Protocoale pentru licitații securizate folosind angajamente de timp

Lucrare de licență

Absolvent
Apostol Alin-Constantin
Coordonator științific
Conf.dr. Ruxandra F. Olimid

FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
UNIVERSITATEA DIN BUCUREȘTI

Cuprins

1. Introducere
   1.1 Motivație
   1.2 Tipuri de licitații

2. Sisteme de angajament
   2.1 Sisteme de angajament Pedersen
   2.2 Sisteme pentru angamanete de timp Boneh-Naor

3. Protocoale pentru licitații securizate
   3.1 Protocolul Boneh-Naor
   3.2 Situația actuală a domeniului - Protocolul Riggs

Motivație

- 2020 - Ken Paxton pornește o urmărire în justiție împotriva Google în legătură cu manipularea licitațiilor de vânzare a reclamelor online [2].
- 2025 - Divizia Antitrust a Departamentului de Justiție SUA anunță o a doua victorie în instanță împotriva Google pe această tematică [5].
- Apare nevoia de dezvoltare de protocoale securizate pentru licitații.

1

[1] Sursa imaginii: `https://www.svgrepo.com/svg/430771/auction`

Tipuri de licitații

1. Licitații deschise - *English Auctions* sau *Dutch Auctions*.
   - Ofertele sunt anunțate public.
   - *English auctions* - se incepe de la un preț minim, participanții anunță oferte mai mari progresiv.
   - *Dutch auctions* - se incepe de la un preț mai mare, care se scade până când un participant acceptă oferta.
   - Necesită un **număr mare de runde** de comunicare.

Tipuri de licitații

2. Licitații cu ofetă secretă - *Vickrey Auctions*[7].
   - Ofertele sunt secrete, deschise la o dată ulterioară de către organizator pentru a determina câștigătorul.
   - Există mai multe metode de a hotărî prețul final. În cazul Vickrey, câștigătorul plătește al doilea cel mai mare preț.
   - Necesită **o singură rundă** de comunicare a ofertelor.
   - Stabilirea unui organizator în care toți participanții să aibă încredere este **dificilă**.

Licitații cu ofertă secretă

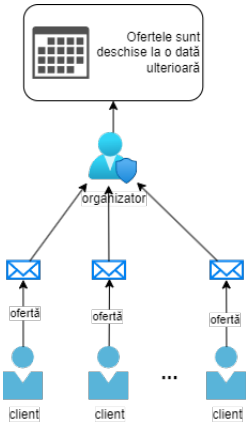

Figura: Licitație de tipul ofertă secretă

Ce sunt sistemele de angajament?

Sisteme de angamanet (*commitment schemes*)

Sunt protocoale criptografice care permit unui participant să realizeze un angajament asupra unei valori, ascunzând valoarea inițială, cu posibilitatea de a o devălui mai târziu prin publicarea valorii de deschidere a angajamentului.

Un astfel de sistem trebuie să:

- asigure confidențialitatea valorii inițiale. (*hiding*)
- ofere certitudinea că angajamentul este legat de valoarea inițială. (*binding*)

Etapele unui sistem de angajament

Un sistem de angajament este alcătuit, în general, din două etape:

1. **Etapa de angajament**: Alice alege o valoare de deschidere aleatoare și creează un angajament pentru o anumită valoare.
2. **Etapa de deschidere**: Alice publică valoarea de deschidere, iar Bob poate să alfe valoarea inițială legată de angajament.

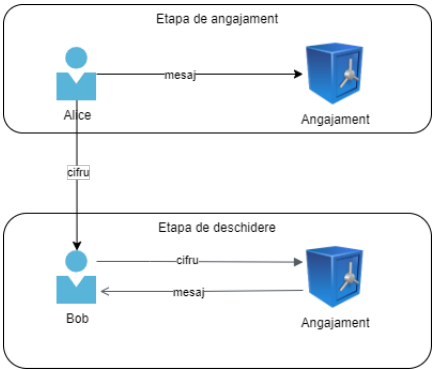

Figura: Abstractizare a unui sistem de angajament

Sisteme de angajament Pedersen

Este un sistem prezentat de T.P. Pedersen în lucrarea [4] care se bazează pe dificultatea rezolvării **problemei logaritmului discret** în criptografie [3].

1. **Etapa de angajament**:
   - Pentru un grup ciclic de ordin q număr prim G_q, Alice alege două numere $g, h \in G_q$ cu g generator, astfel încât să nu se cunoască valoarea $log_g h$ (problema logaritmului discret trebuie să fie dificilă).
   - Pentru un mesaj $m \in \mathbb{Z}_q$, Alice alege aleator $\alpha \in \mathbb{Z}_q$ și calculează valoarea angajamentului $C = g^m \cdot h^\alpha \bmod q$ pe care o trimite lui Bob.
2. **Etapa de deschidere**: Bob primește de la Alice valoarea de deschidere $\pi = (m, \alpha)$, apoi verifică faptul că $C = g^m h^\alpha \bmod q$.

Sisteme de angajament Pedersen

- **Confidențialitatea** valorii inițiale reiese din dificultatea rezolvării problemei logartimului discret pentru un adversar.
- Sistemul Pedersen oferă certitudinea că **valoarea angajamentului** C este **legată** de valoarea inițială m.

Sisteme pentru angajamente de timp - Boneh-Naor

Sistemele pentru angajamente de timp (*timed commitment schemes*) sunt o **extindere** a sistemelor de angajament clasice, oferind, în plus, o etapă de deschidere forțată.

- Acțiunea de deschidere forțată (*force opening phase*) presupune realizarea unui efort computațional secvențial considerabil, depinzând de un parametru de timp T, fără intervenția participantului care a creat angajamentul, în vederea obținerii valorii inițiale.
- Rezolvă următoarea problemă: dacă Alice refuză să ofere valoarea de deschidere sau o pierde, Bob poate să execute acțiunea de recuperare forțată, obținând mesajul inițial M în cel mult timp T.

Sisteme pentru angajamente de timp - Boneh-Naor

Aceste sisteme trebuie să îndeplinească următoarele proprietăți [1]:

- Recuperare **verificabilă**
- Recuperare **demonstrabilă**
- Recuperare **imună la atacuri paralele** [1]:

$$\left|\Pr\left(\mathcal{A}(\text{angajament}, M) = \text{“da”}\right) - \Pr\left(\mathcal{A}(\text{angajament}, R) = \text{“da”}\right)\right| < \epsilon$$

Inițializarea sistemului Boneh-Naor

- Alice generează aleator două numere prime p, q cu $|p| = |q| = \lambda$ și $p \equiv q \equiv 3 \pmod 4$, apoi calculează $N = pq$ pe care îl trimite lui Bob, unde λ reprezintă un parametru de securitate.
- Se stabilește parametrul de timp T care reprezintă *timpul* necesar execuției etapei de deschidere forțată a angajamentului. În cadrul acestui sistem, dacă $T = 2^k$ atunci vor fi necesare 2^k înmulțiri modulare pentru a finaliza faza de deschidere forțată [1].

Etapa de angajament

Alice dorește să realizeze un angajament care să conțină un mesaj $M \in \{0,1\}^n$, atunci ea și Bob trebuie să parcurgă următorii pași [1]:

1. Alice calculează $Q = \prod_{i=1}^{b} q_i^N$, unde $q_1, q_2, ..., q_b$ reprezintă numerele prime mai mici decât un parametru B, apoi alege aleator un element $h \in \mathbb{Z}_N$ și calculează $g = h^Q \pmod N$.
2. Persoana care dorește să facă angajamentul calculează $u = g^{2^{2^k}} \pmod N$, calculând întâi valoarea intermediară $a = 2^{2^k} \pmod{\phi(N)}$, apoi $u = g^a \pmod N$.
3. În cadrul acestui pas se determină valoarea S a angajamentului, cu $S_i = M_i \oplus lsb(g^{2^{2^k - i}} \mod N)$. Alice trimite $C = (h, g, u, S)$ către Bob.

Recuperare verificabilă

Pentru ca sistemul să îndeplinească proprietatea de **recuperare verificabilă**, Alice trebuie să îi dovedească lui Bob faptul că algoritmul pentru etapa deschidere forțată se va încheia cu succes, dezvăluind valoarea M, fără a executa efectiv acel algoritm pentru a verifica acest fapt. Această proprietate a algoritmului se demonstrează prin verificarea că u este construit în mod corect, adică $u = g^{2^{2^k}} \pmod{N}$.
Alice construiește șirul de valori

$$W = (g^2, g^4, g^{16}, g^{256}, \ldots, g^{2^{2^i}}, g^{2^{2^k}}) \mod N$$

Apoi arată că în fiecare triplet de forma $(g, w_{i-1}, w_i), \forall i \in \{1, 2, \ldots, k\}$ este adevărat că $w_{i-1} = g^x, w_i = g^{x^2}, \forall i \in \{1, 2, \ldots, k\}$, adică $w_{i-1}^2 = w_i \pmod{N}, \forall i \in \{1, 2, \ldots, k\}$.

Etapa de deschidere

1. Bob calculează și el valoarea $Q = \prod_{i=1}^{b} q_i^N$.
2. Alice trimite valoarea $v' = h^{2^{2^k - n}}$ către verificator. Acesta calculează $v = v'^Q \bmod N$ și verifică faptul că $v^{2^n} = u \bmod N$.
3. Având acum la dispoziție valoarea $v = g^{2^{2^k - n}} \bmod N$, Bob poate să calculeze fiecare componentă din cheia $K = K_1 K_2 K_3 ... K_n$ astfel: $K_i = lsb(v^{2^{(n-i)}}) = lsb((g^{2^{2^k - n}})^{2^{(n-i)}}) = lsb(g^{2^{(n-i)} \cdot 2^{2^k - n}}) = lsb(g^{2^{2^k - i}}), \forall i \in \{1, 2, ..., n\}$. Mai apoi, pentru a obține mesajul pentru care Alice a făcut angajamentul, se calculează $M_i = S_i \oplus K_i, \forall i \in \{1, 2, ..., n\}$.

Etapa de deschidere forțată

Alice poate alege să nu trimită valoarea $v' = h^{2^{2^k - n}}$ către verificator. Astfel, Bob calculează el însuși $v = g^{2^{2^k - n}} \bmod N$, apoi urmează aceeași pași ca în etapa de deschidere standard în vederea obținerii cheii $K = K_1 K_2 K_3 ... K_n$. Se observă că pentru a calcula valoarea v' sunt necesare $(2^k - n)$ ridicări la pătrat mod N [1].

Alte proprietăți ale sistemului Boneh-Naor

Mesajul M este legat de angajamentul $C = (h, g, u, S)$, adică un verificator poate deschide angajamentul doar la valoarea M [1].

Sistemul pentru angajamente de timp Boneh-Naor satisface proprietatea de **recuperare imună la atacuri paralele** [1].

Sistemul pentru angajamente de timp Boneh-Naor *ascunde* valoarea inițială M [1].

Riscuri de securitate în cadrul lictațiilor online

Licitațiile de tip Vickrey prezentate anterior sunt predispuse la anumite riscuri de securitate în mediul online [6]:

- Dacă partea terță autorizată în care toți participanții au încredere are acces la valorile din ofertele acestora în timpul procesului de licitație, aceasta poate introduce o ofertă secretă cu doar ϵ mai mică decât valoarea depusă de către câștigător, maximizând astfel profitul vânzătorului.
- Dacă gazda nu are acces la valori, ea poate face anumite oferte strategice, urmând ca mai apoi să se folosească doar de cea care aduce cel mai mare profit vânzătorului, refuzând să le folosească pe celelalte.
- Un participant care este complice cu gazda (diferită de vânzător) poate trimite mai multe oferte, ca mai apoi să se publice doar cele oferte care îi avantajează pe amândoi.

Protocolul propus de D.Boneh și M.Naor

D. Boneh și M.Naor propun un protocol care asigură onestitatea, bazat pe sistemul de angajamente de timp definit de aceștia [1]:

1. Participanții creează un angajament de timp pentru oferta lor și îl trimit pe acesta gazdei. Aceasta verifică validitatea angajamentului și respinge sau acceptă participanți în funcție de rezultatul verificării.
2. Când toți participanții au trimis angajamentele sau timpul pentru licitație se încheie, atunci gazda postează pe un *avizier* angajamentele și realizatorii acestora.
3. Dacă un participant își găsește numele pe avizier și vede că a fost acceptat, atunci acesta poate iniția etapa de deschidere, pentru a-și face publică oferta.
4. Dacă un participant refuză să trimită deschiderea angajamentului său, atunci gazda licitației poate să îl deschidă forțat pentru a publica oferta conținută de angajament.

Parametrul de timp T

Un aspect important pentru un astfel de protocol reprezintă alegerea parametrului de timp $T = 2^k$ în funcție de cât se dorește să dureze o licitație.
Pentru $|N| = 2048$ de biți, folosind cele mai bune implementări cunoscute avem următoarele rezultate [6]:

- FPGA-urile (eng. orig. *Field Programmable Gate Array*) pot atinge 2^{24} ridicări la pătrat modulare pe secundă.
- ASIC-urile (eng. orig. *Application Specific Integrated Circuit*) pot atinge 2^{28} ridicări la pătrat modulare pe secundă.

Analiza de timp a deschiderii forțate

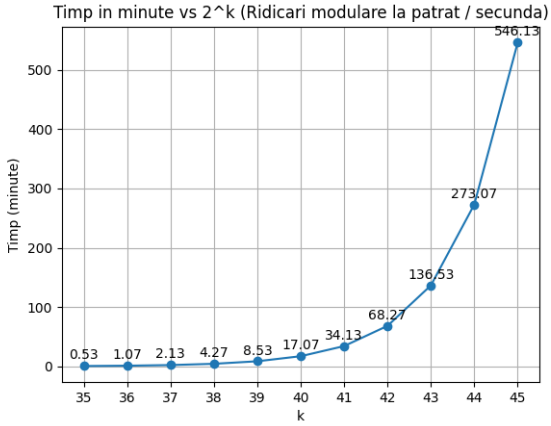

Figura: Analiza de timp a deschiderii forțate, pentru diferite valori ale lui $T = 2^k$, presupunând o putere de calcul de 2^{30} ridicări modulare la pătrat pe secundă.

Simularea protocolului

În cadrul simulării se creează patru containere de Docker care comunică între ele prin request-uri HTTPS:

1. Un server care reprezintă gazda/vânzătorul licitației.
2. Doi clienți care comunică doar cu serverul pentru a participa la licitație.
3. Un container de Redis.

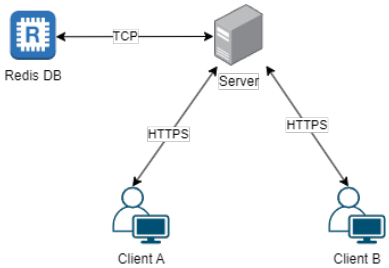

Figura: Comunicare între containere

Simularea protocolului

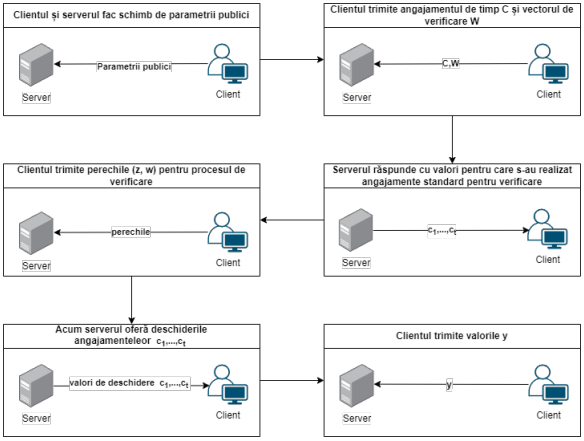

Figura: Ilustrarea etapelor de comunicare între server și client

Interfața grafică

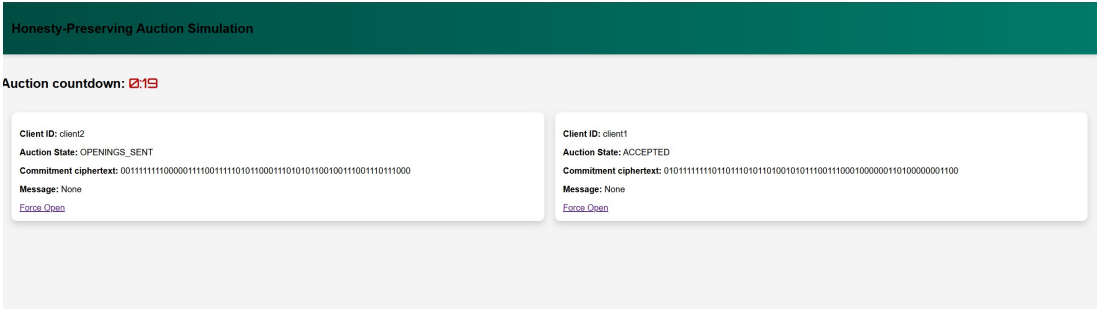

Figura: Stări intermediare în timpul protocolului

Interfața grafică

Figura: Clientul *client1* a inițiat faza de deschidere

Figura: Pentru clientul *client2* s-a realizat deschidere forțată

Protocolul Riggs [6]

- Bazat tot pe angajamente de timp.
- Verifică faptul că un participant are destui bani cât să plătească suma din oferta făcută.
- Folosește tehnologia **blockchain**.
- Utilizează demonstrații *zero-knowledge* de apartenență asupra unui interval (eng. orig. *zero-knowledge range-proofs*) și demonstrații de exponențiere (eng. orig. *proof of exponentiation*).

Demo și întrebări