**UNIVERSITATEA “ALEXANDRU IOAN CUZA” DIN IAȘI**

**FACULTATEA DE INFORMATICĂ**



LUCRARE DE LICENȚĂ

**Titlu**

**propusă de**

### Prenume Nume

**Sesiunea:** *luna, anul*

**Coordonator științific**

**Titlu Prenume Nume**

**UNIVERSITATEA “ALEXANDRU IOAN CUZA” DIN IAȘI**

**FACULTATEA DE INFORMATICĂ**

**Titlu**

**Prenume Nume**

**Sesiunea:** *iulie, 2019*

**Coordonator științific**

**Titlu Prenume Nume**

Avizat,

**Prof. Dr. Țiplea Ferucio Laurențiu**

Data: ……………….. Semnătura: ………………

**Declarație privind originalitatea conţinutului lucrării de licenţă**

Subsemntatul(a) **Bolocan Diana** domiciliul în **România, jud. Galați, mun. Galați, str. Saturn, nr. 28, bl. B4, ap. 3** născut(ă) la data de **10 septembrie 1997**, identificat prin CNP **2970910170010**, absolvent(a) al(a) Universităţii „Alexandru Ioan Cuza” din Iaşi, Facultatea de **Informatică** specializarea **Informatică**, promoţia **2019**, declar pe propria răspundere, cunoscând consecinţele falsului în declaraţii în sensul art. 326 din Noul Cod Penal şi dispoziţiile Legii Educaţiei Naţionale nr. 1/2011 art.143 al. 4 si 5 referitoare la plagiat, că lucrarea de licenţă cu titlul: … elaborată sub îndrumarea **Prof. Dr. Țiplea Ferucio Laurențiu**, pe care urmează să o susţin în faţa comisiei este originală, îmi aparţine şi îmi asum conţinutul său în întregime.

De asemenea, declar că sunt de acord ca lucrarea mea de licenţă/disertaţie să fie verificată prin orice modalitate legală pentru confirmarea originalităţii, consimţind inclusiv la introducerea conţinutului său într-o bază de date în acest scop.

Am luat la cunoştinţă despre faptul că este interzisă comercializarea de lucrări ştiinţifice in vederea facilitării fasificării de către cumpărător a calităţii de autor al unei lucrări de licenţă, de diploma sau de disertaţie şi în acest sens, declar pe proprie răspundere că lucrarea de faţă nu a fost copiată ci reprezintă rodul cercetării pe care am întreprins-o.

Data: ………………………… Semnătura: ……………………...

**Declarație de consimțământ**

Prin prezenta declar că sunt de acord ca Lucrarea de licență cu titlul „*Titlul complet al lucrării*”, codul sursă al programelor și celelalte conținuturi (grafice, multimedia, date de testetc.) care însoțesc această lucrare să fie utilizate în cadrul Facultății de Informatică.

De asemenea, sunt de acord ca Facultatea de Informatică de la Universitatea „Alexandru Ioan Cuza” din Iași, să utilizeze, modifice, reproducă și să distribuie în scopuri necomerciale programele-calculator, format executabil și sursă, realizate de mine în cadrul prezentei lucrări de licență.

Contents

[Prenume Nume 1](#_Toc11146761)

[Introducere 7](#_Toc11146762)

[Capitolul 1. Noțiuni teoretice 9](#_Toc11146763)

[1.1 Noțiuni criptografice 9](#_Toc11146764)

[1.2 Noțiuni circuite Booleene 9](#_Toc11146765)

[Capitolul 2. Sisteme criptografice KP-ABE, extensie pentru circuite Booleene 10](#_Toc11146766)

[2.1 Descrierea extensiei 10](#_Toc11146767)

[2.2 Atacul Backtraking 12](#_Toc11146768)

[2.3 Complexitate 15](#_Toc11146769)

[2.4 Alte abordări 15](#_Toc11146770)

[2.5 Obiectiv 16](#_Toc11146771)

[2.6 Concluzii 16](#_Toc11146772)

[Capitolul 3. Prezentarea soluției 17](#_Toc11146773)

[3.1 Schimbarea fizică a circuitului 17](#_Toc11146774)

[3.2 Schimbarea sistemul criptografic 17](#_Toc11146775)

[3.3 Complexitatea noii scheme 17](#_Toc11146776)

[3.4 Concluzii 17](#_Toc11146777)

[Concluzii finale 18](#_Toc11146778)

[Bibliografie 19](#_Toc11146779)

# Introducere

Problema securității informației a apărut încă din primele zile ale comunicării, dându-l ca exemplu pe Iulius Cezar care folosește cifrul cu deplasare pentru a-și păstra mesajele confidențiale încă din anul 50 î.Hr.. Această necesitate pentru secretizarea informației a devenit din ce în ce mai importantă în mod special în perioadele de război. Printre mariile realizări în domeniul securității informației putem aminti Mașina Enigma, mecanism electromagnetic criptografic cu rotoare capabil de a cripta și decripta mesaje secrete.

Actualmente, mașinile de calcul au devenit obiecte indinspesabile oricărei persoane și prin urmare securitatea informației se află pe același nivel de necesitate. Dezvoltarea tehnologică rapidă este în acord cu necesitățle și așteptările contextului internațional. Cererea imensă a pieței, concurența dintre companiile rivale au dus la apariția unei puteri computaționale mari și de calitate la prețuri accesibile. Mașinile de calcul sunt mai la îndemână ca niciodată, fie prin achiziție directă din magazine, fie prin serviciile Cloud oferite și cu toate acestea, schimbările continue și rapide fac ca acestea să rămână susceptibile la atacuri de securitate.

Toate asptectele menționate mai sus duc la concluzia că securitatea informației va rămâne un domeniu solicitat și de o importanță mare, cu o gamă variată și constantă de probleme ce trebuie rezolvate. Astfel, îmi încep lucrarea de licență cu scopul de a generaliza și eficientiza pe cât posibil un aspect din acest larg domeniu menționat, și anume schemele criptografice KP-ABE în circuite Booleene prezentate în articolul de specialitate [1]. Noua abordare propusă se bazează atât pe aplicare de principii fundamentale din criptografie, cât și pe modificarea structurii fizice a circuitelor.

În Capitolul 1 se vor detalia noțiunile folosite în noua abordare, menite a fi suport teoretic pentru deciziile luate în privința modalității de soluționare a problemei generalizării și eficentizării sistemului criptografic.

În Capitolul 2 se vor prezenta articolele care stau la baza lucrării de licență, abordându-se subiecte precum complexitatea sistemului criptografic, soluționarea atacului Backtracking (atac foarte important care îngreunează generalizarea schemelor criptografice în circuitele Booleene), obiectivele propuse a fi atinse și alte abordări întâlnite.

Capitolul 3 conține soluția propusă, alături de explicații pentru deciziile făcute, demonstrații de securitate, complexitatea noii scheme și o concluzie în care se vor evidenția diferențele dintre abordările menționate mai sus.

# Capitolul 1. Noțiuni teoretice

Înainte de a începe descrierea lucrării de licență se vor prezenta noțiuni teoretice care stau la baza lucrării și care vor ajuta la buna înțelegere a acesteia. În acest capitol se vor prezenta atât noțiuni teoretice din domeniul criptografic, cât și despre circuite Booleene.

# Noțiuni criptografice

*Grup ciclic multiplicativ.* Un grup este o tuplă , unde este o mulțime și este o operație binară, care satisface următoarele proprietăți:

Un grup se numește multiplicativ dacă operatorul este operatorul de înmulțire.

Un grup este ciclic dacă prin aplicări repetate a operatorului se pot obține toate elementele grupului. Un astfel element particular din care se poate construi tot grupul se numește *generator*, notat *.*

*Forme biliniare.* Fie trei grupuri ciclice de același ordin. O formă biliniară de la la este o funcție unde pentru

.[[1]](#footnote-1)

*Problema logaritmului discret.* Logaritmii discreți sunt logaritmi definiți în contextul grupurilor ciclice multiplicative. Fie un generator al grupului ciclic multiplicativ . Știm că fiecare element al lui poate fi scris ca . Problema logaritmului discret este definită astfel: dat și să se găsească ().[[2]](#footnote-2) Există grupuri pentru care rezolvarea problemei este dificilă (precum , unde este un număr prim mare). Grupuri preferate folosite în criptografie sunt și subgrupurile ciclice ale curbelor eliptice peste corpuri finite.[[3]](#footnote-3)

*Problema decizională biliniară Diffie-Hellman.* Problema computațională Diffie-Hellman spune că, date fiind și cu random uniform și independent alese din , valoarea arată ca un element oarecare din , grup multiplicativ ciclic. Problema decizională Diffie-Hellman are pe lângă valorile de mai sus și pe , cu ales de asemenea random uniform și independent din și arată că și sunt computațional indisitingibile.[[4]](#footnote-4) Problema decizională biliniară Diffie-Hellman în grupul bilinear este problema distingerii dintre și date fiind cu generator pentru și valori random alese din . Asumpția problemei decizionale biliniară Diffie-Hellman în spune că nu există algoritm de timp polinomial care să rezolve problema în cu cel mult un avantaj neglijabil [1].

*Structuri de acces.* Fie o mulțime de elemente care se numesc în acest caz *atribute.* O mulțime de submulțimi nenule ale lui se numește *structură de acces autorizată* și are ca scop definirea utilizatorilor autorizați într-un sistem criptografic. Orice altă submulțime care nu aparține lui reprezintă un utilizator *neutorizat*. Structura de acces neautorizată se notează de obicei cu .

# Noțiuni circuite Booleene

*Circuit Boolean.*

*Teorema echivalenței.*

# Capitolul 2. Sisteme criptografice KP-ABE, extensie pentru circuite Booleene

Criptarea bazată pe atribute de acces (ABE) este un tip de criptare pe chei publice, în care identitatea utilizatorului este definită ca un set de atribute (exemplu: rolurile unui angajat într-o companie), fiind subclasată în key-policy ABE (KP-ABE) și în chiphertext-policy ABE (CP-ABE).[[5]](#footnote-5)

În CP-ABE [2], informația criptată poate fi accesată numai de utilizatorii ale căror credențiale satisfac politica de securitate. O politică de securitate poate fi definită peste atribute folosind conjuncții, disjuncții și porți , unde reprezintă numărul de atribute care trebuie să fie prezente dintre cele . Autorizația este inclusă în mesaul încriptat, astfel permisiunea realizându-se implicit.

În KP-ABE [3], politica de access este codificată în cheia secretă a utilizatorului, mesajul criptându-se după setul de atribute. Fiecărei chei îi este asociată o structură de acces care specifică ce tip de criptotext poate decripta. Structura de acces folosită este un arbore, ale cărui noduri frunze sunt toate elementele din setul de atribute. Fiecare criptotext are etichetat un set de atribute descriptive.

# Descrierea extensiei

În lucrarea de bază [1] a licenței se demonstrează posibilitatea acomodării schemei KP-ABE pentru circuite Booleene (monotone) folosindu-se forme biliniare. Sistemul criptografic are la bază patru algoritmi pentru setup, criptare, generare de chei și decriptare:

1. este primul algoritm apelat în sistem, care primește ca parametru de intrare λ, un parametru de securitate, ce va returna un set de parametrii publici (PP) și o cheie secretă (MSK). Se folosește parametru λ pentru alegerea unui număr prim , a două grupuri multiplicative și de ordin , a unui generator din și a unei forme biliniare . Se definește setul de atribute, și pentru fiecare atribut din . La final, setul de parametrii arată în felul următor:
2. este algoritmul de criptare a mesajului primit peste setul de atribute în care se alege un și se returnează
3. generează o cheie de decriptare pentru structura de acces definită de circuitul pentru inputuri astfel:

* Se generează din , unde reprezintă un algoritm ce returnează o listă de partajări pentru firele de input asociate secretului , ca în Fig. 1.
* Se returnează , unde , pentru fiecare

1. primește ca parametrii valorile și definite anterior și decriptează astfel:

* Se calculează , unde , pentru fiecare și , și este o listă de simboluri , pentru fiecare
* Se generează o listă de valori în asociate fiecărui fir din input prin , algoritm determinist care returnează rezultatul evaluării în setul de atribute
* Se calculează , unde este firul de output al circuitului

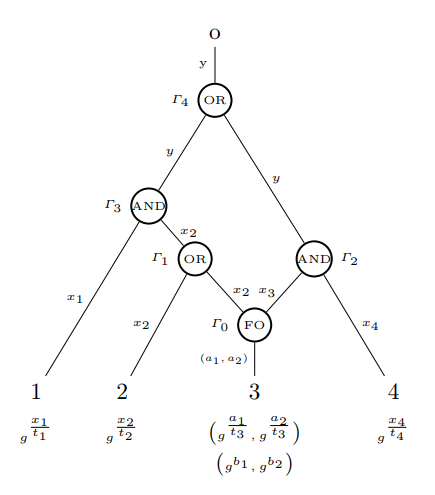


Fig. 1. Setup în circuitul Boolean [1]

Procesul de construcție pe porțile circuitului Boolean se realizează astfel:

* Pentru și : și
* Pentru și : pentru fiecare element se alege random uniform și se calculează astfel încât . și
* Pentru și , : pentru fiecare , se alege random uniform și se calculeaza astfel încât . , și

Soluția propune adăugarea unor porți ajutătoare fanout (FO), care elimină șansa atacului backtraking.

# Atacul Backtraking

Atacul backtraking reprezintă o exploatare a scurgerii de informații din poarta discutat în lucrările [1, 5].

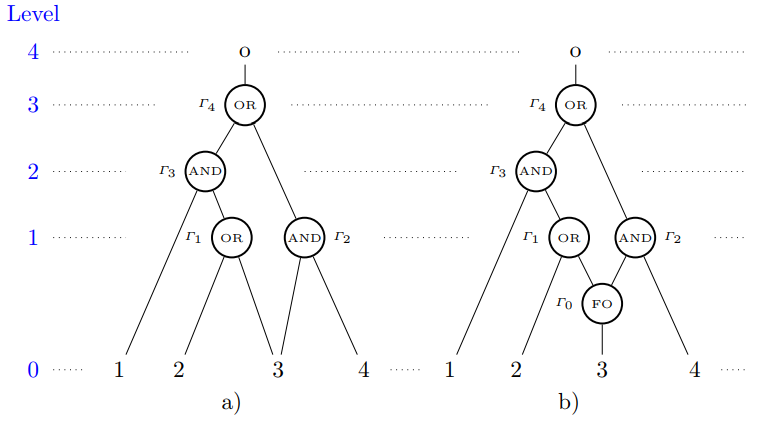


Fig. 2. a). Circuit Boolean în care apare atacul backtraking [1]

Fig. 2. b). Circuit Boolean în care atacul backtraking este soluționat prin folosirea porții ajutătoare [1]

În procesul de cosntrucție , poarta , , trimite mai departe valoarea din firul către firele de input și . Astfel, dacă se încearcă o decriptare pe atributele în circuitul boolean din Fig. 2. a). atunci utilizatorul este autorizat și primește cheia de decriptare. Pentru atributul 2 se cunoaște valoarea și știm că din funcționalitatea porții descrisă mai sus, deci Astfel, valoarea calculată la firul de input pe atributul 2 „migrează” la atributul 3 prin poarta . Acest lucru nu ar trebui să se întâmple și numai seturile de atribute sunt autorizate în acest caz.

După cum se poate vedea mai sus, atacul backtraking apare doar atunci când există un fanout mai mare de 1 în circuit, altfel nu ar reprezenta o problemă de securitate. Două modalități de prevenire a atacului sunt limitarea fanout-ului circuitului Boolean la 1 din lucrarea [4] (discutată în secțiunea 1.4 a lucrării de licență) sau modificarea sistemului criptografic prin adăugarea unei porți ca în Fig. 2. b). [1].

Motivul pentru care poarta rezolvă problema atacului backtraking este la baza funcționalității ei. Deoarece aceasta împarte valorile care corespund unic unei etichete , astfel ...

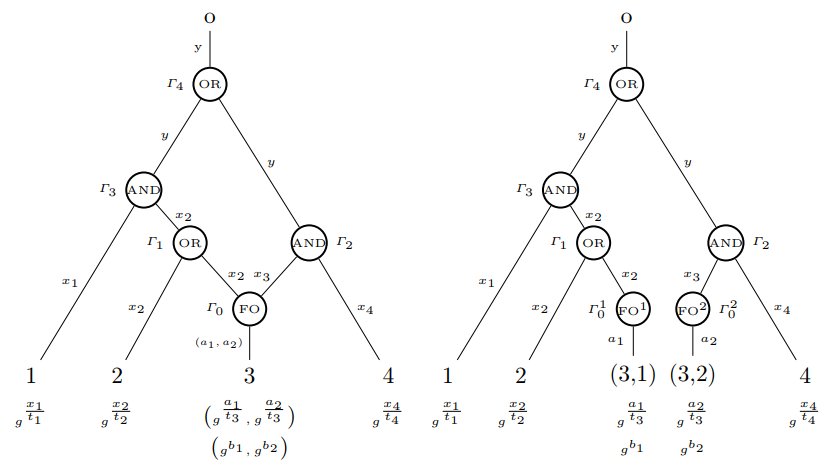


Fig. 3. a). Circuit boolean cu poartă [1]

Fig. 3. b). Arborele de acces pentru circuitul alăturat[1]

# Complexitate

După cum se poate observa din funcționalitatea schemei criptografice, cea mai costisitoare structură o reprezintă cheia de decriptare. Mărimea acesteia depinde scrict de complexitatea circuitului Boolean, crescând rapid în prezența porților .

Pentru a putea discuta de complexitatea schemei, presupunem că circuitul Boolean are fire de input și porți cu fanout de cel mult .

Cel mai fericit caz de complexitate este atunci când nu exista porți pe același drum. Din cele fire de input, o să aibă cel puțin două și cel mult valori partajate, restul având strict una, în final cheia de decriptare având componente.

Cel mai puțin fericit caz este atunci când există porți pe același drum. Poarta de pe nivelul cel mai înalt va trimite cel mult partajări către o poartă pe un nivel mai jos, care la rândul ei va trimite cel mult partajări. Atfel, la final vor exista cel mult partajări trimise către unele firele din input, unde reprezintă numărul de nivele care conțin porți .

# Alte abordări

La prima vedere, o soluție foarte ușoară (și care s-a dovedit a fi mai eficientă decât schema criptografică prezentată anterior) este separarea forțată a firelor, limitându-se astfel fanout-ul la 1. O astfel de abordare se detaliază în lucrarea [4], care are la bază articolul de specialitate [1]. Contribuția adusă în această lucrare constă în conversia tuturor fanout-urilor mai mari decât 1 în fanout-uri de strict 1 (exemplu Fig. 4.), astfel se renunță la porțile ajutătoare , schema criptografică păstrând restul funcționalităților neschimbate.

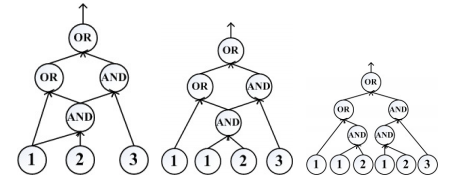


Fig. 4. Reconstrucția circuitului Boolean [4]

Complexitatea cheii de decriptare în schema criptografică de mai sus este în cel mai bun caz și în cel mai rău caz și nu mai există lista de valori partajate .

# Obiectiv

Porțile FO elimină șansa atacului backtraking, dar sunt foarte costisitoare pentru cheia de decriptare și reprezintă operații în plus pentru întărirea sistemului criptografic. Abordarea anterioară descrisă mai sus, are de asemenea dezavantajele ei. Deși este mai eficientă, aduce adăugări consistente în structura circuitului Boolean, pe lângă cele de la cheia de decriptare.

Luând în seamă aceste considerente, se dorește eficientizarea pe cât de mult posibil a schemei prin reducerea spațiului fizic al circuitului și a mărimii cheii de decriptare.

# Concluzii

# Capitolul 3. Prezentarea soluției

După cum s-a putut observa pe parcursul prezentării lucrării, cea mai mare dificultate întâlnită în schemele criptografice descrise a fost impusă de fanout-ul în porțile . Abordările anterioare aduc modificări fie în domeniul criptografic [1], fie în domeniul circuitelor [2], însă niciuna nu îmbină ambele domenii cu adevărat. De aceea, mi-am propus să contribui cu o soluție care s-a dovedit a fi simplă și eficientă și care reușește să le unească pe amândouă.

Noua schema criptografică are două mari componente: o parte de analiză a circuitului Boolean și una de înlocuire de porți în zone particulare.

# 3.1 Schimbarea fizică a circuitului

# 3.2 Schimbarea sistemul criptografic

# 3.3 Complexitatea noii scheme

# 3.4 Concluzii

# Concluzii finale

# Bibliografie

[1] Ferucio Laurențiu Țiplea și Constantin Cătălin Drăgan. Key-policy Attribute-based Encryption for Boolean Circuits from Bilinear Maps. În BalkanCryptSec 2014, Istanbul, Turcia, 16-17 Octombrie, 2014, paginile 175-193, LNCS 9024

[2] John Bethencourt, Amit Sahai și Brent Waters. Ciphertext-policy attribute based encryption. În IEEE Symposium, Security and Privacy, 2007, paginile 321–334. IEEE Computer Society, 2007

[3] Vipul Goyal, Omkant Pandey, Amit Sahai și Brent Waters. Attribute-based encryption for fine-grained access control of encypted data. În ACM Conference on Computer and Communications Security, paginile 89–98. ACM, 2006. Preprint în IACR ePrint 2006/309

[4] Peng Hu și Haiying Gao. A Key-Policy Attribute-based Encryption Scheme for General Circuit from Bilinear Maps. În International Journal of Network Security, Vol.19, Nr.5, paginile 704-710, Septembrie 2017

[5] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai și Brent Waters. Attributebased encryption for circuits from multilinear maps. In Ran Canetti și JuanA. Garay, editori, Advances in Cryptology CRYPTO 2013, volumul 8043 de Lecture Notes in Computer Science, paginile 479–499. Springer Berlin Heidelberg, 2013. Preprint în IACR ePrint 2013/128

1. https://people.csail.mit.edu/alinush/6.857-spring-2015/papers/bilinear-maps.pdf [↑](#footnote-ref-1)
2. https://www.doc.ic.ac.uk/~mrh/330tutor/ch06s02.html [↑](#footnote-ref-2)
3. https://en.wikipedia.org/wiki/Discrete\_logarithm#Cryptography [↑](#footnote-ref-3)
4. https://en.wikipedia.org/wiki/Decisional\_Diffie%E2%80%93Hellman\_assumption [↑](#footnote-ref-4)
5. https://crypto.stackexchange.com/questions/17893/what-is-attribute-based-encryption [↑](#footnote-ref-5)