

Raport de cercetare pentru UROP

Dragoş 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]

2 Scheme de partajare

In cazul unor criptosisteme acestea nu pot fi compromise chiar daca adversarul dispune de o putere computationala nelimitata. Cateva exemple de criptosisteme care garanteaza securitatea teoretica-informationala sunt: schemele de partajare, unele protocoale multi-party computation, preluarea intr-un mod sigur(securizat?) informatii de la baze de date. Securitatea teoretica vine insa cu un cost: efortul computational depus este mult mai mare decat in cazul schemelor care nu garanteaza securitatea teoretica (se bazeaza pe dificultatea computationala unor probleme cunoscute). [2]

O schema de partajare consta in distribuirea unui obiect, o informatie secreta \mathcal{S} la mai multi participanti intr-un mod astfel incat oricare grup predefinit inainte sa poate reconstitui secretul \mathcal{S} .

2.1 Criptare vs scheme de partajare

2.2 Securitatea Teoretica a Informatiei

2.3 Constructii existente

Primele scheme de partajare au fost dezvoltate independent de Adi Shamir si George Blakley in 1979. [3, 4] Denumite si scheme de treshold, acestea rezolvau cazul in care oricare grup de participanti cu cardinalul $\geq k$ (dimensiunea thresholdului) puteau reconstitui secretul S din partile primite de la dealer. Daca schema este perfect sigura atunci oricare grup cu un numar de participanti $< k$ nu obtineau vreo informatie despre S .

Alte scheme de partajare bazandu-se pe grupuri speciale de acces (in cazul schemei lui Shamir, acestea trebuia sa aiba cardinalul $\geq k$) au fost dezvoltate de Ito, Saito, si Nishizeki, realizand o generalizare a schemei lui Shamir. [5] Benaloh si Leichter au demonstrat ca schemele de partajare threshold nu pot garanta construirea decat unei fractiuni din multimea functiilor de partajare. Cei doi prezinta un exemplu trivial pentru care schema lui Shamir este insuficienta: consideram cazul in care vrem sa partajam un secret unor 4 participanti: A, B, C, D astfel incat $A + B = S$ si $C + D = S$, iar restul de combinatii ale share-urilor sa nu poate reconstitui S unde cu $+$ notam operatia de reuniune a share-urilor dintre 2 persoane. [6]. Dezavantajul acestor scheme este dimensiunea share-urilor, facand adesea majoritatea constructiilor impracticabile. [7] De asemenea, s-au dezvoltat scheme pentru modele de calcul neconventional, cum ar fi cel cuantic. [8]

2.4 Schema lui Shamir

2.5 Schema Ito, Saito, si Nishizeki

In continuare vom descrie modalitatea de distribuire a share-urilor de la care au pornit Ito, Saito si Nishizeki pentru ca schema sa aiba o structura de acces $\mathcal{A} \subseteq 2^P$ unde P este mulimea de participanti in cadrul procesului. Fie o multime de participanti $P = P_1, P_2, \dots, P_n$.

- Alegem doua numere intregi k si M , $k \leq M$ si un $q = p^z$ unde p este un numar prim iar z numar intreg pozitiv. Fie $K = GF(q)$
- Alegem $a_1, a_2, \dots, a_{k-1} \in K - 0$ intr-un mod aleator
- Luam polinomul $f(x) = a_{k-1} * x^{k-1} + a_{k-2} * x^{k-2} + \dots + a_1 + S$.
- Alegem M elemente distincte, $x_1, x_2, \dots, x_M \in K - 0$ si $Q = \{s_i = f(x_i), 1 \leq i \leq M\}$
- Alegem $S_i \subseteq Q, 1 \leq i \leq n$ si atribuim fiecarui participant P_i pe S_i . Denumim functia care se ocupa de atribuire $Assign : P \rightarrow 2^Q$. [5]

In mod evident, pentru ca modul de atribuire a share-urilor $Assign$ sa respecte structura de acces \mathcal{A} atunci $\mathcal{A} = \bigcup_i |Assign(i)| \geq k$

3 Sisteme de stocare folosind scheme de partajare

În această secțiune vom arăta câteva întrebări ale schemelor de partajare. Considerăm cazul în care vrem să stocăm rapoarte medicale, imagini, documente clasificate pe un timp îndelungat într-un mediu electronic. Pe parcursul timpului, pot apărea în schimb, diverse probleme precum dezastre naturale, defecțiunea unor componente hardware, eroare umană, etc. [9] Un sistem de stocare necesar nevoilor noastre trebuie să satisfacă cel puțin următoarele 3 condiții:

- Disponibilitatea: Informația trebuie să rămână accesibilă tot timpul, în ciuda căderilor hardware.
- Integritatea: Abilitatea sistemului de a răspunde cererilor într-un mod care garantează corectitudinea lor.
- Confidentialitatea: O persoană care nu face parte din grupul de acces să nu obțină permisiunea de a afla informații de orice fel despre datele existente în sistem

Una dintre soluțiile existente în a construi acest sistem ar putea fi criptarea datelor însă aceasta nu garantează confidentialitatea lor pentru un adversar fără o limită computațională. Majoritatea tehnicilor de criptare se bazează pe dificultatea factorizării unui număr sau cea a calculării logaritmului discret însă o dată cu dezvoltarea calculatoarelor cuantice aceste probleme nu vor mai fi atât de dificile. [10]

O alternativă la soluția cu criptare care asigură confidentialitatea dar și redundanța necesară este întrebarea sistemelor de stocare bazate pe scheme de partajare.

3.1 Arhitecturi existente

4 Rezultate obținute

4.1 Arhitectura sistemului

4.2 Erori găsite în articol

4.3 Verificarea rezultatelor

4.4 Publicarea articolului

References

1. Katz, J., Lindell, Y.: Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series). Chapman & Hall/CRC (2007)
2. Csirmaz, L.: The size of a share must be large. Journal of cryptology **10.4** (1997) 223–231
3. Blakley, G.: Safeguarding cryptographic keys. Proceedings of the 1979 AFIPS National Computer Conference (1979) 313–317
4. Shamir, A.: How to share a secret. Commun. ACM **22**(11) (1979) 612–613

5. 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
6. 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
7. Beimel, A.: Secret-sharing schemes: a survey. In: *Coding and cryptology*. Springer (2011) 11–46
8. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. *Physical Review A* **59**(3) (1999) 1829
9. Storer, M.W., Greenan, K.M., Miller, E.L., Voruganti, K.: Potshards - a secure, recoverable, long-term archival storage system. *TOS* **5**(2) (2009)
10. 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