

Komerční výrobky pro kvantovou kryptografii

Cryptofest'05

Miroslav Dobšíček

Katedra počítačů, Fakulta elektrotechnická
České vysoké učení technické v Praze

19. března 2005



O čem bude řeč

Kryptografie

Kryptografie se zejména snaží řešit:

- autorizovanost přístupu
- autenticitu dat
- integritu dat
- **bezpečnou komunikaci**
- bezpečné počítání
- **generování náhodných čísel** (v jistém smyslu)

Bezpečná komunikace

Bezpečná komunikace:

- zpravidla řešená symetrickou šifrou
 - jednoduchá implementace
 - rychlé
 - "rozumné" délky klíčů

Problém s klíčem

- Klíč musí být přenesen po bezpečném kanále.
- Kdybychom měli bezpečný kanál tak nemusíme šifrovat.

⇒ **Klíč přeneseme pomocí asymetrické šifry (RSA).**



Výměna klíčů

Výměna klíčů pomocí asymetrického šifrování:

- 1 Osoba A vygeneruje klíč k .
- 2 Zašifruje ho veřejným klíčem osoby B .
- 3 Podepíše ho pomocí svého privátního klíče.
- 4 B ověří podpis pomocí veřejného klíče osoby A .
- 5 B použije na dešifrování svůj privátní klíč a získá klíč k .
- 6 Celé to funguje, protože je obtížné vygenerovat k jednomu klíči jeho protějšek.



Problém

Asymetrické šifry jsou založeny na úlohách z teorie čísel. Například faktorizace na prvočíselný rozklad nebo výpočet diskretních logaritmů.

Problém

! Obtížnost těchto úloh není dokázána !

- Úlohy jsou tzv. podmíněně bezpečné.
 - Podmíněně znamená, že nesmí být objeven efektivní algoritmus
- V roce 1994 Peter Shor našel efektivní algoritmy pro kvantový počítač.

⇒ Nová kryptografická primitiva musí být založena na nepodmíněně bezpečných úlohách. Nejlépe na fyzikálních zákonech.



Kvantová mechanika

Kvantová mechanika:

- Zatím nejúplnější fyzikální pohled na fungování světa.
- **Vhodný kandidát pro kryptografické aplikace.**
- Fyzika malých částic.
- Masivní paralelismus.
- Nelokální vlastnosti (propletení).



Qubit

Qubit

Nejjednodušší kvantově mechanický systém je kvantový bit - qubit.

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

kde α, β jsou komplexní amplitudy pravděpodobnosti;
 $|\alpha|^2 + |\beta|^2 = 1$.

$|0\rangle, |1\rangle$ jsou báze dvojdimenzionálního komplexního Hilbertova prostoru.



Báze vektorového prostoru

- Máme prostor \implies potřebujeme bázi.
- Všechny prvky prostoru potom můžeme vyjádřit jako lineární kombinaci bázevých vektorů.

Standardní báze

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Jiný příklad možné báze (tzv. duální báze)

$$|0'\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |1'\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$



Fyzická realizace qubitu

Qubit lze realizovat libovolným dvojdimenzionálním kvantovým systémem

Technicky nejlépe zvládnuté systémy:

- Polarizace fotonu (vertikální/horizontální)
- 1/2-spinový moment částice (nahoru/dolů)

Některé základní vlastnosti

- 1 Vývoj izolovaného kvantového systému lze popsat unitární maticí.
- 2 Neexistuje unitární matice, která pro neznámý stav $|\phi\rangle$ provede operaci:

$$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$$

⇒ Neznámý kvantový stav nelze kopírovat - "no-cloning theorem".



Příklad unitární matice

Hadamardova rotace:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Příklad maticového násobení:

$$\text{Nechť } |\phi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \text{pak}$$

$$H|\phi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$



Destruktivní měření

Při měření kvantového stavu, za účelem získání klasické hodnoty, qubit kolabuje s danou pravděpodobností na jednu z bází. Tento kolaps je ireversibilně destruktivní.

Příklad

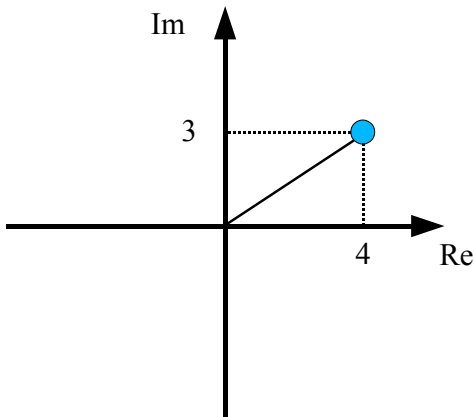
$$|\phi\rangle = \frac{6}{10}|0\rangle + \frac{8}{10}|1\rangle$$

Při měření zkolabuje qubit na stav $|\phi'\rangle = |0\rangle$ s pravděpodobností $(\frac{6}{10})^2$. S pravděpodobností $(\frac{8}{10})^2$ zkolabuje na stav $|\phi'\rangle = |1\rangle$.



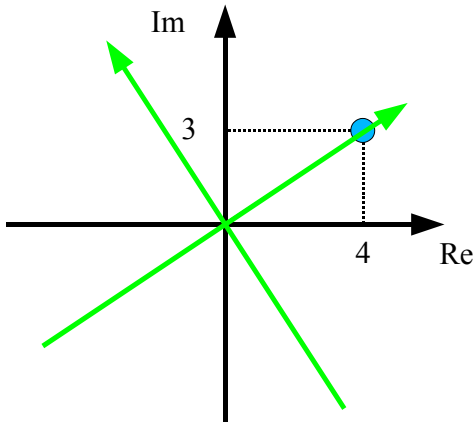
Lehká analogie ke komplexnímu číslu

$$z = 4 + 3i$$



Rotace souřadného systému

Pokud potočím osy a začnu dělat projekce do nich dostanu jiné hodnoty.



Neurčitost báze

Nosná myšlenka o neurčitosti bází

- 1 Qubit není nic jiného než vektor.
- 2 Vektor v sobě nenesení žádnou informaci o bázi ve které byl vytvořen a ve které má být měřen.

Tato myšlenka spolu s neklonovacím teorémem tvoří základ protokolu BB84 (G. Brassard, Ch. Bennet - 1984) pro kvantovou distribuci klíčů.

Kvantová distribuce klíčů

Rámcové schéma protokolu BB84

- 1 Alice vygeneruje klíč k , který chce distribuovat.
- 2 Dále vygeneruje stejně dlouhý náhodný řetězec b .
- 3 Odesílá Bobovi bity klíče k a podle řetězce b je kóduje jako qubity ve std. bázi nebo duální bázi.
- 4 Bob si vygeneruje náhodný řetězec, podle kterého provádí měření ve std./duální bázi. Úspěšný bude zhruba na 50%.
- 5 Alice potom Bobovi sdělí na kterých pozicích chyboval a zbytek se stává požadovaným klíčem.



Útočník Eva

- 1 Eva nemůže qubity kopírovat pro pozdější zpracování.
- 2 Její jediná možnost je metoda **změř a přepošli dál**.
- 3 Eva nezná správné báze pro měření \implies musí tipovat.
- 4 Její destruktivní změny způsobí, že ji Alice a Bob vždy detekují.



Komerční výrobky pro kvantovou kryptografií

Komerční výrobky

- Všechny velké firmy z IT již pracují na komerčních výrobcích.
- Skutečně hotové výrobky mají pouze relativně neznámé firmy MagiQ a id Quantique.
 - Kvantová distribuce klíčů pomocí optického vlákna.
 - Rychlost: řádově 100kb/s.
 - Do vzdálenosti: max 70Km.
 - Cena: řádově 50 000 \$.
 - Generování kvantově náhodných čísel.
 - Rychlost: řádově 10Mb/s.



Navajo od firmy MagiQ



QKC systém od firmy id Quantique



Generátor náhodných čísel od id Quantique

