Univerzita Tomáše Bati
Fakulta aplikované informatiky

PT LAB

Post-kvantová kryptografie – nejen ta asymetrická

Ing. Petr Žáček, Ph.D.
zacek@utb.cz

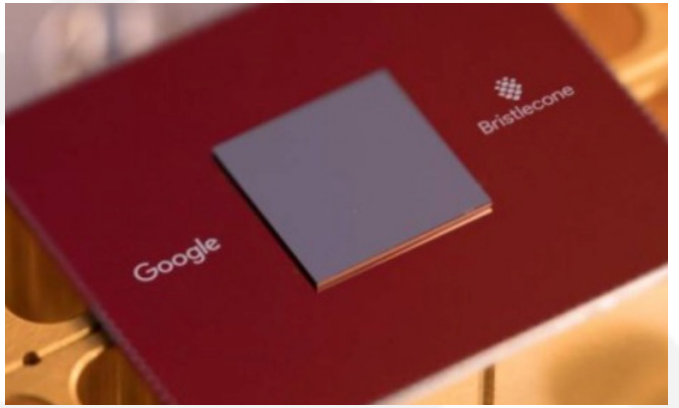
Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
PT LAB – Penetration Testing Laboratory

Bezpečnostní seminář CRYPTO 2022 (AFCEA)
24.3.2022

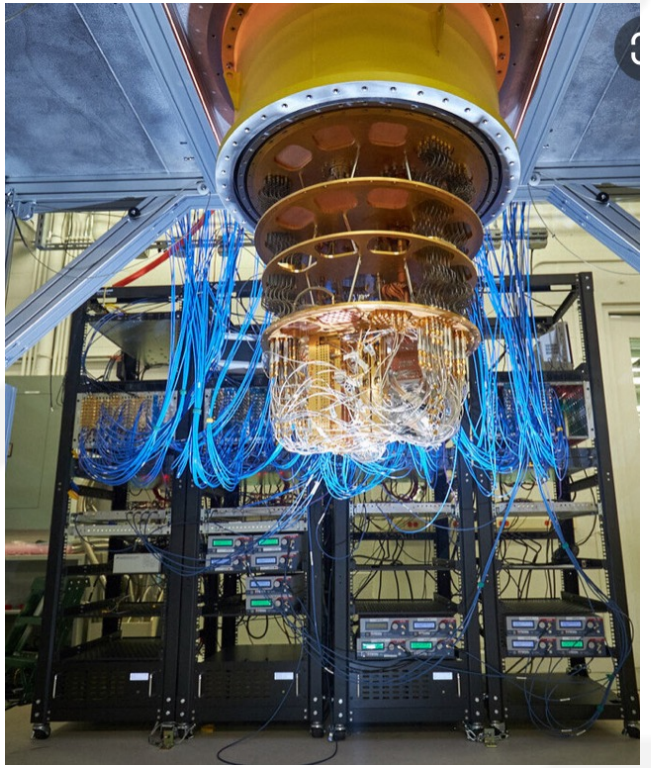
Obsah

1. Úvod / předmluva
2. Aktuální stav
3. Asymetrická post-kvantová kryptografie
4. Symetrická post-kvantová kryptografie
5. Ukázka – PT Lab (Kryptografický systém SMALLIE)

Úvod – kvantový počítač



- Každý o něm slyšel, ale málo kdo ho viděl … (od cca 1980)
- Všichni se ho „bojí“ -> je důvod ?
  - ANO i ne (silné „PR“)
- Není kvantový počítač jako kvantový počítač



Úvod – druhy kvantových počítačů

- Ideální kvantový počítač -> programovatelný a řešící každý problém
  - Aktuálně nedosažitelné – cena, velikost, málo qubitů, programovatelnost
- Specializované a „pseudo“ kvantové počítače
  - Medicína, počasí, ekonomika, RSA
- Proč trvá vývoj tak dlouho ?
- Problematika fyziky, chemie a matematiky
  - Proto spousta druhů …

Bavíme se o post-kvantové kryptografii

- Není kryptografie založená na kvantové fyzice
- Ani nefunguje pomocí kvantových počítačů
- Ale staví na předpokladu prolomení aktuální kryptografie pomocí kvantových počítačů
- Příprava jako obrana proti kvantovým počítačům -> **Už nyní !!!**

Příchod kvantových počítačů

- „Zde není otázkou jestli, ale KDY ?“
- Prolomení kryptografie, jak ji známe .. (když nastane, jak dlouho potrvá změna ?
  - Běžící služby, shodan.io atd …
- Které ? „Zejména“ asymetrické -> certifikáty, podpisy, výměna klíčů (PKI)
  - (RSA, eliptické křivky, diffie-hellman) -> problematiky faktorizace a diskrétního logaritmu

Příchod kvantových počítačů

- Aktuálně se to týká koho ? Kdo bude ovlivněn ?
  - Nemyslíme ideální kvantový počítač.

- Týká se to všech …
  - RSA, DSA, výměna klíčů, eliptické křivky .. Prakticky celý internet a prakticky všechna naše komunikace …

- Uživatel -> HTTPS (TLS v1.3) -> stále Diffie-Helmann, RSA už jen pro DSA … (žádná velká změna v kontextu post-kvantové …)

Asymetrická + post-kvantová kryptografie

- RSA 1977
  - „Prolomeno“ 1994 -> Peter Shor (Shorův faktorizační algoritmus)
  - 1997 veřejný/odtajněný
  - Zatím klíče velikosti 2048 nebo 4096+ bitů
- Bez kvantového počítače -> 1061 bitů

- Proč se tedy používá ? Lehčí navýšit než vyměnit .. Eliptické křivky ?

Asymetrická + post-kvantová kryptografie

- Nabízelo by se zvětšit RSA klíče ? … mnohem víc ?
  - Nevyplatí se …
  - Pro představu
    - Nárůst bezpečnosti RSA s klíčem 512 bitů na 1024 teď -> 250000 krát složitější
    - Nárůst bezpečnosti RSA s klíčem 512 bitů na 1024 s kvantovým počítačem -> 8 krát složitější
    - Nárůst bezpečnosti RSA s klíčem 1024 bitů na 2048 teď -> řádově 6*10^14 krát složitější
    - Nárůst bezpečnosti RSA s klíčem 1024 bitů na 2048 s kvantovým počítačem -> 8 krát složitější
  - Využití klíčů 20MB a více .. (umocňování velkých čísel)

Asymetrická + post-kvantová kryptografie

- Aktuální možnosti
  - Nové algoritmy -> post-kvantová kryptografie a/nebo QKD (kvantová distribuce klíčů)
  - Existují ?? Ano a je jich poměrně hodně … (šifrování/výměna klíčů i podepisování)
    - Od 2017 běží NIST -> kandidáti třetího kola (konec 2024 ?)
      - NTRU
      - Classic McEliece (velmi starý ☺ jako RSA 1978) -> pomalý
      - SABER
      - CRYSTALS-KYBER

      - Podepisování -> CRYSTALS-DILITHIUM, FALCON, Rainbow
- https://github.com/open-quantum-safe/liboqs

Symetrická vs. Asymetrická kryptografie

- Pokud je zapojena asymetrická .. Problém (výměna klíčů)
  - Opět prakticky všude ..
  - Retence dat
  - QKD -> náročné a drahé -> za mě ale vhodné řešení

- Symetrická -> odolná ? (ANO)
  - Ideální kvantový počítač
  - Specializovaný -> algoritmy .. Viz dále

Symetrická post-kvantová kryptografie ???

- Existuje ???
  - Oficiálně neexistuje …
  - Existují post-kvantové symetrické algoritmy ? ANO … AES-256 a cokoliv co má víc jak 128 (160) bitů se bere za post-kvantovou …
  - Protože se počítá dvojnásobné urychlení hledání symetrických klíčů hrubou silou – aktuálně 80 bitů (Groverův algoritmus)

- eAES -> mutace s délkou 512 bitů a 30 rundami -> analogie RSA ?
- Článek 2016 -> **The block symmetric ciphers in the post-quantum period (IEEE)**

Symetrická post-kvantová kryptografie

- Shorův algoritmus není zdaleka konec …
  - Grover‘s search method -> kvadratické urychlení (Asymetrika/symetrika)
  - Simon‘s period finding -> exponenciální urychlení (Asymetrika/symetrika)
  - Hidden subgroup problém -> generalizace Shorova, Simonova a mnoha dalších algoritmů
- A mnoho dalších … https://quantumalgorithmzoo.org

Symetrická post-kvantová kryptografie - možnosti

- V porovnání s asymetrickou … přímo nejsou
- Využití AES-256 …
  - Či dalších šifer s délkou klíče minimálně 256 bitů
- Co se stane, když bude AES prolomen v kontextu kvantových počítačů ?
  - Máme čas ? .. Znovu retence

Výzkum PT Lab

- Vzniká symetrická bloková šifra s kódovým označením SMALLIE
- Jeví se jako post-kvantová
- Nemá skoro nic společného s aktuálními šiframi

Výzkum PT Lab

- Základní myšlenka ->
  - Co Kvantový počítač potřebuje znát algoritmus šifry + kryptoanalytický
  - Co kdybychom nevěděli algoritmus ? Vlastnosti ? Další aspekty šifrovacího algoritmu ?
  - Ale zároveň dodrželi „Security through obscurity“ ?
  - Která šifra je potvrzena za neprolomitelnou ? Vernamova šifra
  - Pokus o nový pohled na věc

SMALLIE

- „Symetrická bloková šifra“ -> aktuálně více než desátá verze
  - Délka klíče -> 111 Bajtů
- Kromě klíče -> parametrizace + vliv náhodných dat
- Algoritmus a vlastnosti šifrování nejsou známy
  - Sestaveno před šifrováním a neustále se mění a vše souvisí se vším
  - Šifra k zašifrování dat ale i šifry
- Změny -> náhodně + pseudo-náhodně
- Náhodně polymorfní symetrický blokový kryptografický systém
  - Sada šifrovacích algoritmů

SMALLIE

- Konkrétní průběh šifrování není předem znám
- Stejná data, stejné parametry, stejný „klíč“ ->
  - Vždy jiná náhodná data
  - Zašifrovaná jiným náhodným způsobem
- Ze zašifrovaných dat nevíme .. Šifra k zašifrování dat ale i šifry
  - Konkrétní šifrovací algoritmus
  - Délku vstupních dat
  - Vlastnosti šifrování
  - Doba šifrování, průběh
  - Vše se mění … aktuálně více jak 10 vlastností

SMALLIE

- Funkční ukázka

SMALLIE

- Budoucnost
  - Stabilizace algoritmů -> systému
  - Kryptoanalýza a důležité prověření bezpečnosti
  - Optimalizace

  - Snad certifikace/standardizace a nasazení.

  - QKD + Symetrická

Univerzita Tomáše Bati
Fakulta aplikované informatiky

PT LAB

Post-kvantová kryptografie – nejen ta asymetrická

Ing. Petr Žáček, Ph.D.
zacek@utb.cz

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
PT LAB – Penetration Testing Laboratory

Bezpečnostní seminář CRYPTO 2022 (AFCEA)
24.3.2022