ANALIZA EFICIENȚEI DE APLICARE A TRANSFORMĂRILOR HADAMARD ÎN METODELE CRIPTOGRAFICE

Gheorghe PURCEL

Universitatea Tehnică a Moldovei, Facultatea Electronică și Telecomunicații,
Departamentul Telecomunicații și Sisteme Electronice, grupa SSET-172, Chișinău, Republica Moldova

Autorul corespondent: Gheorghe, Purcel, gheorghe.purcel@srco.utm.md

Rezumat. *Este prezentată analiza aplicabilității transformatei Hadamard în tehnologii informaționale. Cercetarea eficienței metodei criptografice Pseudo-Hadamard-Transform în algoritmul de criptare SAFER. Determinarea avantajelor și dezavantajelor acestui algoritm pentru a identifica riscuri de securitate și avantajele comparative între algoritmi din familia SAFER. Cercetarea implementării metodei criptografice SAFER+ pentru tehnologia Bluetooth. Compararea algoritmilor SAFER+ cu alți algoritmi propuși pentru tehnologia respectivă.*

Cuvintele-cheie: *Criptare, transformări Hadamard, SAFER, metoda Harrington.*

Introducere

Ritmul accelerat de dezvoltare a tehnologiilor informaționale a creat necesitatea formării unor rețele de comunicații flexibile și sigure. În scopul asigurări segmentului de siguranță a rețelelor de comunicații se impun măsuri suplimentare de siguranță la nivel software, care constituie transmiterea informației prin canalele de transmisiune în formă criptată. În scopul creării unui proces de criptare viabil și cu o utilizare optimă a resurselor echipamentelor, putem implementa transformata Hadamard. Aceasta reprezintă un exemplu a unei clase generalizate, care realizează o operație ortogonală, simetrică, involutivă asupra numerelor reale.

Aplicabilitatea transformatei Hadamard

Folosirea transformatei Hadamard și a matricelor de tip Hadamard în sistemele de comunicații, permite filtrarea, codarea și crearea algoritmilor de criptarea care oferă siguranță înaltă a cifrului, folosire minimă a resurselor echipamentului și timp redus de criptare. Avantajul decisiv al transformatei Hadamard constă în aceea că pentru transformarea liniară datorită structurii matricelor, se solicită mai puține operațiuni elementare, calculul mai rapid și un consum mai mic de resurse.

Avantajele și siguranța

Familia algoritmilor SAFER este compusă din șapte algoritmi. Algoritmii au fost publicați pe parcursul a mai multor ani și cu publicarea fiecărui nou algoritm, metoda criptografică SAFER devine mai sigură, rapidă și eficientă. Publicarea versiunilor mai noi presupunea înlăturarea neajunsurilor și mărirea siguranței de criptare a algoritmului. Astfel algoritmii dispun de rezervă mare în cazul procedurii de criptare întărită prin mărirea cheii de criptare, cerințe joase de resurse utilizate. Ca neajuns reprezenta procedura de generare a sub cheilor, care a fost depășită la ultimele versiuni, prin modificare algoritmului de generare [1].

Compararea algoritmilor pentru tehnologia Bluetooth

Criptarea în tehnologia Bluetooth asigură siguranța împotriva atacurilor de căutare exhausivă a codului PIN, atacurilor de localizare, aflării cheilor secret schimbate între stații. În calitate de algoritm de securitate a fost utilizat SAFER+, care folosește transformate Fast-Walsh-Hadamard. Oferind o securitate ridicată din motiv că dispune de bloc de rotație între fiecare rundă din SAFER+ existent. În primul rând aceștia folosesc transformare liniară Pseudo-Hadamard, pentru crearea difuziei necesare. În al doilea rând utilizează factori constanți aditivi (vectori de polarizare) în programarea pentru evitarea tastelor slabe. Se compune din două unități principale: calea datelor de criptare și unitatea de planificare a cheilor [2].

Metoda Harrington

În scopul securizării tehnologiei Bluetooth sa propus următoarele metode criptografice: Triple DES, Pipelined AES, ECDH, Safer Plus, SAFER ++. Compararea algoritmilor are loc în baza criteriilor : timpului, frecvenței, transferul de date, numărul necesar de lovituri pentru un atac. Pentru crearea unui clasament a algoritmilor în baza criteriilor comparați au fost utilizat funcția Harrington. Construirea acestei funcții generalizate este ideea de a transforma valorile naturale ale răspunsurilor particulare într-o scară fără dimensiuni a preferențiuni. Scopul său este de a stabili corespondența dintre parametrii fizici și psihologici în (Tabelul 1, Figura 1) [3].

Tabelul 1

Analiza comparativă a metodelor criptografice după metoda Harrington

Algoritmi de criptare	Y_1	Y_2	Y_3	Y_4	d_1	d_2	d_3	d_4	Parametrul D	Nota
Pipelined AES	88.33	12.56	688787	52.68	0.2	0.25	0.2	0.2	0.21	Foarte slab
Triple DES	99	10.1	943999	46.63	0.07	0.2	0.63	0.1	0.25	Slab
ECDH	78.08	14.82	722519	59.19	0.40	0.38	0.32	0.37	0.37	Satisfăcător
Safer Plus	65.44	16.63	873736	67.11	0.63	0.56	0.42	0.63	0.64	Bine
Safer++	37.19	26.88	16005882	124.14	0.98	0.98	0.98	0.97	0.97	Excelent

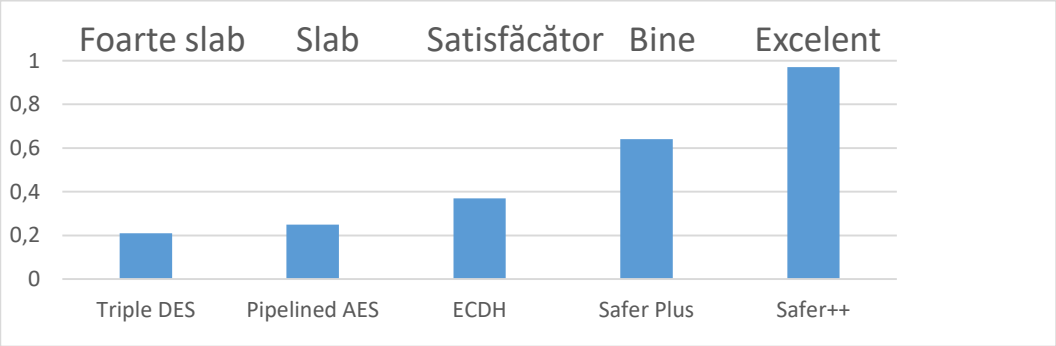

Figura 1. Rezultatele analizei comparative a metodelor criptografice după parametrul D.

Concluzii

Rezultatele analizei comparative arată că SAFER++ modificat a îmbunătățit securitatea în comparație cu algoritmul de criptare anterior. La fel acesta a devenit mai rapid datorită procedurii modificate de generare a cheilor și procedurii de transformare liniară, care a fost considerabil modificată prin optimizarea procedurii de calcul. Pentru tehnologia Bluetooth metoda de criptare SAFER+ oferă o securitate ridicată din motiv că dispune de bloc de rotație între fiecare rundă a algoritmului. Se utilizează algoritmul SAFER++ din două motive, deoarece este cel mai bun după toți parametri și în plus mai deține o rezervă considerabilă în avans cei permite sa deducem că va fi actual încă o perioada îndelungată.

Referințe web:

1. *MathWorks: Wals-Hadamard Transform*. https://mathworks.com/help/signal/ug/walshhadamard-transform.html.
2. *International Journal of Wireless & Mobile Network*, Sharmila D. https://www.researchgate.net/publication/41099634.
3. M. F. RESHETNEV, *Generalized Harrington's Desirability Function for the Comparative Analysis of Technical Facilities.* https://cyberleninka.ru/article/n/obobschennaya-funktsiya-zhelatelnosti-harringtona-dlya-sravnitelnogo-analiza-tehnicheskih-sredstv/viewer.