Kryptografické protokoly

Stříbrnice, 12.-16.2. 2011

Kryptografie

- Nauka o metodách utajování smyslu zpráv a způsobech zajištění bezpečného přenosu informací
- xTeorie kódování
- xSteganografie

Historie

Klasická kryptografie

- 3000 př.n.l. - Egypt, netradiční hyeroglify
- 500 př.n.l. - Řecko, skytale
- 50 př.n.l. - Řím, Caesar

Moderní kryptografie

- 2.sv.v. - Enigma

Kryptografické protokoly

- Kryptografický protokol – algoritmus, kterým se řídí 2 (nebo více) subjektů, aby mezi nimi proběhla bezproblémová spolupráce.
- Míra důvěry by měla být minimální
- Budeme se zabývat protokoly pro řešení „zdánlivě neřešitelných problémů“ (seemingly unsolvable problems)

Házení mincí

- Alice a Bob se rozvedli a už si navzájem nevěří. Po telefonu chtějí náhodně vybrat toho, kdo získá auto.

Házení mincí

- Alice a Bob se rozvedli a už si navzájem nevěří. Po telefonu chtějí náhodně vybrat toho, kdo získá auto.

- Protokol 1:
- Alice pošle Bobovi zašifrovaně panna nebo orel, pomocí jednosměrné funkce f. Bob si tipne, který z kryptotextů je panna, pokud si tipl správně, získá auto. Pro kontrolu pak Alice pošle Bobovi f.

Házení mincí

- Protokol 2:
- Alice si vybere 2 velká prvočísla p,q. Pošle Bobovi n=pq. Bob si vybere $y \in \{1,\ldots, n/2\}$ a pošle Alici x=y^2 mod n. Alice spočítá všechny 4 druhé odmocniny z x: x_1, n-x_1, x_2, n-x_2. Má tedy 2 možnosti vhodného y, pokud si tipne správně, dostane auto.

Házení mincí

- Obě strany by měly ovlivňovat výsledek a akceptovat ho. Pravděpodobnosti výher obou hráčů by měly být stejné.
- Výsledek protokolu by měl být 0,1 nebo zamítnuto
- Pokud se obě strany chovají správně, výsledek by měl být 0 nebo 1. Pokud ne, pak je zamítnuto
- Problém: Pokud jedna strana zná výsledek dříve, pak by mohla zajistit možnost zamítnuto

Házení mincí pomocí jednosměrné funkce

- Alice vybere funkci f a pošle definiční obor Bobovi
- Bob vybere x,y z D(f) a pošle je Alici
- Alice pošle Bobovi jedno z f(x), f(y)
- Bob si tipne, které z nich to je
- Alice mu řekne jestli si tipnul správně nebo špatně
- Pokud jí to Bob nevěří, pošle mu f

Problém: Alice může najít takovou funkci, že f(x)=f(y) pro lib. x,y

Bitový závazek

- Alice si vybere bit b a zaváže se k němu
- Alice už nemá šanci ho změnit
- Bob se nemůže dozvědět, jaký bit si Alice vybrala

Bitový závazek

- Alice si vybere bit b a zaváže se k němu
- Alice už nemá šanci ho změnit
- Bob se nemůže dozvědět, jaký bit si Alice vybrala

Bez počítačů:

- Alice napíše na papírek b a zamkne ho do skříňky, v otevřené fázi dá Bobovi klíč, aby se přesvědčil, že je tam opravdu b

Bitový závazek

Protokol 1:

- Alice zvolí jednosměrnou funkci f a sudé (liché) číslo x, jestliže zvolený bit je 0 (1) a pošle Bobovi f(x) a f
- Problém – Alice může znát liché x a sudé y takové, že f(x)=f(y)

Bitový závazek

Protokol 2:

- Alice zvolí f, 2 nahodná čísla x,y a bit b. Bobovi pošle (f(x,y,b),x). Ověření – pošle Bobovi trojici f,x,y

Bitový závazek

- Má 2 části:
  - Závazek – pomocí zobrazení f: {0,1} x $X \rightarrow Y$, kde X, Y jsou konečné množiny. Závazek potom je f(b,x), kde x je z X
  - Otevřená fáze – člověk se závazkem pošle pro kontrolu potřebné informace druhému

Bitový závazek

- Každý protokol pro bitový závazek by měl splňovat:
  - Pro žádné b a x, by Bob neměl být schopen z f(b,x) určit b
  - V otevřené fázi by Alice měla být schopná říct b a x, tak že f(b,x) je poslaný závazek, ale neměla by toho být schopná pro opačné b
  - Pokud se oba chovají správně, pak se přijímatel vždy dozví b

Bitový závazek s jednosměrnou funkcí

- Domluví se na funkci f
- Bob zvolí náhodně x a pošle ho Alici
- Alice zvolí náhodně y a její bit b. Pošle Bobovi f(x,y,b)
- V otevřené fázi Alice pošle Bobovi y a b
- Bob spočítá f(x,y,b) a porovná to s přijatou hodnotou

Házení mincí pomocí bitového závazku

- Každý protokol na bitový závazek se dá využít k házení mincí následovně:
  - Alice si „hodí“ mincí a k výsledku-A se zaváže pomocí bitového závazku, který pošle Bobovi
  - Bob si také hodí mincí a výsledek-B pošle Alici
  - Alice zveřejní svůj závazek
  - Bob i Alice spočítaji b=A XOR B

  Problém?
  - Alice ví výsledek už po druhém kroku a Bob ne, tedy může podvádět a tím se dostat do stavu zamítnuto

Bitový závazek pomocí zašifrování

- Bob zvolí náhodný řetězec r a pošle ho Alici
- Alice zašifruje rb pomocí kryptovacího algoritmu E s klíčem k a pošle výsledek Bobovi
- V otevřené fázi Alice pošle Bobovi klíč k

- Bez Bobova náhodného řetězce r by Alice mohla vědět klíč l takový, že Ek(b)=El(b')

Oblivius transfer

- Alice zná více tajemství, chce jedno z nich říct Bobovi a to tak, že Alice nebude vědět, které z nich se Bob dozvěděl
- Alice zná tajemství a chce, aby se ho Bob dozvěděl s pravděpodobností ½ a se stejnou pravděpodobností, aby se dozvěděl odpad. Bob ví, jestli získal tajemství. Alice to neví.

Oblivious transfer

- Alice si zvolí 2 velká prvočísla a pošle Bobovi n=pq
- Bob si zvolí náhodné x a pošle y=x^2 mod n
- Alice spočítá 4 odmocniny (x_1, $-x_1$, x_2, $-x_2$), vybere si jedno z x_1, x_2 a pošle ho Bobovi
- Pokud se trefila do Bobova x, Bob nezíská žádnou novou informaci, pokud ne, Bob získal druhou druhou odmocninu, tedy je schopný faktorizovat n

1-out-of-2 oblivious transfer

- Alice ví dvě tajemství, Bob si vybere jedno z nich, Alice netuší které
- Můžeme si to představit jako krabici se vstupy x_0, x_1, Bob si zvolí c. Výstup je x_c.
- Díky tomu jsme schopni počítat f(x,y) pro libovolnou binární funkci, kde jen Alice zná x a jen Bob y. Oba se dozví f(x,y), ale ani jeden se nedozví nic o y nebo x.

1-out-of-2 oblivious transfer

Protokol:

- Alice si zvolí 2 klíče pro PKC P a pošle je Bobovi
- Bob zvolí klíč k pro SKC S, zašifruje ho pomocí P a jednoho z klíčů a pošle Alici
- Alice je dešifruje a získá klíč k a odpad g. Neví, co je co.
- Alice zašifruje její dvě tajemství. Jedno pomocí k a druhé pomocí g.
- Bob dešifruje obě podle k. Jedno je úspěšné.

Bitový závazek pomocí oblivious transfer

- Alice si zvolí náhodný bit r a její závazek b
- Do OT-box dá vstupy x_0=r a x_1=r xor b
- Bob si zvolí c a získa x_c

Otevřená fáze:

- Alice pošle Bobovi r a b
- Bob zkontroluje, jestli x_c=r xor bc

1-out-of-2 oblivious transfer

- Jak můžou podvádět?
- Jak upravit protokol, aby šance na podvádění byla menší než 2^{-64}?

Hraní karet po telefonu (2 hráči)

- Všechny karty v ruce jsou stejně pravděpodobné
- Karty Alice a Boba jsou disjunktní
- Oba hráči znají svoje karty, ale ne karty protihráče
- Každý z nich je schopný poznat, když druhý podvádí

Hraní karet po telefonu (2 hráči)

Protokol:

- Bob zakóduje každou kartu pomocí e_B a pošle je v náhodném pořadí Alici
- Alice vybere 5 z nich a pošle je Bobovi (to je Bobova ruka)
- Alice vybere dalších 5 karet, zašifruje je pomocí e_A a pošle je Bobovi
- Ten je dešifruje pomocí d_B a pošle je zpět Alici, ta je dešifruje a to je její ruka

Karty – 3 hráči

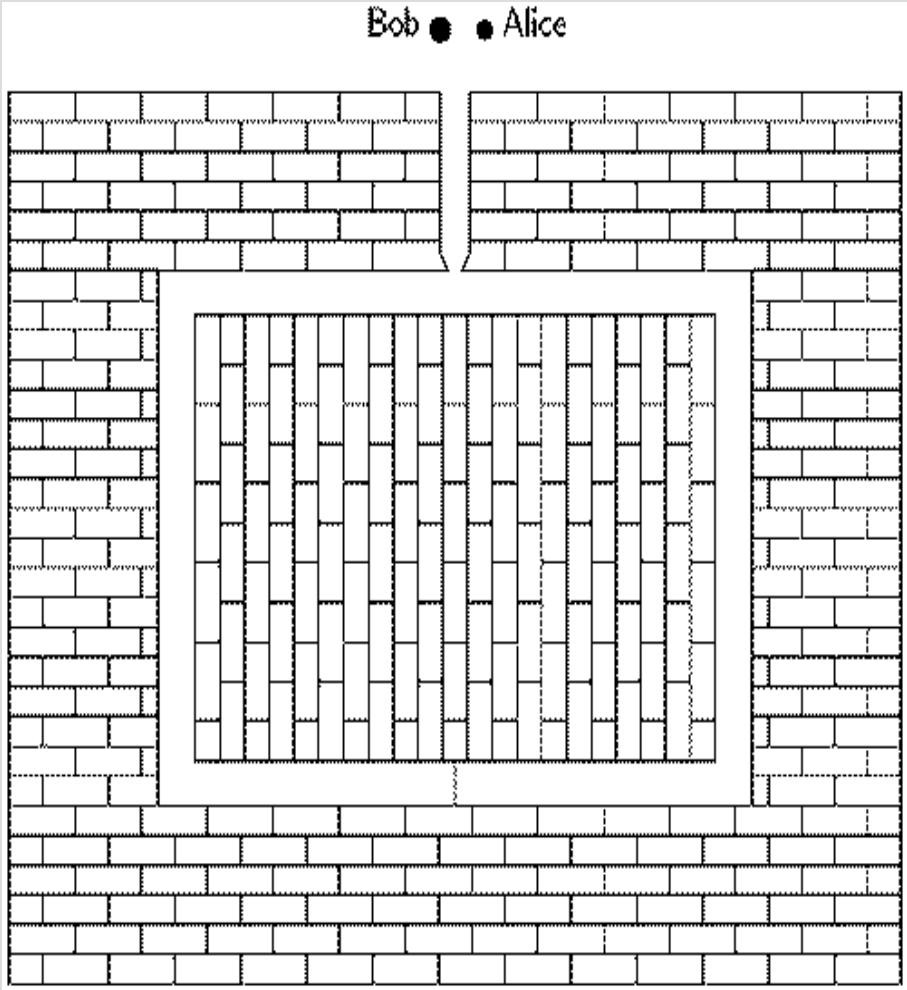
- Alice zakóduje všech 52 karet $e_A(w_i)$ a pošle je Bobovi
- Ten vybere 5 z nich, zakóduje je pomocí e_B a zbylé karty pošle Carol
- Carol si vybere 5 a zakóduje je pomocí e_C
- Bob a Carol pošlou svých 5 karet Alici, ta je dekóduje pomocí d_A a pošle jim je zpět
- Bob a carol dekódují svoje karty
- Bob vybere 5 karet ze zbylých karet a pošle je Alici

Zero-knowledge proof

- Dokazující chce přesvědčit kontrolovatele, že zná nějakou informaci bez toho, aby se o ní kontrolovatel cokoliv dozvěděl

- Například n=670592745=12345x54321, to je důkaz toho, že n není prvočíslo. Rozhodně ale není zero-knowledge

Zero-knowledge proof



Neizomorfnost grafů

- Vstup: Dva grafy G_1 a G_2 s množinou uzlů {1,..,n}
- Vic zvolí $i \in \{1,2\}$ a permutaci množiny {1,..,n} a pošle Peggy graf H, který je vytvořen z G_i pomocí dané permutace
- Peggy pošle zpět $j \in \{1,2\}$ takové, že G_j je takové, že je izomorfní s H
- Vic zkontroluje, jestli se i=j
- Tento proces zopakují n-krát

Věkový problém

- Bob (věk j) a Alice (i) chtějí zjistit, kdo z nich je starší, aniž by prozradili svůj věk
- Bob si zvolí náhodné x a spočítá $k=e_A(x)$ a pošle Alici $s=k-j$
- Alice spočítá čísla $y_u=d_A(s+u)$, $0<u<101$, pak zvolí velké prvočíslo p a spočítá $z_u=y_u \bmod p$
- Alice pošle Bobovi posloupnost $z_1,..z_i,z_{i+1}+1,...z_{100}+1$
- Bob zkontroluje, jestli je j-té číslo kongruentní s x modulo p

Zero-knowledge proof

- n=pq, kde p a q jsou velká prvočísla.Peggy chce přesvědčit Victora, že zná rozklad n. Vymyslela následující protokol:

- Zopakují 20krát:
  - Vic náhodně zvolí x<n a spočítá $y=x^2 \bmod n$
  - Peggy spočítá 4 odmocniny a jednu pošle Vicovy
  - Vic zkontroluje, jestli je to opravdu druhá odmocnina

Je to zero knowledge proof?