Kvantové počítače – algoritmy (RSA a faktorizace čísla)

http://marble.matfyz.cz

14. 4. 2004

1. Algoritmus RSA

- Asymetrické šifrování. Existuje dvojice tajného a veřejného klíče, takže není nutné předat klíč jiným bezpečným kanálem.
- Generování klíče (prováděno pouze jedenkrát):
  - zvolí se dvě velká náhodná prvočísla p a q,
  - $n = pq$,
  - $\varphi(n) = (p-1)(q-1)$ ... Eulerova funkce,
  - zvolí se e, f taková, že $ef \equiv 1 \ \{\mathrm{mod}\ \varphi(n)\}$.
- Po vygenerování klíče se zcela smažou čísla p a q (nebudou už na nic potřeba), číslo e se spolu s n publikuje jako veřejný klíč dostupný komukoliv. Číslo f se bezpečně uchová jako tajný (privátní) klíč.
- Šifrovaná zpráva se rozdělí do (dostatečně velkých) bloků reprezentovaných číslem a. Zašifrováním vznikne číslo s:

$$s = a^e \quad \{\mathrm{mod}\ n\}$$

- Pomocí tajného klíče se zpráva opět dešifruje:

$$a = s^f \quad \{\mathrm{mod}\ n\}$$

- Vzhledem k použití modulární aritmetiky se část informace o hodnotě a^e ztratí a zprávu nelze jednoduše dešifrovat pomocí čísla e (například odmocněním).
- Dešifrování funguje na základě Eulerovy věty

$$a^{\varphi(n)} \equiv 1 \quad \{\mathrm{mod}\ n\}$$

pro a, n nesoudělné.

Platí totiž, že $ef = k\,\varphi(n) + 1$, kde $k \in \mathbb{N}$. Pak

$$\left(a^e\right)^f = a\left(a^{\varphi(n)}\right)^k$$

a podle Eulerovy věty je člen $a^{\varphi(n)}$ v modulární aritmetice roven jedné.

- Bezpečnost algoritmu je založena na obtížnosti faktorizace známého čísla n. Pokud budeme znát čísla p a q, není problém odvodit z veřejného klíče klíč tajný.

2. Faktorizace

- Nemožnost faktorizovat složené číslo v polynomiálním čase není dokázána. Nicméně není znám žádný (klasický) algoritmus, který by ji v polynomiálním čase dokázal provést.
- *Shorův algoritmus* provádí faktorizaci v polynomiálním čase s použitím kvantového počítače.[1]
- Faktorizované číslo n je součinem dvou prvočísel p a q. Funkce

$$f_{a,n}(x) := a^x \bmod n$$

pro číslo a menší než n a nesoudělné s n je periodická s periodou r ($r < n$).

Pokud je r sudé a platí, že $(a^{r/2} \bmod n) \neq (n-1)$, pak jsou hledaná prvočísla:

$$p = \mathrm{NSD}(a^{r/2} + 1, n)\,,$$

$$q = \mathrm{NSD}(a^{r/2} - 1, n)\,.$$

---

[1] Kvůli technickým problémům s realizací byla zatím reálně faktorizována jen velmi malá čísla, takže šifrování používané všude na internetu zatím ohroženo není.

– Číslo a zvolíme náhodně. Pokud je soudělné s n, pak $p = \mathrm{NSD}(a, n)$. V opačném případě použijeme výše popsaný postup. Podmínky jsou pro náhodné a splněny s pravděpodobností vyšší než 0,5.
– *Euklidův algoritmus* pro nalezení $\mathrm{NSD}(a, b)$ v polynomiálním čase:

  - BÚNO platí $a > b$,
  - je-li $b = 0$, pak $\mathrm{NSD}(a, b) = a$,
  - jinak $\mathrm{NSD}(a, b) = \mathrm{NSD}(b, a \bmod b)$.

  Po dvou iteracích bude místo b hodnota $(b \bmod (a \bmod b))$, která je určitě menší než $b/2$. Takže pro k-bitové číslo je třeba maximálně $2k$ iterací.
– Zbývá jediná operace, pro kterou zatím nemáme polynomiálním algoritmus – určení periody funkce $f_{a,n}(x)$.

3. Výpočet funkce $f_{a,n}$ a určení periody

- Provedeme kvantový výpočet funkce se vstupním registrem šířky $2L$. Počítač po něm bude ve stavu

$$\frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} |x\rangle_{\text{in}} |f_{a,n}(x)\rangle_{\text{out}} \,.$$

  Hodnota $L \in \mathbb{N}$ je zvolena tak, aby $2^L \geq n$.
- Měřením na *výstupním* registru získáme na *vstupním* registru superpozici všech argumentů, které odpovídají hodnotě $f_{a,n}$ změřené na výstupu.
- Po měření na výstupním registru tedy na vstupním zbývá superpozice hodnot, které tvoří periodickou posloupnost s periodou r, ovšem posunutou o neznámou hodnotu danou konkrétním změřeným výstupem.
- Při měření na *vstupním* registru dostáváme jednotlivé hodnoty, ze kterých lze odhadnout periodu funkce, ale pro danou minimální pravděpodobnost roste počet potřebných výpočtů a měření exponenciálně s délkou vstupu.
- Pokud dokážeme na vstupním registru (*po* měření na *výstupním* registru) provést *Fourierovu transformaci*, zbavíme se tím posunu a počet opakování měření nutný pro danou pravděpodobnost už poroste jen polynomiálně.

4. Diskrétní Fourierova transformace

- Definice:

$$(\mathcal{F}f)(k) := \frac{1}{N}\sum_{x=0}^{N-1} f(x)\exp\left(-2\pi i\frac{xk}{N}\right)$$

  pro transformaci posloupnosti $f(x)$ o N prvcích.
- Pokud má exponenciální člen stejnou periodu jako funkce (posloupnost) f, sčítají se příspěvky stejného směru a získáme hodnotu s maximální absolutní velikostí.
- Aplikace na vstupní registr délky $2L$:

$$|x\rangle_{\text{in}} \to \frac{1}{2^L}\sum_{y=0}^{2^{2L}-1}\exp\left(2\pi i\frac{xy}{2^{2L}}\right)|y\rangle_{\text{in}}\,,$$

$$\sum_{x=0}^{2^{2L}-1} c_x|x\rangle_{\text{in}} \to \sum_{y=0}^{2^{2L}-1}\left[\frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}\exp\left(2\pi i\frac{xy}{2^{2L}}\right)c_x\right]|y\rangle_{\text{in}}\,.$$

- Po měření na vstupním registru tedy získáme nejpravděpodobněji hodnoty blízké násobkům $2^{2L}/r$, kde r je hledaná perioda.

5. Závěr

- Shorův algoritmus řeší faktorizaci složeného čísla v polynomiálním čase.
- Jde o pravděpodobnostní algoritmus, takže někdy nemusí dát správný výsledek. Ovšem pro danou minimální pravděpodobnost závisí složitost výpočtu na délce vstupu polynomiálně.
- Výpočet na kvantovém počítači je navíc omezen pravděpodobností vzniku chyby. Tato pravděpodobnost roste velmi rychle s narůstajícím časem výpočtu.
- Pravděpodobnost bezchybného výpočtu s L qubity, který trvá čas t je úměrná

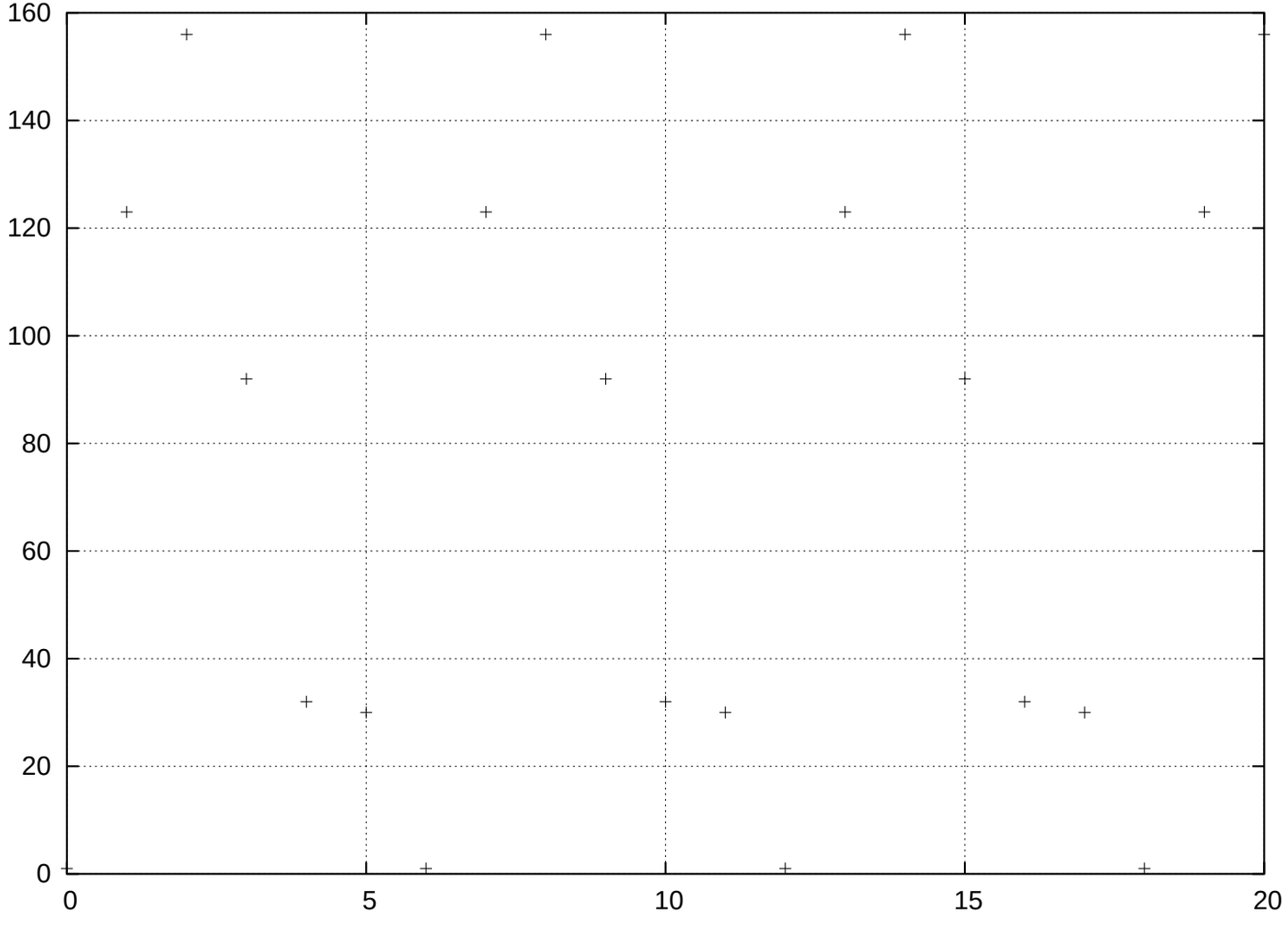
$$\exp(-Lt)\,.$$

- Toto způsobuje exponenciální závislost počtu nutných opakování na délce vstupu.
- U klasických počítačů existuje stejný problém, ale pravděpodobnost chyby je zanedbatelně malá i při velkých časech a počtech bitů.
- Možným řešením je použít samoopravné kódy.

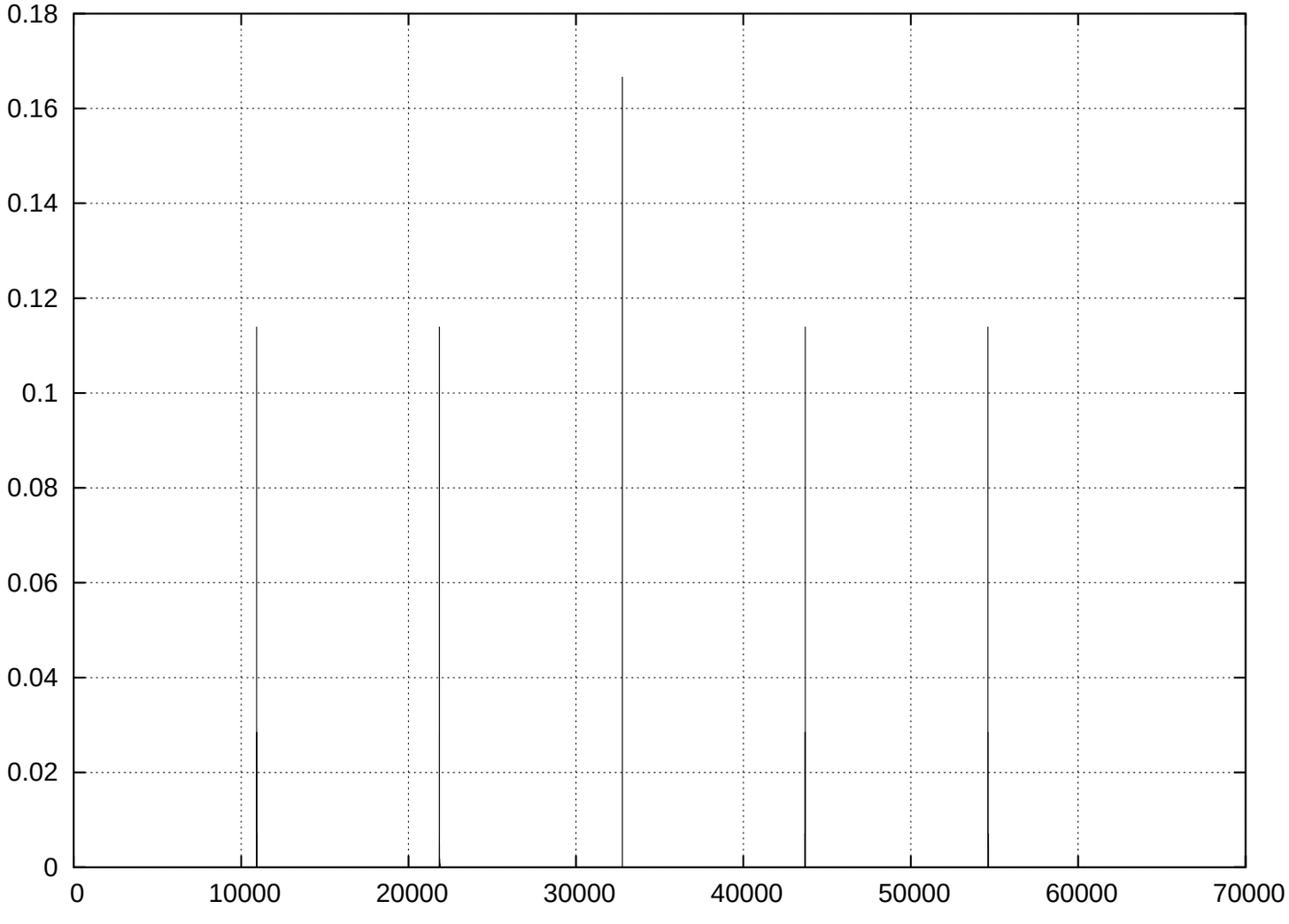
6. Literatura

- Miloslav Dušek: Koncepční otázky kvantové teorie, Olomouc, 2002
- Matthew Cobby: Fourier Tutorial (text dostupný na webu)
- blíže nespecifkované zápisky z různých přednášek

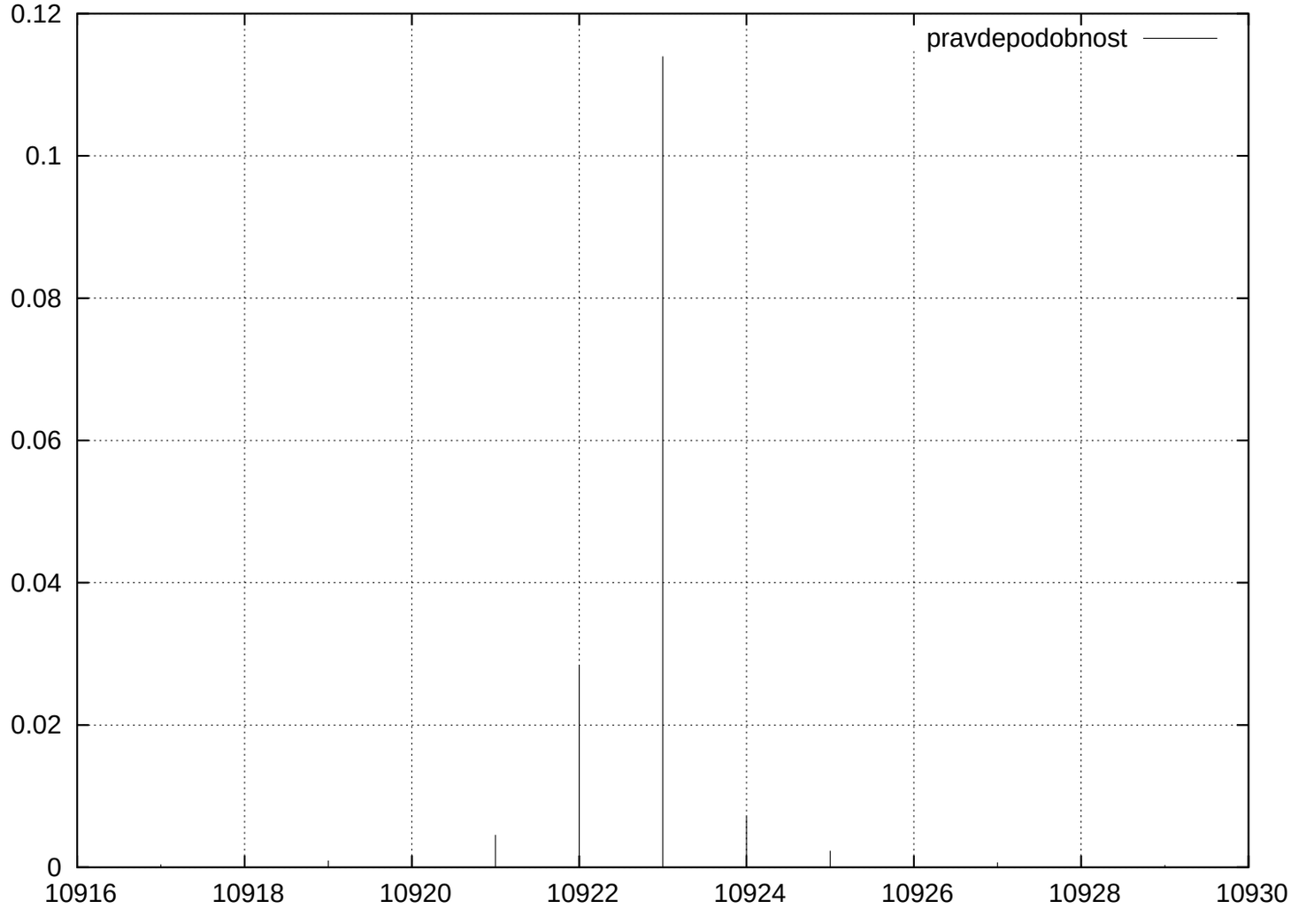
7. Obrázky



Hodnoty $f_{a,n}(x)$ pro $a = 123$ a $n = 217$.



Pravděpodobnosti hodnot ve vstupním registru po provedení DFT.



Pravděpodobnosti hodnot ve vstupním registru po provedení DFT (detail).