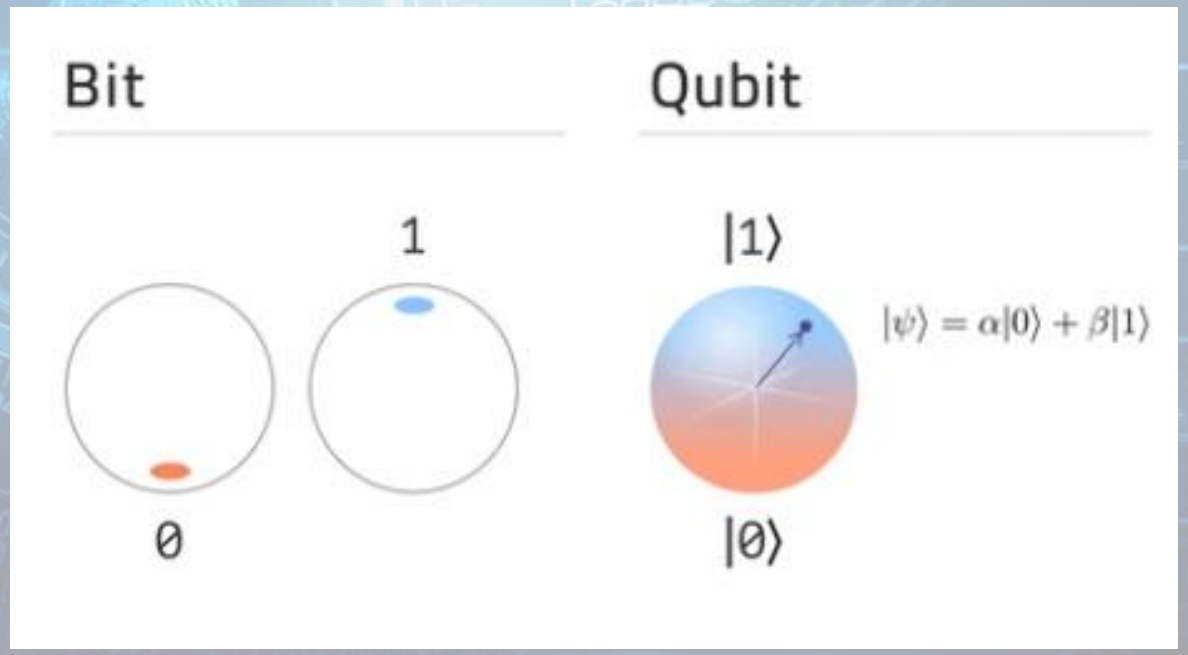
Kriptográfia a kvantumszámítógépek világában

Zentai Dániel
Nemzeti Kibervédelmi Intézet
Biztonsági Elemző Szakterület
daniel.zentai@nki.gov.hu

Kvantumszámítógépek

- Klasszikus bit: 0 vagy 1
- Qubit: szuperpozíció → $\alpha \cdot 0 + \beta \cdot 1$



Kvantumszámítógépek

- Mi a jó hír?
  - Hogy nem létezik. ☺
- És mi a rossz?
  - Feltöri a jelenleg használt kriptográfiai algoritmusokat.
  - RSA → faktorizáció
  - DSA, Diffie-Hellman → diszkrét logaritmus

Kvantumszámítógépek

- Ha nem létezik, akkor miért érdekel minket?
  - Tegyük fel, hogy x évig szeretnénk valamit titokban tartani, y évig tart átállni kvantumszámítógépek ellen is védett eljárások használatára, és z év múlva készül el az első nagy teljesítményű kvantumszámítógép.

Tétel (Michele Mosca):

Ha x + y > z, akkor bajban vagyunk.

RSA titkosítás, aláírás

- A nyilvános kulcs (egyik fele) egy n természetes szám, amit $n=p \cdot q$ alakban állítunk elő, ahol p és q nagy prímszámok.
- Ha a támadó pusztán n ismeretében ki tudja számolni p, vagy q értékét, akkor ki tudja számolni a privát kulcsot is.
- Tehát azt szeretnénk, ha egy nagy szám prímtényezőkre bontása (faktorizáció) nehéz feladat lenne. Kvantumszámítógéppel nem az.

DSA aláírás, Diffie-Hellman kulcscsere

- Nyilvános információ egy p nagy prímszám, és egy 1 és p-1 közé eső (bizonyos kritériumoknak eleget tevő) másik természetes szám. Jelöljük ez utóbbit g-vel.
- A támadó feladata g, p, és g^x mod p ismeretében x meghatározása. Ez a diszkrét logaritmus probléma, ami szintén gyorsan megoldható kvantumszámítógéppel.

Kvantumszámítógépek

- Mi marad biztonságos?
  - Szimmetrikus kulcsú titkosítás (de nagyobb kulcsok kellenek)
  - Hash függvények (de nagyobb output méret kell)
  - **Poszt-kvantum kriptográfia**

Szabványosítás

- NIST Post-Quantum Cryptography Standardization Process
- 82 algoritmus érkezett be
- 2017 december: első forduló, 69 algoritmus
- 2019 január: második forduló, 26 algoritmus
- 2020 július: harmadik forduló, 7 döntős + 8 alternatív jelölt

A jelenlegi állás (a döntősök)

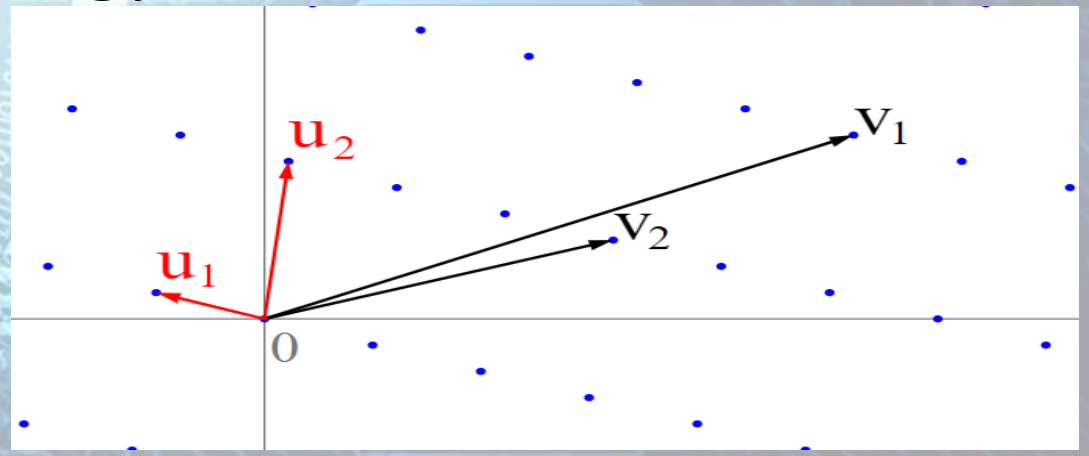
- Titkosítás és kulcscsere
  - Classic McEliece
  - KYBER
  - NTRU
  - SABER
- Digitális aláírás
  - DILITHIUM
  - FALCON
  - Rainbow

Classic McEliece

- Kódelmélet alapú nyilvános kulcsú titkosítás.
- A publikus kulcs egy t természetes szám, és egy t-hibajavító kód kódoló algoritmusa.
- A privát kulcs (többek között) ezen t-hibajavító kód dekódoló algoritmusa.
- Pusztán a kódoló algoritmus ismeretében egy hibajavító kód dekódolása nehéz feladat kvantumszámítógéppel is.

KYBER, NTRU, SABER, DILITHIUM, FALCON

- Rácselmélet alapú nyilvános kulcsú titkosítások, digitális aláírások.
- A publikus és a privát kulcs egy-egy bázisa az n dimenziós rácsnak.
- A támadó feladata a rácsban megtalálni a két egymáshoz legközelebb eső vektort.
  Ez nehéz feladat kvantumszámítógéppel is.



Rainbow

- Többváltozós polinomokra épülő digitális aláírás.
- A publikus kulcs egy többváltozós polinom. (például $p(x,y,z) = 2xy + 3x^3z - y^5z^2 + 2xyz$)
- A privát kulcs a p polinom inverzéről tartalmaz bizonyos információkat.
- Az aláírás biztonsága azon múlik, hogy többismeretlenes nemlineáris egyenletrendszerek megoldása nehéz feladat. Kvantumszámítógéppel is.

Köszönöm a figyelmet!