



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, Dr. Frederic Grosshans (ENS Paris-Cachan, Francie)

Datum: 4. října 2011

Místo konání: katedra optiky, PřF UP Olomouc

Počet účastníků: 5

Program akce: Ve vědecké panelové diskusi se hlavní pozornost věnovala současným a budoucím společným projektům mezi Dr. F. Grosshansem, Dr. V.C. Usenkem a doc. R. Filipem. Panelové diskuse se zúčastnili i další pracovníci MCIN.

Stručný popis práce s cílovou skupinou:

Cílová skupina získala informace v následujících oblastech:

- Dr. Grosshans vysvětlil detailně postup získání bezpečného klíče z hrubých korelovaných dat, pozornost se věnovala uplatnění informace o přenosovém kanálu v tomto postupu.
- Následně byly diskutovány podmínky dostatečné estivace přenosového kanálu.
- Dr. Grosshans hovořil o vlivu šumu laseru a modulátoru na kvalitu zdroje a byly diskutovány současné teoretické výsledky v oblasti kvantové kryptografie s mikrovlnnými zdroji navržené prof. T. Ralphem
- Dr. Grosshans zdůraznil omezenou aplikovatelnost Shannonovy informace pro důkazy bezpečnosti pro konečná data, hovořil o lepším využití Renyiho entropie.
- Dále diskuse pokračovala o využití postselekce pro kvantovou distribuci klíče, byly představeny výsledky dosažené pro atmosférickou komunikaci.
- Diskutovala se nestabilita odhadu bezpečnosti v závislosti na počtu naměřených dat.

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

- Dále s diskuse vedla o kryptografii založené na detekci jednotlivých fotonů, především o podmínce na jednofotonové zdroje.
- Dr. Grosshans upozornil na standardně používanou korelaci intenzit jako kritérium pro kvalitu jedno-fotonového zdroje pokud se ke kódování používá polarizace světla.
- Dr. Grosshans informoval o projektu, kde se pokoušeli experimentálně realizovat distribuci klíče s jednotlivými fotony ze zdroje založeného na NV centrech. Projekt byl zastaven pro technické obtíže. Také informoval o teoretickém projektu zkoumajícím podmínky na přípravu jednofotonového stavu, aby nemusel být použit protokol s kvantovou vějíčkou (decoy-state protocol).
- Dále diskuse pokračovala představením dalšího postupu v oblasti detekce ne-Gaussovských stavů a důkazů pro mnohamódové detekci.
- Předmětem diskuse byla také tzv. „omezená provázanost“ a její aplikace v kvantové distribuci klíče. Především byla diskutována nutnost sdílet destilovatelnou kvantovou provázanost pro vytvoření takového stavu.

Příloha č. 1 – prezenční listiny