Pokročilá kryptologie

Kvantová kryptografie 1

prof. Ing. Róbert Lórencz, CSc., Ing. Tomáš Rosa, Ph.D.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra počítačových systémů

Příprava studijních programů Informatika pro novou fakultu ČVUT je spolufinancována Evropským sociálním fondem a rozpočtem Hlavního města Prahy v rámci Operačního programu Praha — adaptabilita (OPPA) projektem CZ.2.17/3.1.00/31952 – „Příprava a zavedení nových studijních programů Informatika na ČVUT v Praze“.
Praha & EU: Investujeme do vaší budoucnosti

Tato přednáška byla rovněž podpořena z prostředků projektu č. 347/2013/B1a Fondu rozvoje vysokých škol Ministerstva školství, mládeže a tělovýchovy

Obsah přednášky

- Vlastnosti informace
- Kvantový bit - qubit
- Základní charakteristika kvantové kryptografie
- Protokol BB84
- Kvantový registr
- Fenomény kvantového počítání
- Algoritmy pro kvantové počítače
- Kvantová kryptologie

Klasické a kvantové pojetí informace

- Klasická informace
  - Lze libovolně kopírovat. Zejména je možné vytvořit zcela identickou kopii dané zprávy.
- Kvantová informace
  - Nelze vytvořit identickou kopii neznámého kvantového stavu.
    - ★ Vychází z Heisenbergova principu neurčitosti [1].
    - ★ Čtení zprávy zároveň ovlivňuje její obsah.

[1] Heisenbergův princip neurčitosti je matematická vlastnost dvou kanonicky konjugovaných veličin. Nejznámějšími veličinami tohoto typu jsou *poloha* a *hybnost* elementární částice v kvantové fyzice.

$$\triangle x \triangle p \geq \frac{\hbar}{2},$$

kde $\hbar$ je tzv. redukovaná Planckova konstanta.
Čím přesněji určíme jednu z konjugovaných veličin, tím méně přesně můžeme určit tu druhou, a to bez ohledu na kvalitu přístrojů.
Tvrzeni z klasické fyziky: můžeme předpovědět chování systému, pokud známe jeho počáteční stav.
Pro kvantovou fyziku neplati: počáteční stav systému nikdy nemůžeme zjistit dostatečně přesně $\Leftarrow$ nelze dostatečně přesně zjistit oba tyto konjugované veliciny najednou.

Klasická a kvantová kryptografie

- Klasická kryptografie
  - Musí se vyrovnat s možností neomezeného kopírování nosičů klasické informace.
    - ★ Použití klíčů o extrémních délkách – princip one-time pad.
    - ★ Spoléhání na výpočetní složitost.
- Kvantová kryptografie
  - Zakládá na nemožnosti tvorby identických kopií neznámého kvantového stavu.
    - ★ Nejprve se přenese klíč, který se při pozitivní detekci odposlechu zruší.

Kryptografické inženýrství – zrod nového kryptosystému

- Musíme najít správný problém
  - Vyjádření jeho nezvládnutelnosti
    - ★ Principiální logická nemožnost - Vernamova šifra
    - ★ Výpočetní složitost, atp. - asymetrické metody
    - ★ Fyzikální (nikoliv technologická!) omezení - kvantová kryptografie
  - Způsob zadání, ošetření slabých (snadno řešitelných) instancí

- Musíme najít správnou redukci
  - Podle typu schématu: šifra, podpis, autentizace, atp.
  - Jak převést úlohu luštění na úlohu řešení vybraného problému?
  - Navíc, problém musí být možné i speciálně řešit/obejít
    - ★ Při znalosti nějaké informace (tajný klíč) – šifry, podpisy, atp.
    - ★ Při speciálním postupu výpočtu (v cestě jednosměrnosti) – hašovací funkce

Kvantová kryptografie - hlavní rysy

- Nepodmíněná bezpečnost
  - V teoretické rovině lze dokázat bezpečnost systému bez ohledu na prostředky útočníka.
  - V teoretické rovině lze dosáhnout i absolutní bezpečnosti.
  - Předpokládá se, že bezpečnost těchto systémů nebude dotčena ani ve věku kvantových počítačů.
- Hlavní pozornost je zatím věnována přenosu zpráv.
  - S uchováváním kvantově šifrované informace jsou spojeny jisté technologické potíže.
- Některé druhy schémat nejsou dostatečně propracovány.
  - Kvantová schémata digitálního podpisu.

Nepodmíněná bezpečnost...

- Dosud chápána převážně s ohledem na výpočetní sílu protivníka.
  - Nutnost lepšího precizování a objektivního zobecnění.
- I „nereálné“ podmínky jsou nakonec logické podmínky a musíme je znát.

Logické podmínky zůstávají...

- Časté „převlékání“ podmínek
- O výpočetní sílu se nezajímáme, ale tvrdíme, že:
  - útočník má zarušený příjem signálu
  - útočník nemá dostatek rychlé paměti
  - nedokáže ovlivnit plošné rádiové vysílání
  - ....
  - pro útočníka platí kvantová mechanika?

Nepodmíněná bezpečnost - pokračování

Jde o kvalitativní rozdíly

- Zajímáme se o význam čistě logických podmínek (omezení) v reálném světě.
- Rozlišujeme:
  1. podmínky technické (luštění DES) dnes se mi to nechce dělat, nemám chuť/peníze...
  2. podmínky technologické (luštění RSA)dnes nevím, jak to mám zvládnout, ale snad někdy...
  3. podmínky fyzikální (luštění kvantových metod) podle všeho to nikdy udělat nedokážu... (nejsem-li mimozemšťan...)

Kvantový bit - qubit

- Za fyzikální obraz qubitu považujeme libovolný kvantově mechanicky popsaný objekt, jehož stavy jsou prvky dvourozměrného Hilbertova prostoru.
  - Foton (polarizace, fázový posun)
  - Elektron (spin)
  - Atom (spin)
- Formálně:
  - Odpovídajícího naměřené hodnotě (kolaps kvantového systému), $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, kde:
    - $\omega_0, \omega_1 \in C, |0\rangle, |1\rangle$ jsou bázové vektory H_2
    - $|0\rangle, |1\rangle$ nazýváme vlastní stavy qubitu.
  - Měřením qubitu získáme hodnotu odpovídající právě 1 vlastnímu stavu.
  - Superpozici nelze „vidět“.
    - Koeficienty ω_0, ω_1 určují rozdělení výsledků měření.
    - P[MĚŘENÍ= $|\alpha\rangle$] $= |\omega_\alpha|^2, \alpha \in \{0, 1\}$
    - Měřením superpozice zaniká a qubit přechází do vlastního stavu.
- Měřením jednoho qubitu získáme nejvýše 1 bit klasické informace.

Polarizační kódování

- Lineární (”+”)
  - $|0\rangle_{(r)} =$ ”|”
  - $|1\rangle_{(r)} =$ ”−”
  - $|\psi\rangle = \omega_{(r),0}|0\rangle_{(r)} + \omega_{(r),1}|1\rangle_{(r)}$
- Diagonální (”×”)
  - $|0\rangle_{(d)} =$ ”$\diagdown$”
  - $|1\rangle_{(d)} =$ ”$\diagup$”
  - $|\psi\rangle = \omega_{(d),0}|0\rangle_{(d)} + \omega_{(d),1}|1\rangle_{(d)}$

Využití v kryptografii

- *Heisenbergův princip neurčitosti*: nelze současně přesně určit stav daného qubitu vzhledem k lineární a diagonální bázi.
  - Při vhodně zvolené diagonální bázi lze pro ilustraci přímo napsat:
    - ⋆ $|0\rangle_{(r)} = \sqrt{\frac{1}{2}}\,(|0\rangle_{(d)} + |1\rangle_{(d)})$
    - ⋆ $|1\rangle_{(r)} = \sqrt{\frac{1}{2}}\,(|0\rangle_{(d)} - |1\rangle_{(d)})$
  - Interpretace: Čím určitější je stav vzhledem k lineární bázi, tím méně určitý je vzhledem k diagonální bázi a naopak.

Protokol BB84 - Benett-Brassard 1984

Absolutně bezpečné kryptosystémy

- Existuji perfektní kryptossytémy.
- Například **One-Time Pad (OTP)**
- Zůstává ale problém bezpečné distribuce klíčů.

Řešení:

- Distribuce klíče (zřízení společného klíče) na základě kvantového jevu zaručujícího perfektní utajení.
- Protokol BB84 slouží k dohodě na symetrickém klíči využívající kvantových jevů..
  - Ten je následně použit pro systém one-time pad.
- Založen na využití Heisenbergova principu neurčitosti ve spojení s polarizačním kódováním.
- S mírnými obměnami je BB84 používán a rozvíjen dodnes.

Protokol BB84 - příklad průběhu komunikace

1. Odesílatel (Alice): Generuje náhodnou binární posloupnost a provádí její polarizační kódování dle náhodně volené báze.

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
X	+	X	X	X	X	X	+	X	X	+	+	+	+	X	X	+	+	X	+	+	X	X	+	+
/	-	/	/	/	\	\	-	\	/	|	|	|	|	/	\	|	|	\	-	|	\	\	|	|

2. Příjemce (Bob): Dekóduje přijaté fotony dle náhodně volené báze.

/	-	/	/	/	\	\	-	\	/	|	|	|	|	/	\	|	|	\	-	|	\	\	|	|
+	+	X	+	X	X	+	X	+	X	+	+	X	X	+	X	X	+	X	+	X	+	+	+	X
0	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1

3. Odesílatel (Alice): Oznámí Bobovi (veřejně, ovšem s autentizací původu zprávy), jakou bázi v daném kroku použila. To samé učiní Bob. Bity, kde se oba shodli, budou použity pro symetrický klíč.

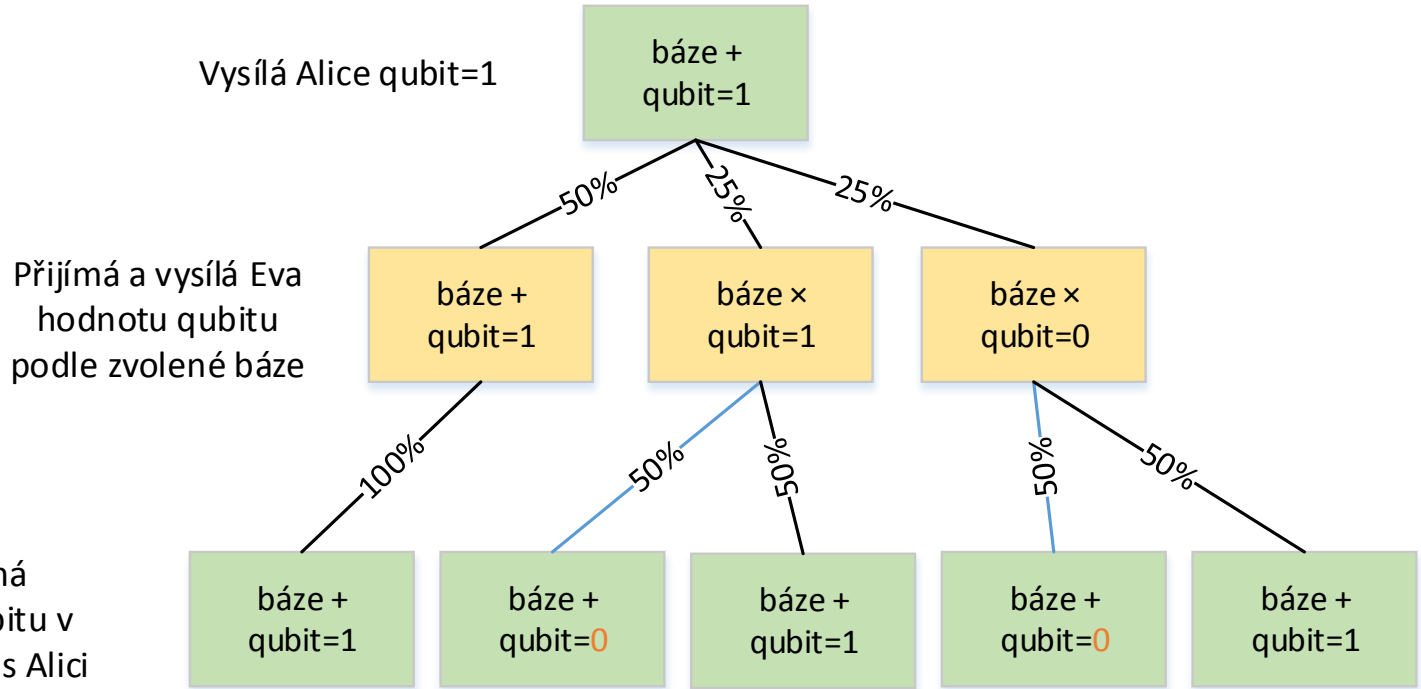
	✓	✓		✓	✓				✓	✓	✓				✓		✓	✓	✓				✓	
	1	**1**		**1**	**0**				**1**	**0**	**0**				**0**		**0**	**0**	**1**				**0**	

Protokol BB84 - detekce odposlechu 1

- Dále je třeba provést detekci odposlechu.
  - Základní idea: Útočník (Eva) svým odposlechem ovlivní stav procházejících qubitů.
  - Alice a Bob obětují část dohodnutého klíče a veřejným kanálem (nutno autentizovat původ zpráv) si porovnají konkrétní přijaté hodnoty.
  - Odposlech se projeví jako chyba v přenosu.
  - Při obětování n bitů je pravděpodobnost detekce soustavného odposlechu $1 - (3/4)^n$.
    - ★ Volbou n lze tuto pravděpodobnost limitně přibližovat k hodnotě 1.
  - V současných systémech se ještě provádí zesílení soukromí (privacy amplification).
    - ★ Cílem je dále minimalizovat Evinu informaci o dohodnutém klíči, která (snad) byla získána nedetekovaným odposlechem.

Protokol BB84 - detekce odposlechu 2

Pozorováním nebo měřením kvantový systém změní svůj stav.
Příklad: **qubit**, $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, když je **qubit** pozorován,
stav **qubitu** se dostane do kolapsu a to tak, že buď $\omega_0 = 0$ nebo $\omega_1 = 0$.



Protokol BB84 - Implementační aspekty

Dva druhy komunikace:

- Kvantová
  - Nutný kvalitní nerušený komunikační kanál mezi Alicí a Bobem.
    - ★ Optický kabel bez běžných infrastrukturních prvků.
    - ★ Nutno znát model chyb.
    - ★ Synchronizace přenosu.
- Klasická
  - Lze použít běžnou síťovou infrastrukturu.
  - Není třeba zajišťovat důvěrnost přenášených zpráv.
  - Musí být zajištěna autentizace původu kontrolních zpráv mezi Alicí a Bobem.
    - ★ Použití rádiového kanálu nemusí být dostatečné.

Protokol BB84 - aplikační aspekty

- Je schopen do jisté míry nahradit asymetrické systémy ve stávajících aplikacích.
  - Zamýšleno zejména s ohledem na teoretické hrozby přicházející z oblasti kvantových počítačů.
- V zásadě dva typy uživatelů:
  - Současní uživatelé asymetrických schémat
    - ★ Získají vyšší teoretickou bezpečnost.
    - ★ Poněkud ztrácejí pohodlí.
    - ★ Ne všechny komponenty lze zatím nahradit (podpis).
  - Současní uživatelé vojenských a zpravodajských systémů
    - ★ Získají větší pohodlí při zachování přibližně stejné úrovně bezpečnosti, jakou jim poskytují současné mechanizmy založené na dlouhých náhodných klíčích.

Experimentální výsledky - dohoda na klíči na vzdálenost 23 km

Muller et al. 1995-96, Ribordy et al. 1998, 2000 (foto: Gisin et al. 2001)

FIG. 13. Geneva and Lake Geneva. The Swisscom optical fiber cable used for quantum cryptography experiments runs under the lake between the town of Nyon, about 23 km north of Geneva, and the centre of the city.

Kvantový registr

- Předpokládejme délku n qubitů.
  - Stavy registru jsou prvky 2^n-rozměrného Hilbertova prostoru.
  - Bázové vektory (vlastní stavy) – příklad pro $n = 2$
    - $\mathbf{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
    - $|\psi\rangle = \omega_{00}|00\rangle + \omega_{01}|01\rangle + \omega_{10}|10\rangle + \omega_{11}|11\rangle$
  - Měřením registru získáme právě jeden z 2^n vlastních stavů.
    - Superpozice nelze přímo „vidět“.
- Kvantový registr představuje základ kvantového počítače.

Fenomény kvantového počítání

- Kvantový paralelismus
  - Díky vlastnostem kvantového registru a linearitě jeho evoluce lze pro n-qubitvé zadání úlohy paralelně řešit všech 2^n úloh současně.
  - Měřením však získáme právě jeden výsledek $\rightarrow$ kvantový paralelismus proto nelze využít takto jednoduše přímo.
- Interference
  - Paralelně získané výsledky se mohou navzájem ovlivňovat.
  - Umožňuje využít síly kvantového paralelismu.
- Provázané stavy (entaglement)
  - Výsledky měření dvou oddělených částí registru mohou být závislé (bez ohledu na vzdálenost obou částí).
  - Úzce souvisí s teleportací kvantových objektů.

Algoritmy pro kvantové počítače 1

Shorův algoritmus (Shor 1994)

- Řeší zásadní úlohy v (pravděpodobnostním) polynomiálním čase.
  - Faktorizace
  - Diskrétní logaritmus – v obecné podobě
- Založen na důmyslném využití kvantové Fourierovy transformace a propojení známých výsledků z teorie čísel a obecné algebry.
- Zásadně ovlivnil pozornost věnovanou kvantovým počítačům.
- Hlavní argument proti PKI (v dnešní podobě) v době existence kvantových počítačů.
- Prakticky odzkoušen na 7-qubitovém počítači.
  - Faktorizace čísla 15, 19. prosince, 2001 (IBM Research).
- Pro praktický dopad vyžaduje *n*-qubitový počítač, kde n je řádu 103 - 104.
  - Akutní nebezpečí tedy nehrozí. Veškeré dostupné prognózy jsou krajně heuristické povahy a pohybují se v řádu desítek let.

Algoritmy pro kvantové počítače 2

Groverův algoritmus (Grover 1996)

- V netříděném seznamu délky N položek je schopen najít daný záznam se složitostí $O(N^{1/2})$.
  - Bylo ukázáno, že tato složitost je nejmenší možná.
- V kryptoanalýze využitelný pro útoky hrubou silou.
  - Seznam tvoří množina všech klíčů a kriterium výběru je dáno například ve tvaru ŠT = EK(OT).
  - Symetrický klíč K délky k bitů lze takto najít se složitostí $O(2^{k/2})$.
    - ★ Zhruba řečeno, algoritmus půlí efektivní délku klíče.

Kvantová kryptologie - jak na ní reagovat

- Z teoretického hlediska existuje pouze jedna kryptologie.
- V budoucnu budou zřejmě koexistovat systémy založené na kvantovém a klasickém přístupu ke zpracování informace.
  - Lze očekávat zejména hybridní systémy.
  - Kvantová kryptografie nevyžaduje kvantové počítače – lze očekávat, že se prosadí dříve, než dojde k zániku některých současných schémat vlivem kvantových počítačů.
- Pokud má mít systém dlouhou morální životnost:
  - Měl by mít modulární architekturu umožňující snadnou výměnu kryptoschémat.
  - Není vhodné soustředit se na jeden úzký druh algoritmu – systém musí být založený na obecných vlastnostech a být tak otevřený.
  - Počítat s tím, že každý jednotlivý algoritmus může být náhle oslaben/prolomen. To platí bez ohledu na kvantové počítače.
  - Je třeba vyhodnotit i morální životnost chráněných dat.
  - Nutno sledovat aktuální vývoj kryptologie. Současná podoba rozhodně není definitivní!