

TODO

Undergraduate Research Opportunities

Dragoș Alin Rotaru

Universitatea din Bucuresti, Romania
r.dragos0@gmail.com

Abstract. None

Keywords: securitate, scheme de partajare

1 Introducere

1.1 Istoric

Termenul de criptografie este definit in dictionarul Oxford ca fiind "arta de a scrie si a rezolva coduri". Criptografia moderna s-a desprins de cea clasica in jurul anilor '80, motivand implementarea rigurozitatii matematice pentru definirea constructiilor criptografice. Asta pentru ca in anii anteriori, experienta a dovedit nesiguranta metodelor de criptare, criptanaliza lor fiind uneori triviala (cifrul lui Cezar, Vigenere ??, ??) sau uneori atinsa cu ceva mai mult efort precum Enigma si alte metode din cel de-al doilea razboi mondial. ??

Criptografia moderna se gaseste pretutindeni in viata de zi cu zi de la ATM-uri, cartele telefonice la semnaturi digitale, protocoale de autentificare, licitatii electronice sau bani digitali, luand amploare o data cu aparitia sistemelor cu cheie publica. O definitie potrivita ar fi "studiul stiintific al tehnicilor pentru a securiza informatia digitala, tranzactiile si calculul distribuit.". [1]

1.2 Motivatie

TODO nu are legătură: faptul ca sunt scheme cuantice nu are impact asupra structurii de acces; e ok sa menționezi, dar atunci faci asta în secțiunea anterioară, când poți să adaugi și alte modalități de definire: scheme bazate pe latice, scheme bazate pe perechi biliniare, scheme cuantice, etc. Dezavantajul schemelor generale de partajare este dimensiunea componentelor, exponentiala in functie de numarul de participanti. [2] De asemenea, s-au dezvoltat scheme pentru modele de calcul neconventional, cum ar fi cel cuantic. [3]

1.3 Structura

TODO

1.4 Securitatea Teoretica a Informatiei

În cazul unor criptosisteme acestea nu pot fi compromise chiar dacă adversarul dispune de o putere computațională nelimitată. Câteva exemple de criptosisteme care garantează securitatea teoretică-informațională sunt: schemele de partajare, unele protocoale multi-party computation, preluarea într-un mod sigur (securizat?) informații de la baze de date. Securitatea teoretică vine însă cu un cost: efortul computațional depus este mult mai mare decât în cazul schemelor care nu garantează securitatea teoretică (se bazează pe dificultatea computațională a unor probleme cunoscute). [4]

2 Scheme de partajare

O schemă de partajare constă în distribuirea unei informații secrete \mathcal{S} la mai mulți participanți $\mathcal{P} = \{P_1, \dots, P_n\}$ astfel încât oricare mulțime de participanți predefinită ca făcând parte dintr-o structură de acces pe care o vom denumi \mathcal{A} să poată reconstitui secretul \mathcal{S} . Formal, o schemă de partajare este reprezentată de o pereche de algoritmi (Gen, Rec):

- $Gen(\mathcal{S}, m)$ este un algoritm care primește la intrare un secret \mathcal{S} și un număr întreg m și întoarce un set de componente s_1, s_2, \dots, s_m .
- $Rec(s_{i_1}, s_{i_2}, \dots, s_{i_q})$ este un algoritm care primește ca parametri de intrare o mulțime de componente și întoarce \mathcal{S} dacă mulțimea $\{P_{i_1}, P_{i_2}, \dots, P_{i_q}\} \in \mathcal{A}$.

Majoritatea schemelor constau în mai multe etape precum:

- *Inițializare*. Presupune inițializarea variabilelor de mediu necesare.
- *Generare*. O entitate autorizată (numită dealer) \mathcal{D} folosește algoritmul Gen pentru a genera componentele.
- *Distribuire*. Componentele sunt trimise participanților cu ajutorul unui mijloc de comunicare sigur, fără ca acestea să fie vizibile unui atacator.
- *Reconstrucție*. Dându-se o mulțime de componente, se folosește algoritmul Rec pentru a recupera secretul \mathcal{S} .

Schemele de partajare se clasifică în funcție de cantitatea de informație secretă pe care o pot obține persoanele care nu fac parte din \mathcal{A} [5]:

- *Sisteme perfecte de partajare*: componentele nu oferă nici o informație teoretică despre \mathcal{S} indiferent de resursele computaționale.

- *Sisteme statistic sigure*: o fracțiune de informație este dezvăluită despre \mathcal{S} independent de puterea computațională a adversarului.
- *Sisteme computațional-sigure de partajare*: se bazează pe faptul ca reconstituirea lui \mathcal{S} se reduce la o problema *dificilă* (spre exemplu problema Diffie-Hellman [6]) în lipsa unor informații oferite doar grupului de acces \mathcal{A} .

În continuare vom prezenta cateva sisteme perfecte de partajare utilizate în cadrul unor arhitecturi pentru stocarea fisierelor pe o durata îndelungată.

2.1 Istoric

Primele scheme de partajare au fost dezvoltate independent de Shamir și Blakley în 1979 [7, 8].

Denumite și scheme majoritare (k, n) , acestea rezolvau cazul în care oricare grup de participanți cu un număr mai mare sau egal decât k (mărimea pragului) poate reconstitui secretul \mathcal{S} din componentele primite de la dealer. Dacă schema este perfect *sigură* atunci oricare grup cu un număr de participanți mai mic decât k nu obține vreo informație despre \mathcal{S} .

Schemele majoritare (spre exemplu schema Shamir) sunt insuficiente pentru a permite partajarea pentru anumite structuri de acces. Considerăm cazul în care vrem sa partajam un secret între 4 participanți: P_1, P_2, P_3, P_4 astfel încât $\{P_1, P_2\}$ și $\{P_3, P_4\}$ să fie singurele mulțimi autorizate pentru reconstrucția secretului \mathcal{S} (i.e. $\mathcal{A} = \{\{P_1, P_2\}, \{P_3, P_4\}\}$). În mod evident, problema nu poate fi rezolvată cu o structură de acces de tip prag: anumite mulțimi de 2 participanți trebuie să poată reconstrui secretul ($\{P_1, P_2\}, \{P_3, P_4\}$), în timp ce altele nu ($\{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}$)

Astfel de scheme de partajare pentru structuri de acces generale au fost dezvoltate de Ito, Saito și Nishizeki, realizând o generalizare a schemei Shamir [9]. Benaloh și Leichter au demonstrat ca schemele de partajare de tip prag nu pot fi folosite pe structuri general monotone (familie de submulțimi ale lui \mathcal{P} cu proprietatea că dacă $A \in \mathcal{A}$ și $A \subset A'$, atunci $A' \in \mathcal{A}$) și obțin o construcție mai eficientă ca Ito et. al din punct de vedere al numărului de componente distribuite participanților [10].

2.2 Schema unanimă

Presupunând ca vrem să împărțim un secret \mathcal{S} la n participanți astfel încât \mathcal{S} sa poată fi recuperat doar daca toți cei n participanți își combină componentele pe care le dețin. Metoda este echivalentă cu o schemă (n, n) majoritară. Un exemplu este schema introdusă de Karin, Greene și Hellman (Fig.1) [11].

Inițializare:

- Fie $S \in Z_q$ unde $q > 1$ și q prim;
- Fie n numărul de participanți;

Generare: Dealerul \mathcal{D} :

- Alege $n - 1$ valori aleatoare $s_i \leftarrow^R Z_p$, $i \in \{1, 2, \dots, n - 1\}$;
- $s_n = S + \sum_{i=1}^{n-1} s_i \pmod{q}$;

Distribuție: Dealerul \mathcal{D} :

- transmite în mod sigur participantului P_i componenta s_i , $i \in \{1, 2, \dots, n\}$;

Reconstrucție: Cei n participanți:

- Calculează $S = \sum_{i=1}^n s_i \pmod{q}$.

Fig. 1. Schema unanimă [11]**2.3 Schema Shamir**

Schema Shamir oferă mai multă flexibilitate decât schema unanima prin faptul ca oricare k (sau mai multi) participanți din cei n pot recupera \mathcal{S} , însă mai puțin de k participanți nu obțin nicio informație despre \mathcal{S} . Schema Shamir este deci o schemă (k, n) majoritară.

Intuitiv, având k puncte în plan (x_i, y_i) , $x_i \neq x_j$ $i, j \in \{1, 2, \dots, k\} \forall i \neq j$, există o curbă polinomială unică care trece prin ele. În schimb, pentru a defini o curbă polinomială de grad k care trece prin $k - 1$ puncte date, există o infinitate de soluții. Evident, orice submulțime de valori s_i de mărime egală cu k este suficientă și necesară pentru a reconstrui polinomul f . După interpolarea componentelor deținute de cel puțin k dintre participanți, secretul \mathcal{S} se determină ca fiind $f(0)$ (Fig. 2) [8].

Pentru un atacator care deține chiar și $k - 1$ valori s_i , acesta nu determină nimic despre \mathcal{S} , spațiul de soluții posibile fiind identic față de situația în care nu reușește să obțină vreo componentă.

2.4 Schema Ito, Saito și Nishizeki

În continuare vom descrie modalitatea de distribuire a componentelor de la care au pornit Ito, Saito și Nishizeki pentru ca schema să aibă o structură de acces

Inițializare:

- Fie $S \in Z_q$ unde $q > 1$ și q prim;
- Fie n numărul de participanți a.i $q > n$;
- Fie k numărul minim de componente puse în comun pentru a determina pe S ;

Generare: Dealerul \mathcal{D} :

- Alege n valori distincte $x_i \leftarrow^R Z_q, i = 1, 2, \dots, n$;
- Alege $a_i \leftarrow^R Z_q, i \in \{1, 2, \dots, k-1\}, a_{k-1} \neq 0$;
- Construiește polinomul $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + S$;
- Calculează $s_i = f(x_i), i \in \{1, 2, \dots, n\}$;

Distribuție: Dealerul \mathcal{D} :

- Transmite participantului P_i componenta $s_i, i \in \{1, \dots, n-1\}$;

Reconstrucție: Orice mulțime cu dimensiunea k (sau mai mare) de participanți distincți P_1, P_2, \dots, P_k :

- Interpolează punctele s_i pentru a obține polinomul f :

$$f(x) = \sum_{i=1}^k s_i \prod_{1 \leq j \leq k, j \neq i} \frac{x - x_j}{x_i - x_j} \quad (1)$$

- Află secretul reconstruit $S = f(0)$.

Fig. 2. Schema Shamir [8]

$\mathcal{A} \subseteq 2^P$ (submulțime a setului de participanți) monotona (i.e. $\forall A \in \mathcal{A}, A \subseteq A' \Rightarrow A' \in \mathcal{A}$). Folosind construcția unei scheme majoritare (k, n) autorii au reușit să descrie elementele din \mathcal{A} folosind rezultatul unei reuniuni de mulțimi de componente cu un număr de elemente mai mare sau egal decât k (Fig. 3) [9]. Notăția $x : Pr$, înseamnă că x are proprietatea Pr .

Dezavantajul acestei structuri este numărul de componente necesar pentru o structură de acces oarecare \mathcal{A} . Un mod simplu de construire al funcției *Assign* este Pentru mai multe informații despre funcția *Assign*, cititorul interesat poate citi în [9]. **TODO prezentarea trebuie să fie de sine stătătoare, trebuie măcar să explici în cuvinte ce înseamnă**

3 Sisteme de stocare de lunga durată

În această secțiune vom arăta câteva întrebări ale schemelor de partajare. Considerăm cazul în care vrem să stocăm rapoarte medicale, imagini, docu-

Inițializare:

- Fie q un număr prim $q, q > 1, z \in \mathbb{N}$ nenul și $\mathcal{C} = GF(p^z)$;
- Fie $S \in \mathcal{C}$ secretul;
- Fie structura de acces \mathcal{A} ;
- Fie n numărul de participanți;

Generare: Dealerul \mathcal{D} :

- Alege n valori distincte $x_i \leftarrow^R Z_q, i = 1, 2, \dots, n$;
- Alege $a_i \leftarrow^R \mathcal{C} \setminus \{0\}, i \in \{1, 2, \dots, k-1\}, a_{k-1} \neq 0$;
- Construiește polinomul $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + S$;
- Atribue $s_i = f(x_i) \ i \in \{1, 2, \dots, n\}$; Fie $Shares = \{s_1, \dots, s_n\}$;
- Alege $D_i \subseteq Shares \ 1 \leq i \leq n$;
- Alege funcția $Assign : P \rightarrow 2^Q$:
 - $Assign(P_i) = D_i \ 1 \leq i \leq n$
 - $\mathcal{A} = \left\{ Q \subseteq Shares : \left| \bigcup_{P_i \in Q} Assign(P_i) \right| \geq k \right\}$;

Distribuție: Dealerul \mathcal{D} :

- Transmite participantului P_i componenta $Assign(P_i), i \in 1, 2, \dots, n$;

Reconstrucție: Participanții din structura de acces \mathcal{A} :

- Procedenza identic ca in schema Shamir.

Fig. 3. Schema Ito, Saito, si Nishizeki [9]

mente clasificate pe un timp indelungat intr-un mediu electronic. Pe parcursul timpului, pot apare in schimb, diverse probleme precum dezastre naturale, defectiunea unor componente hardware, eroare umana, etc. [12] Un sistem de stocare necesar nevoilor noastre trebuie sa satisfaca cel putin urmatoarele 3 conditii:

- Disponibilitatea: Informatia trebuie sa ramana accesibila tot timpul, in ciuda erorilor de tip hardware.
- Integritatea: Abilitatea sistemului de a raspunde cererilor intr-un mod care garanteaza corectitudinea lor.
- Confidentialitatea: O persoana care nu face parte din grupul de acces sa nu obtina permisiunea de a afla informatii de orice fel despre datele existente in sistem.

3.1 Criptare VS scheme de partajare

Una dintre soluțiile existente pentru a construi acest sistem ar putea fi criptarea datelor folosind o cheie înainte de inserarea lor în spațiul de stocare. În momentul în care un user autorizat dorește să efectueze o citire a unor date, întrebuintează cheia potrivită pentru a le decripta. În practică există algoritmi de criptare eficienți precum AES însă aceștia nu garantează confidențialitatea datelor în cazul în care avem de a face cu un adversar fără o limită computațională. Un dezavantaj al criptării este administrarea cheilor, standardele de securitate schimbându-se în fiecare an. De fiecare dată când cheile sunt înlocuite atunci este necesară recriptarea datelor de pe fiecare bază de date. Cu cât disponibilitatea este mai mare - numărul de noduri duplicate crește - recriptarea lor devine o operație costisitoare.

Majoritatea tehnicilor de criptare se bazează pe dificultatea factorizării unui număr sau cea a calculării logaritmului discret însă o dată cu posibilă dezvoltare a calculatoarelor cuantice aceste probleme nu vor mai fi atât de dificile. [13]

4 Sisteme de stocare de lungă durată bazate pe scheme de partajare

O alternativă la soluția cu criptare care asigură atât confidențialitate cât și redundanța necesară este întrebuintarea sistemelor de stocare de lungă durată bazate pe scheme de partajare. [12, 14, 15]

4.1 PASIS

PASIS este o soluție pentru un sistem descentralizat care oferă beneficii precum securitate, redundanță a datelor și auto-întreținere. Structurile descentralizate împart informația la mai multe noduri folosind scheme de redundanță precum RAID **TODO (R... A... I... D...) - mereu trebuie în paranteză denumirea completă, o singură dată, când se introduce o abreviere** pentru a asigura performanța, scalabilitatea sistemului dar și integritatea datelor. [16] **TODO exact, câteva detalii despre RAID**

PASIS folosește schemele de partajare pentru a distribui informația nodurilor de stocare dintr-o rețea. Aceasta introduce agenți pe partea clientului pentru a scrie sau șterge date din noduri, dar și agenți pentru mentenanță. Componentele obținute **TODO în urma partajării unui fișier sunt TODO nu puse, ci stocate** în rețea cu ajutorul agenților (Fig. 4). Pe lângă conținutul brut al componentelor se adaugă metadate pentru a reține adresa nodului din rețea la care au fost **TODO stocate, nu trimise** dar și noua denumire cu care este salvată în rețea.

Considerând o schemă de partajare majoritară $p - m - n$ unde oricare din cei m participanți pot reconstitui fișierul, dar mai puțin de p nu obțin nicio informație dintr-un total de n componente. **TODO o schema de partajare majoritara are 2 parametri, care sunt aici?! rescriere! atenție, să folosești notațiile de mai înainte: n = nr de participanți, etc.**

Atunci când un participant inițiază o cerere pentru a citi un fișier, agentul PASIS aflat local procedează după cum urmează:

- Caută numele celor n componente care alcătuiesc fișierul într-un serviciu care listează toate datele.
- Inițiază cereri de citire la cel puțin m din cele n noduri.
- În caz ca acesta nu primește cel puțin m răspunsuri se întoarce la pasul anterior încercând interogări la noduri diferite.
- Reconstituie fișierul obținut din cele m componente.

Operația de scriere este similară cu cea de citire, aceasta oprindu-se atunci când în cel puțin $n - m + 1$ noduri s-au stocat cu succes componente. În articol se menționează și compromisul de spațiu-timp **TODO denumirea consacrată în romana este compromis spațiu-timp, nu timp-spațiu** folosite de PASIS **TODO : extinde puțin ce înseamnă asta**. Autorii specifică soluții pentru auto mentenanța sistemului cu ajutorul resurselor umane prin monitorizarea periodică stării sistemului folosind log-uri sau ajustarea parametrilor din cadrul schemei de partajare.

TODO Imi place figura! Dar citeaza lucrarea - și in caption și in text - nu am vazut nicio citare la PASIS!

4.2 GridSharing

În 2005, Subbiah și Blough propun o nouă abordare pentru a construi un sistem de stocare securizat și tolerant la erori numit GridSharing [15].

Schema Shamir nu oferă siguranță în ceea ce privește detectarea sau actualizarea unor componente incorecte introduse de un atacator. Metoda cea mai des folosită este determinarea validității componentelor prin utilizarea semnăturilor electronice. Aceasta este realizată prin scheme de verificare non-interactive precum cea a lui Feldman împreună cu schema Shamir [17] **TODO trebuie reformulat: (1) leaga-l de paragraful anterior; (2) Feldman e o schema de sine statatoare, doar ca este construita pe baza schemei Shamir; cum se folosesc amandoua?**

TODO Subbiah și Blough in loc de Autorii folosesc un sistem care înlocuiește schemele de verificare cu o schemă de partajare unanimă XOR (considerăm cazul $q = 2$ în Fig. 1) pentru a păstra securitatea construcției. În cazul detectării componentelor incorecte, este adoptată o strategie de tipul **TODO replicate-and-voting**. Componentele sunt replicate pe un număr mare de servere astfel încât

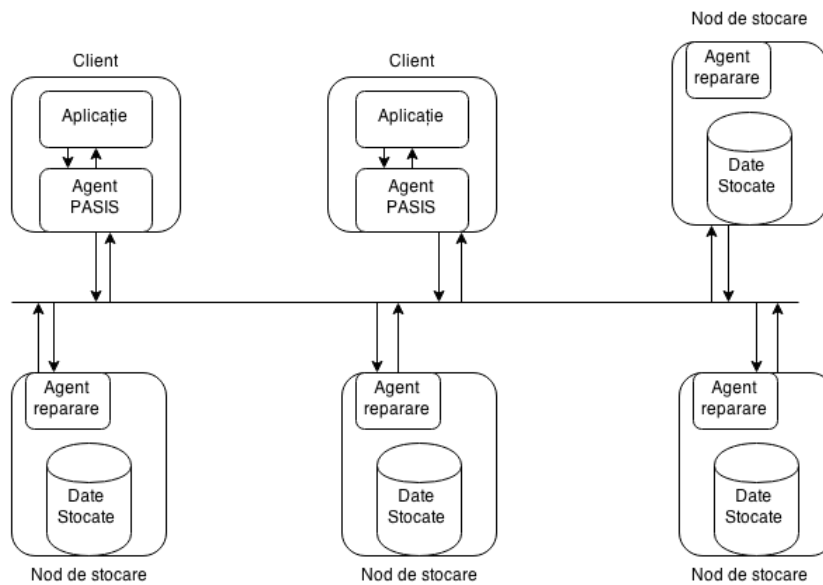


Fig. 4. Arhitectura PASIS cu 4 noduri și 2 clienți []

determinarea validității va fi stabilită în funcție de numărul de servere care le conțin.

Se identifică 3 tipuri de defecțiuni care pot apărea pe serverele unde sunt stocate datele:

- Abandonări: un server este *abandonat* dacă nu mai răspunde vreunui mesaj din rețea și s-a oprit din a mai efectua vreo operație.
- Bizantine: atunci când serverul respectă întotdeauna protocoalele inițiale dar componentele salvate local au fost compromise. **TODO Byzantine înseamnă că nu respectă nici un protocol! Adversarul face ce vrea + stie ce e stocat pe server!**
- Scurgeri de informații: serverul execută protocoalele corect dar e posibil ca un adversar să fi obținut componentele stocate.

Primele 2 modele definite mai sus sunt preluate din calculul cu sisteme distribuite. Cel de-al 3-lea model a fost introdus pentru a defini atacatorul care folosește vulnerabilitățile cu intenția de a *învața* din informații.

Arhitectura GridSharing constă în N servere unde cel mult c servere pot fi abandonate, b servere bizantine și l cu scurgeri de informații. Cele N pot fi aranjate într-un grid cu r linii și N/r coloane (considerăm pentru simplitate că $N \pmod{r} = 0$). Caracteristicile modelului bizantin și cel specific scurgerilor de

informații permit dezvăluirea componentelor unui adversar de pe cel mult $l + b$ servere.

TODO Sa te astepti la intrebari, de tipul: de ce aceste praguri pentru securitate / replicare?

TODO De ce în exemplu rezista la atac? $l + b = 3$, daca adversarul ia control asupra 1 server de pe fiecare linie castiga, adica determina secretul

TODO ce inseamna $\binom{4}{3}$?

Example 1. Considerăm ca împartim un secret \mathcal{S} la 3 linii (participanți) astfel încât sistemul să permită 2 componente de tip b , 1 componentă de tip l și 15 servere. În cazul acesta vom folosi o schemă majoritară XOR $((\binom{4}{3}, \binom{4}{3}) = (3, 3)$.

Vom avea 3 componente, (s_1, s_2, s_3) a.î $s_1 \oplus s_2 \oplus s_3 = \mathcal{S}$. Distribuirea se face în felul următor:

- Serverele situate pe prima linie primesc s_1
- Serverele situate pe a doua linie primesc s_2
- Serverele situate pe a treia linie primesc s_3

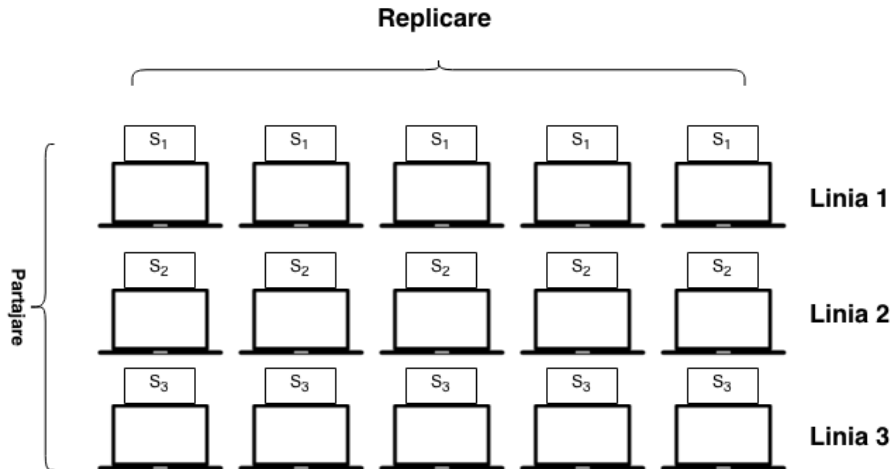


Fig. 5. GridSharing cu 3 linii, 15 servere dintre care 2 bizantine, 1 cu scurgeri de informații **TODO citare**

4.3 POTSHARDS

În 2007 este propus un nou sistem care combină caracteristicile PASIS și Grid-Sharing adăugând posibilitatea de migrarea a datelor la noduri noi: POTSHARDS TODO (Protection Over Time, Securely Harboring And Reliably Distributing Stuff)) - mereu prima data cand folosesti o abreviere trebuie sa o explici

TODO cite! se citeaza la inceput

De asemenea este introdusă o tehnică nouă de găsim a componentelor folosind pointeri aproximativi. Pentru a asigura confidențialitatea, autorii adoptă o schemă de partajare XOR unanimă, la fel ca în GridSharing. POTSHARDS consideră problema în care o persoană neautorizată încearcă să aște informații vulnerabile fără ca aceasta să fie nedetectată. Schemele existente precum PASIS și GridSharing nu îndeplineau această cerință dacă un atacator determină locația componentelor distribuite inițial. TODO nu inteleg - reformulare, explica ce vrei sa zici!

Soluția pe care o oferă această arhitectură este reconstruirea componentelor într-un mod securizat și folosirea semnăturilor algebrice pentru a asigura un grad ridicat de păstrare a integrității fișierelor [18]. POTSHARDS poate fi gândit ca o aplicație pe partea clientului care comunică cu o mulțime de noduri (arhive) independente.

Ca prim pas, POTSHARDS preprocesează fișierul într-un obiect, partajează obiectul în fragmente la care adaugă meta-date, numite *shards* (Fig. 6) [12]. Acestea sunt trimise apoi arhivelor independente, fiecare având propriul domeniu de securitate, localizate în *regiuni*. Pentru a reconstitui cu succes informația inițială, meta-datele shard-urilor conțin detalii despre structura pointerilor aproximativi, indicând regiunea în care se află următorul shard.

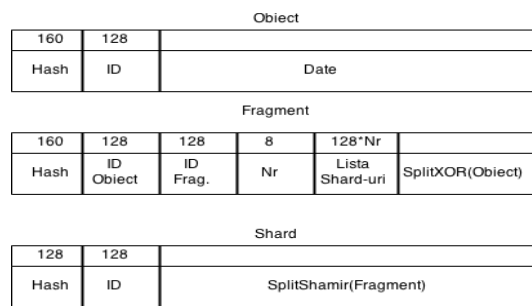


Fig. 6. Entități de date în POTSHARDS. *Nr* e numărul de shard-uri produse de un fragment. *SplitXOR* reprezintă o componentă rezultată în urma partajării unanime XOR. Analog *SplitShamir* reprezintă o componentă rezultată în urma partajării folosind schema Shamir. TODO cite!

Procesul de fragmentare a datelor este prezentat în Fig. 7.

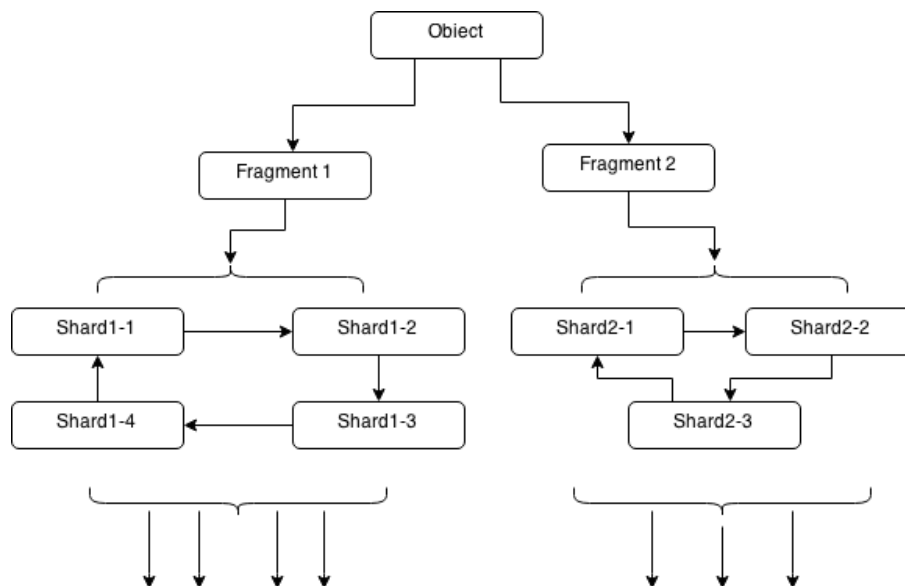


Fig. 7. Distribuirea unui obiect în POTSHARDS

Pentru ca reconstituirea unui fișier să fie fezabilă unui utilizator, acestuia îi este întoarsă o listă cu locațiile exacte shard-urilor corespunzătoare. Obținerea unui shard de către un atacator nu este folositoare, pentru a detecta următorul shard, un atac brut force constă în cereri multiple în zona indicată de pointerul aproximativ. Un astfel de atac nu va trece neobservat de POTSHARDS deoarece unul dintre scopurile sale este să stocheze datele într-un mod cât mai uniform distribuit **TODO spread**. [12]

5 Alouneh et al.

TODO Alt nume poate? Autorii propun un sistem pentru stocarea datelor un timp îndelungat folosind schema Shamir cu câteva modificări. Aceste schimbări se vor arăta esențiale mai târziu în menținerea securității.

5.1 Arhitectura sistemului

În cazul în care dorim să stocăm un fișier în sistem (abordând filozofia majorității sistemelor de operare - orice este un fișier), acesta este preluat de o aplicație de

control pe partea de client pe care îl împarte în blocuri de octeți de lungime k . Pentru fiecare bloc, octeții devin coeficienții unui polinom f , componenta cu indicele i va fi reprezentată de valoarea lui $f(i)$ $i = \{1, 2, \dots, n\}$. Menționăm că toate operațiile se vor efectua în $GF(256)$ modulo un polinom ireductibil (în implementarea sistemului, autorii folosesc $x^8 + x^5 + x^3 + x + 1$). Procedul este descris în detaliu în Fig 8.

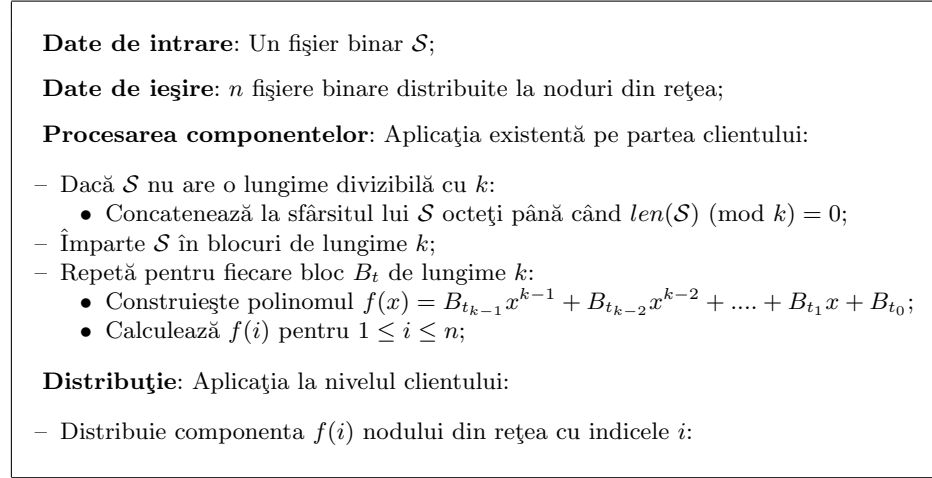


Fig. 8. Schema Alouneh et al. - Generare [19]

Example 2. Vom exemplifica modul de calcul în $GF(256) \pmod{g(x)}$ unde $g(x) = x^8 + x^4 + x^3 + 1$. Luăm polinomul $f(x) = 10 + 15x$ care corespunde unui fișier format din octeții (în această ordine) 10 15.

$$\begin{aligned}
 f(01) \pmod{g(x)} &= 10 + 15 \pmod{g(x)} \\
 &= (x^4) + (x^4 + x^2 + 1) \pmod{g(x)} \\
 &= x^2 + 1 = 000000101_2 \\
 &= 05_{16}
 \end{aligned} \tag{2}$$

$$\begin{aligned}
 f(02) \pmod{g(x)} &= 10 + 15 \cdot 02 \pmod{g(x)} \\
 &= (x^4) + (x^5 + x^3 + x) \pmod{g(x)} \\
 &= 00111010_2 \\
 &= 3A_{16}
 \end{aligned} \tag{3}$$

Pentru reconstituirea unui fișier (9) se interpolează din orice mulțime de componente A cu dimensiune minim k prin metoda lui Lagrange, asemănător schemei

Shamir:

$$f(x) = \sum_{i \in A} f(i) \prod_{j \in A, j \neq i} \frac{x - j}{i - j} \quad (4)$$

Example 3. Vom exemplifica interpolarea 4 pe componentele calculate in 2 si 3 pentru a reconstitui polinomul:

$$\begin{aligned} f(x) &= 05(x - 02)(01 - 02)^{-1} + 3A(x - 01)(02 - 01)^{-1} \\ &= 05(x - 02)03^{-1} + 3A(x - 01)03^{-1} \\ &= F6(05 + 3A)x + F6(05 \cdot 02 + 3A \cdot 01) \\ &= F6 \cdot 3F \cdot x + F6 \cdot 30 = 15x + 10 \end{aligned} \quad (5)$$

Noutatea arhitecturii constă în diminuarea redundanței componentelor la un factor de k , spre deosebire de sistemele descrise în 4.1 sau în 4.3. Reducerea spațiului ocupat este datorat înlocuirii coeficienților cu octeții din fișierul ce va fi partajat. Confidențialitatea este indusă în mod automat de schema lui Shamir.

Date de intrare: Cel puțin k componente provenite din noduri (distincte);

Date de ieșire: Fișierul binar original S ;

Reconstrucție: Aplicația existentă pe partea clientului:

- Repetă pentru fiecare bloc al lui S :
 - Calculează prin interpolare coeficienții lui $f(x) = B_{t_{k-1}}x^{k-1} + B_{t_{k-2}}x^{k-2} + \dots + B_{t_1} + B_{t_0}$
 - Reconstituie blocul B_t
- Șterge octeții de la sfârșitul fișierului adăugați la generare.

Fig. 9. Schema Alouneh et al. - Reconstrucție [19]

6 Rezultate obtinute

Împreună cu mentorul am analizat un articol apărut într-un jurnal de clasă C, prezentat în (5) unde am identificat erori majore ale sale și am implementat sistemul descris de autori pentru a demonstra practic, nu doar teoretic anumite greseli pe care le vom evidenția în următoarele secțiuni. [19]

6.1 Erori gasite in articol

Spre deosebire de schema Shamir, unde coeficientii sunt alesi intr-un mod aleator uniform, acestia sunt extrasi din continutul fisierelor originale. Alegerea este motivata de faptul ca multimea componentelor si efortul computational depus pentru generarea coeficientilor se reduce la un factor de k spre deosebire de schema Shamir.

Natura determinismului duce la cateva atacuri simple in momentul in care un atacator obtine informatiile stocate intr-un nod, indiferent de marimea pragului folosit in metoda de partajare. Datorita acestuia, am aratat 2 atacuri simple in cazul in care componentele sunt calculate in ordine:

- Detectarea tipului unui fisier
- Detectarea tipului de continut unui fisier

Am indicat ca un atac bazat pe felul in care se realizeaza completarea fisierului \mathcal{S} inainte de partajarea sa poate fi fezabil, in conditiile in care s-a demonstrat ca aceasta alegere este esentiala in pastrarea securitatii [20].

6.1.1 Detectarea tipului de fisier

In sistemele de operare, la inceputul fiecarui fisier se afla o secventa de octeți (semnatura sau antet) pentru a determina tipul acestuia. In tabelul (1) gasim 4 din cele mai uzuale antete.

Considerand cazul in care dorim sa partajam un fisier *pdf* cu ajutorul sistemului descris in 5 folosind $k \leq 4$. Polinomul corespunzator $f(x)$ va fi intotdeauna același. Presupunând ca numerotarea nodului i este aceeași, putem determina cu usurinta daca este stocat un fisier *pdf* fara a lua in vedere continutul fisierului.

Cu alte cuvinte, daca un adversar obtine controlul unui singur nod, bazandu-se doar pe valoarea primei componente poate detecta tipul unui fisier.

In plus, pastrand aceeași presupunere, anume ca nodurile isi pastreaza același indice i iar adversarul obtine valorile i si k atunci acesta poate detecta cu o probabilitate ridicata tipul fisierului folosindu-se de prima componenta. Ne asumam posibilitatea datorita faptului ca valoarea lui k este publica iar i poate sa fie descoperita la distribuire (Fig. 8).

Pentru a exemplifica, un adversar poate distinge cu probabilitate ridicata intre fisierele *doc*, *gif*, *pdf*, *png*, *rar*, *wav* si *zip*. In tabelul (2) avem generate componentele pentru $k = 2$ si $n = 5$. Daca un adversar descopera ca valoarea primului nod este 14 atunci acesta afla ca pentru prima componenta corespunde un fisier *gif*. Daca obtine accesul nodului 4 si citește valoarea 205 atunci stie ca fisierul este de tipul *rar*. Daca citește valoarea 27 de pe primul nod atunci stie ca poate

fi un *wav* sau *zip*. Cu toate acestea poate sa distinga cele 2 fisiere daca dezvalui o singura valoare de pe celelalte noduri (2345) pentru ca valorile sunt distincte.

Table 1. Semnături de fisiere

Tip de fișier	Primii 4 octeți
doc	D0 CF 11 E0
gif	47 49 46 38
pdf	25 50 44 46
png	89 50 4E 47
rar	52 61 72 21
wav	52 49 46 46
zip	50 4B 03 04

Table 2. Componentele primului bloc ($k = 2$)

Tip fișier	Nod 1 ($i = 1$)	Nod 2 ($i = 2$)	Nod 3 ($i = 3$)	Nod 4 ($i = 4$)	Nod 5 ($i = 5$)
doc	31	85	154	193	14
gif	14	213	156	120	49
pdf	117	133	213	126	46
png	217	41	121	210	130
rar	51	144	241	205	172
wav	27	192	137	109	36
zip	27	198	141	103	44

6.1.2 Detectarea tipului de conținut

Multe documente urmează un anumit tipar precum contracte, chitanțe, bonuri fiscale sau curriculum vitae. Deoarece majoritatea conținutului rămâne neschimbat, există o probabilitate destul de mare ca multe componente să aibă aceeași valoare. O dată ce un adversar reușește să determine componentele unui nod, poate determina prin analogie tipul de conținut al fișierului original.

Fisierele cele mai vulnerabile sunt cele care conțin o secvență de octeți periodică (imagini cu un pattern repetitiv) sau cele care multi octeți nuli (valoarea componentelor va fi 0).

6.2 Verificarea rezultatelor

Pentru a arata aplicabilitatea rezultatelor in practica, am implementat propunerea descrisa in sectiunea 5 si am testat pe cateva cazuri.

In cadrul implementarii am folosit limbajul Python3.0 in cadrul sistemului de operare ArchLinux.

Python este un limbaj de programare cu tipuri dinamice, disponibil sub licenta open-source [21]. Pentru a realiza comunicarea intre procese am folosit Cerealizer iar distributia componentelor a fost vizual generata cu ajutorul pachetului Matplotlib [22, 23]. De asemenea am folosit sistemul de versionare Git iar codul e gazduit de GitHub [24, 25].

Avand in vedere ca articolul original nu mentioneaza o metoda de padding, am considerat o metoda standard pentru a completa octetii ultimului bloc: alipim la sfarsitul lui \mathcal{S} octetii 80 00 00 ... 00 00 pana cand lungimea ultimului bloc ajunge la k octeti.

Mentionam aceasta metoda doar pentru completitudine, aceasta neafectand rezultatele, considerand doar secventele de octeti de la inceputul fisierului sau antetul său.

6.2.1 Detectarea tipului de fișier

Extindem analiza facuta in sectiunea 6.1.1 asupra tipurilor din tabelul 1 pentru $k = 2$ si crestem valoarea indicelui i pana cand 2 componente devin egale. Fie f_l polinomul de gradul 1 asociat primului bloc al fisierului aflat pe linia l . Analog f_c polinomul de gradul 1 asociat primului bloc al fisierului aflat pe coloana c .

In tabelul 3 calculam valoarea maxima a nodului i pentru care $f_l(i) \neq f_c(i)$. Valoarea -1 indica lipsa de coliziuni ale lui $f_c(x)$, $f_l(x)$ pentru i , $i = 1, 2, \dots, 255$ ($\nexists 1 \leq i \leq 255$ a.î. $f_l(i) = f_c(i)$)).

Deoarece pe diagonala principala toata componentele sunt identice pentru $k \leq 4$ poate fi ignorata. In tabelul 3 observam valoarea 0 pentru perechea (wav, zip) pentru ca $f_{wav}(1) = f_{zip}(1) = 27$ (tabel 1).

In tabelele 4, 5 sunt considerate rezultatele pentru $k = 3$ si $k = 4$. Pentru $k \geq 5$ este nevoie de un antet cu mai mult de 4 octeti.

6.3 Publicarea articolului

Referințe

1. Katz, J., Lindell, Y.: Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series). Chapman & Hall/CRC (2007)

2. Beimel, A.: Secret-sharing schemes: a survey. In: Coding and cryptology. Springer (2011) 11–46
3. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Physical Review A **59**(3) (1999) 1829
4. Csirmaz, L.: The size of a share must be large. Journal of cryptology **10.4** (1997) 223–231
5. Martin, K.M.: Challenging the adversary model in secret sharing schemes. Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts (2008) 45–63
6. Boneh, D.: The decision diffie-hellman problem. In: Algorithmic number theory. Springer (1998) 48–63
7. Blakley, G.: Safeguarding cryptographic keys. Proceedings of the 1979 AFIPS National Computer Conference (1979) 313–317
8. Shamir, A.: How to share a secret. Commun. ACM **22**(11) (1979) 612–613
9. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) **72**(9) (1989) 56–64
10. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Proceedings on Advances in Cryptology. CRYPTO '88, New York, NY, USA, Springer-Verlag New York, Inc. (1990) 27–35
11. Karnin, E.D., Member, S., Greene, J.W., Member, S., Hellman, M.E.: On secret sharing systems. IEEE Transactions on Information Theory **29** (1983) 35–41
12. Storer, M.W., Greenan, K.M., Miller, E.L., Voruganti, K.: Potshards - a secure, recoverable, long-term archival storage system. TOS **5**(2) (2009)
13. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, IEEE (1994) 124–134
14. Wylie, J.J., Bigrigg, M.W., Strunk, J.D., Ganger, G.R., Kiliççöte, H., Khosla, P.K.: Survivable information storage systems. Computer **33**(8) (2000) 61–68
15. Subbiah, A., Blough, D.M.: An approach for fault tolerant and secure data storage in collaborative work environments. In: StorageSS. (2005) 84–93
16. Patterson, D.A., Gibson, G., Katz, R.H.: A case for redundant arrays of inexpensive disks (raid). SIGMOD Rec. **17**(3) (June 1988) 109–116
17. Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: Proceedings of the 28th Annual Symposium on Foundations of Computer Science. SFCS '87, Washington, DC, USA, IEEE Computer Society (1987) 427–438

Table 3. Indicele maxim i a.â componentele primului bloc sa fie distincte($k = 2$)

Tip Fişier	doc	gif	pdf	png	rar	wav	zip
doc	-	169	194	209	170	206	110
gif	169	-	133	137	75	-1	133
pdf	194	133	-	-1	115	151	133
png	209	137	-1	-	229	147	195
rar	170	75	115	229	-	-1	42
wav	206	-1	151	147	-1	-	0
zip	110	133	133	195	42	0	-

Table 4. Indicele maxim i a.î componentele primului bloc sa fie distincte($k = 3$)

Tip Fişier	doc	gif	pdf	png	rar	wav	zip
doc	-	63	-1	-1	-1	-1	-1
gif	63	-	-1	-1	-1	-1	-1
pdf	-1	-1	-	164	-1	119	-1
png	-1	-1	164	-	143	122	129
rar	-1	-1	-1	143	-	143	-1
wav	-1	-1	119	122	143	-	172
zip	-1	-1	-1	129	-1	172	-

Table 5. Indicele maxim i a.î componentele primului bloc sa fie distincte($k = 4$)

Tip Fişier	doc	gif	pdf	png	rar	wav	zip
doc	-	-1	38	95	1	95	98
gif	-1	-	-1	-1	167	-1	-1
pdf	38	-1	-	12	11	119	70
png	95	-1	12	-	243	95	148
rar	1	167	11	243	-	-1	94
wav	95	-1	119	95	-1	-	-1
zip	98	-1	70	148	94	-1	-

18. Schwarz, T.J.E., Miller, E.L.: Store, forget, and check: Using algebraic signatures to check remotely administered storage. In: 26th IEEE International Conference on Distributed Computing Systems (ICDCS 2006), 4-7 July 2006, Lisboa, Portugal. (2006) 12
19. Alouneh, S., Abed, S., Mohd, B.J., Kharbutli, M.: An efficient backup technique for database systems based on threshold sharing. JCP **8**(11) (2013) 2980–2989
20. Vaudenay, S.: Security flaws induced by cbc padding - applications to ssl, ipsec, wtls. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology. EUROCRYPT '02, London, UK, UK, Springer-Verlag (2002) 534–546
21. WebSite: Python programming language - official website (2015) Accesat ultima oară: Februarie, 2015, <https://www.python.org/>.
22. Hunter, J.D.: Matplotlib: A 2D graphics environment. Computing In Science & Engineering **9**(3) (2007) 90–95
23. WebSite: Cerealizer package (2015) Accesta ultima oară: Februarie, 2015, <https://pypi.python.org/pypi/Cerealizer>.
24. WebSite: Github - official website (2015) Accesta ultima oară: Februarie, 2015, <https://www.github.com>.
25. WebSite: Cod github - official website (2015) Accesta ultima oară: Februarie, 2015, <https://www.github.com/rdragos/splitting-scheme>.