



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Název projektu: Mezinárodní centrum pro informaci a neurčitost

Registrační číslo: CZ.1.07/2.3.00/20.0060

Zápis z práce s cílovou skupinou

Název akce: Panelová diskuse A, Prof. Nicolas J. Cerf (Univ. Libre de Bruxelles, Belgie)

Datum: 14. března 2012

Místo konání: katedra optiky, PřF UP Olomouc

Počet účastníků: 4

Program akce: Ve vědecké panelové diskusi se hlavní pozornost věnovala otázce možných aplikací bezšumového kvantového zesilovače a metodám stanovení kapacity kvantových komunikačních kanálů.

Stručný popis práce s cílovou skupinou:

Cílová skupina získala informace v následujících oblastech:

- Jedním z hlavních témat vědecké diskuse byla otázka využití bezšumového kvantového zesilovače pro potlačení ztrát v kvantové kryptografii se spojenými kvantovými proměnnými, což může principiálně zvýšit vzdálenost, na kterou může být tajný klíč generován.
- Vzhledem ke značným technologickým nárokům na experimentální implementaci bezšumového kvantového zesilovače a také z důvodu nízké pravděpodobnosti úspěchu všech stávajících experimentálních realizací tohoto typu zesilovače byla pozornost zaměřena na emulaci bezšumového zesílení pomocí vhodného zpracování experimentálních dat. Bylo diskutováno zejména kryptografické schéma založené na distribuci koherentních stavů a projekci na koherentní stavy na straně příjemce.
- Provedené pilotní numerické výpočty bohužel ukazují, že emulace bezšumového zesilovače je možná pouze za cenu extrémně vysoké filtrace experimentálních dat. Tento postup je pro praktické účely

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Název projektu: Mezinárodní centrum pro informaci a neurčitost

Registrační číslo: CZ.1.07/2.3.00/20.0060

nevhodný, protože neumožňuje získat dostatečné množství dat pro generaci bezpečného tajného šifrovacího klíče. V další diskusi se proto pozornost zaměřila na emulaci bezšumové atenuace, kterou lze provést efektivně pomocí filtrace dat. Bezšumová atenuace může zlepšit distribuci tajného kryptografického klíče skrze šumové zesilující kanály, avšak překvapivě se ukazuje, že v určitých případech může tento postup zlepšit i distribuci klíče skrze ztrátové kanály s přidaným šumem.

- V druhé části panelové diskuse byla pozornost zaměřena na otázku kapacity gaučovských kvantových komunikačních kanálů. Byla diskutována souvislost mezi kapacitou kvantového kanálu, nárůstem entropie při přenosu stavu skrze daný kanál a tzv. majorizací kvantových stavů. Byly prezentovány a diskutovány hypotézy týkající se majorizace kvantových stavů tzv. gaussovskými stavy. Tyto hypotézy jsou v současné době předmětem intenzivního zkoumání ze strany profesora Cerfa a jeho spolupracovníků.

Příloha č. 1 – prezenční listiny