Kvantová distribuce klíče

Úvod do kryptologie

Zdeněk Kabát

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

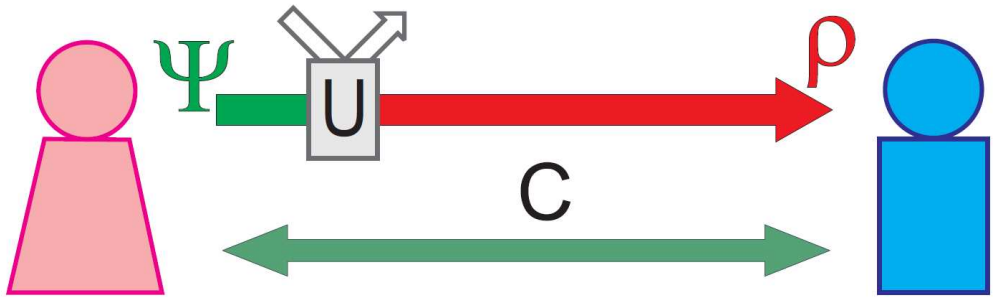
6. května 2010

ÚVOD

Aplikace principů kvantové mechaniky v kryptografii

- Asymetrické šifrování: Shorův kvantový algoritmus pro faktorizaci v polynomiálním čase $\Rightarrow$ nebezpečí pro RSA
- Vernamova šifra (1917): symetrická, nerozluštitelná a optimální (Shannon, 1949) za předpokladů:
  (1) Délka klíče = délka zprávy
  (2) Klíč je dokonale náhodný
  (3) Klíč lze použít jen jednou
- Otázka přenosu klíče $\Rightarrow$ kvantová distribuce klíče (QKD)
- Algoritmus BB84: bezpečný na základně principů QM
- Otázka praktické realizace

ZÁKLADY QKD



- Alice a Bob jsou spojeni 2 kanály:
  - Klasický kanál: autorizovaný, veřejný, jen odposlech
  - Kvantový kanál: libovolná manipulace útočníkem
- Eva – nabourání kvantového a odposlech klasického k.
- Kvantová mechanika: manipulace kvantového kanálu $\Rightarrow$ „degradace“ signálu

Bezpečnost QKD

Bezpečnost založena na principech kvantové fyziky:

- Měření kvantového systému ovlivňuje jeho stav
- *No-cloning theorem*: Nelze vytvořit kopii neznámého kvantového stavu bez ovlivnění původního stavu
- Entanglované páry: Stav jedné částice je určen až po měření na druhé částici

Fyzikální realizace:

- Libovolný kvantový systém zahrnující odpovídající stavy
- Praxe: polarizované fotony + optická vlákna

PROTOKOL BB84

BB84 = Bennett a Brassard, 1984

- Alice: zdroj jednotlivých fotonů – lineární polarizace:
  - Ortogonální stavy v prostoru $\mathscr{H} = \mathbb{C}^2$:

$$|0_+\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |1_+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |0_\times\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |1_\times\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

  - Báze $\mathscr{B}_1 = \{|0_+\rangle, |1_+\rangle\} = +$
  - Báze $\mathscr{B}_2 = \{|0_\times\rangle, |1_\times\rangle\} = \times$,
  - $\{|0_+\rangle, |1_+\rangle\}, \{|0_\times\rangle, |1_\times\rangle\}$ . . . vlastní čísla Pauliho matic

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

- Zpráva je binárně kódována – pro 0 lze vybrat libovolně ze dvou neortogonálních stavů $|0_+\rangle, |0_\times\rangle$, podobně pro 1

Protokol BB84

Dekódování zprávy:

- Při měření v odpovídající bázi je pravděpodobnost správné identifikace qubitu 1
- Při měření v neodpovídající bázi je pravděpodobnost naměření správného i nesprávného qubitu $\frac{1}{2}$ a foton přejde do stavu odpovídajícího výsledku měření
- *Příklad*: Měříme stav $|0_\times\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}$ v bázi $+$, tj. operátorem k této pozorovatelné je Pauliho matice $\sigma_3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \Rightarrow$
  - naměření stavu $|0_+\rangle \ldots P = |\langle 0_+|0_\times\rangle|^2 = \frac{1}{2}$,
  - naměření stavu $|1_+\rangle \ldots P = |\langle 1_+|0_\times\rangle|^2 = \frac{1}{2}$.
- Se stejnou pravd. přejde stav $|0_\times\rangle$ do stavu $|0_+\rangle$ nebo $|1_+\rangle$.

Protokol BB84

Postup v protokolu BB84:

1. Alice zakóduje binárně klíč délky N: pro každý qubit volí polarizaci fotonu v jedné z bází $+$ nebo $\times$. Bob měří jednotlivé fotony *náhodně* v bázi $+$ nebo $\times$.
2. Alice pošle veřejným kanálem báze, ve kterých kódovala qubity a Bob je porovná se svými. Qubity měřené v neodpovídajících bazích se zahodí, zůstane $\sim \frac{N}{2}$ bitů.
3. Alice a Bob obětují určitý počet bitů a porovnají je veřejným kanálem. Pokud se bity shodují, pravděpodobnost odposlechu je velmi nízká a zbylé bity se použijí jako klíč pro Vernamovu šifru.

Útoky na protokol BB84

Útok typu *intercept-resend*

- Eva naruší kvantový kanál, měří polarizaci přijatých qubitů a „zkopíruje“ stav = výsledek svého měření pošle Bobovi
- Eva musí náhodně vybírat bázi:
  - Vybere-li správnou bázi – měřením neovlivní stav fotonu
  - Vybere-li nesprávnou bázi – foton po měření přejde do jiného stavu ($P = \frac{1}{2}$) v druhé bázi $\Rightarrow$ i když poté Bob měří v bázi, v níž byl foton Alicí připraven, dostane s pravd. $\frac{1}{2}$ špatný výsledek
- Měří-li Bob ve správné bázi (jako byl foton poslán), pravděpodobnost nesprávného výsledku je $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$
- Při porovnání k qubitů je pravděpodobnost nezachycení odposlechu $1 - \left(\frac{3}{4}\right)^k \longrightarrow 0$

ÚTOKY NA PROTOKOL BB84

Příklad útoku intercept-resend

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

Útoky na protokol BB84

Útok *photon number splitting* (PNS)

- Praxe: laserové pulsy s počtem fotonů podle Poissonova rozdělení
  - Průměr např. 0,2 fotonu na puls
  - Některé pulsy obsahují 2 fotony
- Eva může dvoufotonové pulsy rozdělit – jeden uložit do kvantové paměti a druhý přeposlat Bobovi
- Po zveřejnění bází klasickým kanálem Eva dekóduje část klíče bez prozrazení odposlechu
- I přes útok PNS lze generovat bezpečný klíč (Gottesman, 2004) – větší nároky na přenos

Implementace

- Společnosti: id Quantique, MagiQ Technologies, SmartQuantum, Quintessence Labs (komerční produkty), Toshiba, HP, IBM, Mitsubishi, NEC, NTT (vývoj)
- První použití: 2004 – starosta Vídně $\rightarrow$ Rakouská banka
- Nejrychlejší přenos: 1 Mbit/s na vzdálenost 20 km, 10 kbit/s na 100 km
- Největší vzdálenost: 148,7 km (optická vlákna), 144 km (vzduch)
- Kvantová počítačová síť: SECOQC Vídeň 10/2008, 200 km optických vláken, 6 míst po Vídni + město St Poelten 69 km od Vídně

Děkuji za pozornost!