Kvantové korelace ve službách kryptografie

František Šrédl, Jindřich Vlach, Oliver Beer

Šifrování dat

Základní principy

- Důvěrnost
- Integrita informací
- Autentizace
- Nepopiratelnost

Asymetrické šifrování

- Dvojice klíčů
  - Veřejný klíč
  - Soukromý klíč
- Využití: Digitální podpis, bezpečný přenos klíčů
- Nevýhoda: Výpočetně náročnější

Příklady: RSA, ECC

Symetrické šifrování

- Jeden společný klíč
- Výhoda: Vysoká rychlost
- Nevýhoda: Nutnost bezpečného sdílení klíče

Příklady: AES, DES

RSA algoritmus

- Založen na obtížnosti rozkladu velkých čísel
- Používá veřejný a soukromý klíč
- Využití:
  - Šifrování
  - Digitální podpis

Matematický základ

- Prvočísla
- Eulerova funkce
- 2048 nebo 4096 bitová verze

$$\phi(p \cdot q) = (p - 1) \cdot (q - 1)$$

Kvantové počítání a komunikace

Kvantové počítače

- Využívá principy kvantové mechaniky
- Potenciálně bude řešit některé úlohy exponenciálně rychleji než konvenční počítače

Qubit (kvantový bit)

- Základní jednotka informace
- Může být v superpozici stavů
- Po měření získáme hodnotu 0 nebo 1

Klasické bity: 0, 1

Qubity: $|0\rangle, |1\rangle$

Kvantové provázání

- Po změření jednoho qubitu dokážeme zjistit stav druhého
- není limitováno vzdáleností ani rychlostí světla

Vybrané platformy

Uvězněné ionty

IonQ

+ Vysoká přesnost
- Pomalé provádění operace

Fotonika

PsiQuantum

+ Nepotřebují chlazení
- Velmi těžké provádět operace na fotonech

Supravodivé qubity

IBM, Google Quantum AI

+ Rychlé kvantové operace
- Potřeba vysokého chlazení

Nejrozšířenější technologie

Základní stavy a superpozice

Qubit je popsán ve dvourozměrném prostoru se základními stavy

$$|0\rangle, |1\rangle$$

Princip superpozice

- Obecný stav qubitu je lineární kombinací obou bází, Dokud není provedeno měření:

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

Metodika protokolu ERP

1) Příprava: Tvorba binární zprávy o délce n.
2) Distribuce: Rozeslání 2n + m provázaných párů qubitů.
3) Náhodnost: Vygenerování lokálních náhodných řetězců (2n).
4) Měření: Měření qubitů ve dvou nezávislých bázích.
5) Zničení: Okamžitá destrukce qubitů ihned po měření.
6) Klíč: Sestavení bezpečného šifrovacího klíče o délce n.

Fyzikální podstata bezpečnosti

- Každé měření (odposlech) nevratně změní stav qubitu.
- Kvantovou informaci nelze zkopírovat bez jejího poškození.
- Pokus o odposlech se ihned odhalí nesouladem při srovnání bází.

Výsledky měření na kvantovém procesoru Heron R2

Původní zpráva	Jaderce zdar
1. přenos	zqvafksazk s
2. přenos	jadercehzdcr
3. přenos	jaderce xdkr
4. přenos	jadupce xdar
5. přenos	jieurce zdcr
6. přenos	jadebked ear
7. přenos	jadurcehxdar
8. přenos	jatirco dir
9. přenos	qnfzccx maf
10. přenos	jalerce zdav

- Průměrná úspěšnost přenesení písmene byla 60,8%
- Přenos jedné zprávy trval ~6 sekund

Děkujeme za pozornost!