Universitatea Tehnică a Moldovei

ANALIZA EFICIENȚEI DE APLICARE A TRANSFORMĂRILOR DE TIP HADAMARD ÎN METODELE CRIPTOGRAFICE

Student: **Purcel Gheorghe**

Coordonator: **Cerbu Olga**
Conf. univ., dr.

Chișinău, 2020

MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admis la susținere
Șef departament:
Sava Lilia, conf. univ,. dr.,
_____
„____”_____ 2020

Analiza eficienței de aplicare a transformărilor de tip Hadamard în metodele criptografice

Teză de master

Student: _____Purcel Gheorghe

Coordonatorul: _____ Cerbu Olga
Conf. univ., dr.

Chișinău, 2020

REZUMAT

Purcel Gheorghe

Tema tezei de master: Analiza eficienței de aplicare a transformărilor de tip Hadamard în metodele criptografice.

Structura lucrării: Introducere, Capitolul 1: Analiza eficienței transformărilor de tip Hadamard; Capitolul 2 : Compararea în baza funcției Harington a algoritmilor de criptare pentru tehnologie Bluetooth, Capitolul 3: Implementartea algoritmului efectiv în criptare; Concluzii; Bibliografia; Anexă; 21 de tabele; 22 fig, 11 formule.

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

Scopul lucrării: Analiza eficienței de aplicare a transformărilor de tip Hadamard în metodele criptografice.

Obiectivele lucrării:

1. Analiza asupra transformatei Hadamard prin studiul detaliat a aplicabilității acesteia în tehnologiile informaționale. Cercetarea utilizării transformatei în algoritmii de criptare a informației.
2. Analiza eficienței metodei criptografice Pseudo-Hadamard-Transform în SAFER. Determinarea avantajelor și dezavantajelor acestui algoritm pentru a identifica riscuri de securitate.
3. Analiza comparativă între metodele criptografice SAFER și SAFER+. Determinarea diferențelor între metodele criptografice și avantajele comparative între algoritmi din familia SAFER.
4. Cercetarea implementării metodei criptografice SAFER + pentru tehnologia Bluetooth. Compararea algoritmului SAFER+ cu alți algoritmi propuși pentru tehnologia respectivă.
5. Analiza eficienței a algoritmilor de criptare pentru tehnologia Bluetooth.
6. Dezvoltarea algoritmului efectiv de criptare.

Metodele aplicate: Analiză comparativă, funcția Harington, metode criptografice.

Rezultatele obținute: Asimilat structura și aplicabilitatea transformatei Hadamard în tehnologii informaționale și criptare. Evidențiat avantajele și neajunsurile metodelor criptografice în structura cărora persistă transformata Hadamard. A fost efectuată o analiză comparativă eficienței a algoritmilor în baza utilizării funcției Harrington. Stabilit corespondența între valorile naturale și parametri psihologici în scopul unei evaluări subiective a metodelor criptografice. Implementat algoritmul efectiv de criptare.

ABSTRACT

Purcel Gheorghe

Title:: Analysis of the effectiveness of application of Hadamard-type transforms in cryptographic methods.

Thesis structure: Introduction, Chapter 1: Analysis of the efficiency of Hadamard-type transformations; Chapter 2: Comparison of Bluetooth technology encryption algorithms based on the Harington function, Chapter 3: Implementation of the actual encryption algorithm; conclusions; bibliography; annex; 21 tables; 22 fig, 11 formulas.

Keywords: Encryption, Hadamard Transformations, SAFER, Harrington method.

Thesis purpose: Analysis of the efficiency of application of Hadamard-type transformations in cryptographic methods.

Objectives:

1. Analysis on the Hadamard transform through the detailed study of its applicability in information technologies. Research of the transform usage in information encryption algorithms.
2. Analysis of the efficiency of the Pseudo-Hadamard-Transform cryptographic method in SAFER. Determine the advantages and disadvantages of this algorithm to identify security risks.
3. Comparative analysis of SAFER and SAFER + cryptographic methods. Determin the differences between cryptographic methods and comparative advantages of algorithms in the SAFER family.
4. Research the implementation of the SAFER + cryptographic method for Bluetooth technology. Comparison of the SAFER + algorithm with other algorithms proposed for the respective technology.
5. Analysis of the efficiency of encryption algorithms for Bluetooth technology.
6. Development of the effective encryption algorithm.

Applied methods: Comparative analysis, efficiency research, algorithm implementation.

The results obtained: The structure and applicability of the Hadamard transform in information technologies and encryption had been assimilated. Determoned are the advantages and disadvantages of cryptographic methods in the structure of which the Hadamard transform persists. A comparative efficiency analysis of the algorithms was performed based on the Harrington function. Established the

correspondence between natural values and psychological parameters for the purpose of a subjective evaluation of cryptographic methods. The effective encryption algorithm was implemented.

CUPRINS

INTRODUCERE

Ritmul accelerat de dezvoltarea a tehnologiilor informaționale în societatea secolului XXI, a creat necesitatea formării unor rețele de comunicații flexibile, sigure cu o acoperire cât mai mare a teritoriilor necesare. Aceasta mai este impusă de partea economică unde la moment în orice segment persistă tehnologiile informaționale sau sunt în proces de implementare. În scopul asigurări segmentului de siguranță a rețelelor de comunicații se impun măsuri suplimentare de siguranță la nivel software. Una din măsurile software de siguranță de bază, constituie transmiterea informației prin canalele de transmisiune în formă criptată.

Criptarea reprezintă procesul de mascare a informației transmise sau păstrate, în scopul ca aceasta să fie ilizibilă fără cunoștințe speciale. Acest lucru este impus de un șir de domenii, unde criptarea informației expediate reprezintă o necesitate stringentă cum ar fi: sistemul bancar, comerțul electronic, conexiunea către stația de la serviciu sau către un echipament de rețea pentru configurări suplimentare, conexiunea către un sistem unic ce deține date confidențiale pentru resursele umane din cadrul instituției, ș.a. În acest sens se utilizează criptarea simetrică. Pe baza acestui tip de criptare au fost dezvoltate mai multe algoritme de criptare. Caracteristicele de bază ale algoritmilor de criptare sunt: viabilitatea, viteza de procesare admisibilă și ușurința în utilizare. Pentru asigurarea acestor caracteristici în fiecare algoritm de criptare se utilizează diferite procese care oferă duritate algoritmului și totodată utilizează resursele echipamentului relativ optim.

În scopul creării unui proces viabil și cu o utilizare optimă a resurselor echipamentelor, a fost implementată metoda elaborată de matematici: francez Jackues Hadamard, germano-american Hans Rademacher, american Josep L. Walsh, a transformării Walsh-Hadamard, Hadamard-Rademacher-Walsh. Aceasta reprezintă un exemplu a unei clase generalizate, care realizează o operație ortogonală, simetrică, involutivă asupra numerelor reale. Poate fi definită recursivă sau binară. Printre avantaje se numără: utilizarea procesării computerizate folosind adunarea, care este mai rapidă cu mult în comparație cu multiplicarea. La fel aceasta se mai utilizează la procesarea digitală a semnalului și imaginilor, reprezentarea compactă a semnalului. Transformarea Walsh-Hadamard o întâlnim într-o mare varietate de aplicații inginerești și științifice, inclusiv în funcții îndoite și tehnici de optimizare

criptanalitică în criptografie. În primul rând este o tehnică utilizată în criptografie, în primul rând cifrul bloc de proiectare. Funcția de bază este de a oferi difuzie criptografică.

O valoare importantă a transformatei respective în criptare se limitează la două proprietăți foarte dorite în criptografie. În primul rând întrucât transformarea în două elemente este reversibilă, tot așa sunt transformate toate transformările de nivel superior din aceasta. Pentru criptografie este important ca transformarea să fie reversibilă, astfel încât decriptarea să poată fi inversa criptării. În al doilea rând pentru orice nivel al transformării este clar că fiecare bloc de ieșire depinde de toate blocurile de intrare. Utilitatea acestei proprietăți este foarte importantă în ceea ce privește difuziunea criptografică.

Un avantaj suplimentar al transformatei în comparație cu alte metode utilizate în criptografie care utilizează înmulțirea 16x16, constă în aceea că pentru transformarea liniară datorită structurii matricelor transformărilor Hadamard, se solicită cu mult mai puține operațiuni elementare. Diferența considerabilă este că la înmulțirea a liniei de 16 biți în matrița 16x16 în general se efectuează 15*16 operații de completări și 16*16 operații de înmulțire. Transformarea Hadamard solicită doar 6 operații de completare.

Proprietățile enumerate demonstrează că transformarea rapidă Wals-Hadamard este o soluție avantajoasă de a calcula eficient liniaritatea și neliniaritatea unui S-box.

BIBLIOGRAFIE

Cărți

1. Hakob, G. Sarukhanyan; Karen O. Egiazarian ; Jaakko Astola, M. Hadamard Transforms
2. Martin Harwit, Neil J.A.Sloane, M. Hadamard Transform Optics
3. Rao K. Yarlagadda, John E. Hershey, M. Hadamard Matrix Analysis and Synthesis

Site web

4. StackExchange: Signal Processing, What is the Walsh-Hadamard Transform and what is it good, 2012 [citat 04.10.2020].
   Disponibil:https://dsp.stackexchange.com/questions/1693/what-is-the-walsh-hadamard-transform-and-what-is-it-good-for.
5. Wikipedia: Hadamard Transform 2020 [citat 04.10.2020].
   Disponibil: https://en.wikipedia.org/wiki/Hadamard_transform.
6. MathWorks: Matlab for Artificial Inteligence, Wals-Hadamard Transform, [citat 06.10.2020].
   Disponibil: https://www.mathworks.com/help/signal/ug/walshhadamard-transform.html.
7. ScienceDirect: Academic Press Library in Mobile and Wireless Communications, Hadamard Transforms 2014 [citat 05.10.2020].
   Disponibil: https://www.sciencedirect.com/topics/engineering/hadamard-transform.
8. Wikipedia: Știință, Tehnologie, Inovație, Criptografie, 2018 [citat 10.10.2020].
   Disponibil: https://ro.wikipedia.org/wiki/Criptografie.
9. Academic: Encyclopedia, Dictionaries, Pseudo-Hadamard transformation [citat 10.10.2020].
   Disponibil: https://enacademic.com/dic.nsf/enwiki/595010.
10. Wikipedia: Știință, Tehnologie, Inovație, Criptografie, SAFER, 2020 [citat 15.10.2020].
    Disponibil: https://en.wikipedia.org/wiki/SAFER.
11. Cryptology ePrint Archive: Fast Pseudo-Hadamard Transforms, [citat 16.10.2020].
    Disponibil: https://eprint.iacr.org/2004/010.pdf.
12. Wikipedia: Știință, Tehnologie, Inovație, Bluetooth, 2018 [citat 20.10.2020].

Disponibil: https://ru.wikipedia.org/wiki/Bluetooth.

13. Wikipedia: SAFER, 2020 [citat 20.10.2020].
    Disponibil: https://en.wikipedia.org/wiki/SAFER.
14. Carte: Gehrmann C, Persson J, Smeets B, Bluetooth Security, 2004 [citat 30.10.2020] ISBN 1-58053-504-6.
    Disponibil: https://books.google.md/books?hl=ru&lr=&id=gUMwDwAAQBAJ&oi.
15. Netguru: Gonzola Acosta, Ways To Create a Safer Bluetooth Connection, 2018 [citat 04.11.2020].
    Disponibil: https://www.netguru.com/codestories/5-ways-to-create-a-safer-bluetooth-connection.
16. Master of Computer Science: Bluetooth Security Analysis and Improvements, 2006 [citat 10.11.2020].
    Disponibil: http://www.cs.sjsu.edu/faculty/stamp/students/cs298ReportSteven.pdf.
17. International Journal of Wireless & Mobile Network, Sharmila D, 2009 [citat 10.11.2020].
    Disponibil: https://www.researchgate.net/publication/41099634.
18. M. F. Reshetnev, Information Satellite Systems, Generalized Harrington's Desirability Function for the Comparative Analysis of Technical Facilities, [citat 25.12.2020].
    Disponibil: https://cyberleninka.ru/article/n/obobschennaya-funktsiya-zhelatelnosti-harringtona-dlya-sravnitelnogo-analiza-tehnicheskih-sredstv/viewer.
19. Wikipedia: SAFER SK-64, 2020 [citat 25.12.2020].
    Disponibil: https://ru.wikipedia.org/wiki/SAFER.