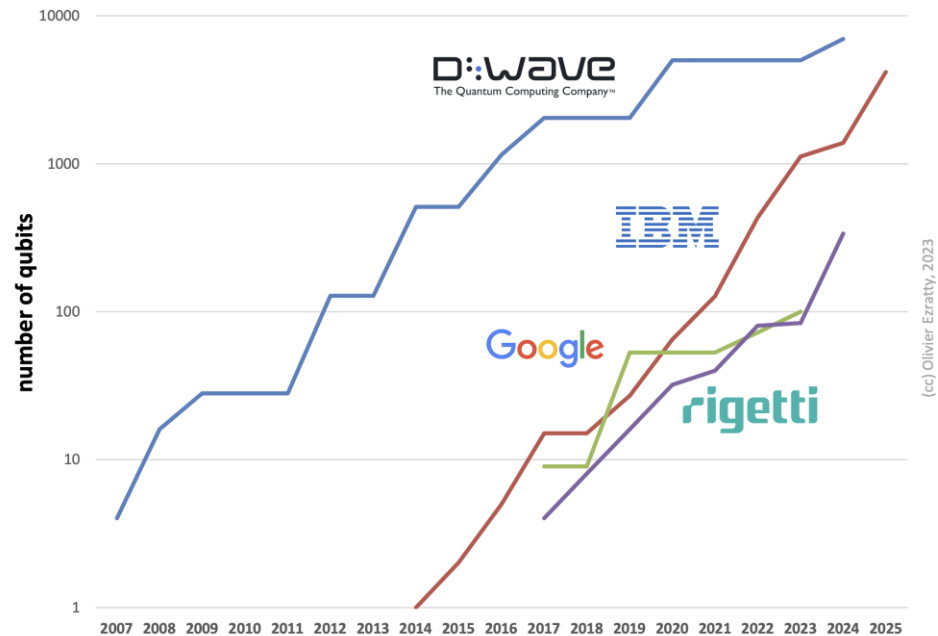
- **Q-day** – den kdy kvantové počítače prolomí RSA-2048



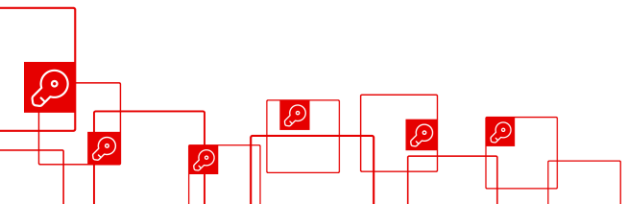
- **Q-day** – den kdy kvantové počítače prolomí RSA-2048
- Útok typu **Harvest-now-decrypt-later** je aktuální!



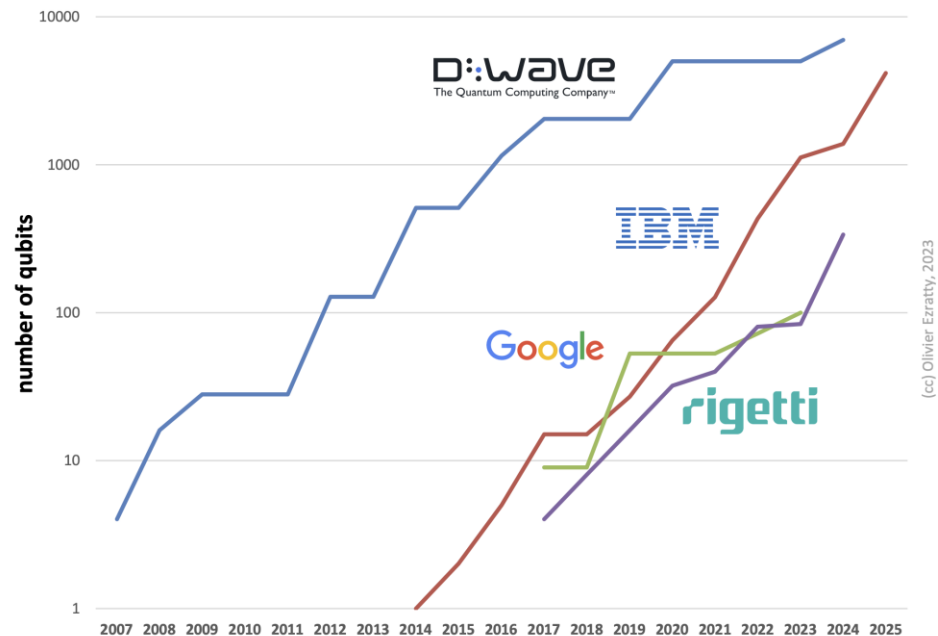
- **Q-day** – den kdy kvantové počítače prolomí RSA-2048
- Útok typu **Harvest-now-decrypt-later** je aktuální!



[10.48550/arXiv.2303.15547](https://arxiv.org/abs/10.48550/arXiv.2303.15547)



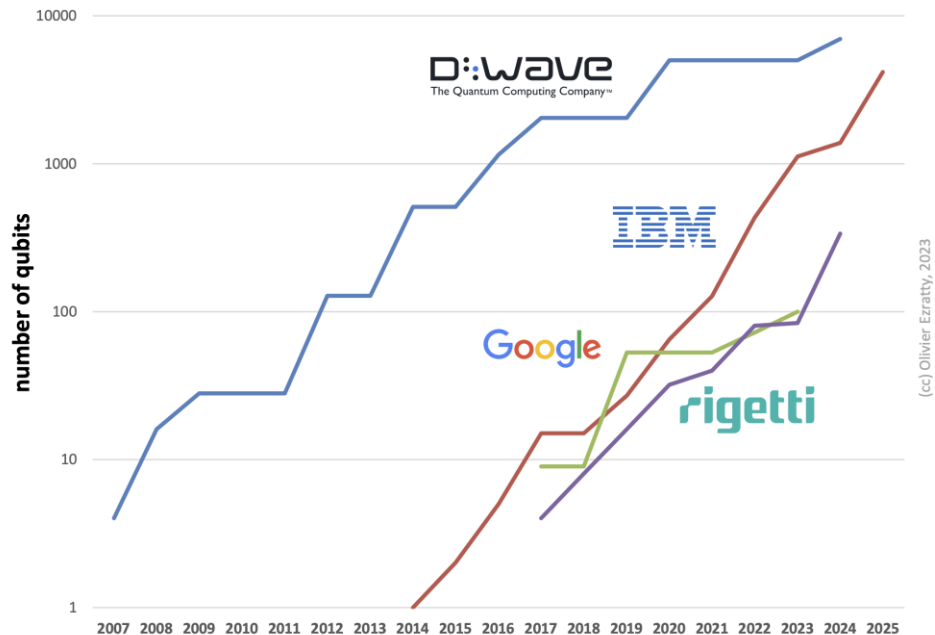
- **Q-day** – den kdy kvantové počítače prolomí RSA-2048
- Útok typu **Harvest-now-decrypt-later** je aktuální!



Čí data nevidíme / neznáme?

[10.48550/arXiv.2303.15547](https://arxiv.org/abs/10.48550/arXiv.2303.15547)

- **Q-day** – den kdy kvantové počítače prolomí RSA-2048
- Útok typu **Harvest-now-decrypt-later** je aktuální!

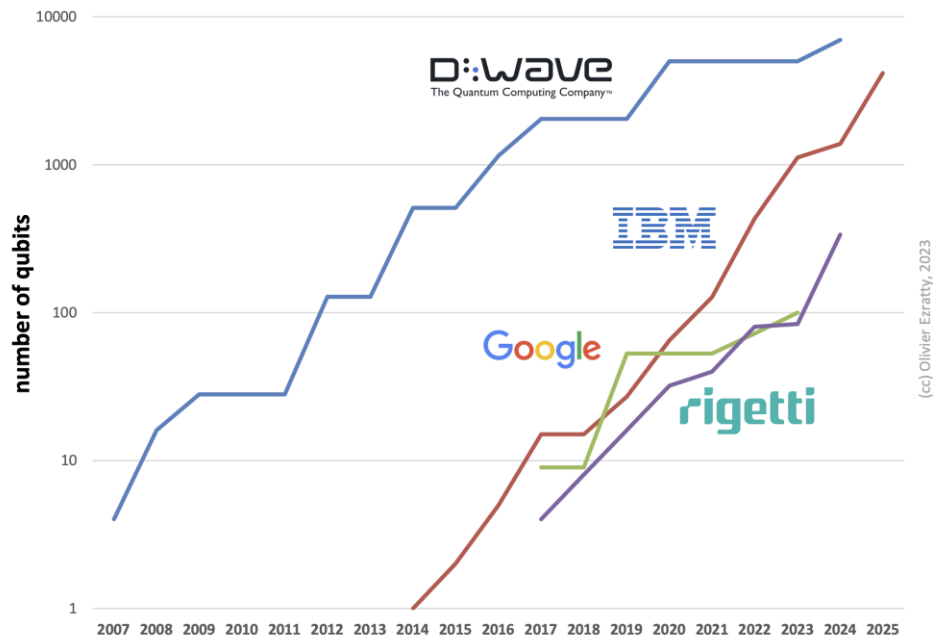


Čí data nevidíme / neznáme?

[10.48550/arXiv.2303.15547](https://arxiv.org/abs/10.48550/arXiv.2303.15547)

IQM, PASQAL
Evropské firmy s >100 qubity

- **Q-day** – den kdy kvantové počítače prolomí RSA-2048
- Útok typu **Harvest-now-decrypt-later** je aktuální!



Čí data nevidíme / neznáme?

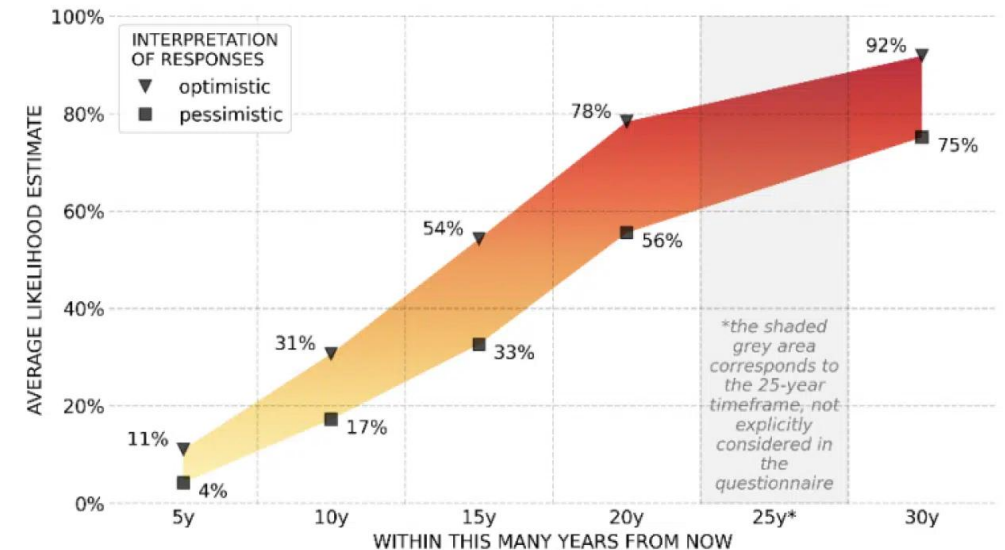
[10.48550/arXiv.2303.15547](https://arxiv.org/abs/10.48550/arXiv.2303.15547)

IQM, PASQAL
Evropské firmy s >100 qubity



2023 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME

Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents



<https://postquantum.com/q-day/q-day-crqc-predictions/>

- Americké NIST a NSA: PQC je hlavní cesta široké migrace, a to již dnes. QKD je specializovaný doplněk pro vybrané optické linky.

PQC: CISA, NIST, NSA
Recommend How to Prepare Now

- Americké NIST a NSA: PQC je hlavní cesta široké migrace, a to již dnes. QKD je specializovaný doplněk pro vybrané optické linky.

PQC: CISA, NIST, NSA
Recommend How to Prepare Now

vlastnosti	PQC	QKD
Způsob řešení		
Služba		
Bezpečnost		
Implementace		
Nasaditelnost		
Cena		

- Americké NIST a NSA: PQC je hlavní cesta široké migrace, a to již dnes. QKD je specializovaný doplněk pro vybrané optické linky.

PQC: CISA, NIST, NSA
Recommend How to Prepare Now

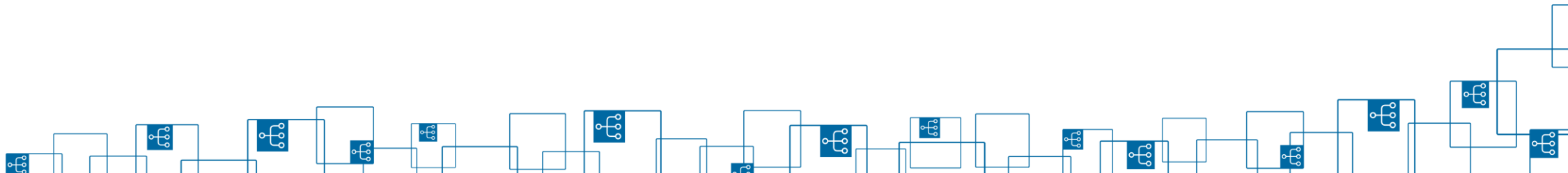
vlastnosti	PQC	QKD
Způsob řešení	nové kryptografické algoritmy	
Služba	výměna klíče + podpisy	
Bezpečnost	výpočetní	
Implementace	software, protokoly, PKI, HSM	
Nasaditelnost	široká / plošná	
Cena	€	

- Americké NIST a NSA: PQC je hlavní cesta široké migrace, a to již dnes. QKD je specializovaný doplněk pro vybrané optické linky.

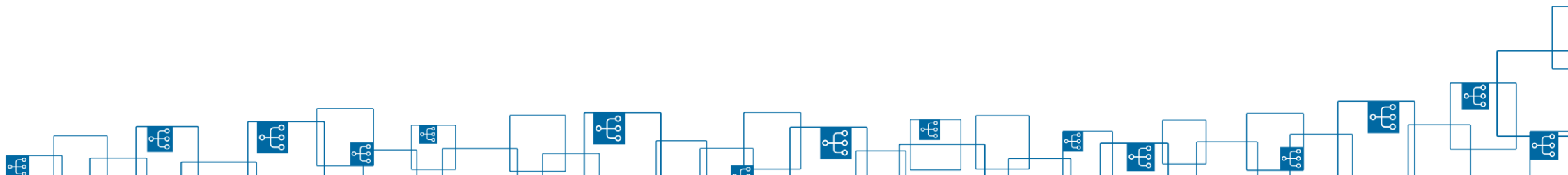
PQC: CISA, NIST, NSA
Recommend How to Prepare Now

vlastnosti	PQC	QKD
Způsob řešení	nové kryptografické algoritmy	fyzikální distribuce klíče
Služba	výměna klíče + podpisy	distribuce klíče
Bezpečnost	výpočetní	informačně-teoretická distribuce klíče*
Implementace	software, protokoly, PKI, HSM	hardware, optika, síťová integrace
Nasaditelnost	široká / plošná	vybrané optické trasy
Cena	€	€ € €

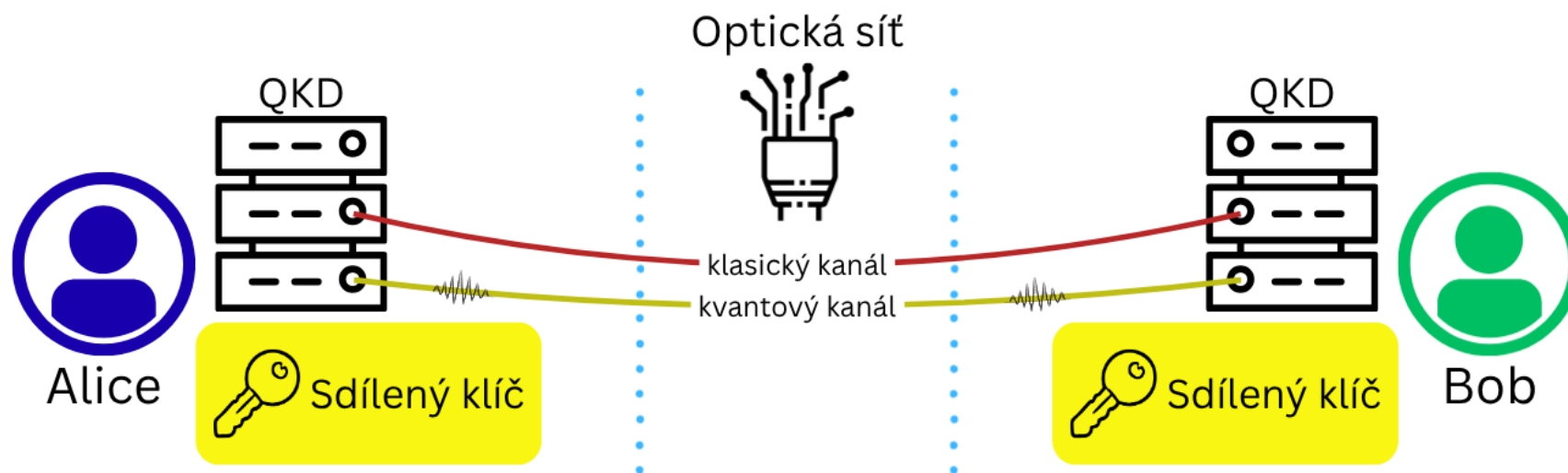
*při splnění protokolových a implementačních předpokladů [NIST IR 8547]



QKD vytváří a sdílí klíč pro sym. kryptografii

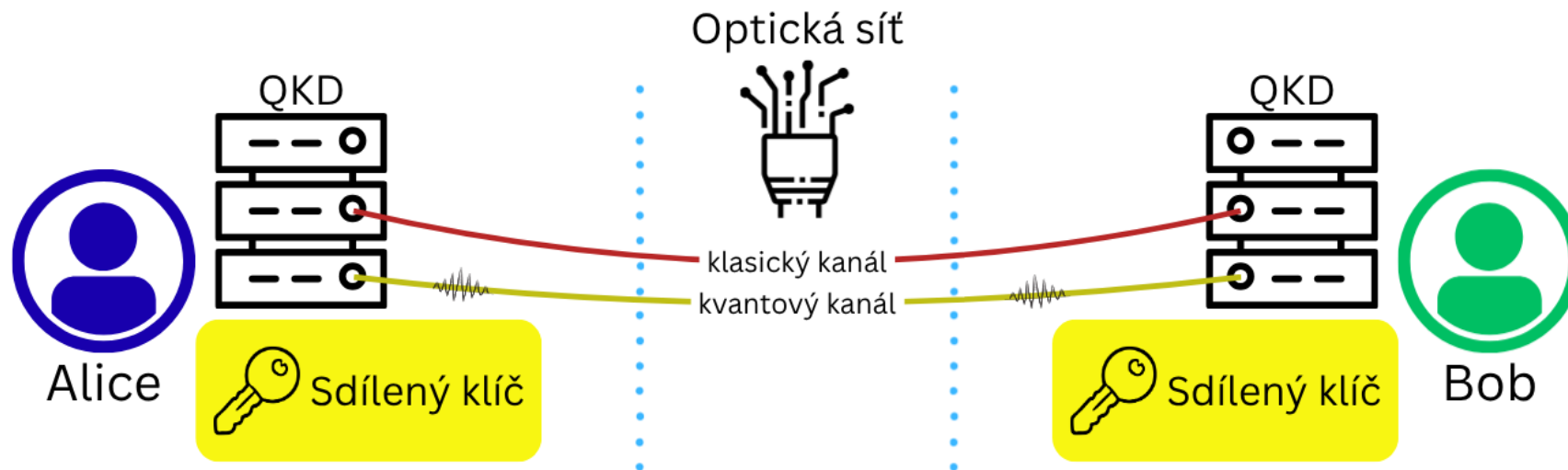


QKD vytváří a sdílí klíč pro sym. kryptografii



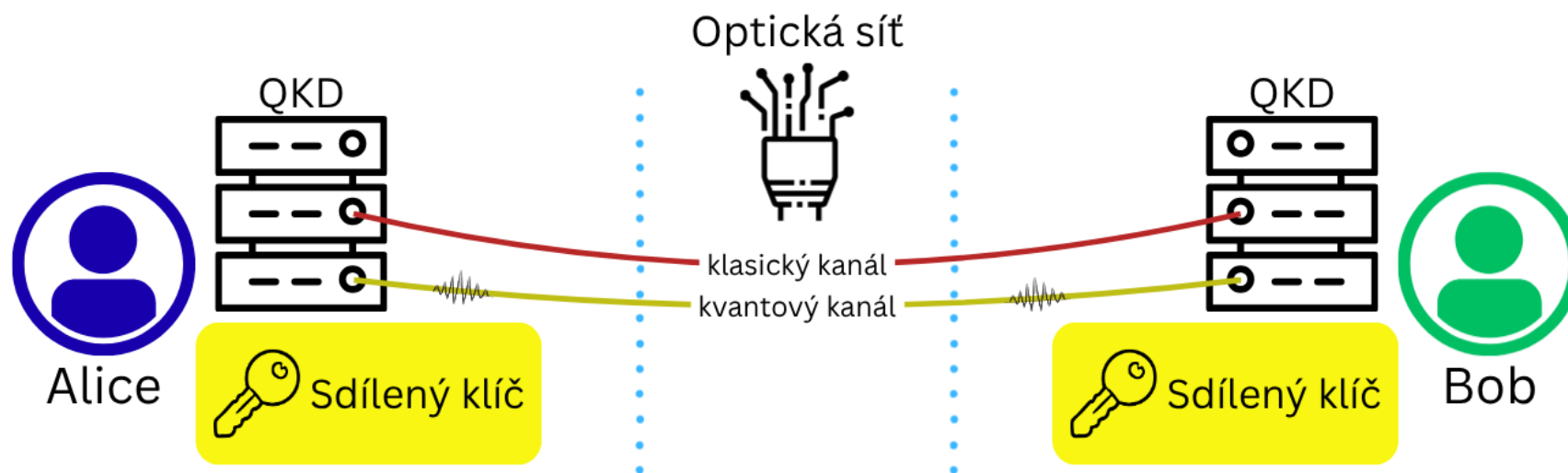
QKD vytváří a sdílí klíč pro sym. kryptografii

- Kvantový kanál přenáší kvantové stavy.



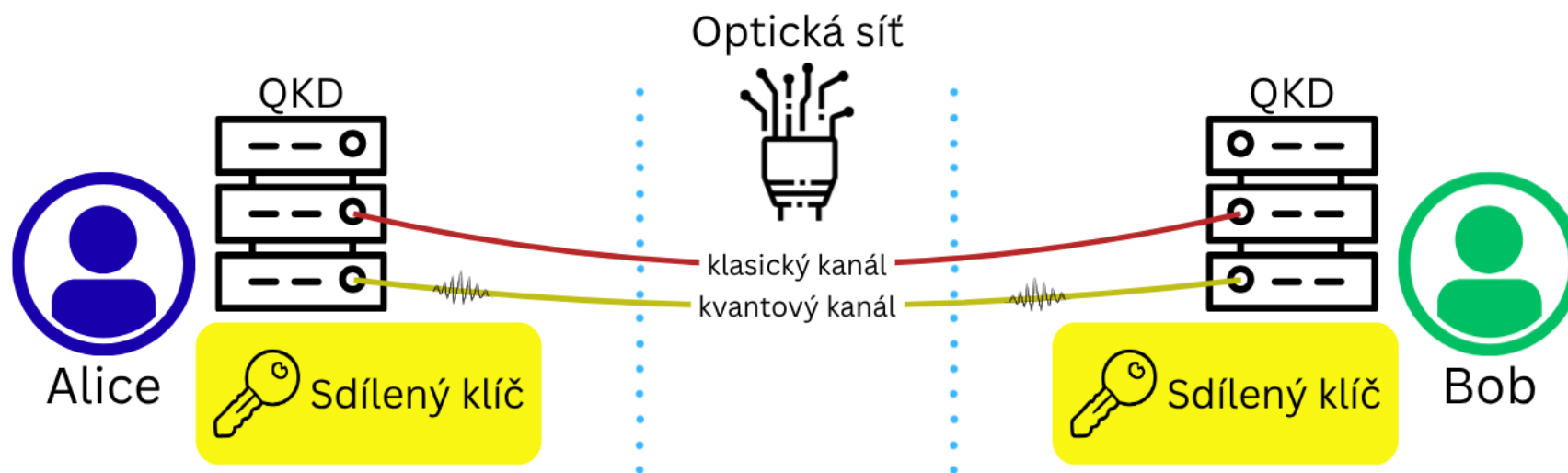
QKD vytváří a sdílí klíč pro sym. kryptografii

- Kvantový kanál přenáší kvantové stavy.
- **Autentizovaný** klasický kanál slouží k synchronizaci a zpracování klíče (MiM).



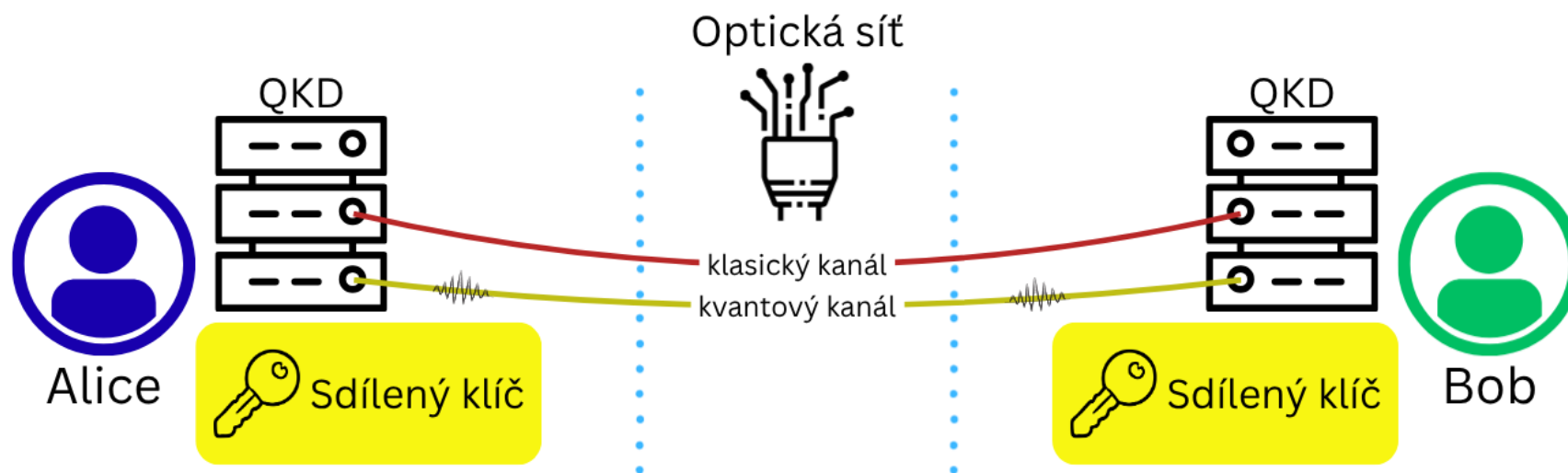
QKD vytváří a sdílí klíč pro sym. kryptografii

- Kvantový kanál přenáší kvantové stavy.
- **Autentizovaný** klasický kanál slouží k synchronizaci a zpracování klíče (MiM).
- Útočník může měřit a podvrhávat kvantové stavy, ale je **odhalen!**

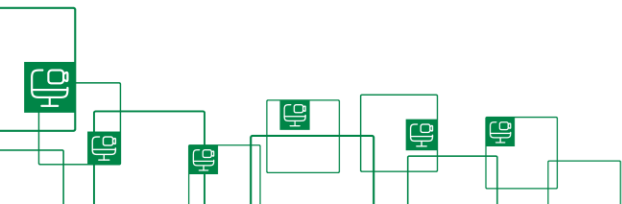


QKD vytváří a sdílí klíč pro sym. kryptografii

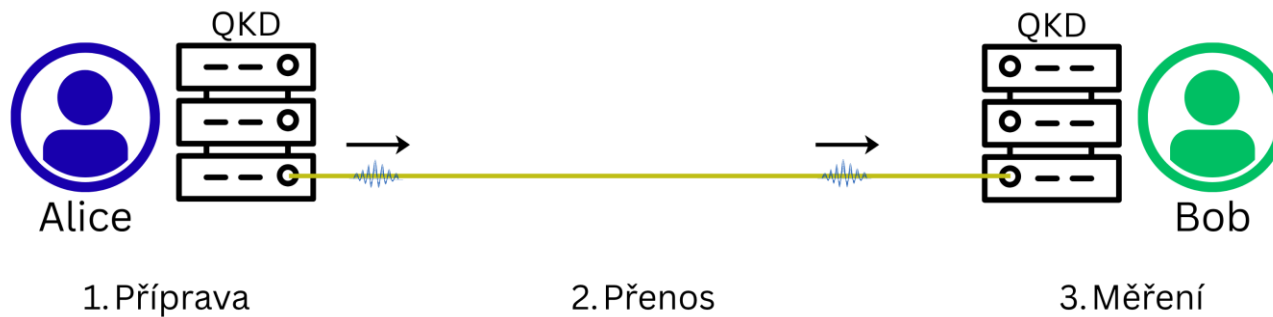
- Kvantový kanál přenáší kvantové stavy.
- **Autentizovaný** klasický kanál slouží k synchronizaci a zpracování klíče (MiM).
- Útočník může měřit a podvrhávat kvantové stavy, ale je **odhalen!**



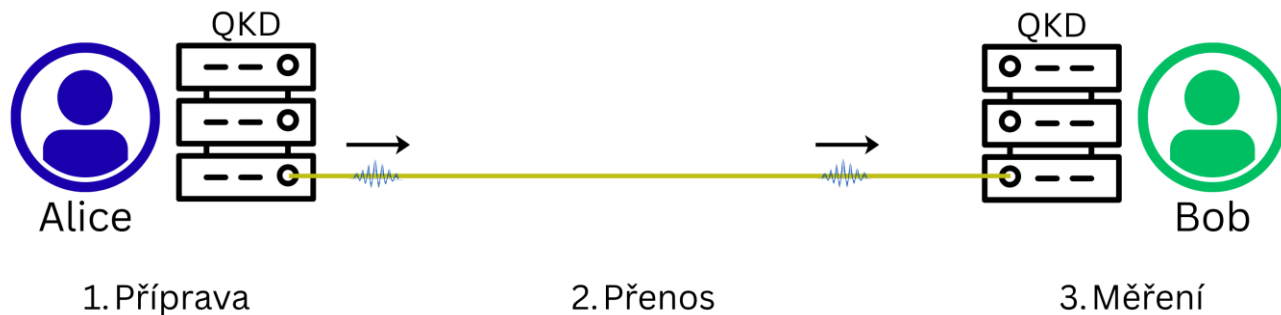
Přenos / generování náhodných čísel



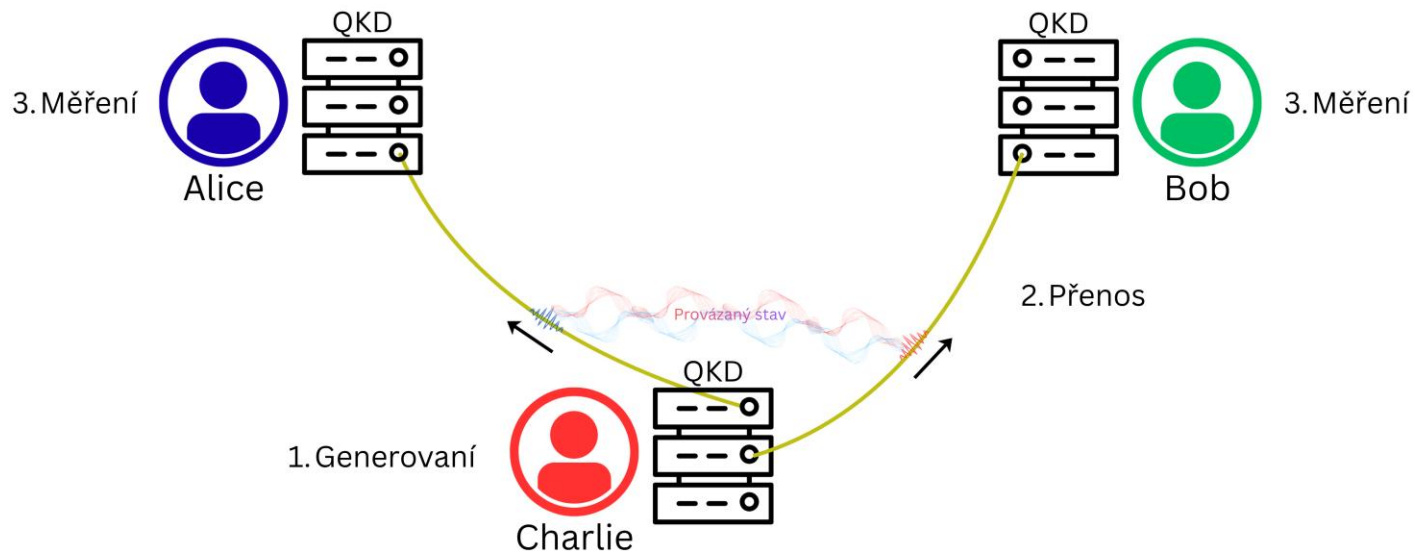
Prepare-and-measure
Alice připraví stav a Bob změří



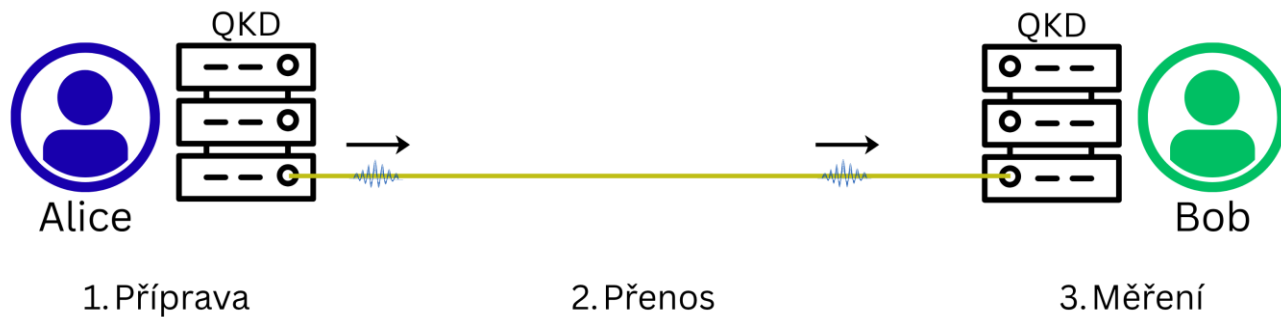
Prepare-and-measure
Alice připraví stav a Bob změří



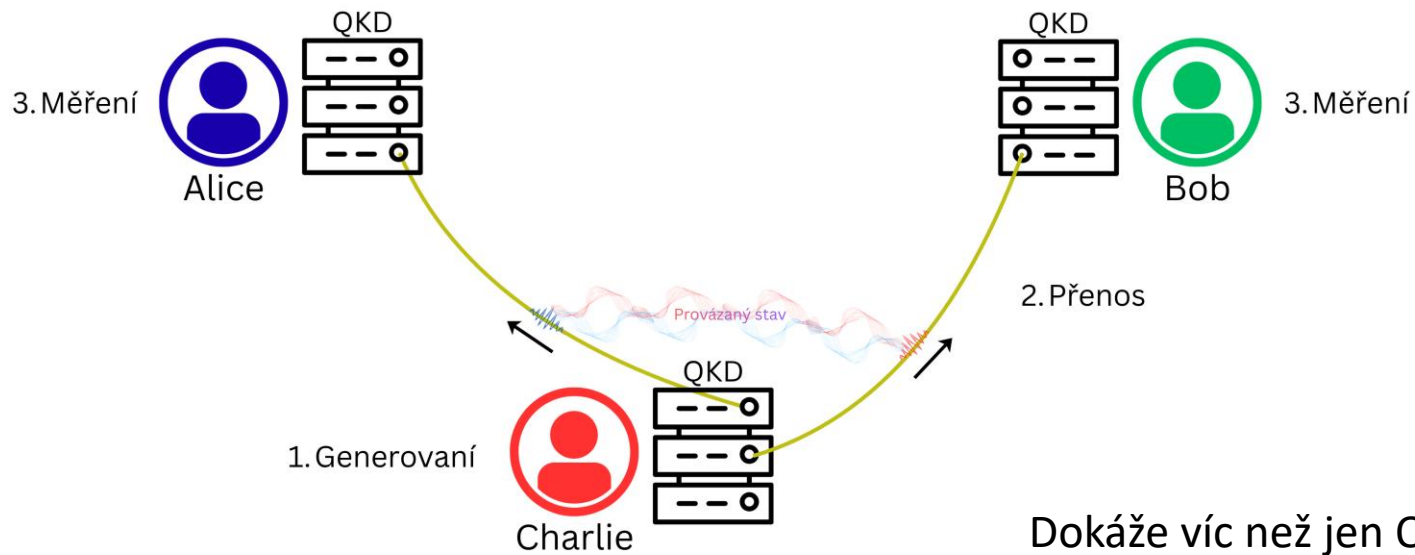
Entanglement-based
obě strany měří provázaný stav



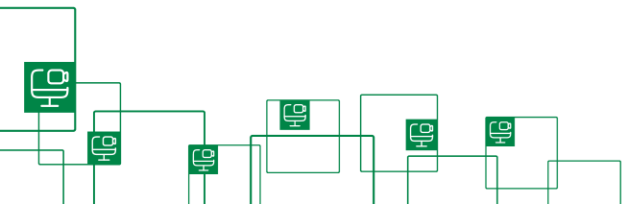
Prepare-and-measure
Alice připraví stav a Bob změří



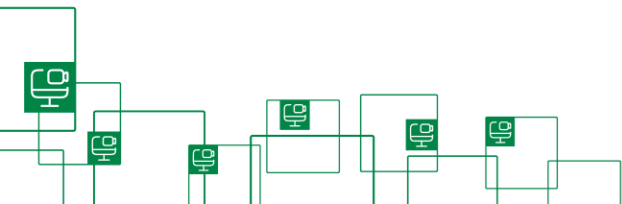
Entanglement-based
obě strany měří provázaný stav



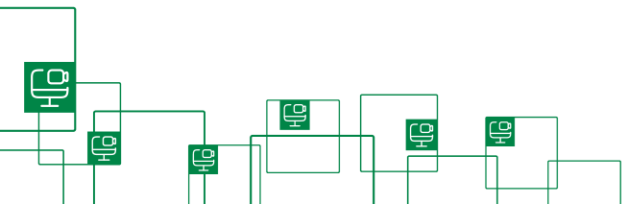
	DV-QKD jednotlivé fotony	CV-QKD kvadratury pole
Prepare-and-measure Alice připraví stav a Bob změří		
Entanglement-based obě strany měří provázaný stav		



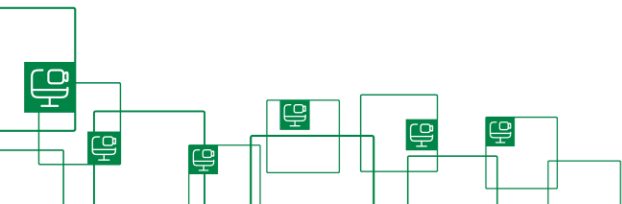
	DV-QKD jednotlivé fotony	CV-QKD kvadratury pole
Prepare-and-measure Alice připraví stav a Bob změří		
Entanglement-based obě strany měří provázaný stav		



	DV-QKD jednotlivé fotony	CV-QKD kvadratury pole
Prepare-and-measure Alice připraví stav a Bob změří	BB84 (decoy state) T12  TOSHIBA	GMCS   KEEQUANT
Entanglement-based obě strany měří provázaný stav	BBM92   QUANTUM OPTICS JENA	Model pro teoretické důkazy
	max 150 km se SKR kb/s	max 80 km se SKR kb/s



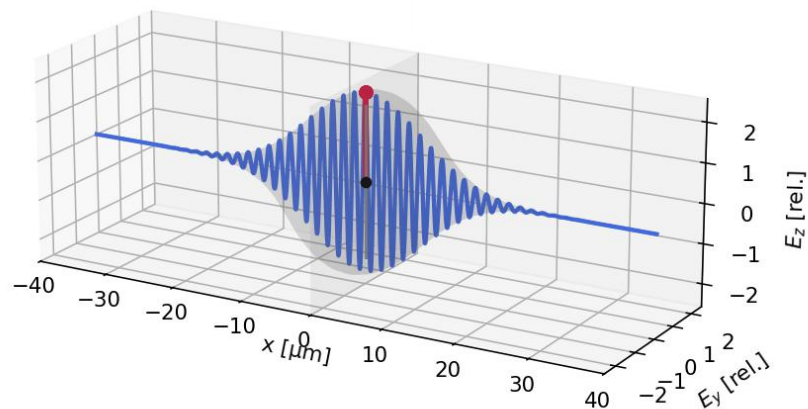
	DV-QKD jednotlivé fotony	CV-QKD kvadratury pole
Prepare-and-measure Alice připraví stav a Bob změří	BB84 (decoy state) T12  TOSHIBA	GMCS   KEEQUANT
Entanglement-based obě strany měří provázaný stav	BBM92   QUANTUM OPTICS JENA	Model pro teoretické důkazy
	max 150 km se SKR kb/s	max 80 km se SKR kb/s



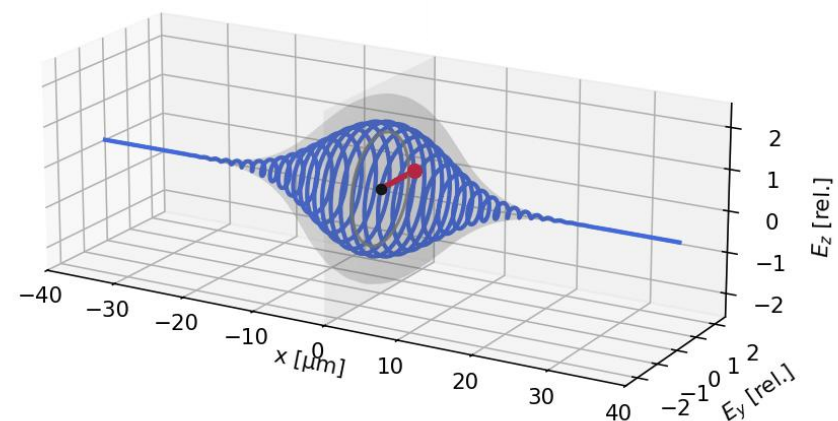
Polarizace popisuje, jak osciluje elektrické pole světla v rovině kolmé ke směru šíření.

Polarizace popisuje, jak osciluje elektrické pole světla v rovině kolmé ke směru šíření.

Horizontální polarizace $|V\rangle$:

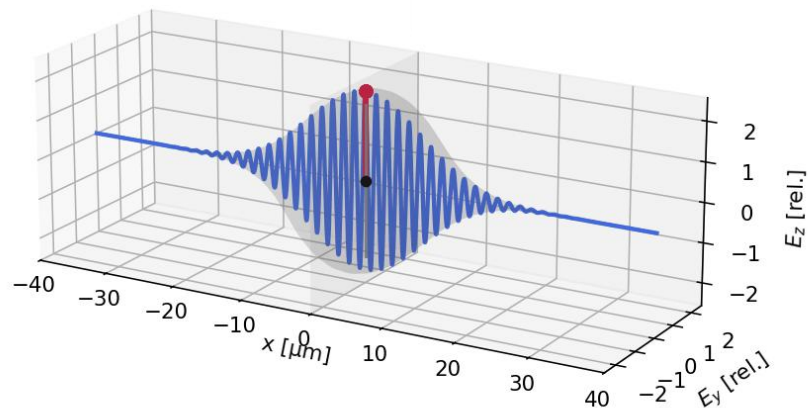


Pravotočivá polarizace $|R\rangle$:

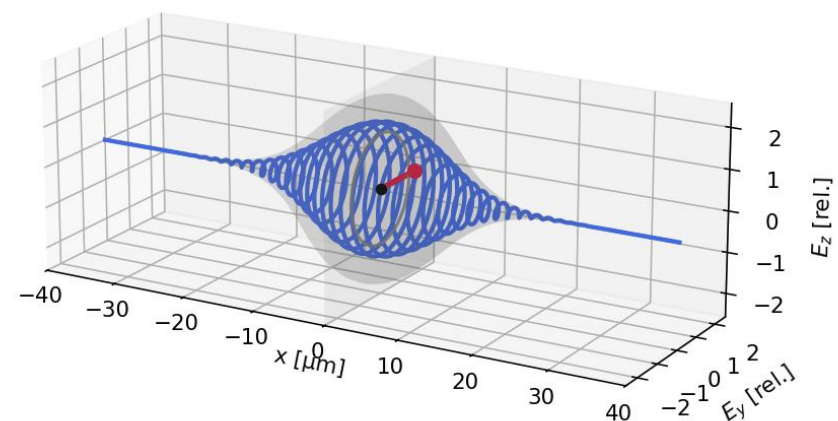


Polarizace popisuje, jak osciluje elektrické pole světla v rovině kolmé ke směru šíření.

Horizontální polarizace $|V\rangle$:



Pravotočivá polarizace $|R\rangle$:

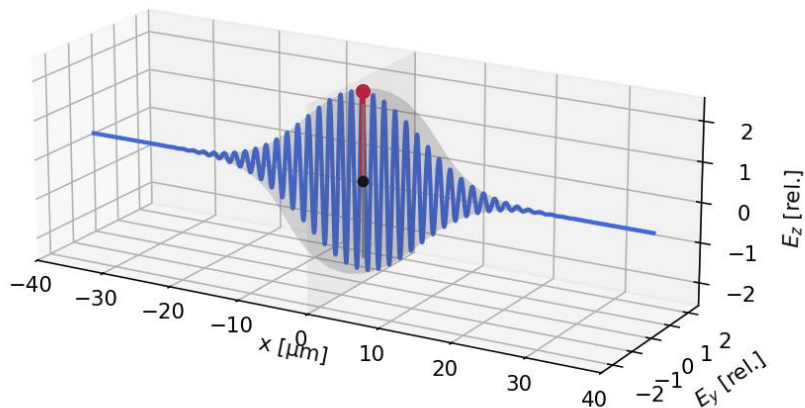


Pro plný popis polarizačního stavu je třeba měřit ve třech bázích:

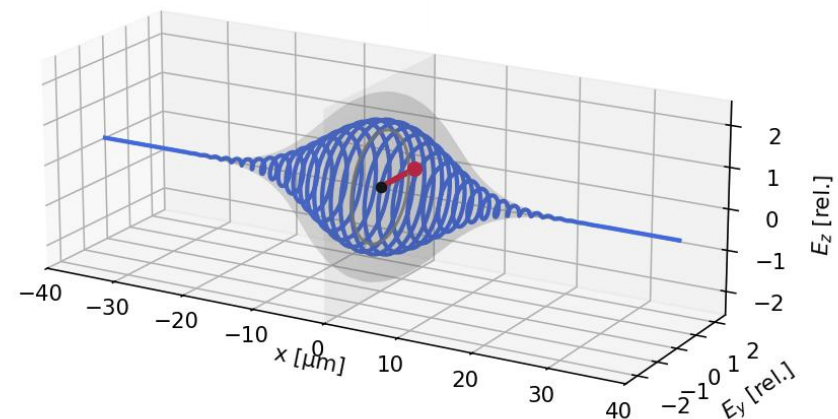
- **H/V báze** rozlišující stavy $|H\rangle$ a $|V\rangle$
- **D/A báze** rozlišující stavy $|D\rangle$ a $|A\rangle$
- **R/L báze** rozlišující stavy $|R\rangle$ a $|L\rangle$

Polarizace popisuje, jak osciluje elektrické pole světla v rovině kolmé ke směru šíření.

Horizontální polarizace $|V\rangle$:



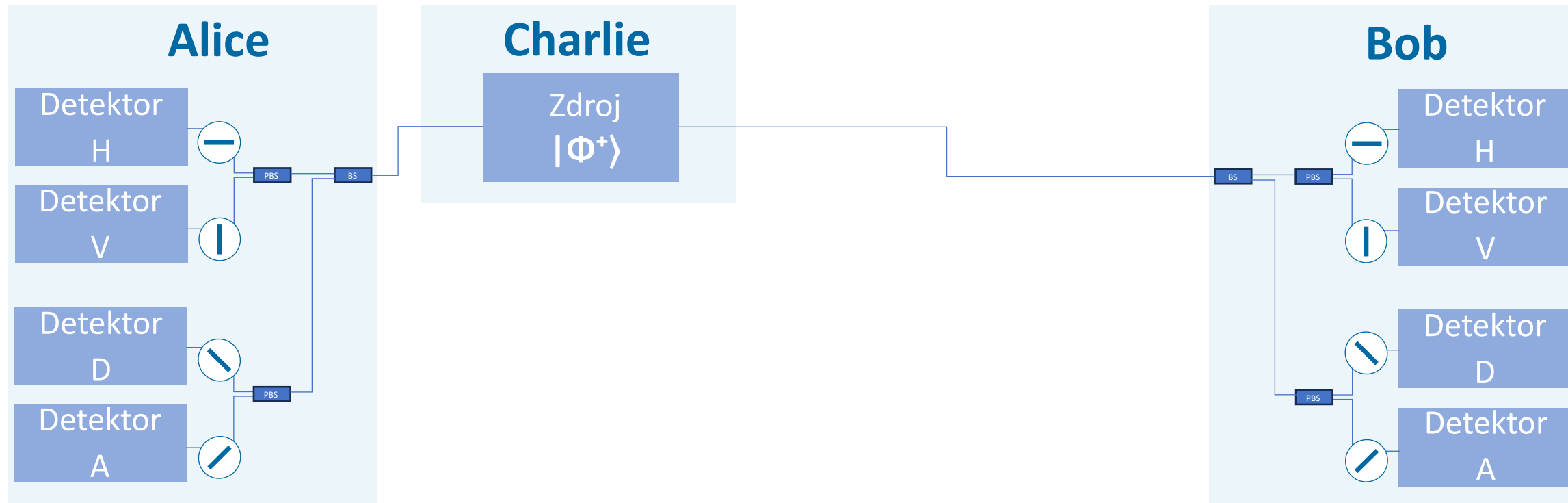
Pravotočivá polarizace $|R\rangle$:

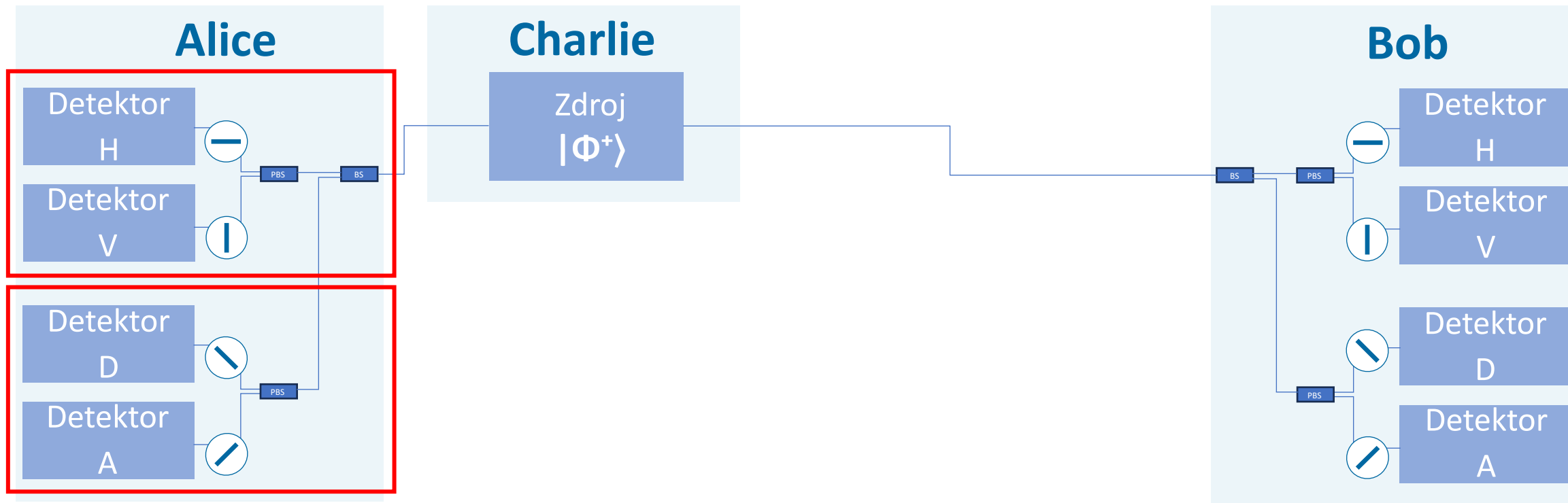


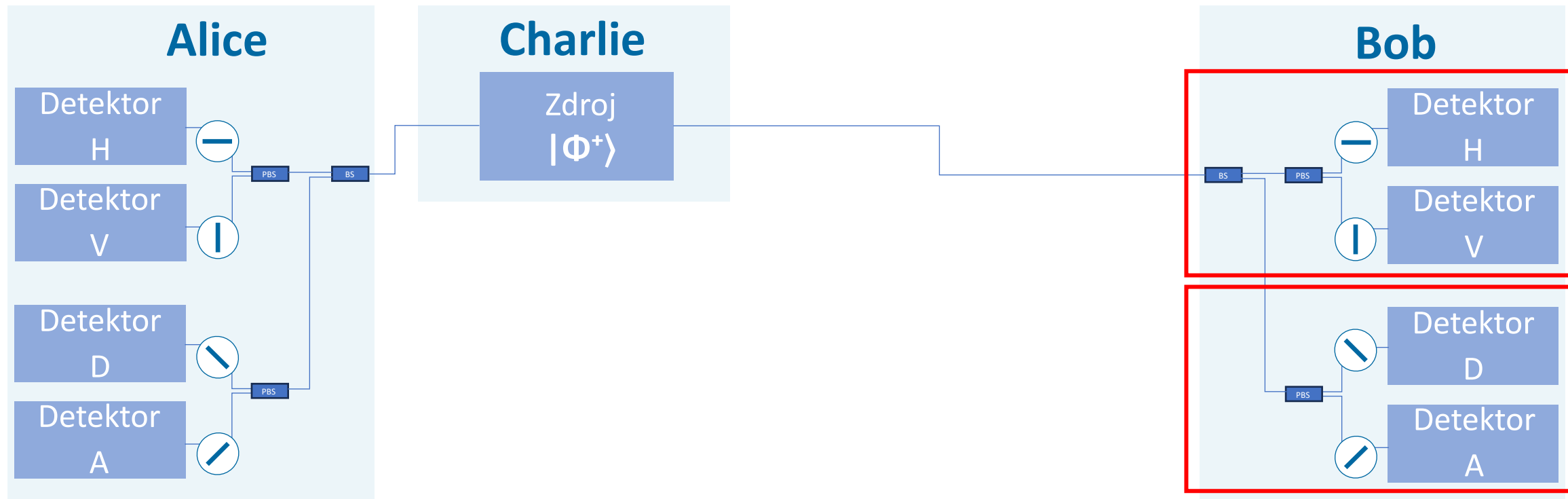
Pro plný popis polarizačního stavu je třeba měřit ve třech bázích:

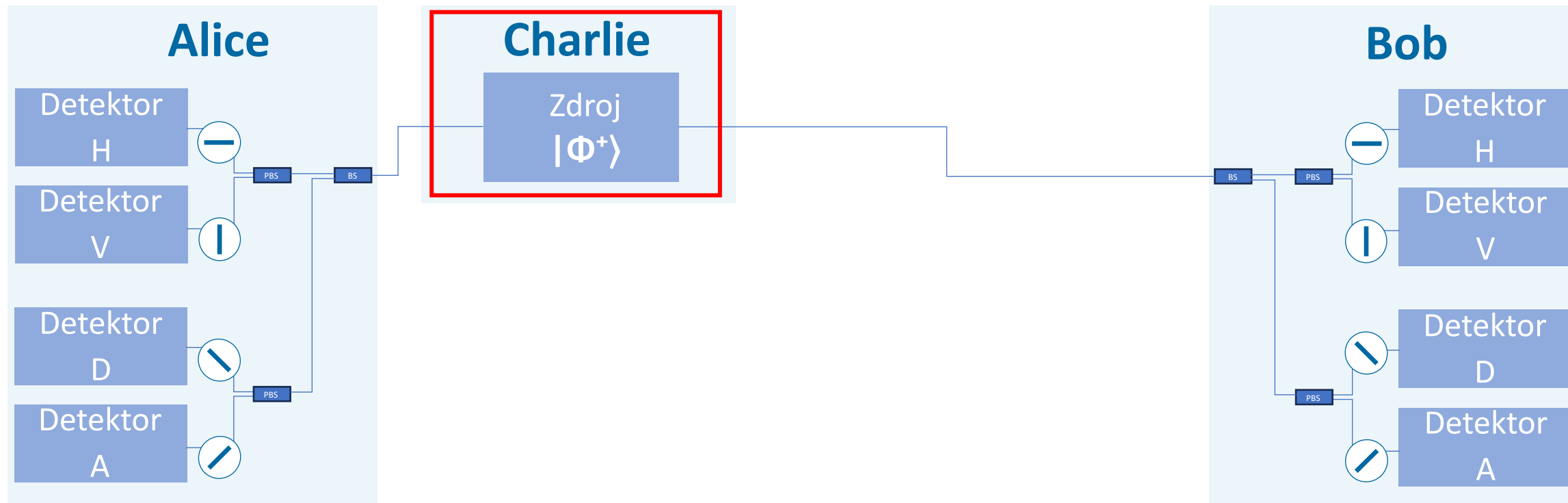
- **H/V báze** rozlišující stavy $|H\rangle$ a $|V\rangle$
- **D/A báze** rozlišující stavy $|D\rangle$ a $|A\rangle$
- **R/L báze** rozlišující stavy $|R\rangle$ a $|L\rangle$

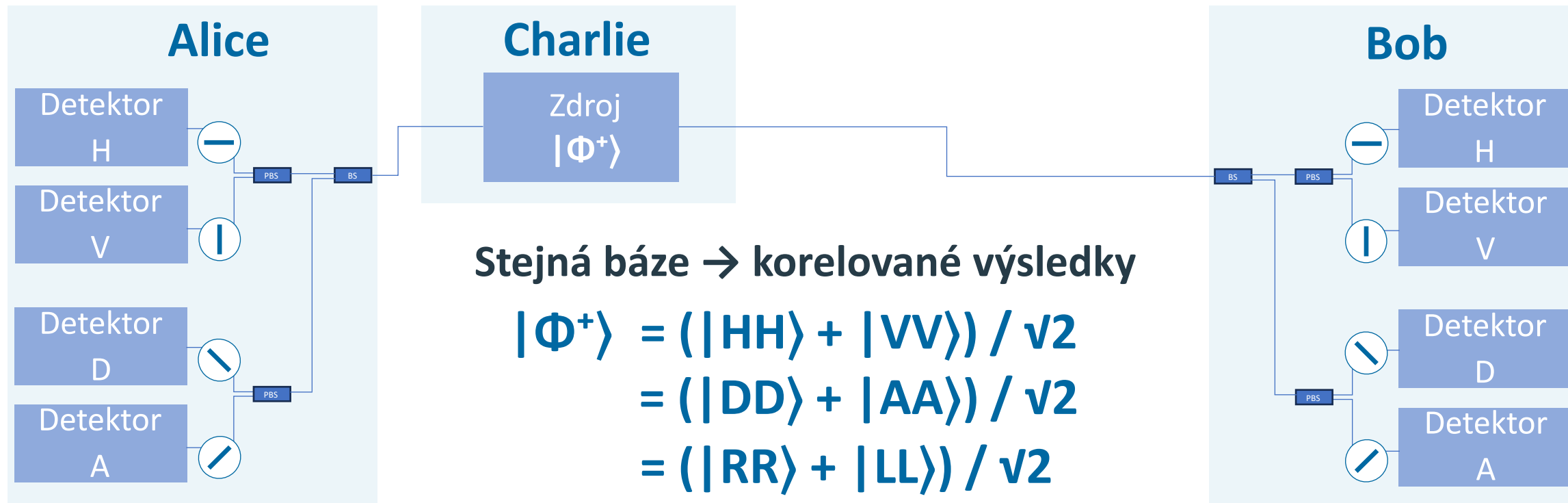
Pro QKD stačí dvě báze

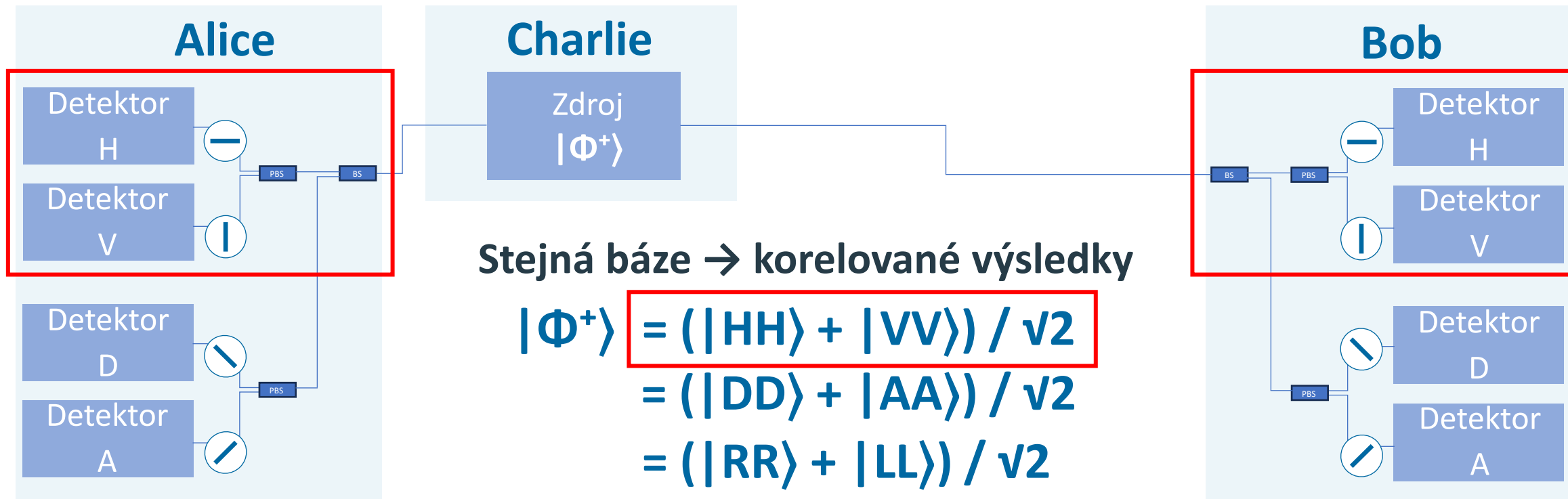


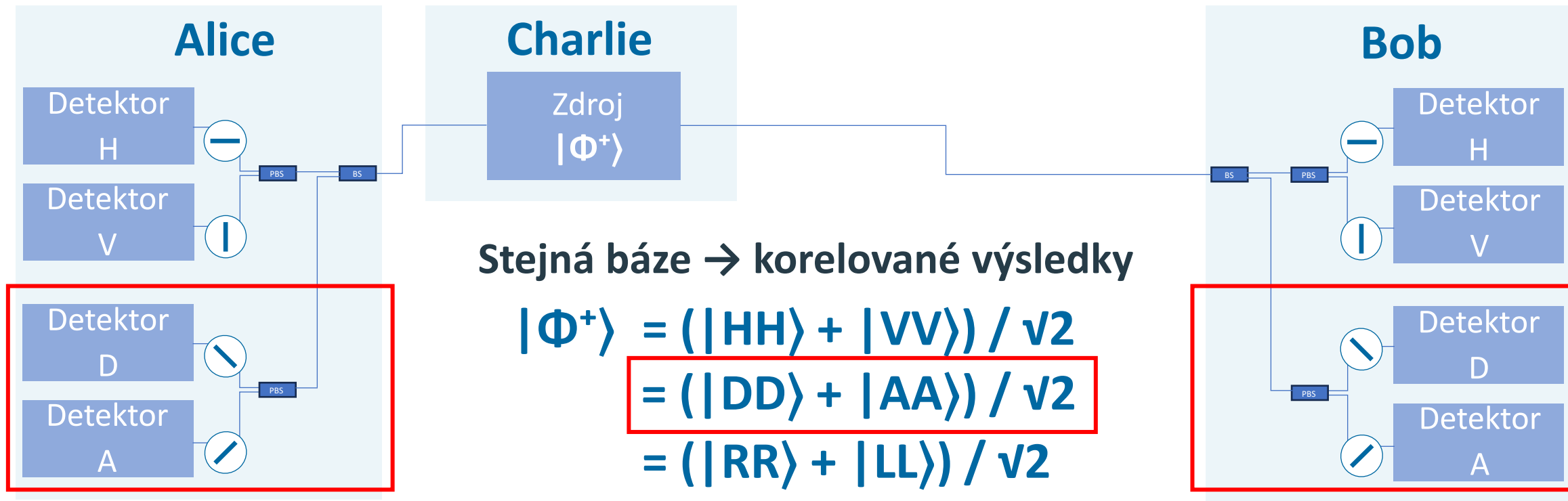


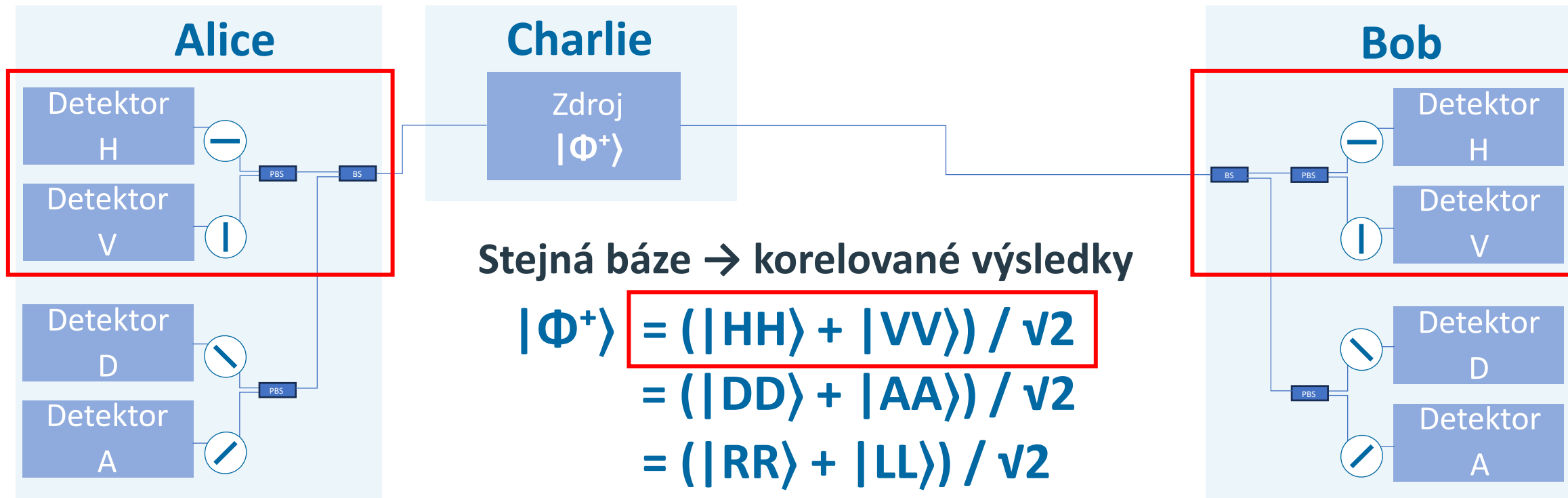


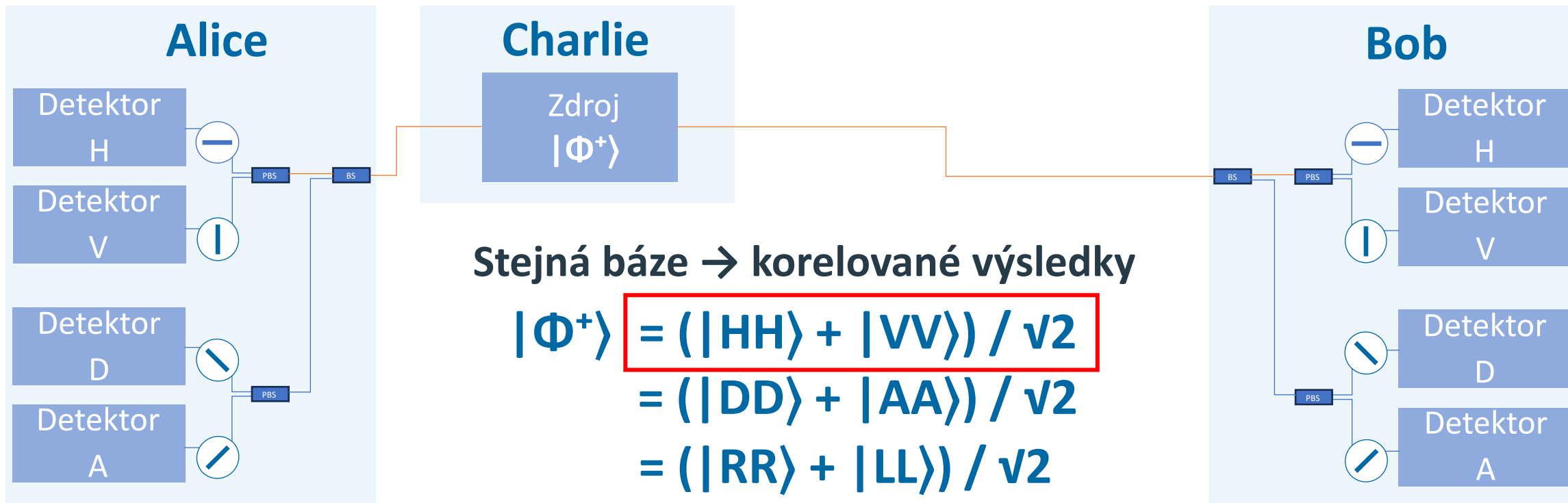


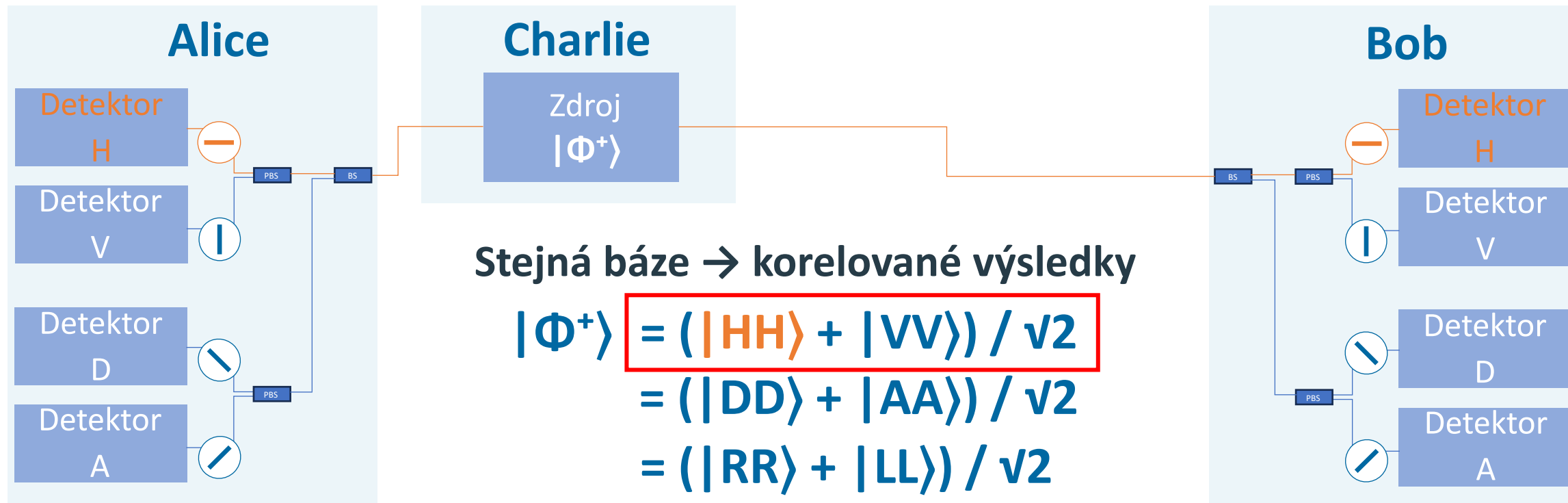


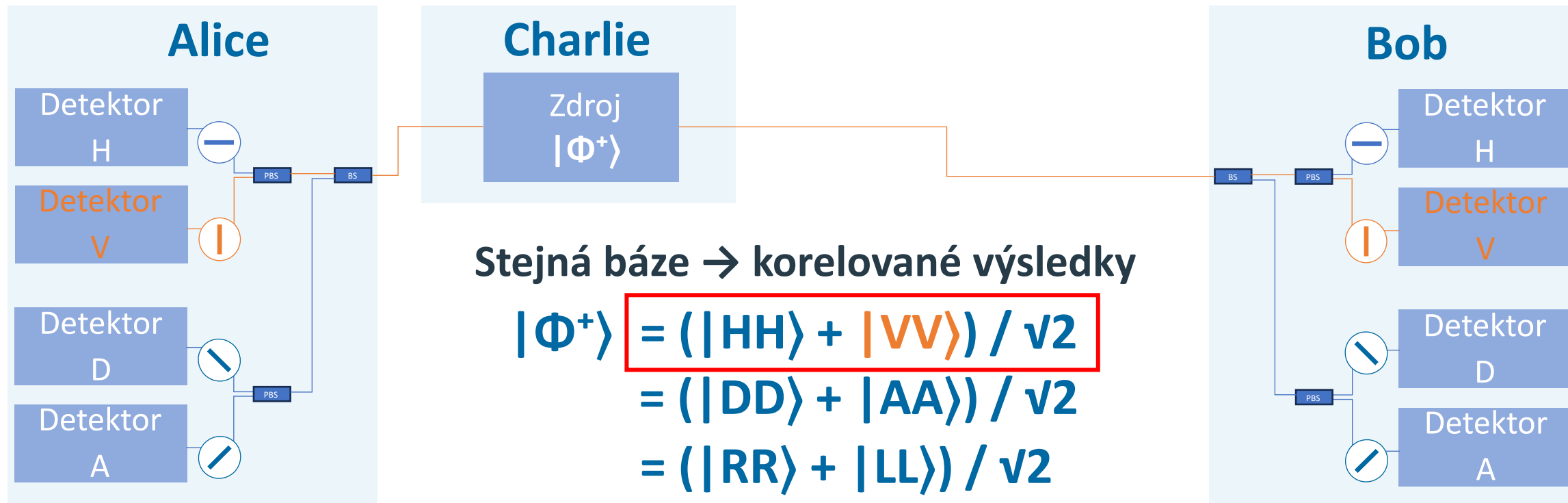


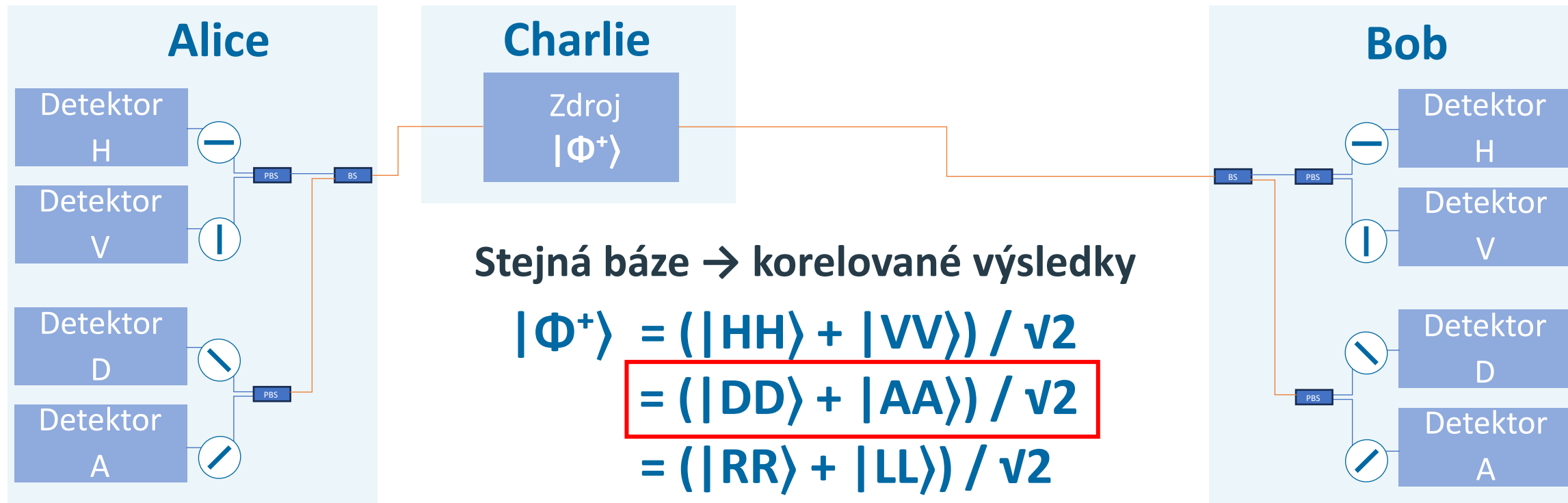


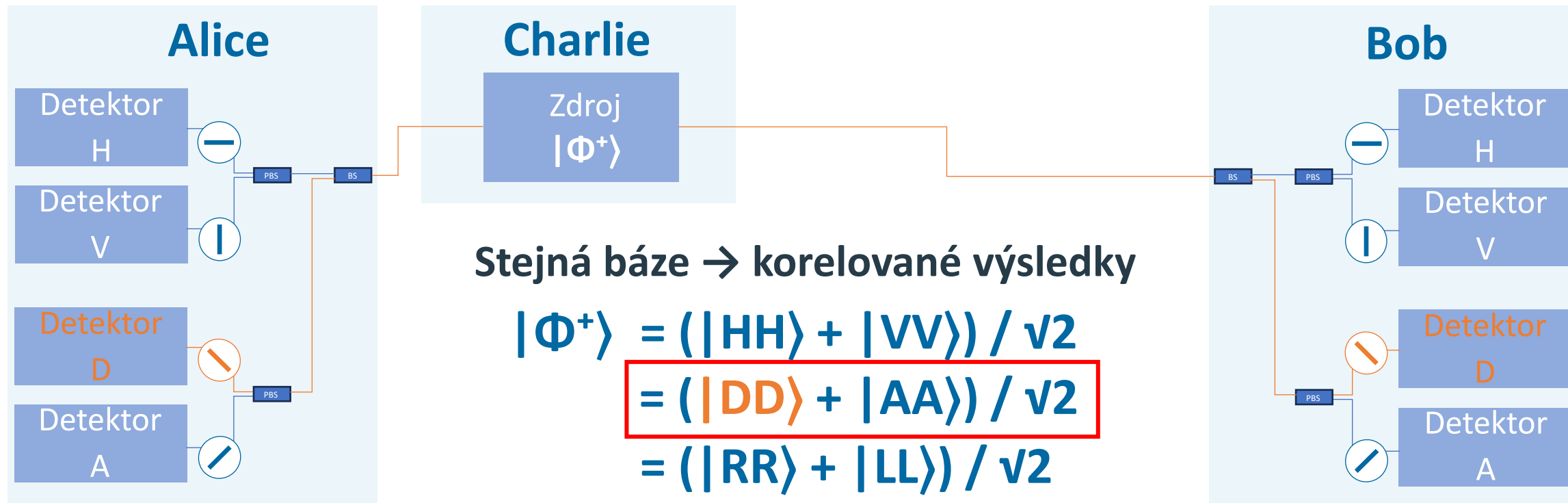


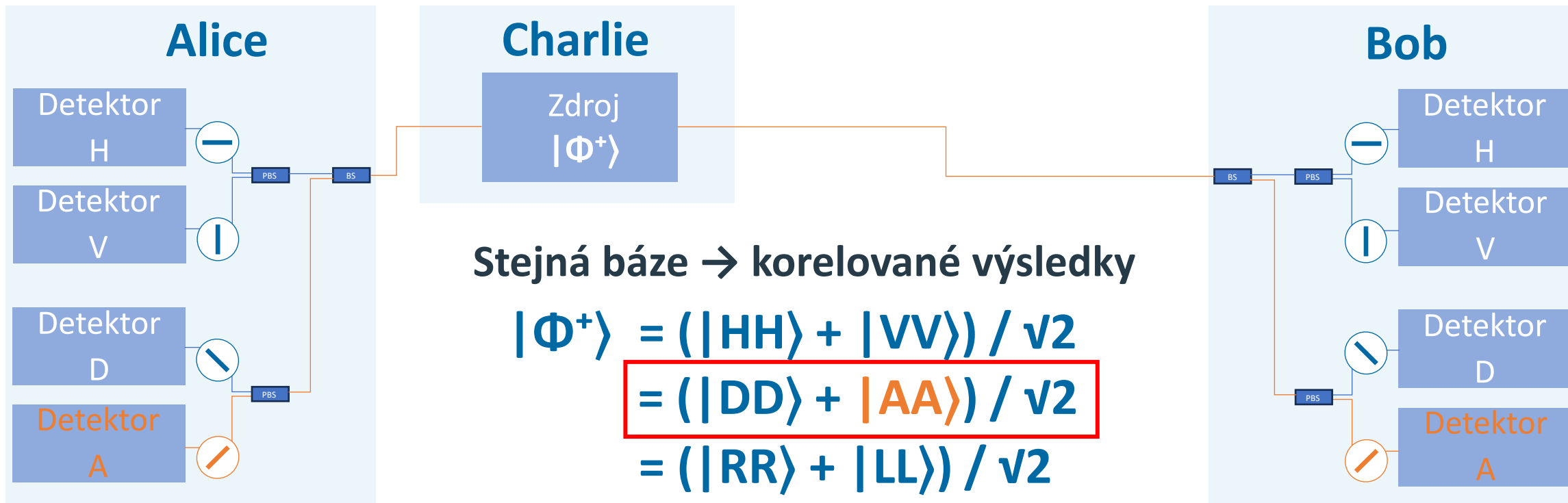


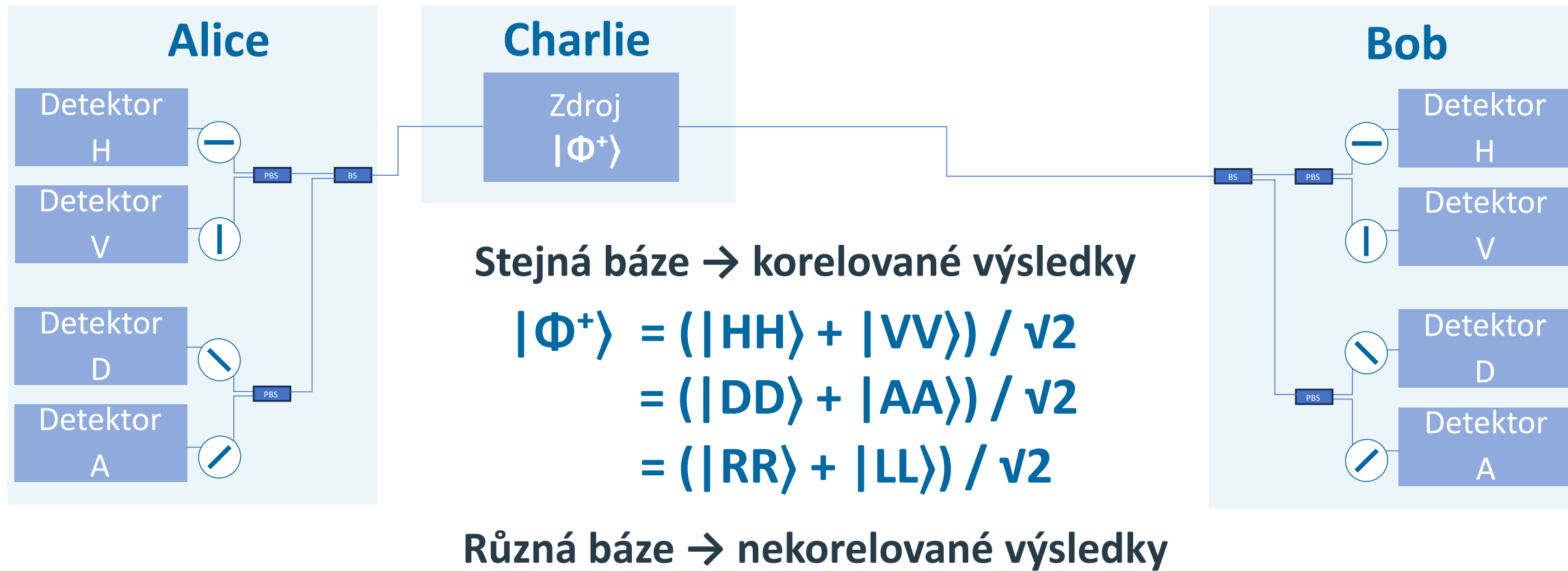


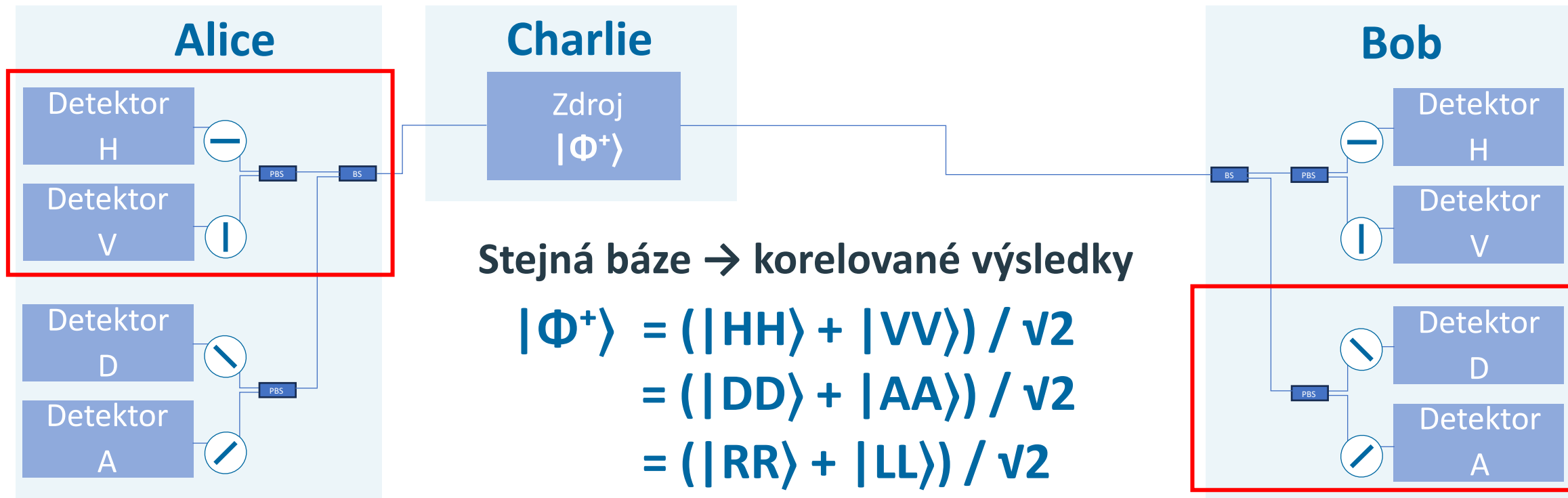










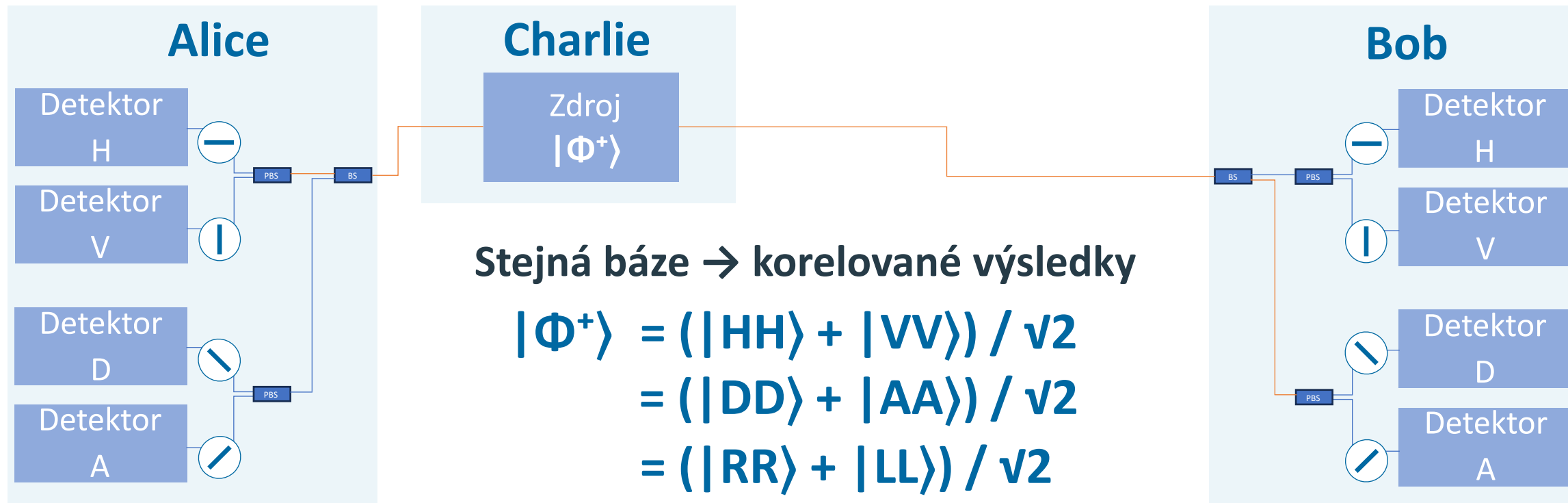


Stejná báze $\rightarrow$ korelované výsledky

$$\begin{aligned}
 |\Phi^+\rangle &= (|HH\rangle + |VV\rangle) / \sqrt{2} \\
 &= (|DD\rangle + |AA\rangle) / \sqrt{2} \\
 &= (|RR\rangle + |LL\rangle) / \sqrt{2}
 \end{aligned}$$

Různá báze $\rightarrow$ nekorelované výsledky

$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$

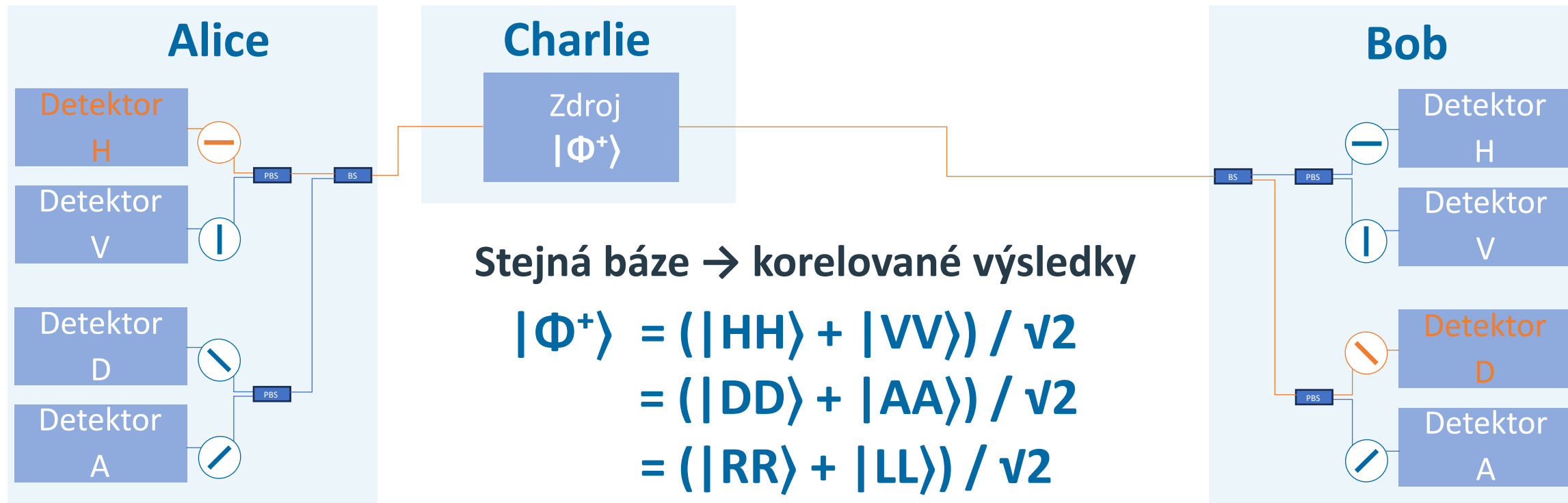


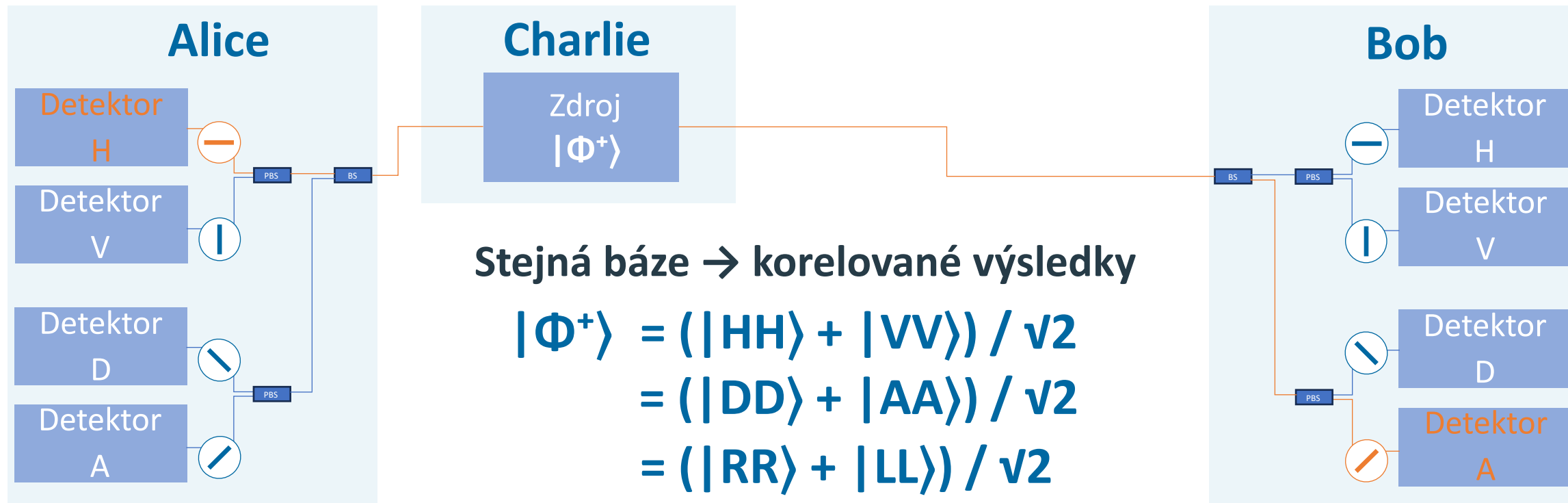
Stejná báze $\rightarrow$ korelované výsledky

$$\begin{aligned} |\Phi^+\rangle &= (|HH\rangle + |VV\rangle) / \sqrt{2} \\ &= (|DD\rangle + |AA\rangle) / \sqrt{2} \\ &= (|RR\rangle + |LL\rangle) / \sqrt{2} \end{aligned}$$

Různá báze $\rightarrow$ nekorelované výsledky

$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$



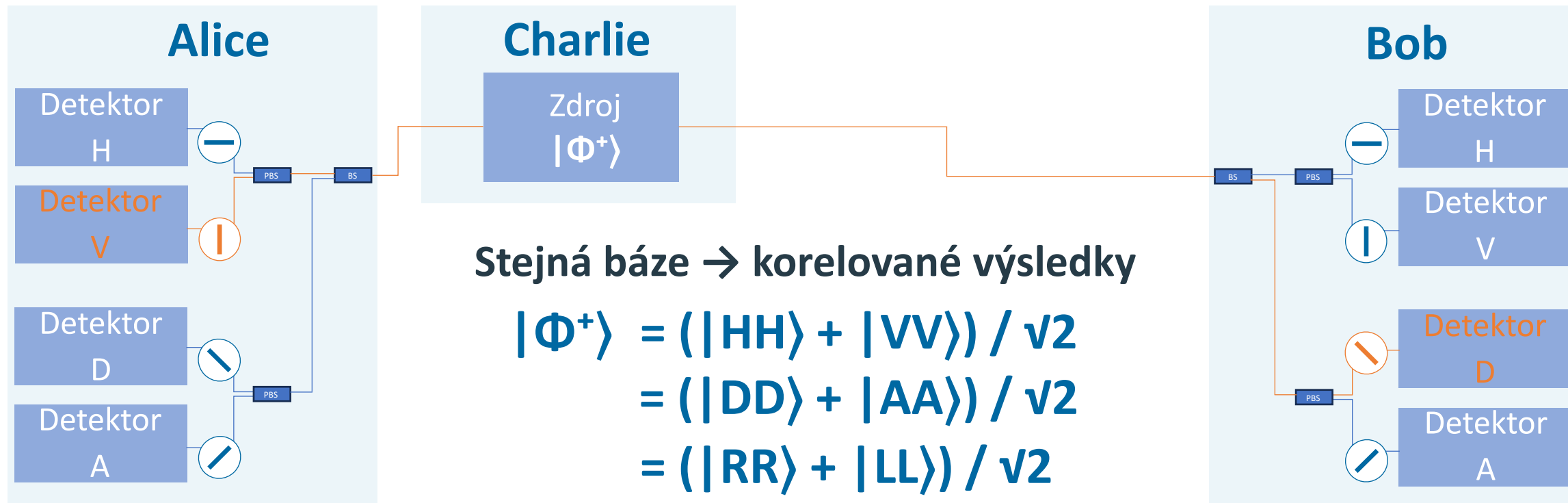


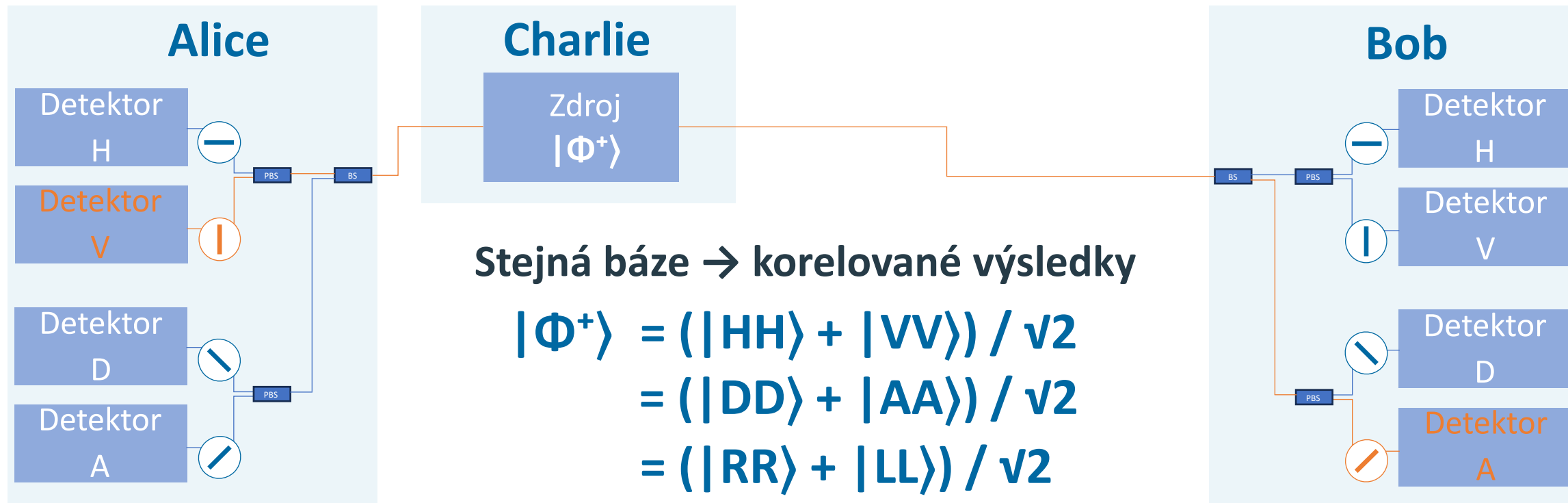
Stejná báze $\rightarrow$ korelované výsledky

$$\begin{aligned}
 |\Phi^+\rangle &= (|HH\rangle + |VV\rangle) / \sqrt{2} \\
 &= (|DD\rangle + |AA\rangle) / \sqrt{2} \\
 &= (|RR\rangle + |LL\rangle) / \sqrt{2}
 \end{aligned}$$

Různá báze $\rightarrow$ nekorelované výsledky

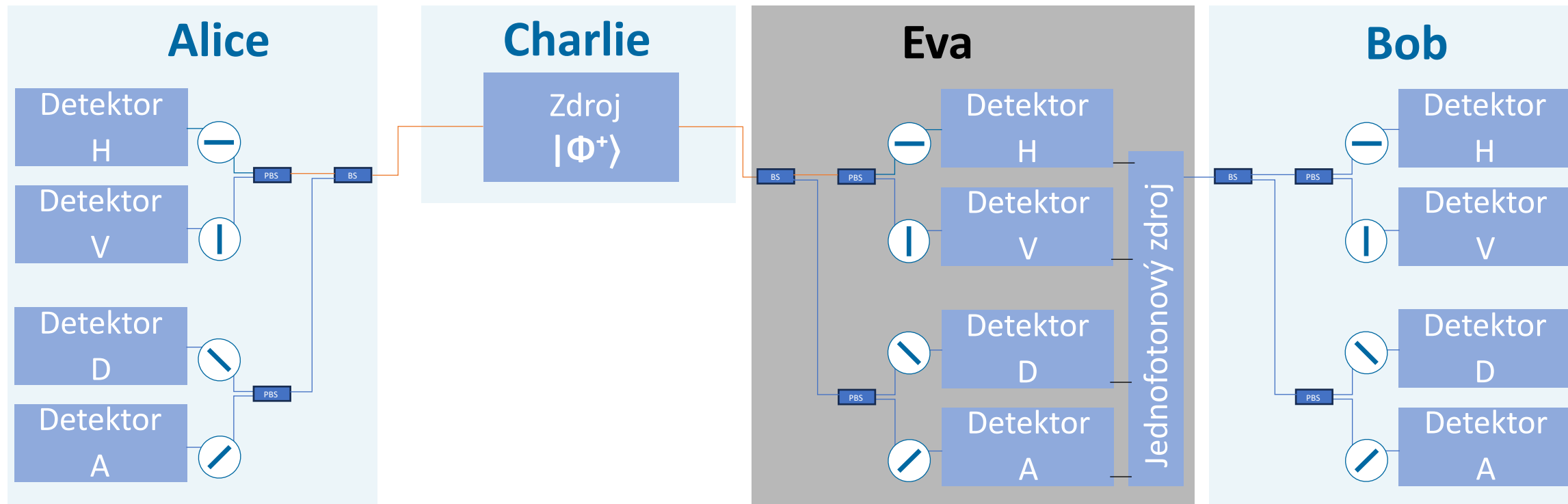
$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$



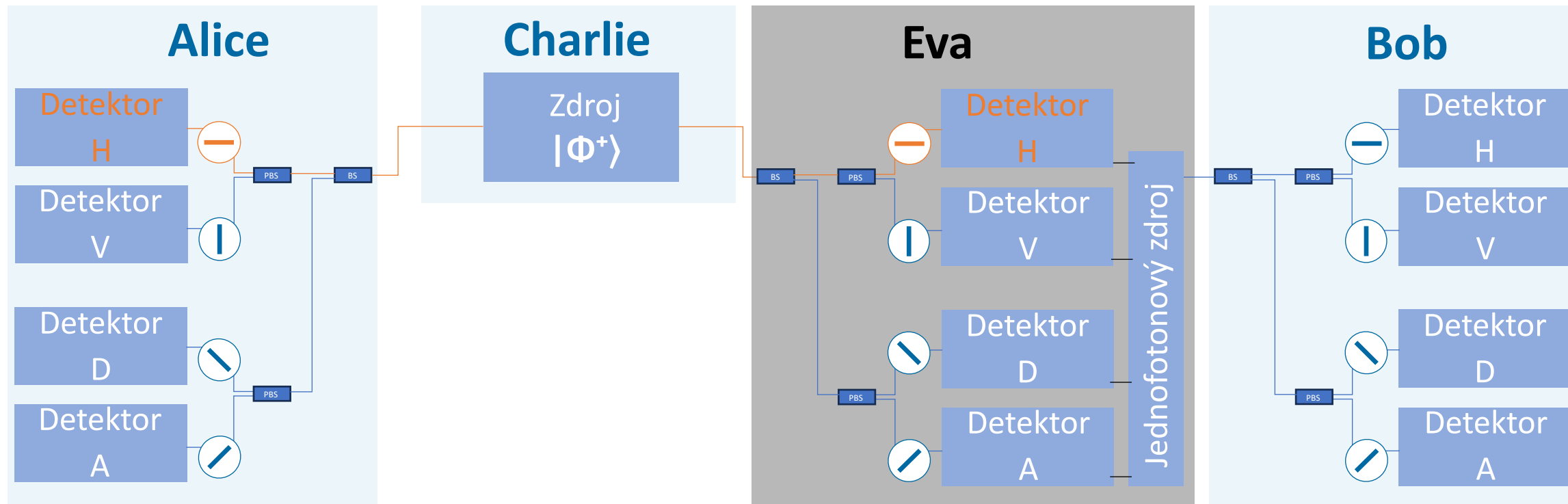


Různá báze $\rightarrow$ nekorelované výsledky

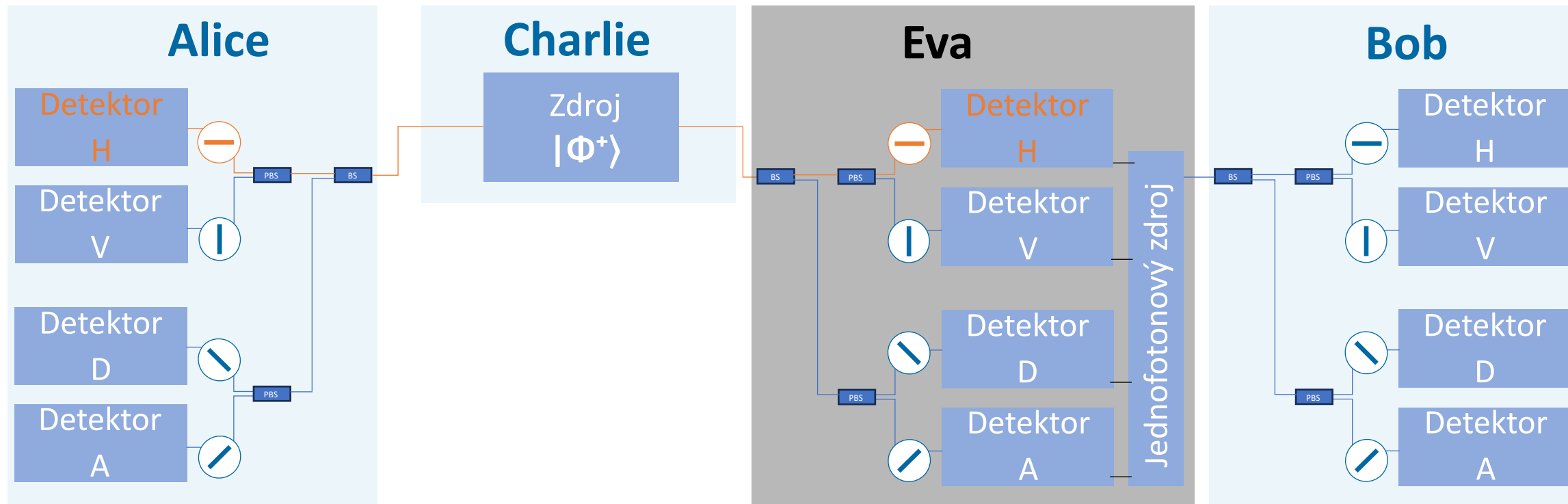
$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$



$$|\Phi^+\rangle = (|HH\rangle + |VV\rangle) / \sqrt{2}$$

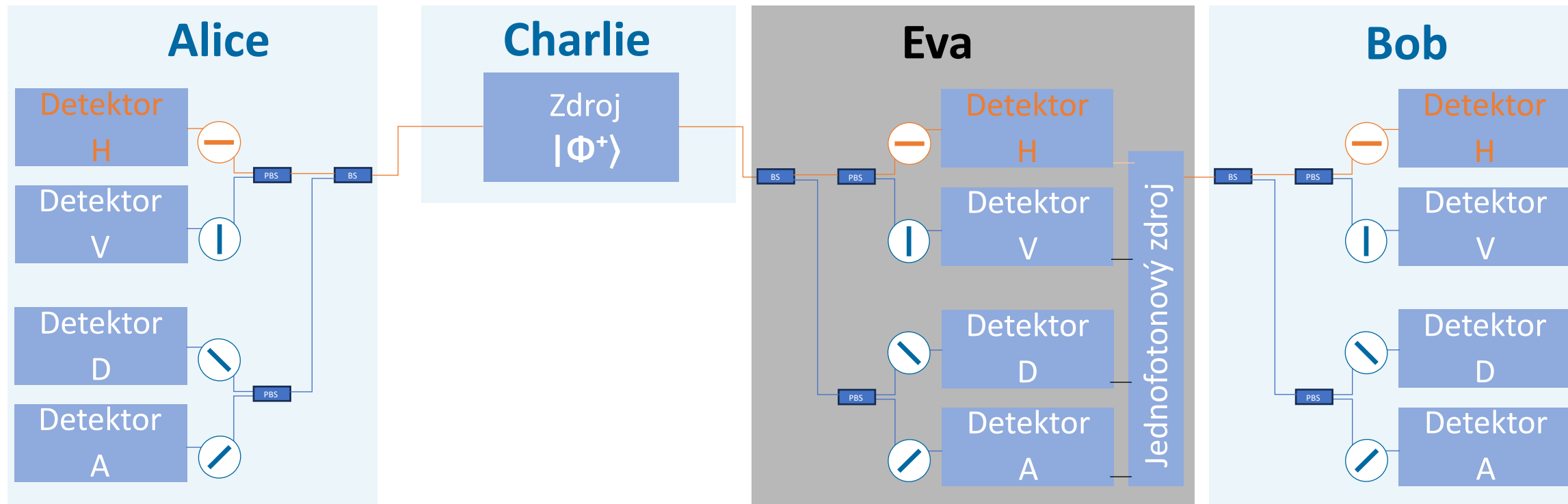


$$|\Phi^+\rangle = (|HH\rangle + |VV\rangle) / \sqrt{2}$$



$$|\Phi^+\rangle = (|HH\rangle + |VV\rangle) / \sqrt{2}$$

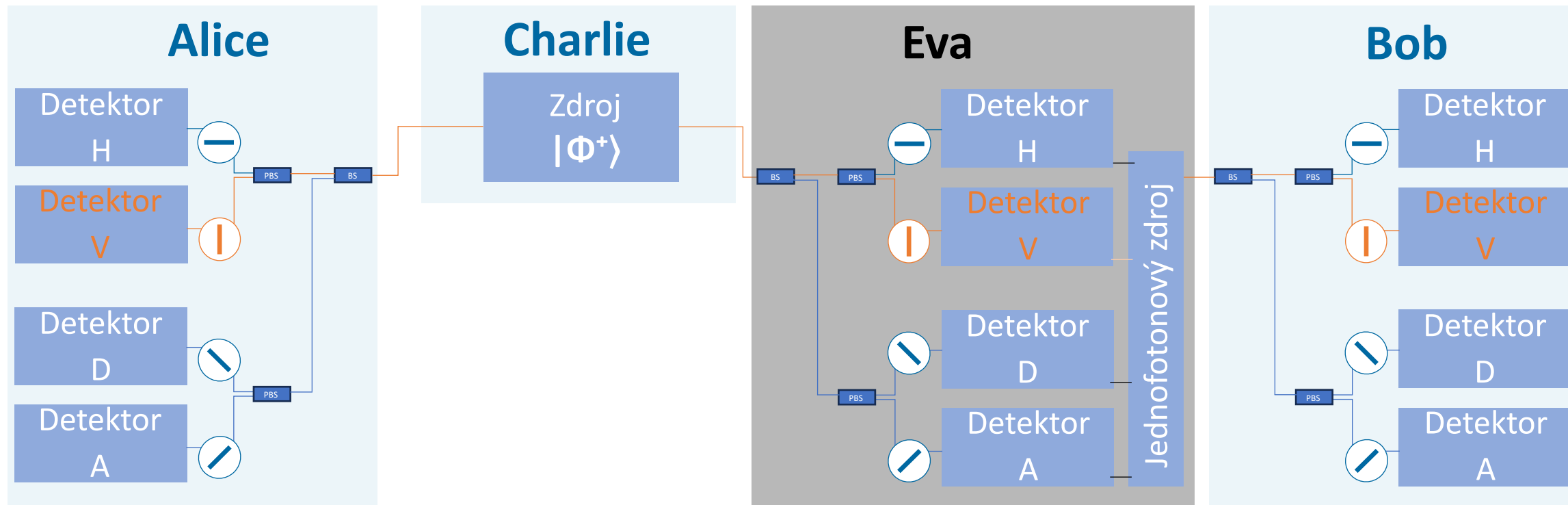
→ Eva vyšle stav $|H\rangle$, proto celkový stav je $|HH\rangle$



$$|\Phi^+\rangle = (|HH\rangle + |VV\rangle) / \sqrt{2}$$

→ Eva vyšle stav $|H\rangle$, proto celkový stav je $|HH\rangle$

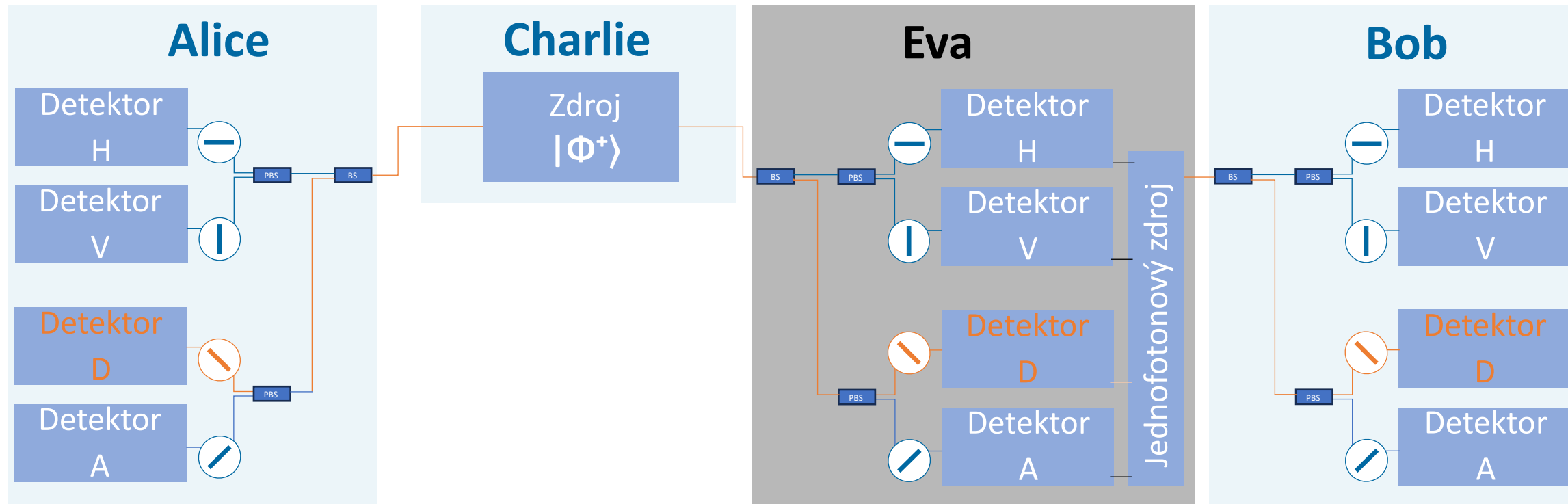
Pokud Eva měřila ve stejné bázi jako Alice a Bob, tak není odhalena



$$|\Phi^+\rangle = (|HH\rangle + |VV\rangle) / \sqrt{2}$$

→ Eva vyšle stav $|V\rangle$, proto celkový stav je $|VV\rangle$

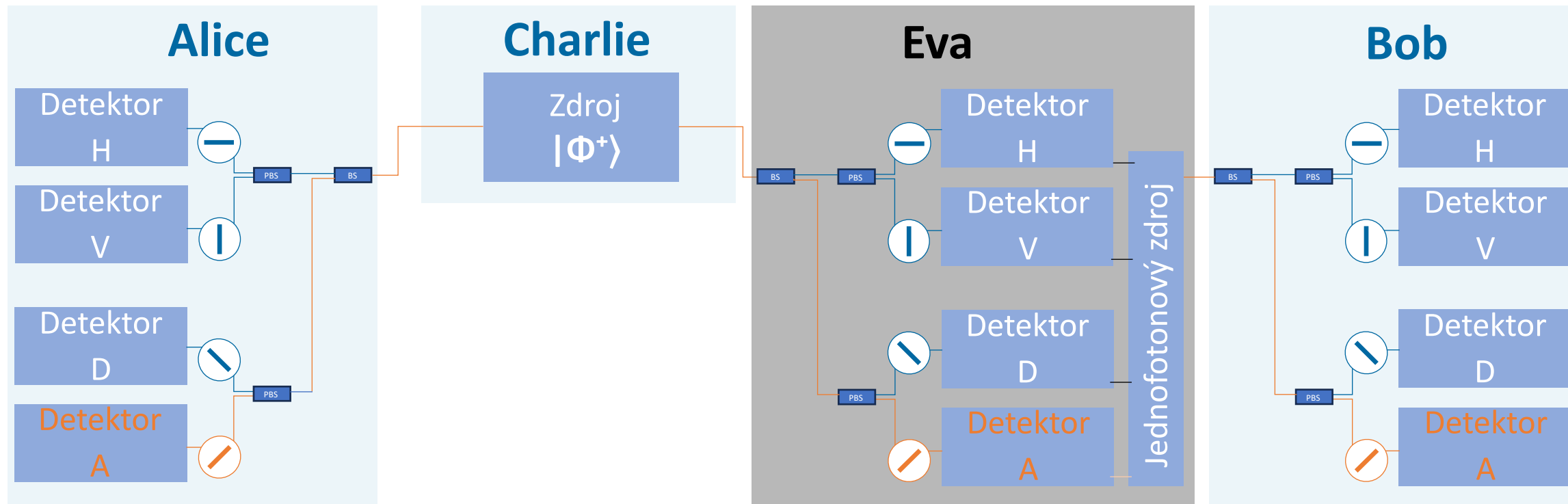
Pokud Eva měřila ve stejné bázi jako Alice a Bob, tak není odhalena



$$|\Phi^+\rangle = (|DD\rangle + |AA\rangle) / \sqrt{2}$$

→ Eva vyšle stav $|D\rangle$, proto celkový stav je $|DD\rangle$

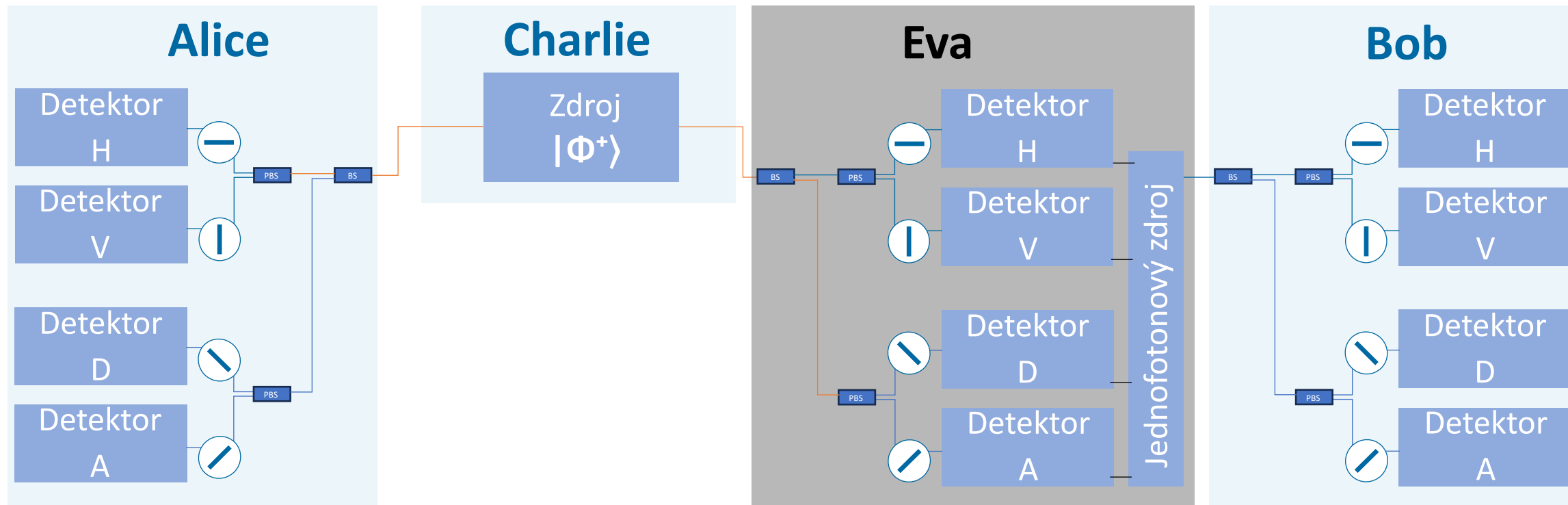
Pokud Eva měřila ve stejné bázi jako Alice a Bob, tak není odhalena



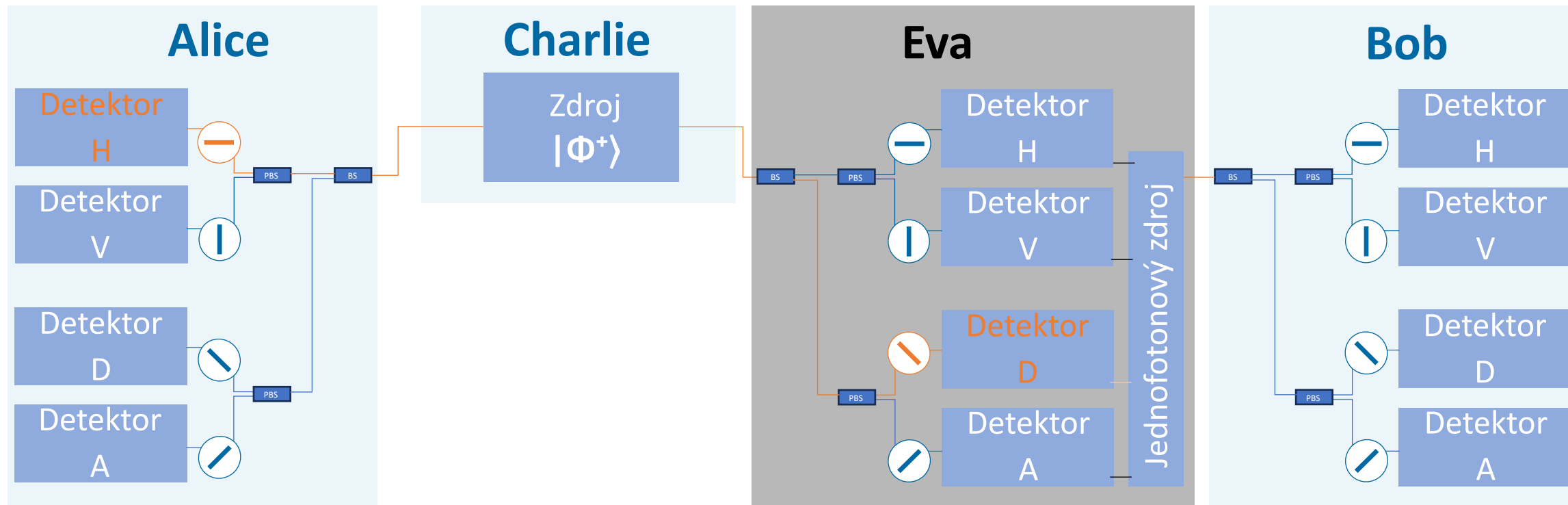
$$|\Phi^+\rangle = (|DD\rangle + |AA\rangle) / \sqrt{2}$$

→ Eva vyšle stav $|A\rangle$, proto celkový stav je $|AA\rangle$

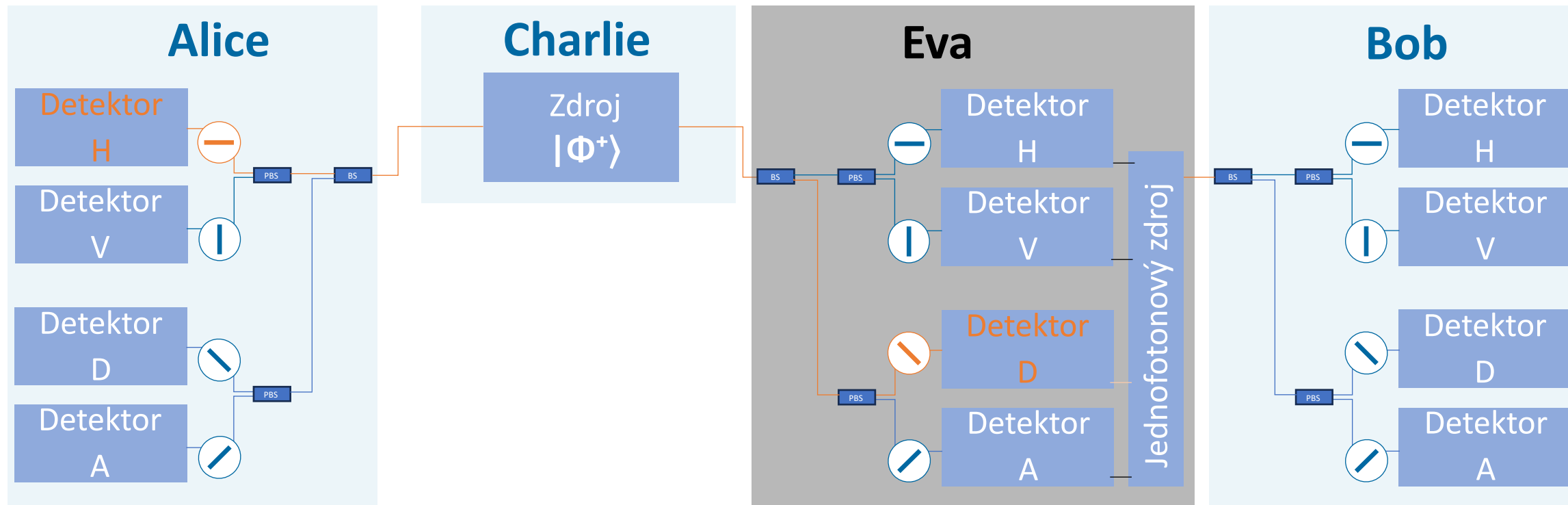
Pokud Eva měřila ve stejné bázi jako Alice a Bob, tak není odhalena



$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$

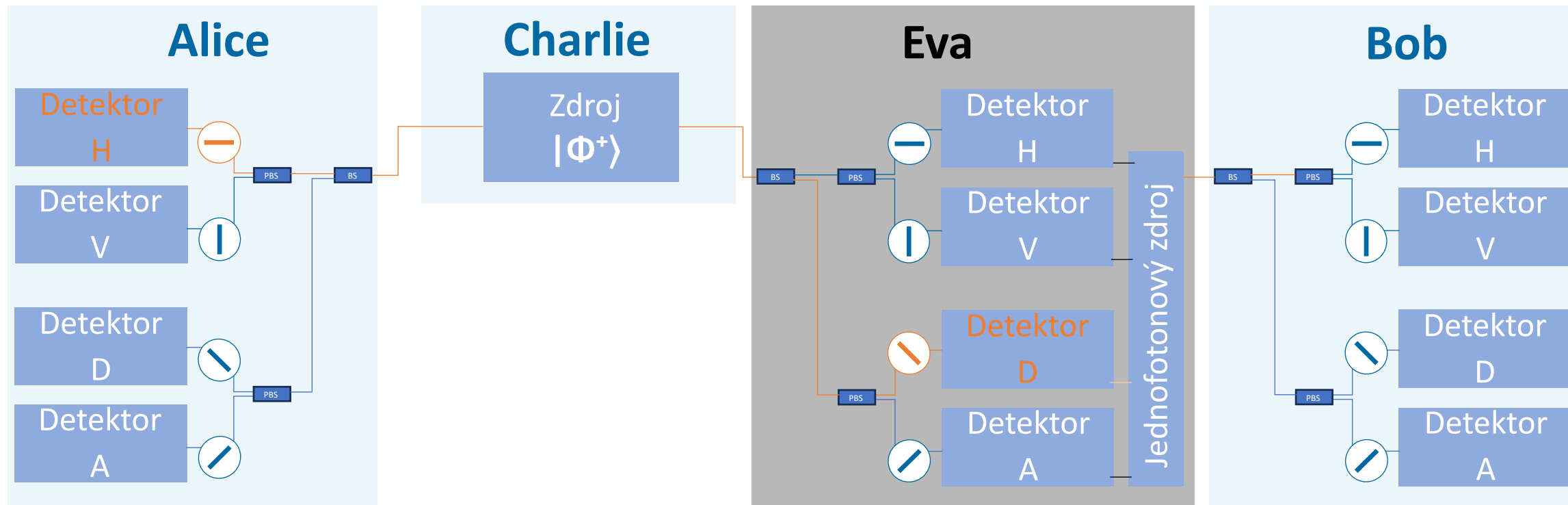


$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$



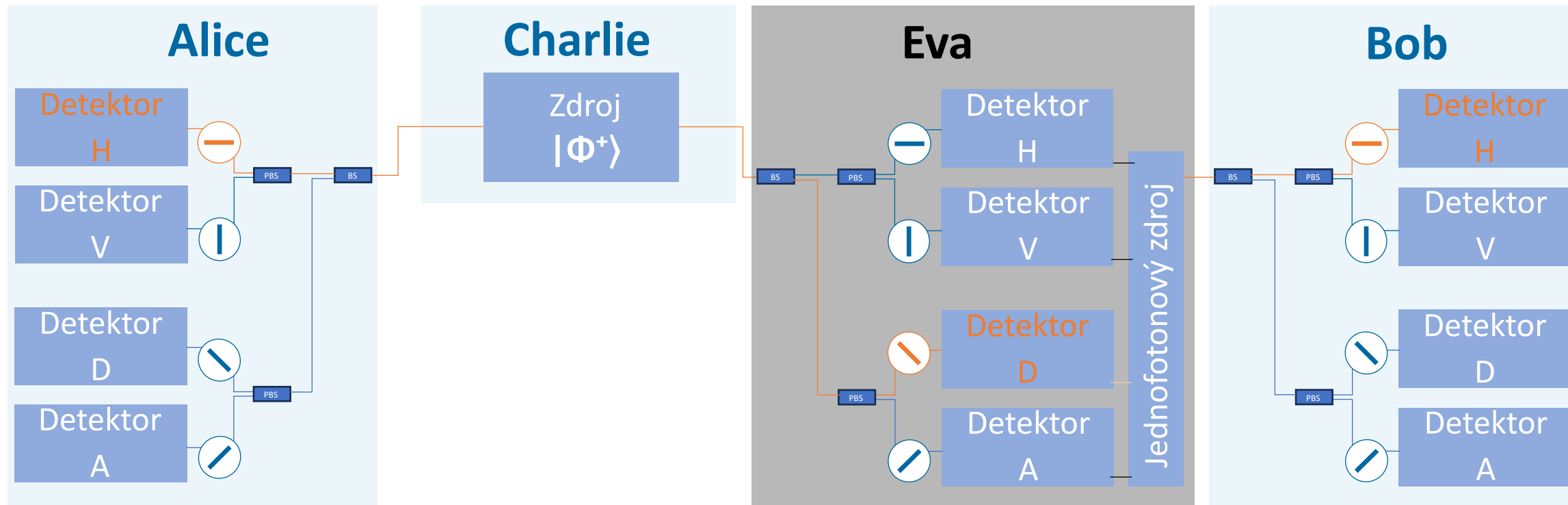
$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$

→ Eva vyšle $|HD\rangle$



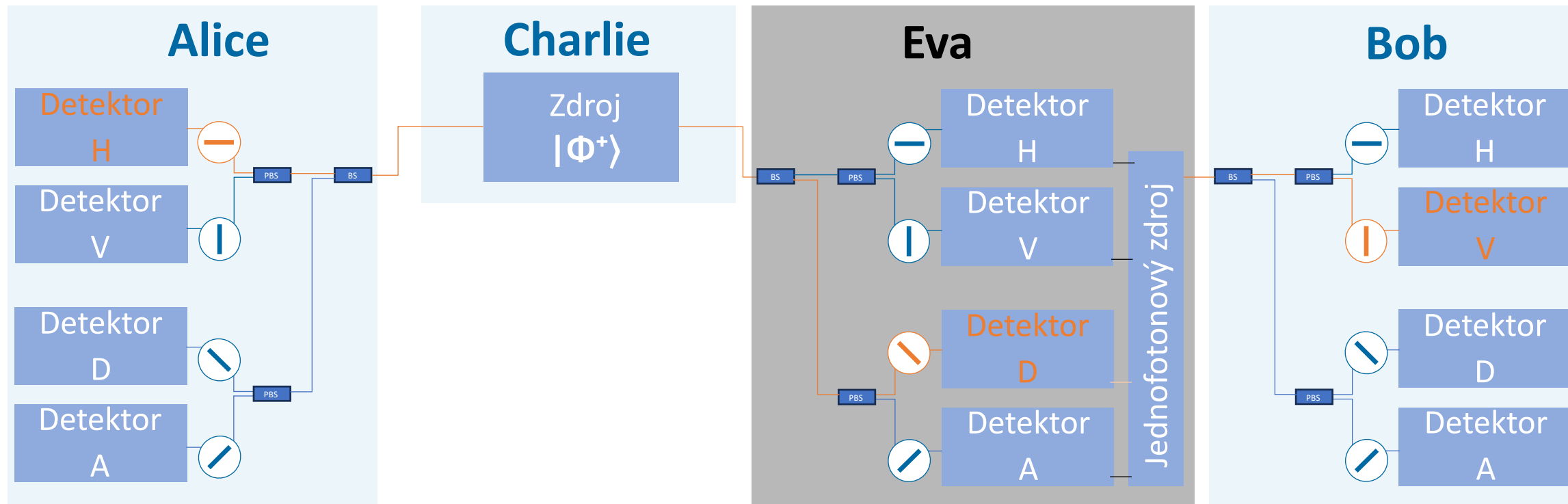
$$|\Phi^+\rangle = (|\text{HD}\rangle + |\text{HA}\rangle + |\text{VD}\rangle - |\text{VA}\rangle) / 2$$

$$\rightarrow \text{Eva vy\AA}le |\text{HD}\rangle = (|\text{HH}\rangle + |\text{HV}\rangle) / \sqrt{2}$$



$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$

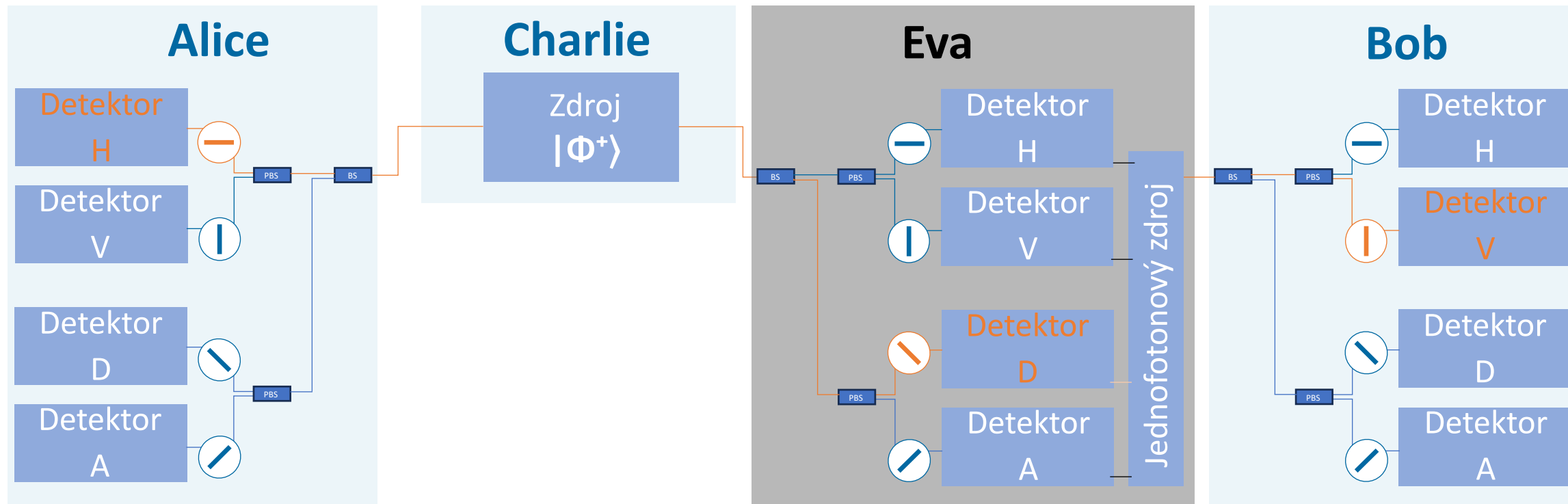
$$\rightarrow \text{Eva vy\text{š}le } |HD\rangle = (|HH\rangle + |HV\rangle) / \sqrt{2}$$



$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$

$$\rightarrow \text{Eva vyšle } |HD\rangle = (|HH\rangle + |HV\rangle) / \sqrt{2}$$

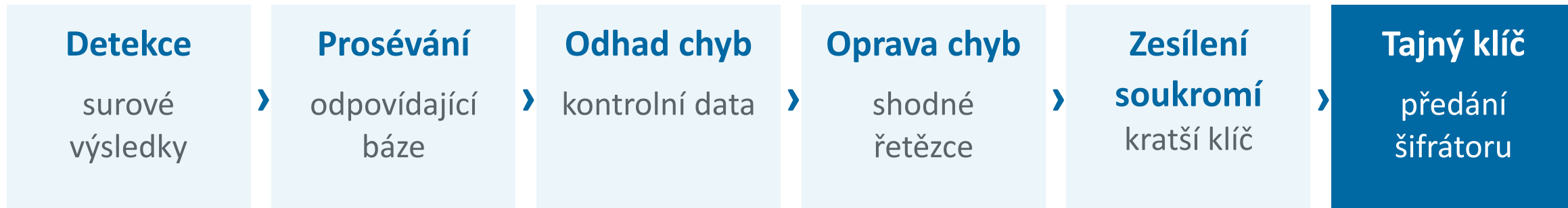
Toto je však korelace, která by se při měření stavu $|\Phi^+\rangle$ neměla realizovat!



$$|\Phi^+\rangle = (|HD\rangle + |HA\rangle + |VD\rangle - |VA\rangle) / 2$$

$$\rightarrow \text{Eva vyšle } |HD\rangle = (|HH\rangle + |HV\rangle) / \sqrt{2}$$

Toto je však korelace, která by se při měření stavu $|\Phi^+\rangle$ neměla realizovat!
Sledování těchto korelací = QBER



QBER

Podíl chybných korelací (bitů)
mezi vyhodnocovanými výsledky.

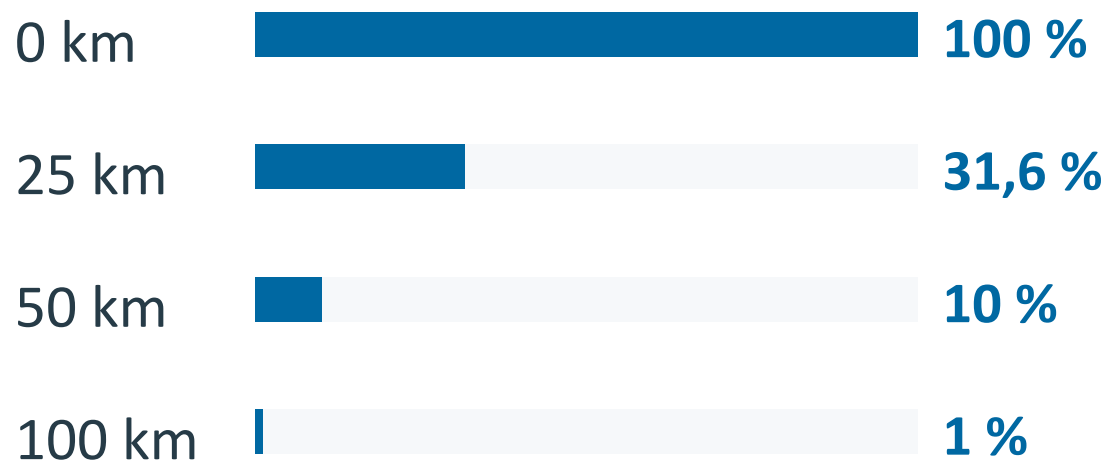
SKR [bit/s]

Rychlost tvorby tajného klíče
po zpracování dat.

Nízký QBER nutně nedokazuje bezpečnost.



Kolik signálu zbývá?



Model: 0,2 dB/km, bez dalších ztrát.

Útlum

Méně zachycených událostí.

Koexistence

Silný datový signál přidává šum.

Drift parametrů linky

Mění se polarizace, fáze i časování.

Cíl CESNETu: začlenit QKD s ostatními službami do optické infrastruktury.



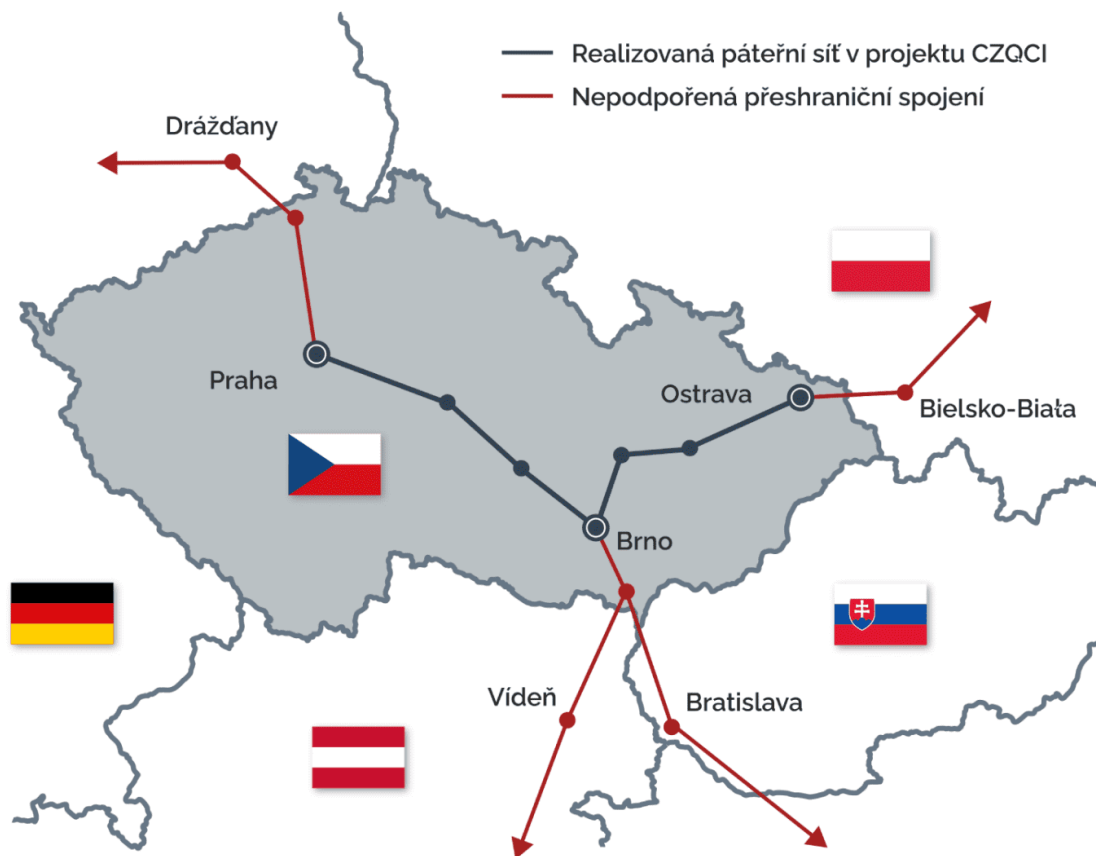
CZQCI	Národní infrastruktura, testování a školení	infrastruktura
NU-CRYPT	QKD + průběžné sledování fyzické trasy	bezpečnost trasy
QUEENTEC	Provázané fotony a koexistence v síti	výzkum
QCI-AT-CZ-PL	Přeshraniční návaznost AT–CZ–PL	navazující projekt
NeSPoQ	QKD + PQC + vysokorychlostní šifrátory	výsledky projektu
SEQRET	CV-QKD pro telekomunikační provoz	výsledky projektu

OPENQKD (2021): dřívější přeshraniční test na infrastruktuře CESNET a PSNC.

Ověřený projektový přehled k září 2026; období a role jsou v záloze.



Páteřní + metropolitní větve, testovací a školicí prostředí



QCI-AT-CZ-PL

Příprava přeshraničního propojení; CESNET v konsorciu.

Ukázka pro UNOB a další uživatele

ÚPT Brno, 15. 12. 2025 • CESNET–ČDT
Šifrovaný přenos i sledování fyzické trasy.



OD KLÍČŮ K ŠIFROVANÝM DATŮM

100 Gb/s

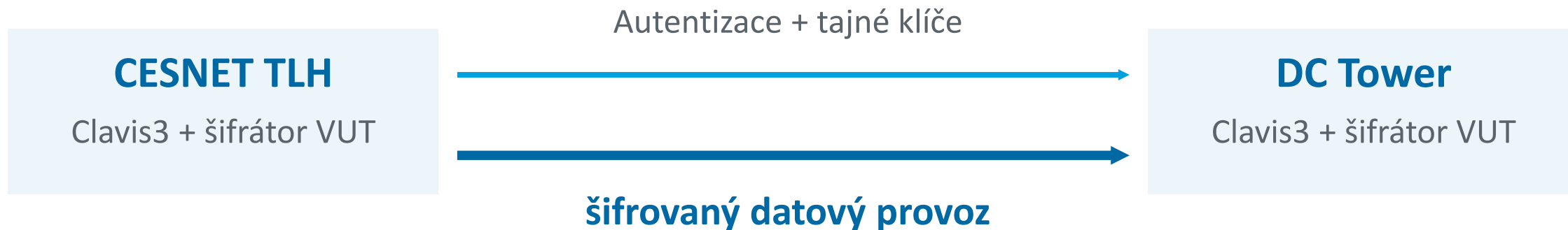
datová linka / šifrátory

9,1 km

CESNET TLH ↔ DC Tower

QKD + PQC

kombinované řešení



Ověřena integrace: QKD systém → šifrátor → běžná síťová aplikace.





UV a FV

37 km

reálná trasa

100 Gb/s

šifrovaný spoj

≈170 kbit/s

Rychlost generování klíčů v tomto zapojení s QKD systémem Toshiba MU

Koherentní snímání + změny polarizace jako doplněk metrik QKD.

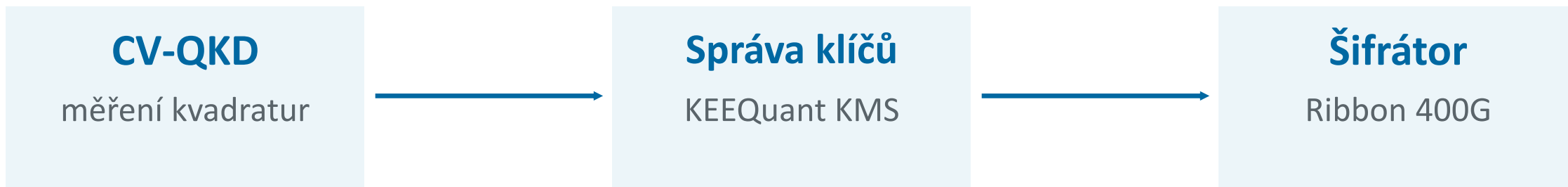
Senzorický přenos monitoruje integritu fyzické trasy



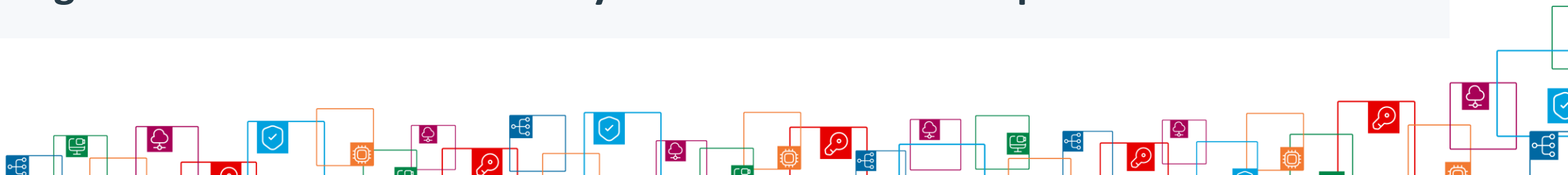
400 Gb/s

datová šifrovací karta Ribbon

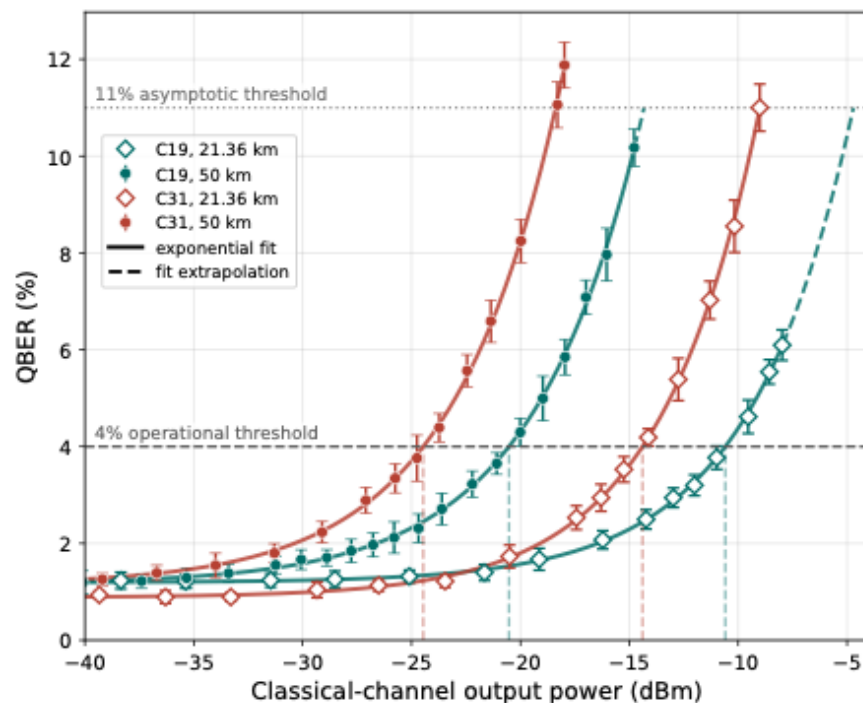
CV-QKD + správa klíčů KEEQuant + optická infrastruktura CESNET



CzechLight Flex ROADM: řízení vlnových kanálů ve sdílené optické síti



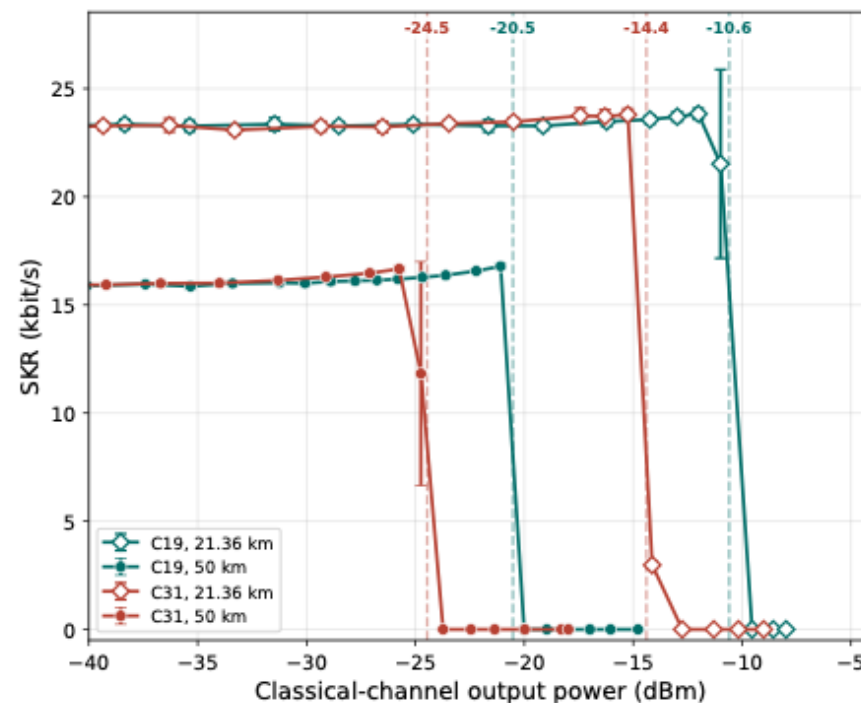
Chybovost QBER



23,83 kbit/s

21,36 km • reálná trasa
klasický kanál -10,6 dBm

Rychlost tajného klíče (SKR)



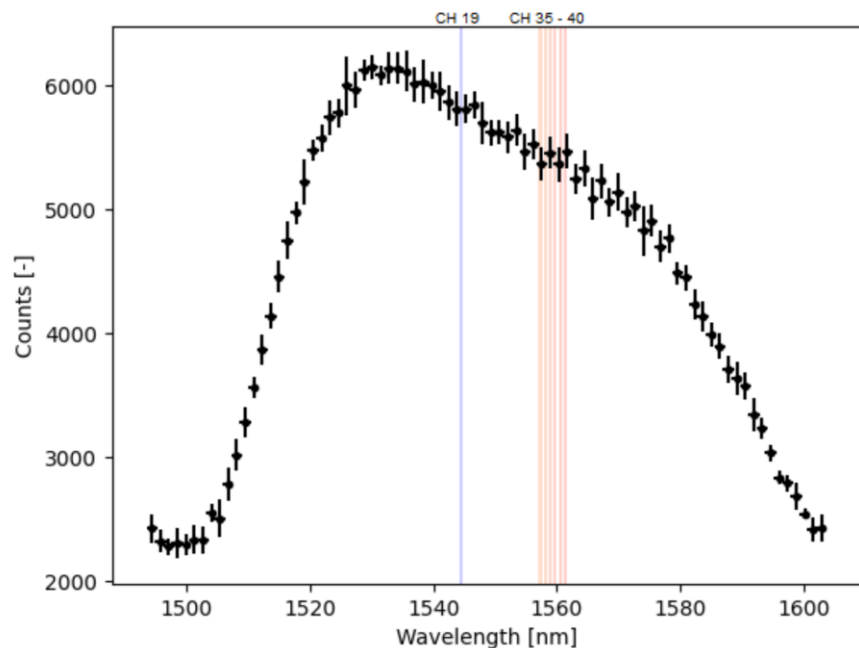
16,79 kbit/s

50 km • vláknová cívka
klasický kanál -20,5 dBm

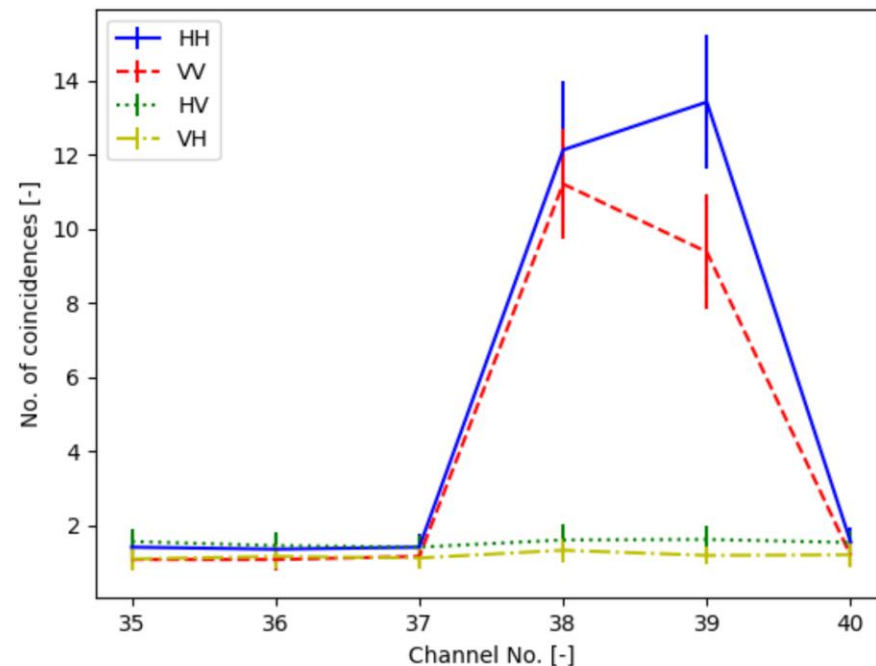
4 % = provozní mez použitého systému, nikoli univerzální limit BBM92.



Spektrum zdroje na DWDM kanály



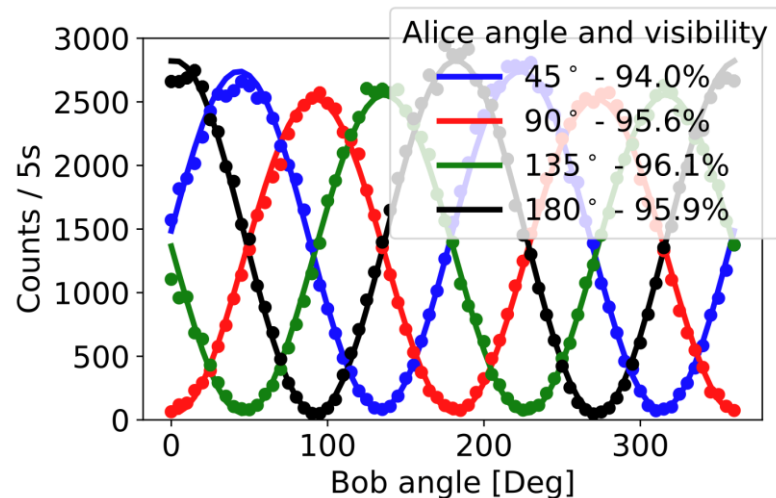
Korelace vybraných kanálů



Laboratorní BBM92: SKR (86 ± 1) bit/s | QBER $(4,8 \pm 0,7)$ %

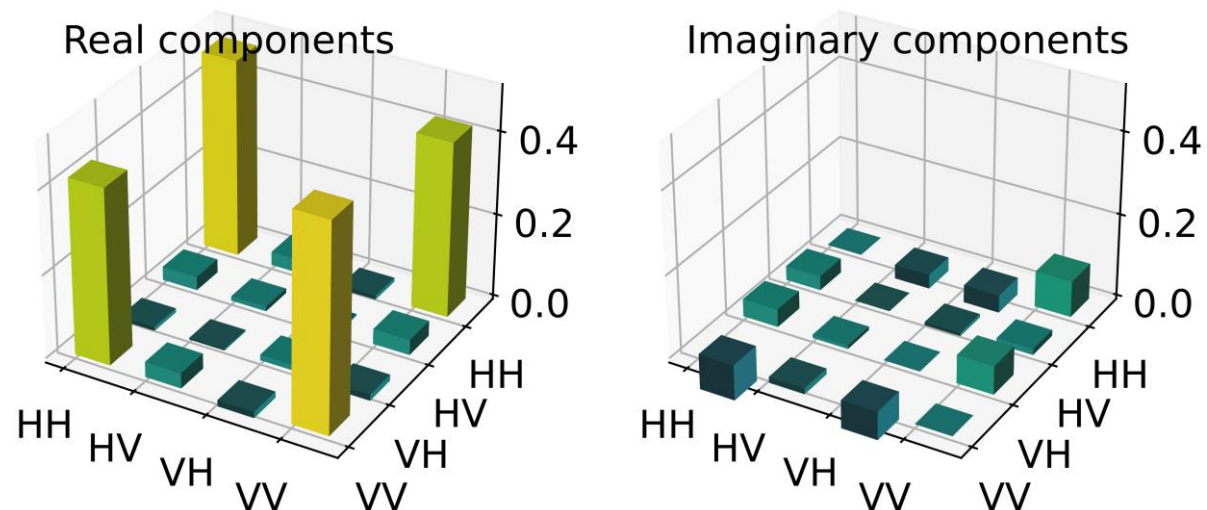


Polarizační korelace



Vizibilita: kontrast koincidenčního signálu.

Kvantová tomografie stavu (QST)

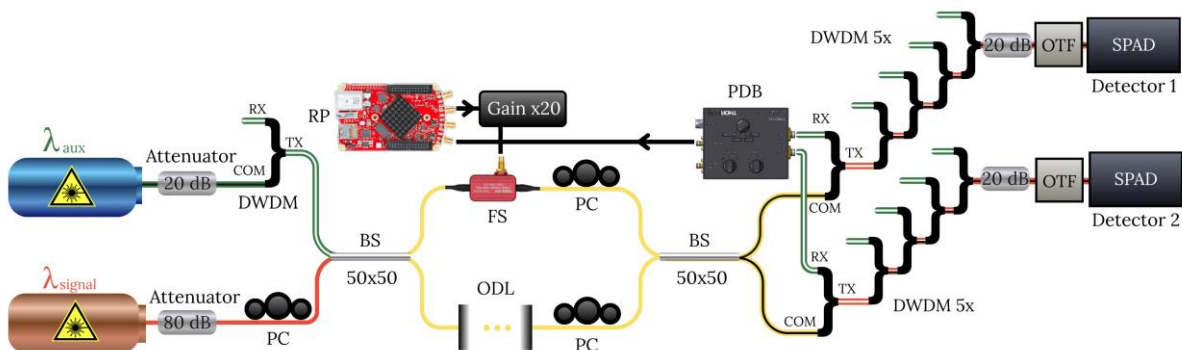


Rekonstrukce matice hustoty ze série polarizačních měření.

Srovnání tří zdrojů v použité měřicí sestavě

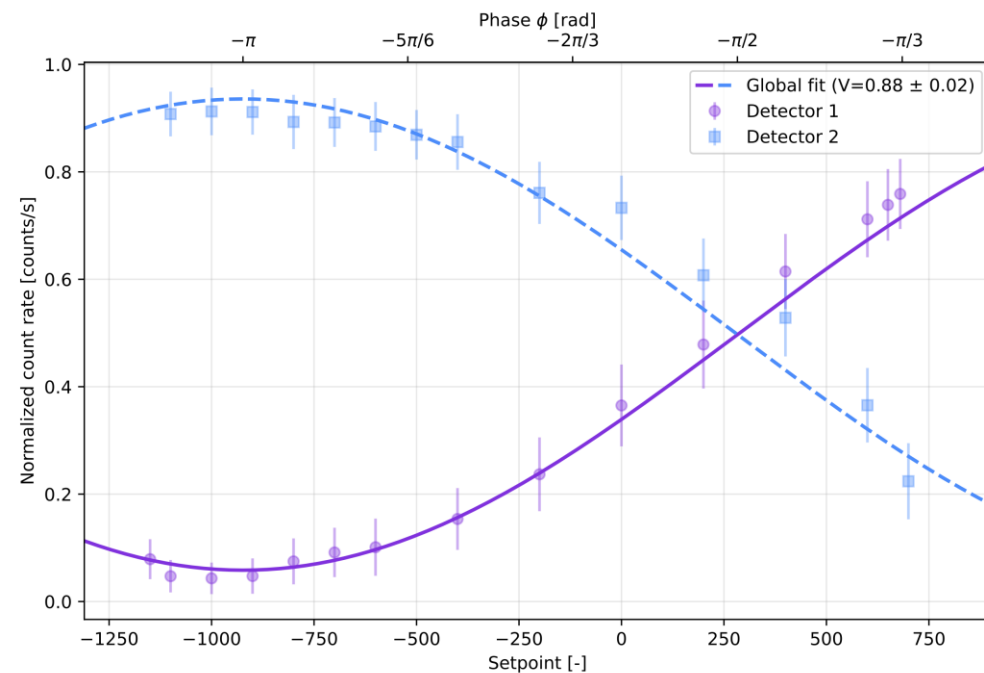
Zdroj (spektrální šířka)	Vizibilita HV	Vizibilita DA	QBER
O-pásmo (100 nm)	96 %	95 %	3 %
C-pásmo (60 nm)	96 %	84 %	5 %
C-pásmo (3 nm)	54 %	73 %	19 %

Diplomová práce O. Galkiny • FJFI ČVUT / CESNET



Pomocný optický kanál

→ FPGA / PID → vláknový stretcher



Viditelnost: 96 % klasicky | 88 % na jednofotonové úrovni

ŽIVÉ MĚŘICÍ DEMONSTRACE

01

QKD

Korelace → QBER
→ model klíčové rychlosti

02

Jednofotonová polarimetrie

Změny ve vlákně
→ časový průběh a spektrum

03

Distribuce přesného času

Časové korelace
→ odhad relativního zpoždění

DALŠÍ APLIKACE · INFORMAČNÍ LISTY U DEMA

04

Distribuované kvantové výpočty

Propojení procesorů
→ společné kvantové operace

05

Kvantová teleportace a prohození provázání

Přenos stavů a spojování
kvantových úseků

06

Certifikovaná kvantová náhodnost

Bellův test (CHSH)
→ certifikace náhodných bitů



■ Klíč, nikoli náhrada celé bezpečnosti

QKD doplňuje šifrování dat, autentizaci a další ochranné mechanismy.

■ Síťová integrace je součást řešení

Koexistence, filtrace, stabilita a propojení se šifrátory.

■ CESNET spojuje provozní zkušenost a výzkum

Reálné trasy, vlastní experimenty, projekty a vzdělávání.



■ Klíč, nikoli náhrada celé bezpečnosti

QKD doplňuje šifrování dat, autentizaci a další ochranné mechanismy.

■ Síťová integrace je součást řešení

Koexistence, filtrace, stabilita a propojení se šifrátory.

Děkuji za pozornost!

■ CESNET spojuje provozní zkušenost a výzkum

Reálné trasy, vlastní experimenty, projekty a vzdělávání.

