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

**FACULTATEA DE INFORMATICĂ**



LUCRARE DE LICENȚĂ

**Schema KP-ABE pentru circuite Booleene generale cu forme biliniare**

**propusă de**

### Diana Bolocan

**Sesiunea:** *iulie, 2019*

**Coordonator științific**

**Prof. Dr. Țiplea Ferucio Laurențiu**

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

**FACULTATEA DE INFORMATICĂ**

**Schema KP-ABE pentru circuite Booleene generale cu forme biliniare**

**Diana Bolocan**

**Sesiunea:** *iulie, 2019*

**Coordonator științific**

**Prof. Dr. Țiplea Ferucio Laurențiu**

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: **Schema KP-ABE pentru circuite Booleene generale cu forme biliniare** 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 „*Schema KP-ABE pentru circuite Booleene generale cu forme biliniare*”, 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.

Cuprins

[Introducere 6](#_Toc11534162)

[Motivație 8](#_Toc11534163)

[Capitolul 1. Noțiuni teoretice 9](#_Toc11534164)

[1.1 Noțiuni criptografice 9](#_Toc11534165)

[1.2 Noțiuni circuite Booleene 10](#_Toc11534166)

[Capitolul 2. Sisteme criptografice KP-ABE, extensie pentru circuite Booleene 12](#_Toc11534167)

[2.1 Descrierea extensiei 12](#_Toc11534168)

[2.2 Atacul Backtraking 15](#_Toc11534169)

[2.3 Complexitate 17](#_Toc11534170)

[2.4 Alte abordări 17](#_Toc11534171)

[2.5 Obiectiv 18](#_Toc11534172)

[2.6 Concluzii 18](#_Toc11534173)

[Capitolul 3. Prezentarea soluției 19](#_Toc11534174)

[3.1 Schimbarea fizică a circuitului 19](#_Toc11534175)

[3.2 Schimbarea sistemul criptografic 20](#_Toc11534176)

[3.3 Securitatea soluției 25](#_Toc11534177)

[(Adversar - Challenger) 26](#_Toc11534178)

[3.4 Complexitatea noii scheme 26](#_Toc11534179)

[3.5 Concluzii 26](#_Toc11534180)

[Concluzii finale 27](#_Toc11534181)

[Bibliografie 28](#_Toc11534182)

# 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.

# Motivație

Securitatea informației a fost întotdeauna un subiect foarte interesant pentru mine datorită caracterului său evolutiv. Este un domeniu al informaticii necesar și răspândit pretutindeni. Importanța acestuia îl face indispensabil oricărei persoane, iar modalitățile de abordare a problemelor implică mereu creativitate și perspective noi de rezolvare.

Din punctul meu de vedere, printre cele mai fascinante subiecte din securitatea informației se numără criptografia, deoarece reușește să îmbine limitările fizice ale mașinii de calcul cu artificii matematice. O altă caracteristică din criptografie care m-a atras a fost faptul că se încearcă găsirea unor modele cât mai sigure și eficiente. Inițial, s-ar crede că un sistem criptografic trebuie să fie perfect, impenetrabil teoretic, însă, deși idealistic se încearcă acest lucru, un model cu timp de rezolvare foarte mare e suficient pentru a asigura practic securitatea necesară. Această necesitate pentru aplicabilitate reprezintă una dintre principalele motive pentru care mi-am dorit să lucrez în acest domeniu.

Astfel doresc să abordez un subiect foarte interesant din securitatea informației și anume criptarea după atribute cu politici de chei, cunoscut și după acronimul KP-ABE (key policy attribute based encryption), în contextul circuitelor Booleene. Scopul lucrării de licență este de a găsi un model de securitate care poate fi aplicat pe circuite Booleene generale.

După cum se poate deduce din denumirea schemei, KP-ABE este un model de securitate bazat pe criptare și decriptare după caracteristici. Un astfel de model se folosește cu scopul de a evita partajarea cheii de decriptare de la un utilizator la altul, creându-se astfel grupuri de utilizatori cu aceleași atribute care au acces individual la funcționalitatea modelului.

O soluție pentru generalizarea schemei criptografice este foarte importantă deoarece un circuit Boolean bazat pe o funcție Booleană nu poate reprezenta orice structură de acces. Astfel mi-am propus să găsesc o abordare care să fie atât viabilă cât și eficientă.

Două dintre modelele care generalizează schema criptografică KP-ABE pentru circuite Booleene sunt discutate pe parcursul lucrării de licență. Una dintre ele, și anume lucrarea [1], este în același timp articolul de bază de la care pornește lucrarea de licență. Ambele articole au ajutat la construcția noului model criptografic ce va fi prezentat în Capitolul 3.

# 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 . Ipoteza 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 .

*Adversar.* Din punct de vedere criptografic, un adversar este un algoritm cu putere computațională nelimitată sau un algoritm cu putere computațională limitată (precum un algoritm de timp polinomial).[[5]](#footnote-5) Adversarul este văzut ca o entitate malițioasă care are ca scop principal trecerea de o proprietate de securitate pentru a descoperi un secret sau corupe de date ș.a.m.d.

*Oracol.* Un oracol este o entitate a cărei securitate se încearcă a se demostra cu ajutorul unui adversar. Jocul criptografic dintre oracol și adversar se bazează pe schimb de răspunsuri, unde adversarul încearcă să găsească informații utile din interacțiunea cu oracolul.

# Noțiuni circuite Booleene

*Circuit Boolean.* Un circuit Boolean este un model matematic pentru circuite logice digitale compus din porți logice și fire.[[6]](#footnote-6) Porțile întâlnite într-un circuit sunt: și ­. Un circuit Boolean se numeste *monoton* dacă este compus numai din porți logice și . În funcție de componența circuitul Boolean, acesta poate fi rescris folosindu-se legea De Morgan.[[7]](#footnote-7)

*Legea De Morgan.* În logica propozițională și algebra Booleană, legile lui De Morgan sunt o pereche de reguli de transformare care permit conjuncțiilor și disjuncțiilor să fie rescrise folosind negația:

[[8]](#footnote-8)

Astfel o poartă logică poate fi rescrisă ca aplicat pe (sau ) și o poartă logică poate fi rescrisă ca aplicat pe (sau ). Această lege va fi folosită mai târziu în descrierea soluției lucrării de licență.

# 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).[[9]](#footnote-9)

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

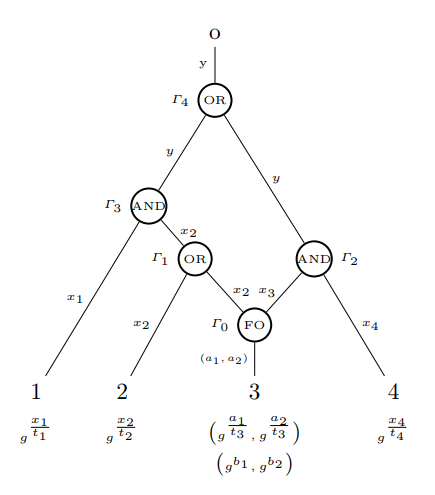


Fig. 1. Setup în circuitul Boolean [1]

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

Processul de reconstrucție se realizează astfel:

* , pentru fiecare
* Pentru cu și definite se asignează
* Pentru cu și definite se asignează
* Pentru cu definit se fac următorii pași:
  1. Se împarte în liste cu pentru fiecare
  2. pentru fiecare 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 fiind discutat în lucrările [1, 5].

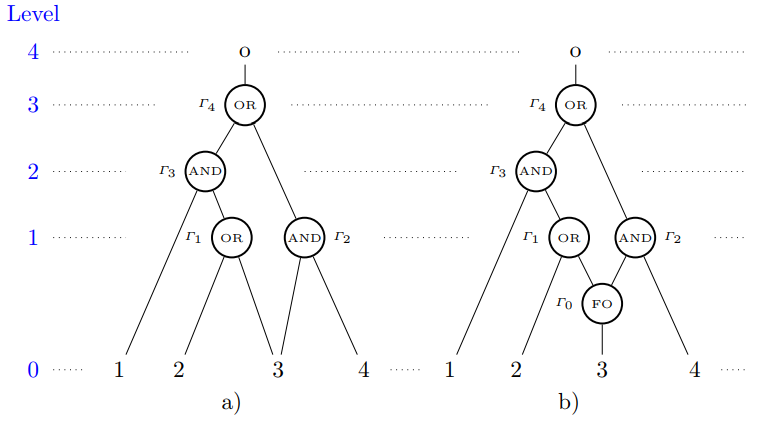


Fig. 2. a). Circuit Boolean în care apare atacul backtraking [1]

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 în câte două valori care depind de adunarea modulară.

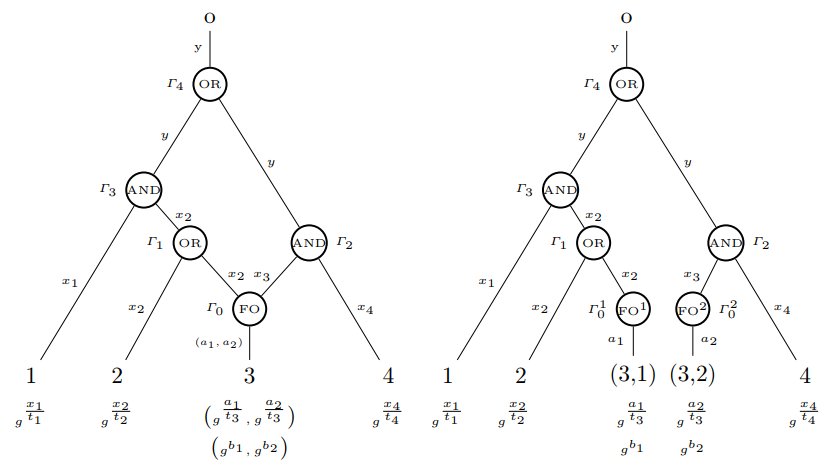


Fig. 3. a). Circuit Boolean cu poartă [1]

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 trecerea 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 funcționalitățile porților neschimbate.

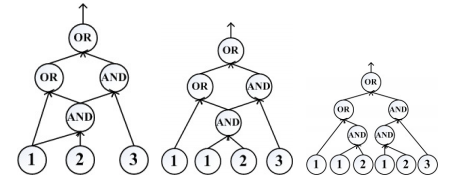


Fig. 4. Reconstrucția circuitului Boolean [4]

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.

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

De continuat

# 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 . Această problemă însă nu apare în cazul porților . De aceea, mi-am propus să contribui cu o soluție care s-a dovedit a fi simplă și care reușește să facă schema KP-ABE utilizabilă în cazul circuitelor Booleene generale fără a adăuga variabile în plus ca în cazul lucrării [1] și fără a mări structura circuitului.

Noua schema criptografică are la bază schimbarea porților cu porți noi . Schimbările aduse la algoritmii și vor fi descrise la secțiunea 3.2.

# 3.1 Schimbarea fizică a circuitului

În toate cele trei lucrări [1, 4, 5] se vorbește despre problema atacului backtraking în circuitele în care porțile au legatură cu un fanout mai mare de 1. În articolul [1], prevenția se face prin securizarea fanout-ului cu ajutorul porților , în articolul [4] fanout-ul este forțat să aibă mărimea de strict 1 expandând circuitul Boolean. În niciuna dintre cele trei lucrări nu se aduc modificări la poarta și nici nu se încearcă înlocuirea acesteia cu o alternativă mai sigură. De aceea, obiectivul acestei lucrări de licență este de a reuși evitarea atacului backtraking prin modificări aduse la porțile problematice . S-a putut observa că această problemă apare strict din cauza funcționalității porții în situații cazuale. Ceea ce se propune în această secțiune este schimbarea fizică a acestuia.

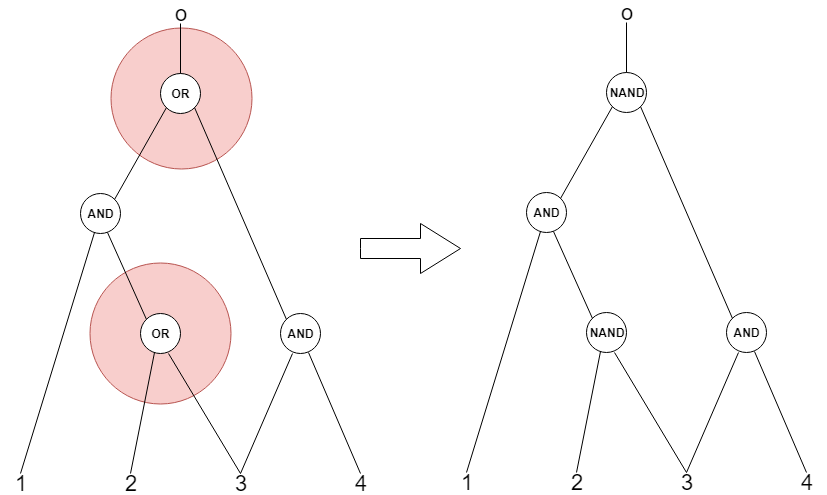


Fig. 5. a). Circuit Boolean susceptibil atacului backtraking

Fig. 5. b). Circuit Boolean . Transformarea porților în porți

Motivul pentru care s-a recurs la modificarea porții în poartă a fost datorită legii De Morgan și a siguranței criptografice a funcționalității porții . Funcționalitatea porții este asemănătoare cu cea a porții , logica noii porți fiind discutată mai îndetaliat în următoarea secțiune 3.2.

# 3.2 Schimbarea sistemul criptografic

Existența unei noi porți aduce cu ea schimbări atât la nivelul fizic al circuitului Boolean, cât și la nivelul algoritmilor criptografici. Astfel algoritmii și necesită niște completări în conformitate cu logica porții .

:

1. Toate porțile circuitului sunt nemarcate
3. Dacă este o poartă nemarcată și cu , atunci:
   1. pentru fiecare element alege random uniform și calculează astfel încât , cu
   2. calculează

* 1. asignează și

1. Dacă este o poartă nemarcată și , atunci:
   1. pentru fiecare element alege random uniform și calculează astfel încât , cu
   2. calculează

* 1. asignează și

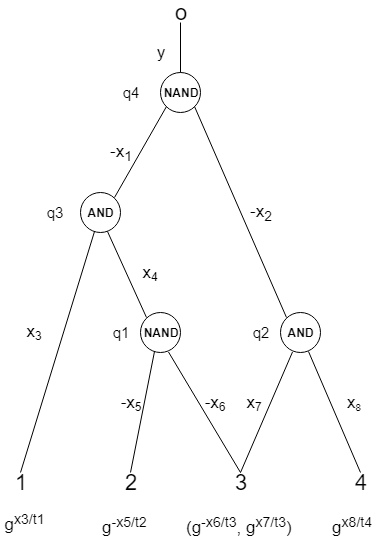


Fig. 6. Algoritmul aplicat pe circuitul Boolean

În continuare se va prezenta algoritmul ­ pe circuitul Boolean din Fig. 6. Se primește parametrul de intrare . Conform algoritmului de criptare , pentru , avem:

* Se alege random
* Se apelează apoi algoritmul în care se fac următorii pași:
  + Pentru poarta notată cu și avem și , unde este generat random uniform din și se calculează astfel .
  + Pentru poarta notată cu și avem și , unde este generat random uniform din și se calculează astfel încât .
  + Pentru poarta notată cu și avem și , unde este generat random uniform din și se calculează astfel încât .
  + Pentru poarta notată cu și avem și , unde este generat random uniform din și se calculează astfel încât .
* Se returnează cheia de decriptare:

.

: Se notează cu lista de valori de pe poziția din .

1. , pentru toate elementele
2. Dacă este o poartă nemarcată cu și definite atunci se asignează

, cu și

1. Dacă este o poartă nemarcată cu și definite atunci se asignează

, cu și

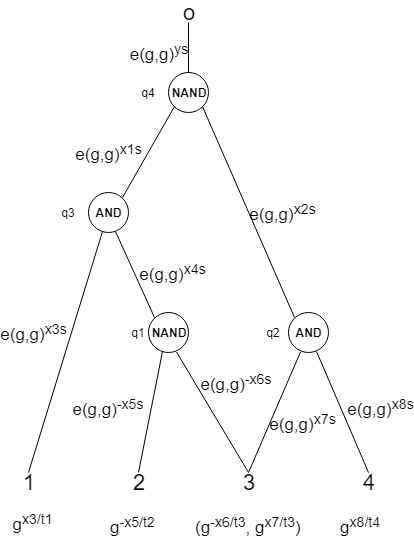


Fig. 7. Algoritmul aplicat pe circuitul Boolean

În continuare se va prezenta algoritmul pe circuitul Boolean din Fig. 7. Se primește cheia de decriptare . Conform algoritmului de decriptare , pentru avem:

* Se apelează apoi algoritmul pe parametrii de intrare , și , unde este circuitul Boolean de mai sus. În avem:
  + Pentru poarta notată avem . Știm din exemplul de mai sus că în și deci .
  + Pentru poarta notată avem . Știm de mai sus că și deci .
  + Pentru poarta notată avem . Știm de mai sus că și deci .
  + Pentru poarta notată avem . Știm de mai sus că și deci
  + returnează structura descrisă mai sus.
* primește structura returnată de
* Mesajul se decriptează astfel:

După cum se poate observa, odată cu eliminarea porții dispare lista de valori din schema criptografică. Calculul porții în se rezumă la aceeași operație multiplicativă ca în cazul porții .

În final, noua schemă KP-ABE pe circuite Booleene este definită astfel:

:

* Se folosește parametrul pentru a alege un număr prim , două grupuri multiplicative de ordin , un generator din și o formă biliniară
* Se definește setul de atribute
* Se alege
* Pentru fiecare se definește
* Se returnează

:

* Se generează random
* Se returnează

:

* Se apelează și se reține valoarea returnată în
* Se returnează , unde pentru fiecare

:

* Se calculează unde , pentru fiecare și , și este o listă de simboluri , pentru fiecare
* Se apelează funcția și se reține în variabila :
* Mesajul se decriptează

# 3.3 Securitatea soluției

Se va începe prin a se arăta că noua schema criptografică este sigură la atacul backtraking. Se cunoaște faptul că problema atacului se poate discuta doar atunci când există porți conectate la un fanout mai mare de 1. În acest model se renunță la ele și se înlocuiesc cu porți Pentru a demonstra că noua construcție previne atacul backtraking se va detalia algoritmul pe noile porți .

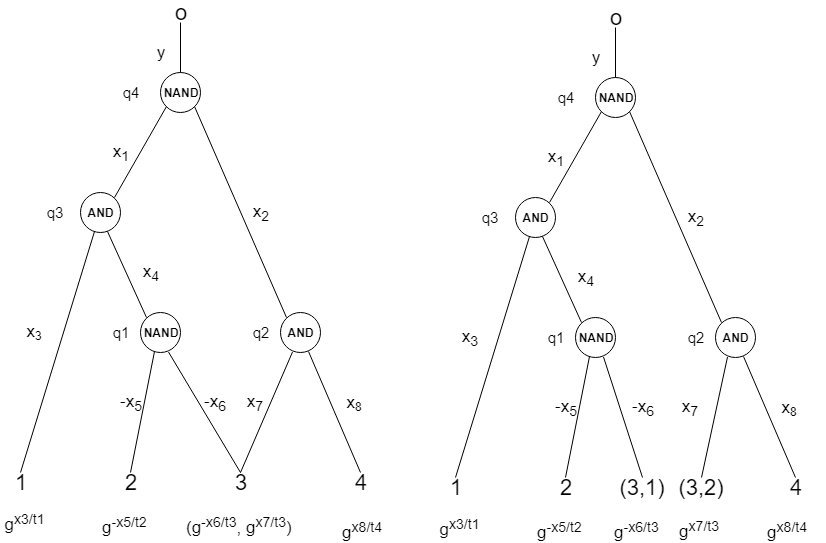


Fig. 8. a). Circuit Boolean

Fig. 8. b). Arborele de acces

În cazul circuitului Boolean din Fig. 8. a)., funcționalitatea porții impune o generare random pentru , iar este definit astfel încât . Dacă s-ar fi păstrat poarta atunci , pe când în această construcție se dorește ca valorile să fie diferite și dependente prin adunare modulară.

Pentru o mai bună înțelegere a demonstrației, se construiește arborele de acces al circuitului Boolean din fig. 8. b). astfel: se multiplică firele circuitului în funcție de numărul de drumuri până la output. Se deosebesc drumurile adăugându-se un identificator. Astfel pentru atributul avem separare în și deoarece există două drumuri spre output.

Se poate observa atât din funcționalitatea porții , cât și din arborele de acces că atacul backtraking nu poate avea loc.

A doua parte din această secțiune este demonstrarea securității modelul cu ajutorul ipotezei problemei decizionale biliniare Diffie-Hellman.

Fie un număr impar prim, și două grupuri multiplicative ciclice de ordin p și o formă biliniară definită astfel .

Se prezintă jocul criptografic dintre adversarul cu timp polinomial de rezolvare și oracolul . Oracolul primește o instanță a ipotezei problemei decizionale biliniare Diffie-Hellman cu ales de către , unde și , generator al grupului multiplicativ ciclic și .

*Inițializare.* Fie mulțimea nenulă de atribute aleasă de adversarul .

*Setup.* Oracolul alege aleator pentru toate atributele și calculează și pentru toate atributele , unde

și publică parametrii publici

*Prima parte.* Adversarul primește acces de la oracol la oracolul de generare de chei de decriptare pentru toate circuitele cu . Din punctul de vedere al adversarului, partajarea de secrete și distribuția cheilor de decriptare trebuie să arate ca în schema originală. Reconstrucția cu ajutorul funcției trebuie să returneze . Odată primită cererea, se convertește circuitul în arbore de acces și începe procesul de partajare de secrete:

* Pentru cu , unde atunci pentru fiecare avem:
  + Dacă atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și . și .
  + Dacă și atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și. și .
  + Dacă și atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și. și .
  + Dacă atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și. și .
* Pentru cu , unde atunci pentru fiecare avem:
  + Dacă atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și . și .
  + Dacă și atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și. și .
  + Dacă și atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și. și .
  + Dacă atunci pentru fiecare se alege aleator uniform și se calculează . Se definesc și. și .

va returna adversarului cheia de decriptare , unde

.

*Challenge.* Adversarul alege două mesaje de aceeași lungime și și le trimite lui , care criptează cu , unde și îl trimite înapoi adversarului. Criptotextul este

Dacă , atunci este o criptare validă a mesajului , altfel este un element aleator din .

*A doua parte.* Adversarul primește incă o dată acces la oracolul generării cheii de decriptare sub aceleași criterii ca în *a doua parte.*

*Presupunerea.* Fie presupunerea adversarului . Dacă atunci returnează , altfel .

Astfel se calculează avantajul lui .

Știm că este ales aleator uniform din , deci De asemenea, observăm că

.

În concluzie, avantajul lui este , demonstrând astfel că modelul criptografic este sigur.

# 3.4 Complexitatea noii scheme

În această secțiune se va prezenta complexitatea modelului propus în comparație cu celelalte două abordări descrise mai sus în Capitolul 2.

Pentru a putea discuta despre complexitatea soluției trebuie mai întâi detaliat algoritmul . Conform funcționalității acestuia, algoritmul partajează secrete prin fire de la output la input astfel:

* Poarta trimite mai departe câte o nouă valoare pentru și pentru pentru fiecare element din
* Poarta trimite de asemenea mai departe câte o nouă valoare pentru și pentru pentru fiecare element din

În concluzie, algoritmul trimite pentru fiecare fir din circuitul Boolean câte o nouă valoare și deci numărul de valori depinde strict de numărul de fanout-uri și dimensiunea lor. S-a observat că în cel mai rău caz numărul de elemente crește exponențial în funcție de numărul de nivele ale circuitului, lucru ce era de așteptat datorită funcționalității algoritmului. Prin urmare putem discuta despre cazurile de complexitate astfel:

1. Cazul cel mai favorabil este acela în care există o construcție care să genereze exact elemente. Cel mai simplu și evident exemplu este atunci când poate fi scris sub forma . În această situație toate firele circuitului Boolean primesc strict o valoare și deci pe nivelul de atributelor se vor găsi elemente care construiesc cheia de decriptare.
2. Cazul cel mai puțin favorabil este acela când desfășurarea circuitului Boolean se face pe nivele unde firele comunică toate cu poarta învecinată. Funcționalitatea algoritmului impune creerea de noi valori pentru fiecare nou input primit prin fir și creează o listă nouă cu aceste noi valori pentru fiecare fir în parte, creând astfel de două ori numărul de valori de pe nivel anterior. Cheia de decriptare ajunge să aibă ca număr de elemente .

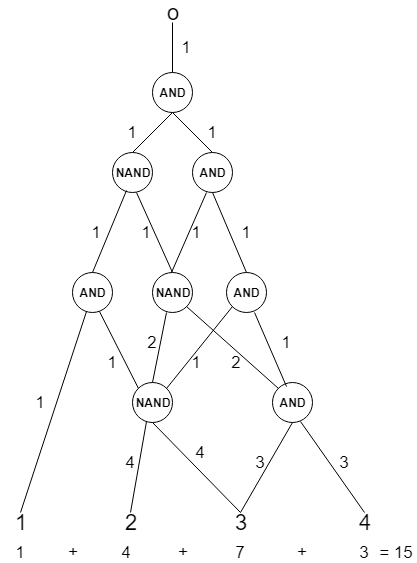


Fig. 9. Exemplu circuit Boolean . Număr de valori pentru cheia de decriptare

Fie numărul de atribute și numărul de porți cu fanout de dimensiune . În continuare, se prezintă complexitățile celorlalte scheme criptografice în comparație cu cea a soluției propuse.

|  |  |  |  |
| --- | --- | --- | --- |
| Caz | Soluția [1] | Soluția [4] | Soluția propusă |
| Favorabil |  |  |  |
| Cel mai puțin favorabil |  |  |  |

Din tabel se poate observa că numărul de elemente din această schemă criptografică nu depinde de dimensiunea fanout-ului și nici de numărul de fanout-uri. Schema criptografică depinde strict de complexitatea circuitului Boolean.

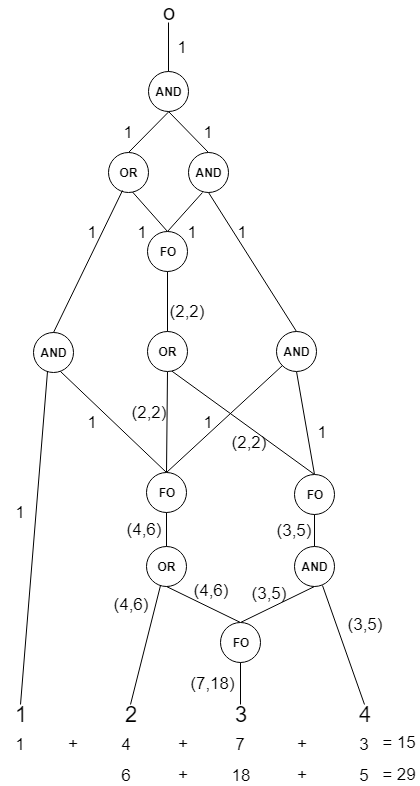


Fig. 10. Exemplu circuit Boolean . Număr de valori pentru cheia de decriptare pentru modelul din lucrarea [1].

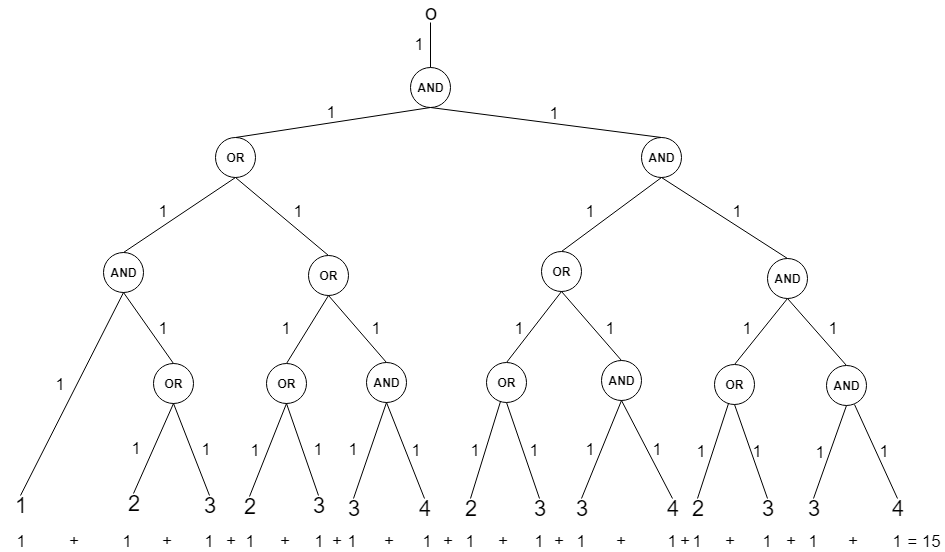


Fig. 11. Exemplu circuit Boolean . Număr de valori pentru cheia de decriptare pentru modelul din lucrarea [4].

După cum se poate observa din imaginile de mai sus, schemele criptografice definite în lucrările [1, 4] au propriile lor dezavantaje. În cazul întâlnit în Fig. 10. modelul generează pe lângă cele 15 elemente de bază, încă 29 datorită funcționalității porții , pe când în Fig. 11. nu se mai produc noi variabile dar dimensiunea circuitului Boolean crește.

# 3.5 Concluzii

Noua schemă criptografică este sigură la atacul backtraking prin funcționalitatea porților și . De asemenea, aceasta reușește să-și mențină nivelul de securitate ridicat datorită principiului deciziei biliniare Diffie-Hellman.

Complexitatea modelului depinde strict de numărul de nivele al circuitului Boolean și nu interesează cât de complex este acesta. Funcționalitatea porților permite păstrarea structurii compacte a circuitului, evitându-se astfel adăugarea de noi porți sau extinderea acestuia. Pe lângă aceasta, eliminarea porților reduce numărul de valori reținute și de calcule necesare obținerii acestora.

În concluzie, noua schemă criptografică este o schemă sigură și mai eficientă decât construcțiile precedente.

# 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. Attribute based 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. Curs Introducere în Criptografie. Perfect Security, Prof. Dr. Ferucio Laurețiu Țiplea [↑](#footnote-ref-5)
6. https://en.wikipedia.org/wiki/Boolean\_circuit [↑](#footnote-ref-6)
7. https://en.wikipedia.org/wiki/Logic\_gate [↑](#footnote-ref-7)
8. https://en.wikipedia.org/wiki/De\_Morgan%27s\_laws [↑](#footnote-ref-8)
9. https://crypto.stackexchange.com/questions/17893/what-is-attribute-based-encryption [↑](#footnote-ref-9)