Sdílení tajemství

Prezentace na předmět UKRY

David Celný

12. března 2014

Požadavky na sdílená hesla

Cíle

- k odemknutí potřebujeme více sub hesel
- težké (nemožné) prolomení hesla s nedostatečným počtem sub-hesel
- odpovídající velikost všech sub-hesel a hlavního hesla
- (bonus) generování sub-hesla bez nutnosti měnit hlavní heslo
- (bonus) různé váhy jednotlivých hesel

Přístupy řešení

Přístupy

- Naivní přístup (prosté dělení, náhodné rozdíly, XOR)
- Mignottův přístup
- Asmuthův-Bloomův přístup
- Blakleův přístup
- Shamirův přístup

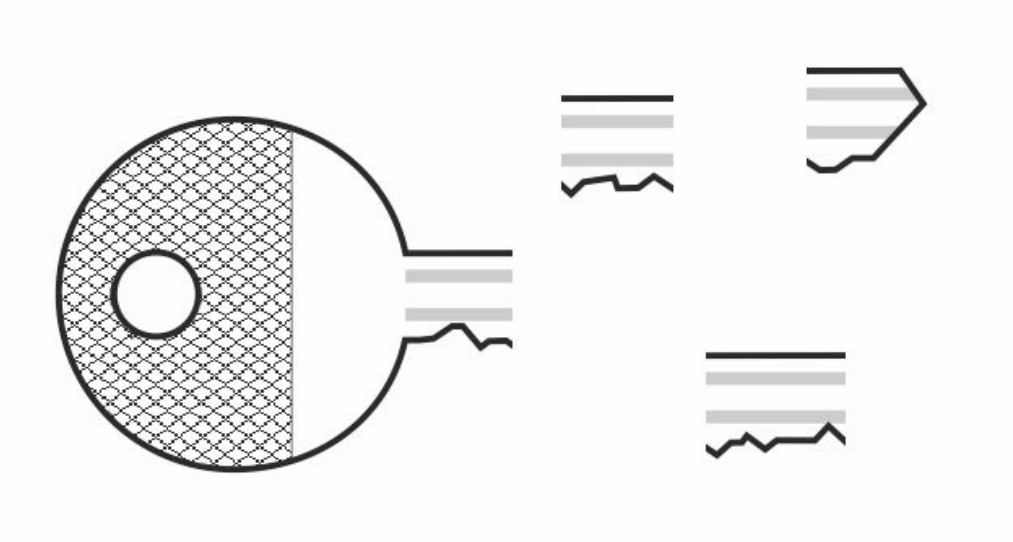
Označení

- n délka hlavního hesla
- k počet sub-hesel
- u minimální počet nutný k odemknutí

Naivní přístup

Prosté dělení

- lehké prolomení hlavního hesla
- sub heslo je délky $\frac{n}{k}$, celková velikost sub-hesel je n
- $u = k$ jinak nelze



Lepší přístupy

Náhodné rozdíly

- nemožné prolomení hlavního hesla bez všech sub-hesel
- $u = k$ jinak nelze

XOR

- nemožné prolomení hlavního hesla bez všech sub-hesel
- z vlastnosti $(A \,\mathbf{xor}\, B) \,\mathbf{xor}\, B = A$
- $u = k$ jinak nelze

Čínská věta o zbytcích

Znění

Předpokládejme že $m_1, m_2, \ldots, m_k$ jsou navzájem po dvou nesoudělná přirozená čísla, $m_i \geq 2$ pro $i = \hat{k}$. Potom pro posloupnost přirozených čísel $(a_i)_1^k$ existuje číslo x které řeší následující systém kongruencí:

$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1) \\ x &\equiv a_2 \ (mod\ n_2) \\ &\vdots \\ x &\equiv a_k \ (mod\ n_k) \end{aligned}$$

Navíc platí, že všechna řešení x tohoto systému jsou kongruentní modulo $N = n_1 n_2 \ldots n_k$

Mignottův přístup

Princip, vlastnosti

- pomocí Mignottovi posloupnosti $M(u, k)$ pro kterou platí
  - $m_1 < m_2 \cdots < m_k$ kde m_i jsou po dvou nesoudělná
  - $\prod_{i=k-u+2}^{k} m_i < \prod_{i=1}^{u} m_i$ kde S volíme mezi produkty
- sub-heslo $\{s_i, m_i\}$ získáme jako $s_i = S \ mod \ m_i$
- velikost sub-hesel $= 2 * u$
- následně generování dalších sub-hesel už je obtížnější

Asmutův-Bloomův přístup

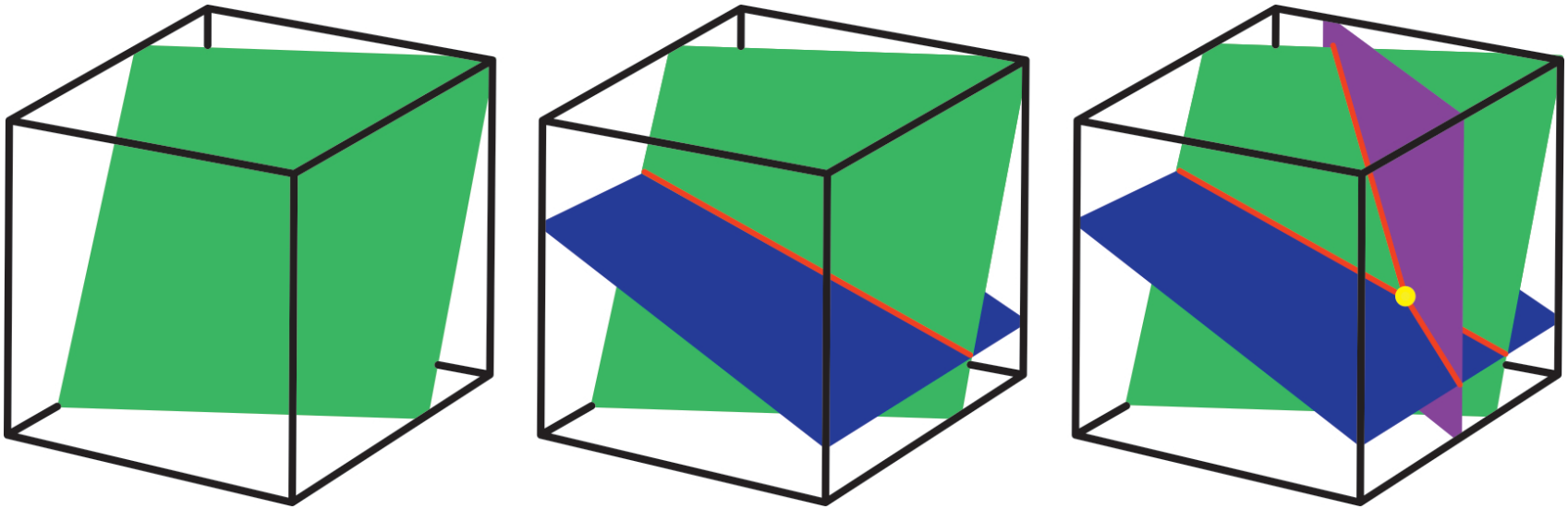
Princip, vlastnosti

- pomocí Asmuthovy-Bloomovy posloupnosti $AB(u, k)$ pro kterou platí
  - $m_0 < m_1 < m_2 \cdots < m_k$ kde m_i jsou po dvou nesoudělná
  - $m_0 * \prod_{i=k-u+2}^{k} m_i < \prod_{i=1}^{u} m_i$
  - S volíme z $\mathbb{Z}/m_0\mathbb{Z}$ a α tak že $S + \alpha * m_0 < \prod_{i=1}^{u} m_i$
- sub-heslo $\{s_i, m_i\}$ získáme jako $s_i = (S + \alpha * m_0)\ mod\ m_i$
- velikost sub-hesel $= 2 * u$
- následně generování dalších sub-hesel už je obtížné
- bezpečnější oproti Mignottovi kde sub-hesla obashují informaci o S

Blakleův přístup

Princip, vlastnosti

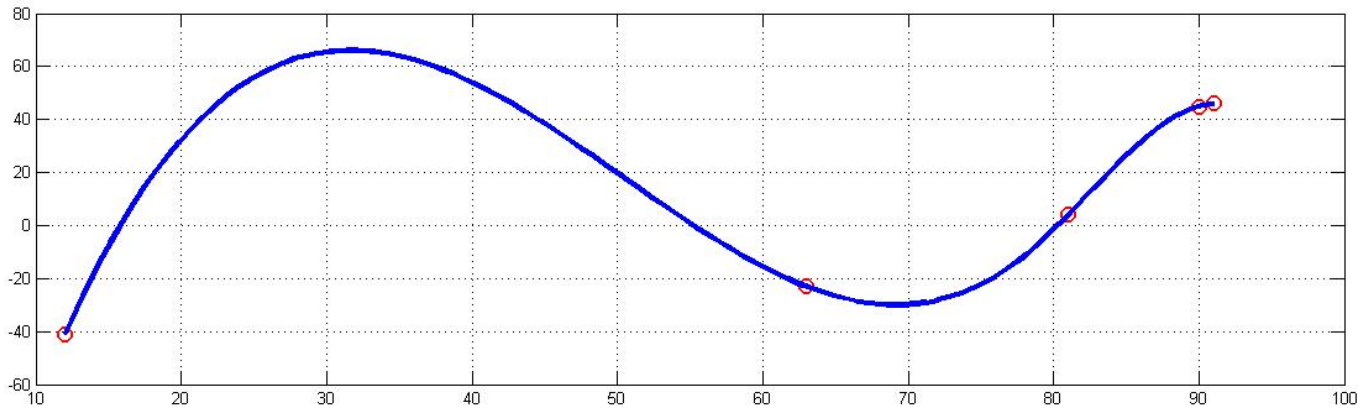
- z vlastnosti určení bodu v prostoru jako průsečík $h \nparallel$ nadrovin
- rovnice nadroviny: $a_1 x_1 + a_2 x_2 + \cdots + a_h x_h = b$
- celková velikost sub-hesel $\doteq u * (u + 1)$
- možnost generovat další, při speciální volbě těžké prolomit



Shamirův přístup

Princip, vlastnosti

- polynomiála stupně r je jednoznačně určena $r+1$ body
- polynomiála: $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{r+1} x^{r+1}$
- celková velikost sub-hesel $\doteq 2 * u$
- možnost generovat další, těžké prolomit



Na závěr

Shrnutí

- představeno několik možných přístupů
- poskytnuto strovnání těchto přístupů
- ukázka čínské věty o zbytcích
- nejlépe vychází Shamirův-Princip založený na chování polynomů

Obrázek : Čínský ekvivalent pro zbytek

Reference

Reference

- http://www.datagenetics.com/blog/november22012/index.html
- http://en.wikipedia.org/wiki/Secret_sharing
- http://en.wikipedia.org/wiki/Chinese_remainder_theorem
- Použité obrázky jsou autorské (jejich použití jen se souhlasem autora)