Secret-sharing pe curbe eliptice

Palaşcă Silvia
Facultatea de Matematică,Universitatea "Al.I.Cuza", Iaşi, Romania
palascutza@yahoo.com

Cuprins

1 Introducere

Ideea lucrării pleacă de la două concepte fundamentale: "cunoaşterea e putere", respectiv, "divide et impera " şi îşi propune tratarea unor aspecte de bază în criptografie, cum ar fi generarea cheii şi apoi aplicarea rezultatelor în criptarea, respectiv decriptarea unui mesaj şi,pe viitor, semnătura digitală aplicată unui mesaj public.

Ca element distinctiv, se vor realiza protocoale utilizând curbele eliptice, această abordare fiind justificată prin dimensiunea redusă a cheii, relativ la nivelul de siguranţă oferit.

Am considerat necesar să tratăm problema din punctul de vedere al unui grup de utilizatori, în comparaţie cu abordările clasice, de tipul 1:1, şi am creat protocoale plecând de la ideea de secret-sharing.

Noţiunea de *secret-sharing* se aplică unui grup format din n persoane, dintre care fiecare deţine o parte dintr-un secret, oricare k persoane putând reconstitui secretul, oricare k-1 neavând această putere.

2 Consideraţii generale

Securitatea în contextul colaborării prin reţele de tip Internet este o noţiune vitală pentru derularea oricărei colaborări. Implicarea mai multor entităţi cu drepturi egale într-un demers de semnare a unui document sau de citire a unui mesaj destinat grupului respectiv sunt aspecte ce îşi găsesc zilnic aplicaţii în cadrul corporaţiilor.

Protocoalele existente momentan se bazează, de multe ori, pe existenţa unei instanţe considerate "de încredere", sau pe memorarea brută a cheilor secrete, ce sunt apoi folosite pentru decriptare, verificare. Aceste prezumţii pot fi eliminate în anumite cazuri, prin distribuirea cheilor secrete şi utilizarea lor sub o forma modificată, crearea unor "umbre".

Au fost propuse modele care sa rezolve această problemă, însă majoritatea se bazează pe inelele Z_p, unde p nr. prim. În această lucrare se vor utiliza curbele eliptice, mai precis, grupul punctelor finite de pe o curba eliptică, pentru elaborarea protocoalelor.

3 Analiza problemei

Pentru ilustrarea problemei se consideră următorul exemplu: având dată o organizaţie multinaţională cu n filiere în n ţări, fiecare având un director, se cere să se realizeze un pachet de protocoale de securitate care să permită luarea deciziilor contractuale astfel:sfie suficienţi k membrii pentru a citi un contract destinat organizaţiei dar sa fie necesari toiţi cei n membrii pentru a trimite un mesaj criptat din partea organizaţiei.

Se doreşte ca metoda implementată să acorde putere egală tuturor, dar fară realizarea numărului stabilit de persoane să nu se poată lua nicio decizie.Există o putere centralizată iniţială, care apoi nu mai intervine în controlul funcţionării organizaţiei, pachetul de securitate cerut va trebui să aibă capacitatea de auto-menţinere şi excludere automată a adversarilor.

Problema propusă necesită câte un protocol pentru fiecare dintre următoarele acţiuni:

- **generarea cheilor**, având în vedere toate restricţiile impuse;
- **decriptarea** în comun de către cel puţin k membrii a unui mesaj primit;
- **semnarea in comun** a unui mesaj public de cel putin k membrii;
- **verificarea semnăturii** aplicate de cel puţin k membrii de către orice instanţă.

Noţiunile implicate în definirea protocoalelor includ:

1. Criptografie clasică peste câmpuri finite
   - Protocolul El-Gamal;
   - DSA;
2. Interpolare Lagrange
3. Curbe eliptice
   Grupul punctelor finite pe o curba eliptică
   (problema logaritmului discret)
4. Secret-sharing (verificabil)

4 Noţiuni

4.1 Criptografie clasică peste câmpuri finite

Ne vom referi în continuare la sisteme de criptare cu cheie publică. Protocoalele existe de criptare,utilizează operaţii peste câmpuri finite, de obicei acestea fiind de tipul Z_p, unde p este un număr prim.

4.1.1 El Gamal

1. Utilizatorul alege p prim, g generator pentru Z_p şi alege $a \in \{0, ..., p-1\}$
2. Calculează $g^a \mod p$
3. publică (p, g, g^a)
4. pentru criptarea mesajului M se alege aleator k şi se calculează $(g^k, M(g^a)^k)$
5. pentru decriptare, în momentul când se primeşte (m,n) se calculează $m' = m^a \pmod p$, apoi $M = nm'^{-1}$

4.1.2 DSA-algoritm semnătură digitală

Această secţiune tratează algoritmul de generare şi verificare a semnăturii digitale aplicate unui mesaj public M,cu parametrii domeniului (p,q,g), unde p-prim, q cu proprietatea $q|(p-1)$, g-generator al lui Z_p, de către o entitate care are cheia publică y şi cea secretă x, adică $g^x = y$.

Generarea semnăturii digitale

1. Se alege k, astfel încât $1 \leq k \leq q-1$;
2. Se calculează $X = g^k \pmod p$ şi $r = X \pmod q$. Dacă $r = 0$,atunci se repetă pasul 1;
3. Se calculează $k^{-1} \pmod q$;
4. Se calculează $e = H(M)$, unde H-funţie de trunchiere;
5. Se calculează $s = k^{-1}(e + xr) \pmod q$.Dacă $s = 0$, atunci se repetă pasul 1;
6. Semnătura mesajului M este (r,s).

Verificarea semnăturii digitale

1. Se verifică dacă r şi s sunt în intervalul [1,q-1];
2. Se calculează $e = H(M)$;
3. Se calculează $w = s^{-1} \pmod q$;
4. Se calculează $v_1 = ew \pmod q$ şi $v_2 = rw \pmod q$;
5. Se calculează $X = g^{v_1} y^{v_2} \pmod p$ şi $v = X \pmod q$
6. Se acceptă dacă $v = r$;

4.2 Curbe eliptice

4.2.1 Grupul punctelor finite pe o curbă eliptică

O curbă eliptică poate fi definită peste orice câmp(de numere reale, raţionale sau complexe), însă cele folosite în criptografie sunt în general, definite peste câmpuri finite.

O curbă eliptică E constă în elemente numite puncte, de tipul (x,y) care satisfac ecuaţia:

$$y^2 = x^3 + ax + b \ \ (mod\ p)$$

, unde $a, b \in Z_p$ constante, astfel încât $4a^3 + 27b^2 \neq 0$, p număr prim,împreună cu un element singular, notat O, numit "punctul de la infinit",(intuitiv, punctul de la vârful şi baza unei linii verticale). Punctele de pe E, cu excepţia lui O, se numesc puncte finite.

Numărul de puncte de pe E ,inclusiv O se numeşte **ordinul** curbei şi se notează $\#E(Z_p)$.

O curbă eliptică împeună cu o lege de tip aditiv are structură de grup.

Suma a doua puncte $P_1(x_1, y_1), P_2(x_2, y_2)$ se defineşte ca fiind $P_3(x_3, y_3)$ unde:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

iar

$$\begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} & P_1 \neq P_2 \\ \lambda = \frac{3x_1^2 + a}{2y_1} & P_1 = P_2 \end{cases}$$

Punctul de la infinit are rolul lui 0 din Z_p. Astfel:

$$\begin{cases} P + O = P \\ P + (-P) = O \end{cases}$$

Punctele unei curbe eliptice se pot aduna, însă nu se pot multiplica.

Se poate efectua, totuşi o multiplicare scalară, de fapt, o adunare repetată a aceluiaşi punct.Astfel, $nP = \underbrace{P + P + ... + P}_{n\ ori}$

Ordinul unui punct P pe o curba eliptică, definită peste un câmp finit ,$E(Z_p)$ este cel mai mic întreg pozitiv ,r, astfel încât $rP = O$.

4.2.2 Problema logaritmului discret

Fie G un punct aparţinând curbei E, astfel încât G are ordinul un număr prim, r cu condiţia că r^2 nu divide ordinul curbei, $\#E(Z_p)$. Atunci, un punct P satisface relaţia $P = lG$ dacă şi numai dacă $rP = O$. Coeficientul l se numeşte **logaritmul discret** al punctului P, relativ la punctul G.Logaritmul discret este un întreg modulo r.Aşdar,

cheia privată-întreg s, modulo r;

cheia publică-un punct W aparţinând curbei E,definit de relaţia $W = sG$

Astfel, se poate observa legătura existentă între logaritmul discret în câmpuri care apare în criptografia clasică şi logarimul discret al unui punct aparţinând unei curbe eliptice .

4.3 Secret sharing (verificabil)-VSS

1. Fiecare persoană din grup, p_i alege un polinom aleatoriu $f_i(z)$ peste Z_p de grad t:

$$f_i(z) = a_{i0} + a_{i1}z + ... + a_{it}z^t$$

2. p_i trimite $A_{ik} = g^{a_{ik}} \ \ mod\ p, k = 0, 1, ..., t.$

3. p_i calculează $f_i(j) \ \ mod\ q\ , j = 0, 1, ..., t$ şi trimite s_{ij} lui p_j

4. Fiecare p_j verifică ceea ce a primit , calculând pentru $i = \overline{1, n}$:

$$g^{s_{ij}} = \prod_{k=0}^{t} (A_{ik})^{j^k} \ \ mod\ p$$

   -daca nu se verifică pentru un indice i, atunci p_j sanctionează p_i.

5. Dacă există mai mult de t sancţiuni contra lui p_i aceasta este automat descalificată, dacă nu, pentru fiecare sancţiune din partea unei p_j dezvăluie s_{ij} corespunzător.Dacă aceasta nu satisface relaţia precedentă, e descalificat. Mulţimea Q desemneaza toţi cei ramaşi valizi.

6. Cheia publică y se calculează ca fiind:

$$y = \prod_{i \in Q} A_{i0} \ \ mod\ p$$

7. Valorile publice de verificare pentru fiecare persoană sunt:

$$A_k = \prod_{i \in Q} A_{ik} \ \ mod\ p\ k = 1, .., t.$$

8. Cheile secrete pentru fiecare persoană:

$$x_j = \sum_{i \in Q} s_{ij} \ \ mod\ q$$

9. Cheia secretă a grupului: $x = \sum_{i \in Q} a_{i0} \ \ mod\ q$

5 Protocoale

5.1 Generare chei

Presupunem că lucrăm peste **câmpul Galois de cardinal q**,notat (GF(q)),unde q prim sau o putere a unui număr prim.
În acest câmp fiecare persoană are un identificator cunoscut de toţi ceilalţi, fie acesta p_i. Fie n, numărul total de persoane, notate $\{p_1, p_2, ..., p_n\}$, unde $p_i \in GF(q)^*$
Fie E/GF(q) un grup aditiv bazat pe o curbă eliptică convenabil aleasă şi fie T un punct din E/GF(q).**Cardinalul mulţimii E/GF(q)** este un nr. prim sau are un factor prim mare, pe care îl notăm cu **p**.
Vom îmbunătăţi algoritmul VSS prezentat anterior şi îl vom adapta la curbe eliptice.
Vom nota:

- k+1 numărul de persoane necesare pentru a descifra secretul;
- T un punct cunoscut pe curba eliptică;
- $T' = dT$Poate fi generat chiar de persoanele din grup fără a fi cunoscut însă de niciuna astfel: fiecare alege $r_i \in GF(q)$, calculează apoi transmite r_iT, urmând ca $T' = \sum r_iT$.
- Q-mulţimea persoanelor nedescalificate.

1. Alegem 2k+2 numere aleatoare $a_{it}, b_{it} \in GF(q), t = 0, ..., k$ drept coeficienţi pentru două polinoame de grad k.
$$f_i(z) = \sum_{k=0}^{k} a_{it} z^t \quad f_i'(z) = \sum_{k=0}^{k} b_{it} z^t;$$
2. Fiecare p_i calculează $s_{ij} = f_i(p_j) \mod q$ si $s'_{ij} = f'_i(p_j) \mod q$ pe care le trimite lui p_j
3. Fiecare p_i calculează k+1 valori publice: $P_{it} = (a_{it}T) \oplus (b_{it}T')$
4. Fiecare p_i verifică relaţia:
$$(s_{ji}T) \oplus (s'_{ji}T') = \sum_{t=0}^{k} p_i^t P_{jt}$$
şi în cazul în care nu se realizează egalitatea pentru un j, atunci p_i sancţionează p_j
5. Dacă p_i a primit o sancţiune de la p_j retrimite valorile s_{ji}, s'_{ji}
6. Dacă p_i a primit mai mult de k+1 sancţiuni, este descalificat, deoarece informaţia lui secretă poate fi calculată prin interpolare Lagrange;de asemenea, este descalificat dacă a retransmis valori false;
7. Pentru mulţimea de persoane nedescalificate se calculează cheia publică comună:
   - Fiecare p_i calculează $A_{i0} = a_{i0}T$ pe care îl trimite tuturor;
   - Cheia publică este:
$$y = \sum_{j \in Q} A_{j0}$$

5.2 Recuperarea secretului

Considerând o eventuală renotare, fie $\{p_1, ..., p_k\}$,persoanele din mulţimea Q .Considerăm polinomul:
$$F(z) = \left(\sum_{t \in Q} a_{t0}\right) + \left(\sum_{t \in Q} a_{t1}\right) z + ... + \left(\sum_{t \in Q} a_{tk}\right) z^t$$

Având la dispoziţie s_i, informaţiile secrete ale fiecărei persoane şi ştiind că $s_i = F(p_i)$, prin interpolare Lagrange putem calcula toţi coeficienţii lui F(z), deci, inclusiv valoarea F(0). Remarcând faptul că $y = F(0)T$, secretul grupului este aflat.

5.3 Decriptarea în comun de către cel puţin k membrii a unui mesaj primit- folosind El-Gamal

În[1] este prezentat următorul algoritm, care poate fi replicat şi în alte probleme:

Se presupune că grupul are în comun **secretul s**, şi **cheia publică y**.

1. Cel care trimite mesajul alege $K \in GF(q)$, iar mesajul criptat capăta forma $(\widetilde{T}, \widetilde{M})$, unde $\widetilde{T} = KT$ şi $\widetilde{M} = M + Ky$;
2. Fiecare din cele k+1 persoane care decid să colaboreze îşi calculează "umbra":

$$u_i = \left(\prod_{j=1}^{k+1} \frac{p_j}{p_i - p_j} \right) s_i$$

3. La fiecare mesaj, grupul alege un ε ;
4. p_i calculează $T_i = \varepsilon u_i \widetilde{T}$ şi apoi transmite T_i;
5. p_i primeşte $T_j, (j \neq i, j = 1, ..., k+1)$ şi obţine $U = \sum_{t=1}^{k+1} T_t = (\varepsilon \sum_{t=1}^{k+1} u_i)\widetilde{T}$;
6. Decriptarea mesajului se face prin: $M = \widetilde{M} - U\varepsilon^{-1}$

5.4 SS-ECDSA

Algoritmii de semnare si verificare a semnăturii digitale bazate pe secret-sharing şi curbe eliptice

Pentru a putea adapta algoritmul clasic de semnătură digitală, trebuie definiţi parametrii curbei eliptice, şi anume, (q,GF,a,b,T,n,h), unde p-ordinul punctului T de pe curba eliptică $y^3 = x^2 + ax + b$ definită peste câmplu Galois GF şi h ordinul lui $\#E(GF(q))/n$.

Se consideră că fiecare persoană deţine o cheie publică, o cheie privată şi o umbră $u_i, i = \overline{1, n}$, determinate în algoritmii anteriori.

Semnarea în comun a unui mesaj public, de cel putin k membrii

1. Fiecare alege $c_i,\ i = \overline{1, k}\ 1 \leq c_i \leq n - 1$;
2. Se calculează $K = \sum_{i-1}^{k} c_i \ \ (mod\ n)$;
3. Se calculează $KT = (x_1, y_1)$ şi se converteşte $x_1 \rightarrow \overline{x_1} \ \ (mod\ n)$;
4. Se calculează $r = x_1 \ \ (mod\ n)$, dacă $r = 0$, e revine la pasul 1;
5. Se calculează $K^{-1} \ \ (mod\ n)$;
6. Se calculează $H(M)$ care se transformă într-un întreg e;
7. Se calculează $s = K^{-1}(e + \sum_{i=1}^{k} u_i r) \ \ (mod\ n)$;
8. Semnătura mesajului M este (r,s);

Verificarea semnăturii digitale aplicate de un grup

1. Se verifică dacă r şi s aparţin intervalului $[1, n-1]$;
2. Se calculează $H(M)$ care se transformă într-un întreg e;
3. Se calculează $w = s^{-1} \pmod n$;
4. Se calculează $v_1 = ew \pmod n$ şi $v_2 = rw \pmod n$;
5. Se calculează $X = v_1 T + v_2 Q$, unde $Q = \sum A_{j0}$, cheia publică a grupului;
6. Dacă $X = 0$ se respinge, dacă nu, se calculează coordonata x a lui X în $v = x_1 \pmod n$;
7. Se acceptă semnătura dacă $v = r$.

6 Probleme deschise, direcţii viitoare

Ramâne de cercetat problema găsirii unui algoritm eficient(polinomial) de calculare a logaritmului discret peste câmpuri sau a logaritmului discret pe curbe eliptice.

[1] propune introducerea unui contor de timp pentru limita în care o persoană trebuie să trimită partea sa de informaţie.Această măsură are rolul de a preveni un atac exhaustiv.

Studierea importanţei şi adaptarea schemelor clasice din criptografie în limbajul curbelor eliptice.

7 Bibliografie

- **[1] Tang, C., Wu, O.** ***An Efficient Proactive Share Refreshing Scheme for Secret Sharing in Distributed Systems. GLOBECOM 2006***;
- **[2] Hankerson, D.,Menezes, A.,Vanstone, S.** ***Guide to elliptic curve cryptography****,Springer-Verlag, New York, 1974,2003*;
- **[3] Patriciu, V.,Pietrosanu M.,Bica I.** ***Securitatea comertului electronic****, Editura All, Bucureşti, 2001*;
- **[4] Fisher,M.J.** ***Lecture notes 20****, Yale University, Department of computer science*;
- **[5] Litcanu, R.** ***Suport curs****,Universitatea "Al.I.Cuza", Iaşi , 2007*