Šifrovanie a hrozba kvantových počítačov[1]

Tomáš Fabšič

Fakulta elektrotechniky a informatiky
Slovenská technická univerzita v Bratislave
(FEI STU)

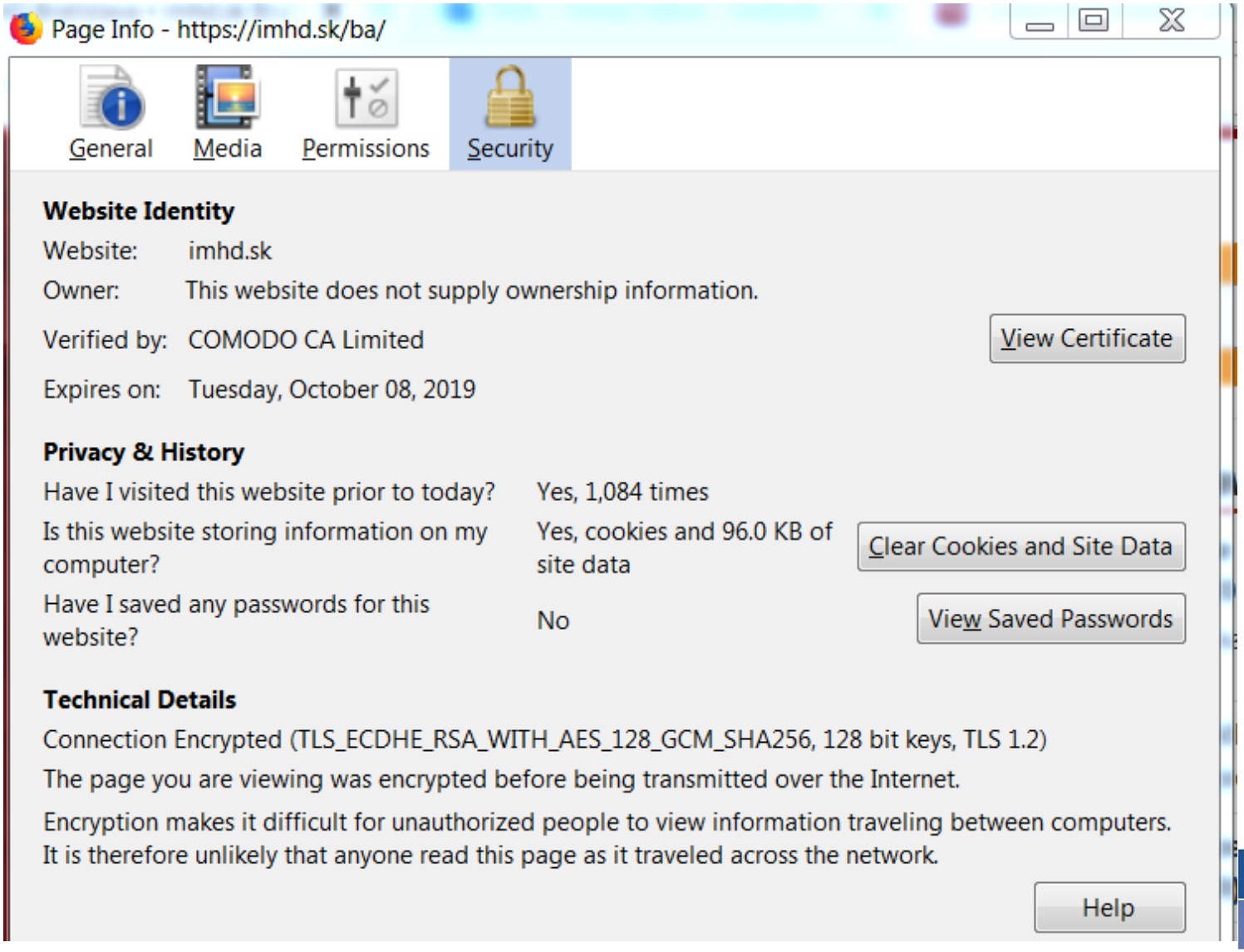
30. septembra 2019

[1] Support from the NATO SPS Project G5448 is acknowledged.

Outline

Contents

Šifrovanie na webe



Šifrovanie na webe

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

O kryptológii

- Kryptológia - veda zaoberajúca sa bezpečnou komunikáciou
- V prednáške budem používať pojmy:
  - Kryptografia = kryptológia
  - Kryptosystém = šifra

O kryptológii

- Kryptológia - veda zaoberajúca sa bezpečnou komunikáciou
- V prednáške budem používať pojmy:
  - Kryptografia = kryptológia
  - Kryptosystém = šifra

Hlavné ciele kryptológie

- Dôvernosť - utajiť obsah komunikácie.
- Integrita správy - zabezpečiť, aby správu počas jej prenosu nemohol nikto nepozorovane zmeniť.
- Autentizácia - zabezpečiť, že odosielateľ správy je tým, za koho sa vydáva.
- Nepopieratelnosť - zabezpečiť, aby odosielateľ správy nemohol poprieť, že on je jej autorom. (digitálne podpisy)

Za účelom dosiahnutia týchto cieľov sa používajú šifry!

Hlavné ciele kryptológie

- Dôvernosť - utajiť obsah komunikácie.
- Integrita správy - zabezpečiť, aby správu počas jej prenosu nemohol nikto nepozorovane zmeniť.
- Autentizácia - zabezpečiť, že odosielateľ správy je tým, za koho sa vydáva.
- Nepopieratelnosť - zabezpečiť, aby odosielateľ správy nemohol poprieť, že on je jej autorom. (digitálne podpisy)

Za účelom dosiahnutia týchto cieľov sa používajú šifry!

Hlavné ciele kryptológie

- Dôvernosť - utajiť obsah komunikácie.
- Integrita správy - zabezpečiť, aby správu počas jej prenosu nemohol nikto nepozorovane zmeniť.
- Autentizácia - zabezpečiť, že odosielateľ správy je tým, za koho sa vydáva.
- Nepopieratelnosť - zabezpečiť, aby odosielateľ správy nemohol poprieť, že on je jej autorom. (digitálne podpisy)

Za účelom dosiahnutia týchto cieľov sa používajú šifry!

Hlavné ciele kryptológie

- Dôvernosť - utajiť obsah komunikácie.
- Integrita správy - zabezpečiť, aby správu počas jej prenosu nemohol nikto nepozorovane zmeniť.
- Autentizácia - zabezpečiť, že odosielateľ správy je tým, za koho sa vydáva.
- Nepopieratelnosť - zabezpečiť, aby odosielateľ správy nemohol poprieť, že on je jej autorom. (digitálne podpisy)

Za účelom dosiahnutia týchto cieľov sa používajú šifry!

Hlavné ciele kryptológie

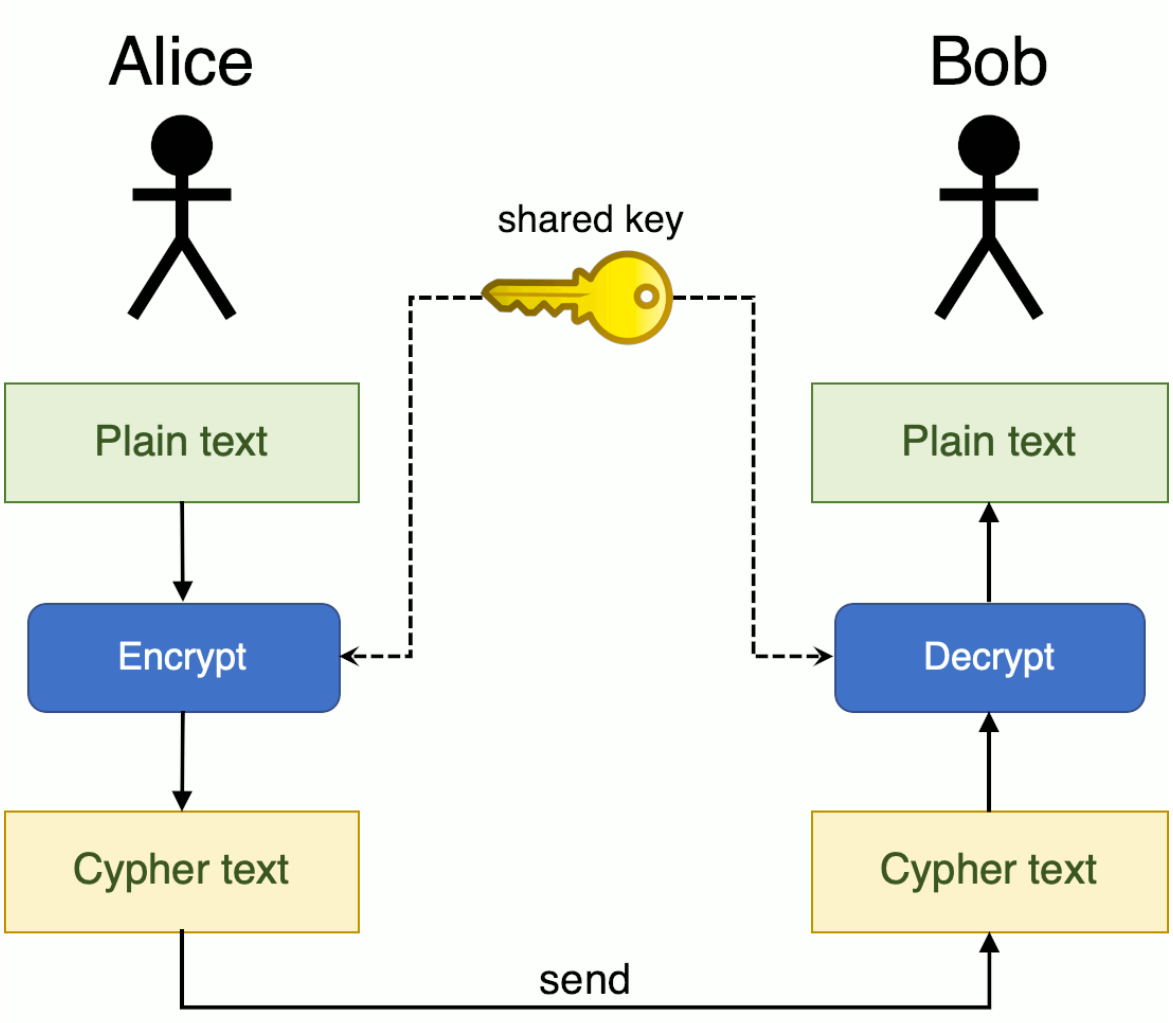
- Dôvernosť - utajiť obsah komunikácie.
- Integrita správy - zabezpečiť, aby správu počas jej prenosu nemohol nikto nepozorovane zmeniť.
- Autentizácia - zabezpečiť, že odosielateľ správy je tým, za koho sa vydáva.
- Nepopieratelnosť - zabezpečiť, aby odosielateľ správy nemohol poprieť, že on je jej autorom. (digitálne podpisy)

Za účelom dosiahnutia týchto cieľov sa používajú šifry!

Typy šifier

- Symetrické šifry
- Asymetrické šifry

Symetrické šifry



Obr.: Source: https://www.coengoedegebure.com/surviving-an-infosec-job-interview-cryptography/

Symetrické šifry

- Predpokladáme, že Alica a Bob zdielajú kľúč (kľúč je postupnosť bitov).
- Nikto, kto nepozná kľúč, nevie správu dešifrovať.
- Ako sa Alica a Bob dohodnú na kľúči, ktorý budú používať?

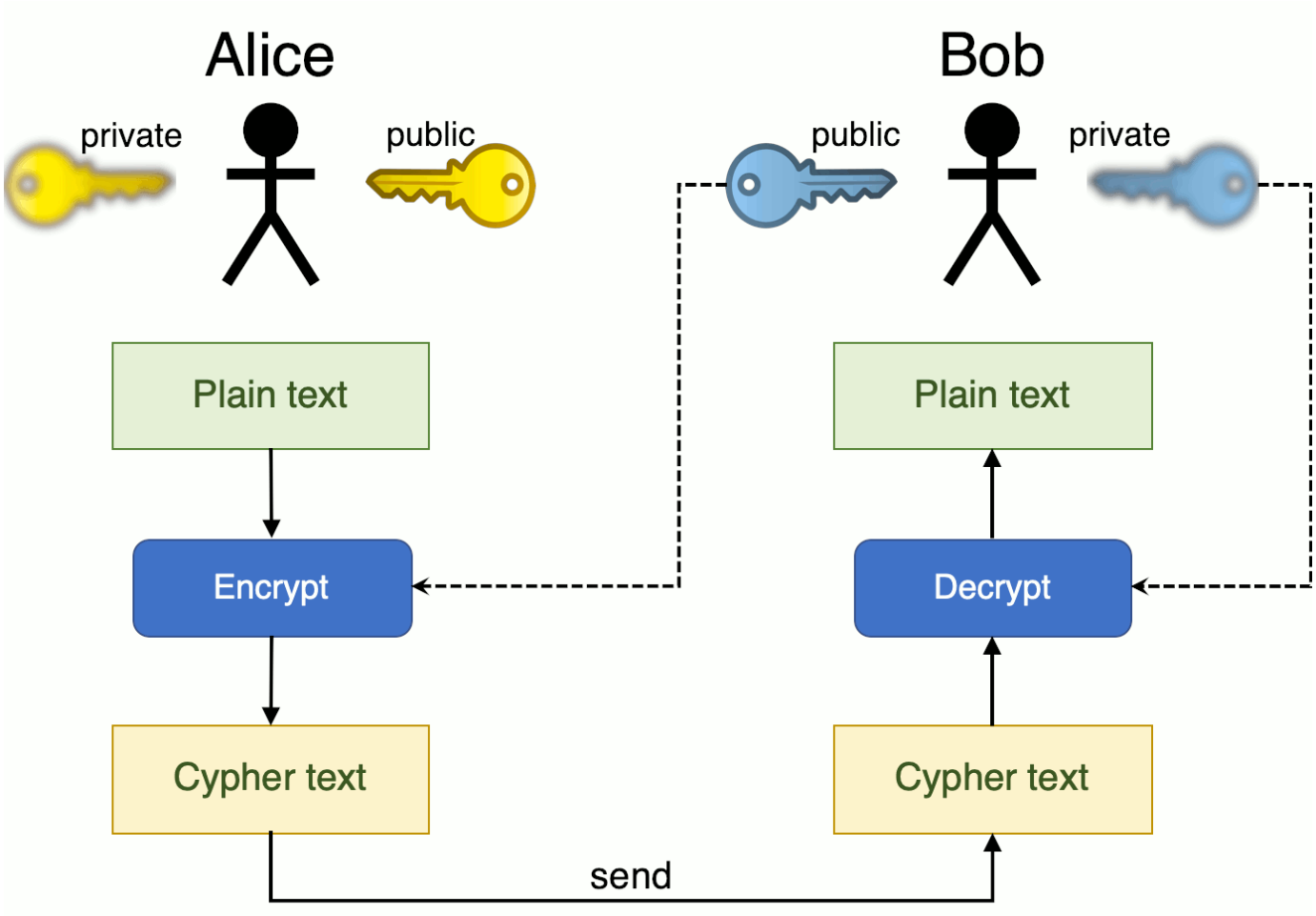
Symetrické šifry

- Predpokladáme, že Alica a Bob zdielajú kľúč (kľúč je postupnosť bitov).
- Nikto, kto nepozná kľúč, nevie správu dešifrovať.
- Ako sa Alica a Bob dohodnú na kľúči, ktorý budú používať?

Asymetrické šifry

- Používajú sa na výmenu kľúča pre symetrické šifry, na digitálne podpisy, ...

Asymetrické šifry



Obr.: Source: https://www.coengoedegebure.com/surviving-an-infosec-job-interview-cryptography/

Asymetrické šifry a ťažké problémy

- Iba Bob vie dešifrovať správu od Alice, lebo iba on pozná svoj súkromný kľúč.
- Medzi Bobovým verejným kľúčom a jeho súkromným kľúčom musí byť nejaký vzťah. (Inak by asymetrická šifra nemohla nefungovať.)
- Tento vzťah ale nesmie umožniť, aby niekto druhý vedel z verejného kľúča určiť súkromný kľúč. (Inak by asymetrické šifrovanie nebolo bezpečné.)
- Preto sú asymetrické šifry založené na výpočtových problémoch, ktoré ľudstvo nevie riešiť.

Asymetrické šifry a ťažké problémy

- Iba Bob vie dešifrovať správu od Alice, lebo iba on pozná svoj súkromný kľúč.
- Medzi Bobovým verejným kľúčom a jeho súkromným kľúčom musí byť nejaký vzťah. (Inak by asymetrická šifra nemohla nefungovať.)
- Tento vzťah ale nesmie umožniť, aby niekto druhý vedel z verejného kľúča určiť súkromný kľúč. (Inak by asymetrické šifrovanie nebolo bezpečné.)
- Preto sú asymetrické šifry založené na výpočtových problémoch, ktoré ľudstvo nevie riešiť.

Asymetrické šifry a ťažké problémy

- Iba Bob vie dešifrovať správu od Alice, lebo iba on pozná svoj súkromný kľúč.
- Medzi Bobovým verejným kľúčom a jeho súkromným kľúčom musí byť nejaký vzťah. (Inak by asymetrická šifra nemohla nefungovať.)
- Tento vzťah ale nesmie umožniť, aby niekto druhý vedel z verejného kľúča určiť súkromný kľúč. (Inak by asymetrické šifrovanie nebolo bezpečné.)
- Preto sú asymetrické šifry založené na výpočtových problémoch, ktoré ľudstvo nevie riešiť.

Asymetrické šifry a ťažké problémy

- Iba Bob vie dešifrovať správu od Alice, lebo iba on pozná svoj súkromný kľúč.
- Medzi Bobovým verejným kľúčom a jeho súkromným kľúčom musí byť nejaký vzťah. (Inak by asymetrická šifra nemohla nefungovať.)
- Tento vzťah ale nesmie umožniť, aby niekto druhý vedel z verejného kľúča určiť súkromný kľúč. (Inak by asymetrické šifrovanie nebolo bezpečné.)
- Preto sú asymetrické šifry založené na výpočtových problémoch, ktoré ľudstvo nevie riešiť.

Príklad ťažkého problému: faktorizácia na prvočísla

- Uvažujme číslo 15.
- Jeho faktorizácia na prvočísla je 15=3*5.
- Ak by sme si ale zvolili veľmi veľké číslo, nevedeli by sme ho v rozumnom čase faktorizovať.
- Dôvod: Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Pozor! To neznamená, že taký algoritmus v budúcnosti nie je možné vymyslieť.

Príklad ťažkého problému: faktorizácia na prvočísla

- Uvažujme číslo 15.
- Jeho faktorizácia na prvočísla je 15=3*5.
- Ak by sme si ale zvolili veľmi veľké číslo, nevedeli by sme ho v rozumnom čase faktorizovať.
- Dôvod: Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Pozor! To neznamená, že taký algoritmus v budúcnosti nie je možné vymyslieť.

Príklad ťažkého problému: faktorizácia na prvočísla

- Uvažujme číslo 15.
- Jeho faktorizácia na prvočísla je 15=3*5.
- Ak by sme si ale zvolili veľmi veľké číslo, nevedeli by sme ho v rozumnom čase faktorizovať.
- Dôvod: Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Pozor! To neznamená, že taký algoritmus v budúcnosti nie je možné vymyslieť.

Príklad ťažkého problému: faktorizácia na prvočísla

- Uvažujme číslo 15.
- Jeho faktorizácia na prvočísla je 15=3*5.
- Ak by sme si ale zvolili veľmi veľké číslo, nevedeli by sme ho v rozumnom čase faktorizovať.
- Dôvod: Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Pozor! To neznamená, že taký algoritmus v budúcnosti nie je možné vymyslieť.

Šifra RSA a problém faktorizácie na prvočísla

- Bob si náhodne vygeneruje dve veľké prvočísla p a q.
- Súkromným kľúčom Boba budú tieto dve prvočísla.
- Jeho verejným kľúčom bude číslo $n = p * q$.

Šifra RSA a problém faktorizácie na prvočísla

- Bob si náhodne vygeneruje dve veľké prvočísla p a q.
- Súkromným kľúčom Boba budú tieto dve prvočísla.
- Jeho verejným kľúčom bude číslo $n = p * q$.

Šifra RSA a problém faktorizácie na prvočísla

- Bob si náhodne vygeneruje dve veľké prvočísla p a q.
- Súkromným kľúčom Boba budú tieto dve prvočísla.
- Jeho verejným kľúčom bude číslo $n = p * q$.

Problém faktorizácie ešte raz

- Na skoršom slajde som napísal:
  Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Presnejšia formulácia:
  Ľudstvo nepozná efektívny algoritmus na faktorizáciu pre klasické počítače!
- Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!

Problém faktorizácie ešte raz

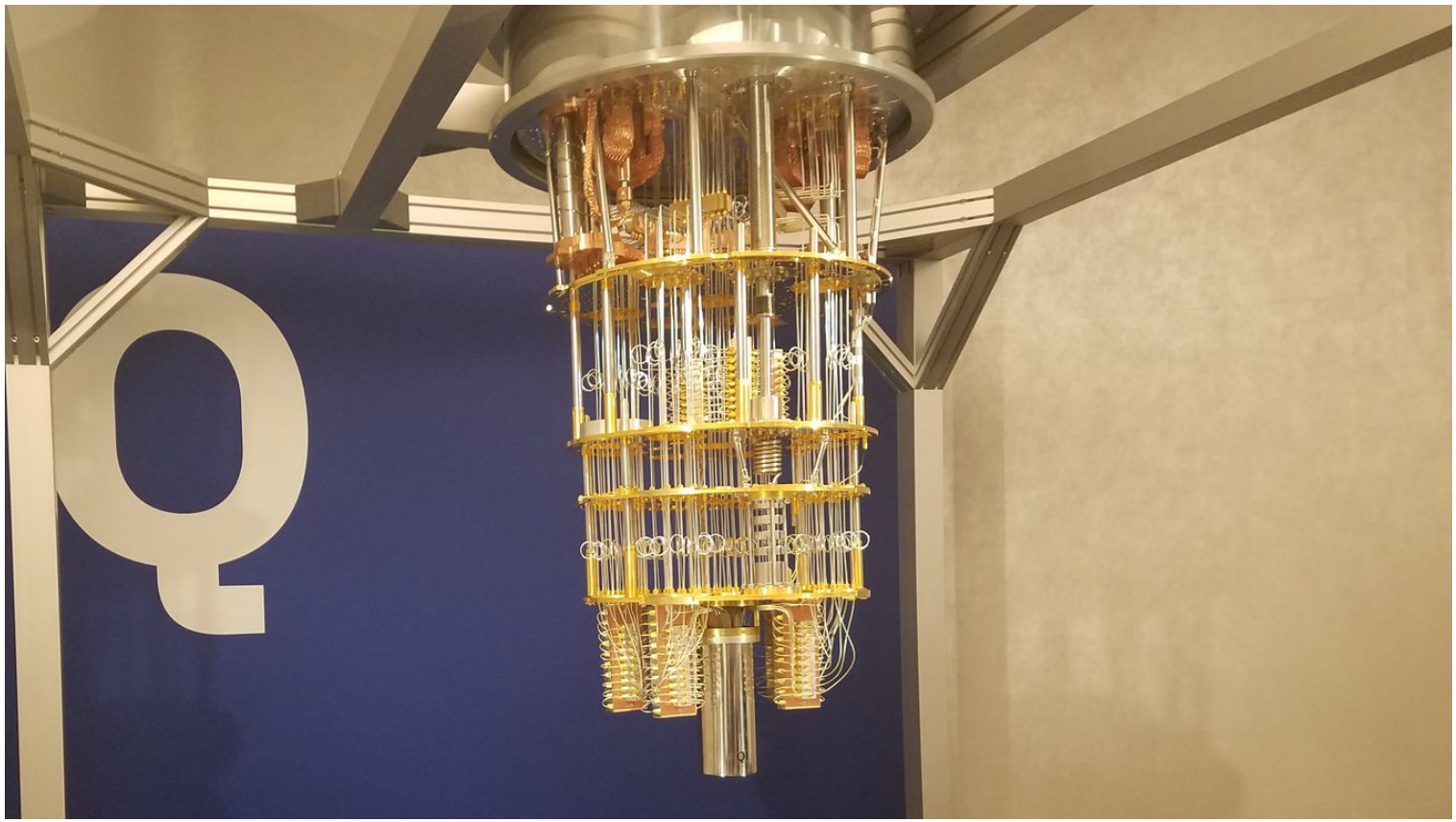
- Na skoršom slajde som napísal:
  Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Presnejšia formulácia:
  Ľudstvo nepozná efektívny algoritmus na faktorizáciu pre klasické počítače!
- Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!

Problém faktorizácie ešte raz

- Na skoršom slajde som napísal:
  Ľudstvo nepozná efektívny algoritmus na faktorizáciu!
- Presnejšia formulácia:
  Ľudstvo nepozná efektívny algoritmus na faktorizáciu pre klasické počítače!
- Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!

Contents

Kvantové počítače



Obr.: Source: https://www.axios.com/quantum-computing-edges-toward-mainstream-dfd65971-1a41-4b83-a410-9f9c8fb965e6.html

Čo je to kvantový počítač?

- Kvantová mechanika - fyzikálna teória popisujúca správanie atómov a subatomárnych častíc.
- Kvantový počítač - zariadenie, ktoré na výpočty využíva princípy kvantovej mechaniky.

Čo je to kvantový počítač?

- Kvantová mechanika - fyzikálna teória popisujúca správanie atómov a subatomárnych častíc.
- Kvantový počítač - zariadenie, ktoré na výpočty využíva princípy kvantovej mechaniky.

Kvantové počítače a ťažké problémy

- Na skoršom slajde som napísal:
  Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!
- To znamená, že dostatočne veľký kvantový počítač by dokázal zlomiť RSA.
- Ľudstvo pozná kvantové algoritmy na efektívne riešenie každého z ťažkých problémov, na ktorých sú postavené dnes bežne používané asymetrické šifry.
- Ak by existoval výkonný kvantový počítač, súčasná infraštruktúra na bezpečnú komunikáciu na internete by už nebola postačujúca.

Kvantové počítače a ťažké problémy

- Na skoršom slajde som napísal:
  Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!
- To znamená, že dostatočne veľký kvantový počítač by dokázal zlomiť RSA.
- Ľudstvo pozná kvantové algoritmy na efektívne riešenie každého z ťažkých problémov, na ktorých sú postavené dnes bežne používané asymetrické šifry.
- Ak by existoval výkonný kvantový počítač, súčasná infraštruktúra na bezpečnú komunikáciu na internete by už nebola postačujúca.

Kvantové počítače a ťažké problémy

- Na skoršom slajde som napísal:
  Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!
- To znamená, že dostatočne veľký kvantový počítač by dokázal zlomiť RSA.
- Ľudstvo pozná kvantové algoritmy na efektívne riešenie každého z ťažkých problémov, na ktorých sú postavené dnes bežne používané asymetrické šifry.
- Ak by existoval výkonný kvantový počítač, súčasná infraštruktúra na bezpečnú komunikáciu na internete by už nebola postačujúca.

Kvantové počítače a ťažké problémy

- Na skoršom slajde som napísal:
  Ľudstvo ale pozná efektívny algoritmus na faktorizáciu pre kvantové počítače!
- To znamená, že dostatočne veľký kvantový počítač by dokázal zlomiť RSA.
- Ľudstvo pozná kvantové algoritmy na efektívne riešenie každého z ťažkých problémov, na ktorých sú postavené dnes bežne používané asymetrické šifry.
- Ak by existoval výkonný kvantový počítač, súčasná infraštruktúra na bezpečnú komunikáciu na internete by už nebola postačujúca.

Na upokojenie

- Ľudstvo zatiaľ nevie postaviť dostatočne výkonné kvantové počítače!
- Ale intenzívne sa na tom pracuje!

Na upokojenie

- Ľudstvo zatiaľ nevie postaviť dostatočne výkonné kvantové počítače!
- Ale intenzívne sa na tom pracuje!

Kvantové počítače v súčasnosti

- Výkon kvantového počítača sa vyjadruje počtom qubitov.
- Najväčšie kvantové počítače v súčasnosti majú 70 qubitov.
- Na zlomenie RSA by sme potrebovali kvantový počítač s výkonom 20 miliónov qubitov.

Kedy budú výkonné kvantové počítače?

- Ťažká otázka.
- Niektorí vedci tvrdia, že je pravdepodobné, že do 20 rokov budú existovat kvantové počítače schopné zlomiť RSA.

Kedy budú výkonné kvantové počítače?

- Ťažká otázka.
- Niektorí vedci tvrdia, že je pravdepodobné, že do 20 rokov budú existovat kvantové počítače schopné zlomiť RSA.

Contents

Problémy ťažké aj pre kvantový počítač

- Existujú výpočtové problémy, pre ktoré ľudstvo nepozná efektívny kvantový algoritmus.
- Príklad: Dekódovací problém.

Dekódovací problém

- Nech $k < n$.
- Nech $\mathbf{m}$ je vektor bitov dĺžky k.
- Nech $\mathbf{e}$ je vektor bitov dĺžky n s malým počtom jednotiek. Počet jednotiek vo vektore $\mathbf{e}$ označíme ako w.
- Nech $\mathbf{G}$ je náhodne generovaná matica bitov s plnou hodnosťou a s rozmerom $k \times n$.
- Nech

$$\mathbf{y} = \mathbf{mG} + \mathbf{e}.$$

- Úloha:
  Sú známe $\mathbf{y}$, $\mathbf{G}$, w.
  Zistite $\mathbf{m}$.

Postkvantové šifry

- Na dekódovacom probléme (a aj na niektorých iných problémoch) vieme postaviť asymetrické šifry, ktoré by mali byť odolné aj voči kvantovému počítaču.
- Takéto šifry voláme postkvantové šifry.
- Vývoj kvalitných nových šifier a implementácia novej infraštruktúry na bezpečnú komunikáciu na internete si vyžaduje veľa času.
- Preto sa už teraz veľká časť kryptografickej komunity venuje postkvantovej kryptografii.

Postkvantové šifry

- Na dekódovacom probléme (a aj na niektorých iných problémoch) vieme postaviť asymetrické šifry, ktoré by mali byť odolné aj voči kvantovému počítaču.
- Takéto šifry voláme postkvantové šifry.
- Vývoj kvalitných nových šifier a implementácia novej infraštruktúry na bezpečnú komunikáciu na internete si vyžaduje veľa času.
- Preto sa už teraz veľká časť kryptografickej komunity venuje postkvantovej kryptografii.

Postkvantové šifry

- Na dekódovacom probléme (a aj na niektorých iných problémoch) vieme postaviť asymetrické šifry, ktoré by mali byť odolné aj voči kvantovému počítaču.
- Takéto šifry voláme postkvantové šifry.
- Vývoj kvalitných nových šifier a implementácia novej infraštruktúry na bezpečnú komunikáciu na internete si vyžaduje veľa času.
- Preto sa už teraz veľká časť kryptografickej komunity venuje postkvantovej kryptografii.

NIST

- NIST je americký inštitút pre štandardy a technológiu.
- V roku 2016 vyhlásil NIST súťaž NIST Post-Quantum Cryptography Standardization Process.
- Cieľom súťaže je vytvoriť kryptografické štandardy odolné voči kvantovým počítačom.
- Do decembra 2017 mohli vedecké tímy z celého sveta posielať do súťaže návrhy šifier odolných voči kvantovému počítaču.
- Prišlo 69 návrhov.
- Tieto návrhy sú verejné a sú verejne analyzované kryptografickou komunitou.
- Do druhého kola súťaže prešlo 26 návrhov.
- Očakávaný koniec súťaže: 2022-2024

Postkvantová kryptografia na FEI STU

- Ľudia:
  - Otokar Grošek
  - Pavol Zajac
  - Viliam Hromada
  - TF
- Analýza existujúcich návrhov postkvantových šifier.
- Návrhy nových postkvantových šifier.

Postkvantová kryptografia na FEI STU

- NATO SPS project: Secure Implementation of Post-Quantum Cryptography.
  - 2013-2016
  - Účastníci:
    - Tel Aviv University, Israel
    - Florida Atlantic University, USA
    - Jean Monnet University, France
    - FEI STU
- NATO SPS project: Secure Communication in the Quantum Era.
  - 2018-2021
  - Účastníci:
    - Florida Atlantic University, USA
    - Universidad Rey Juan Carlos, Spain
    - University of Malta
    - FEI STU

Contents

Odporúčané zdroje

- Stránka súťaže NIST Post-Quantum Cryptography Standardization Process: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- Správa NISTu o hrozbe kvantového počítača: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
- Postkvantové šifry odporúčané skupinou významných kryptografov: https://pqcrypto.eu.org/docs/initial-recommendations.pdf