Universitatea Alexandru Ioan Cuza din Iaşi, România
Departmenutul de Informatică

Reziduuri pătratice și aplicații în criptografie

- rezumat extins -

de

Anca-Maria Nica

îndrumător

Prof. Dr. Cătălin Dima

2020

Comisia de doctorat:

Conf.Dr. Adrian Iftene - preşedinte comisie
Universitatea Alexandru Ioan Cuza din Iaşi
Prof.Dr. Cătălin Dima - îndrumător
Universitatea Alexandru Ioan Cuza din Iaşi /
"Paris Est Creteil - Val de Marne"
Prof.Dr. Constantin Popescu - referend
Universitatea din Oradea
Prof.Dr. Ferucio Laurenţiu Ţiplea - referend
Universitatea Alexandru Ioan Cuza din Iaşi
Conf.Dr. Octavian Catrina - referend
Universitatea Politehnică din Bucureşti
Conf.Dr. Mihai Dumitru Prunescu - referend
Universitatea din Bucureşti

Cuprins

Prefață **1**
Vedere de ansamblu asupra tezei 1
Contribuțiile tezei 3

Lista de publicații **7**

1 Introducere în criptografie și reziduuri pătratice **9**

2 Noțiuni preliminare **13**

3 Despre distribuția QR **15**
3.1 Numărarea QR și QNR în mulțimea $a + X$ 16
3.1.1 Cazul modulilor primi 17
3.1.2 Cazul modulilor RSA 20
3.2 Calculul probabilităților peste mulțimile $\mathrm{Y}(a + X)$. 27

4 Aplicații ale QR în IBE **29**
4.1 Schema IBE a lui Cocks 29
4.1.1 Criptotextele schemei Cocks IBE 30
4.1.2 Testul Galbraith 34
4.1.3 Variantele anonime ale schemei lui Cocks . . 36
4.2 Schema BGH 38
4.2.1 Polinoame asociate 40
4.2.2 Schema BGH și securitatea acesteia 41
4.2.3 O nouă analiză de securitate pentru schema $BasicIBE$ 42

4.3 Schemele IBE bazate pe QR nesigure 43
4.3.1 Schema lui Jhanwar și Barua 43
4.3.2 Alte scheme IBE nesigure bazate pe QR . . 44
4.4 Autentificarea mutuală continuă 44
4.4.1 Real privacy management 44
4.4.2 Descrierea RPM 45
4.4.3 CMA și securitatea datelor 46
4.5 Generatori pseudo-aleatori 48

5 De la IBE la ABE **51**
5.1 Introducere 51
5.2 ABE și atacul backtracking 53
5.2.1 Schema sigură KP-ABE_Scheme_1 55
5.3 KP-ABE pentru circ. Bool. prin SS și aplic. mlin. . 57
5.3.1 Schema sigură KP-ABE_Scheme_2 58

6 Concluzii și probleme deschise **63**

Bibliografie selectivă **66**

Prefață

Punctul de pornire al cercetării noastre a fost dorința de a căuta o variantă eficientă a schemei IBE a lui Cocks. Astfel, am analizat mulțimea de întregi obținuți prin adunarea unui reziduu pătratic cu un element din $\mathbf{Z}_n^*$, adică mulțimea $a+QR_n$, așa cum vom vedea mai amănunțit în Capitolul 3 din această teză. O altă motivație în studiul nostru l-a constituit necesitatea unei demonstrații riguroase a testului lui Galbraith (GT) - analizat în detaliu în Secțiunea 4.1.2. Un alt obiectiv de interes îl constituie analiza anonimatului și a securității schemei IBE a lui Cocks, dimpreună cu aplicații ale acestei scheme IBE și studiul criptării bazate pe atribute (ABE), care reprezintă o generalizare a criptării bazate pe identitate (IBE) deosebit de utilă în contextul calculului în cloud, în asigurarea controlului accesului în cloud și așa mai departe. Acestea reprezintă principalele subiecte descrise în această lucrare.

Vedere de ansamblu asupra tezei

În cele ce urmează am prezentat succint capitolele din teză.

Capitolul 1: Introducere în criptografie și reziduuri pătratice
În primul capitol, după o scurtă vedere de ansamblu asupra tezei, am prezentat câteva etape din istoria criptologiei. Ne-am concentrat asupra unei subramuri din criptografia cu chei publice (PKE), și anume IBE bazată pe reziduuri pătratice. Acesta reprezintă una

dintre domeniile în care am aplicat câteva din rezultatele noastre matematice din Capitolul chapter 3.

Nivelul de securitate al unei scheme criptografice se demonstrează în general folosind jocurile de securitate. Tot în acest prim capitol sunt prezentate domeniile în care reziduurile pătratice sunt de mare interes, urmate de descrierea stadiului cercetării în ceea ce privește subiectele discutate în teză.

Capitolul 2: Noțiuni preliminare Acest capitol introduce câteva notații, definiții și rezultate elementare din teoria numerelor, probabilități și complexitate, pe care le vom folosi de-a lungul tezei.

Capitolul 3: Despre distribuția reziduurilor pătratice Cercetarea noastră a dus la obținerea unor rezultate importante, oferind formule exacte pentru cardinalii mai multor mulțimi cu anumite șabloane Jacobi. Aceste rezultate se găsesc în acest capitol. În Secțiunea 3.2 am prezentat câteva exemple de calcul al probabilităților asupra mulțimilor analizate anterior. Aceste probabilități prezintă un mare interes nu doar în ceea ce privește crearea schemelor de criptare ci și în diverse probleme cum ar fi securitatea anumitor criptosisteme sau generatori pseudo-aleatori.

Capitolul 4: Aplicații ale reziduurilor pătratice în criptarea bazată de identitate În acest capitol prezentăm câteva aplicații ale rezultatelor noastre din Capitolul 3. Tot aici analizăm în profunzime criptotextele schemei lui Cocks, ceea ce ne va ajuta în demonstrația testului Galbraith. Descriem apoi varianta anonimă a lui Joye la schema IBE a lui Cocks într-o manieră mult simplificată față de articolul original. Acest rezultat a fost prezentat la conferința MFOI2019, [51] și publicat in extenso în [3]. Pornind de la schema BGH care este IND-ID-CPA sigură [8], am obținut în [62] o mărginire superioară a demonstrației de securitate a acestei scheme, rezultat abordat în Secțiunea 4.2.3. BGH reușește să obțină criptotexte mult mai scurte decât schema

lui Cocks dar cu costul unei criptări mult mai lente. Din păcate pierderea securității unei scheme poate interveni foarte ușor, după cum vom vedea în cazul unor încercări de îmbunătățire a eficienței timp a schemei BGH, așa cum a demonstrat Adrian Schipor în [60]. Aceste rezultate au fost prezentate în mod comparativ în [74].

Apoi am detaliat o tehnică de autentificare mutuală continuă (CMA), numită RPM, arătând cum putem combina una din cele patru configurații ale acesteia cu schema lui Cocks, obținând o variantă de CMA mult îmbunătățită și rezistentă la atacuri.

Capitolul 5: De la criptarea bazată pe identitate la criptarea bazată pe atribute Capitolul 5 prezintă o generalizare a IBE, ce are o mare aplicabilitate într-o varietate de de nișe cum ar fi calculul în cloud și Internetul lucrurilor (IoT). Începem printr-o scurtă introducere în ABE - criptarea bazată pe atribute -, structura generală și corectitudinea unei scheme ABE, apoi descriem atacul backtracking și dăm câteva detalii mai de profunzime referitoare la schemele KP-ABE. În Secțiunile **??** am prezentat două scheme eficiente KP-ABE, însoțite de demonstrațiile lor de securitate, detalii de implementare, aplicații, complexitate și comparații.

Capitolul 6: Concluzii și probleme deschise În acest ultim capitol am conturat concluziile, am prezentat probleme deschise în ceea ce privește rezultatele obținute în această teză și am trasat câteva direcții viitoare.

Contribuțiile tezei

După introducerea și preliminariile din Capitolele **??**, următoarele capitole expun munca noastră de cercetare după cum urmează. În Capitolul 3 sunt prezentate rezultatele pe care le-am dezvoltat relativ la mulțimi de forma $QNR_m(a + QR_m)$ - mulțimea non-reziduurilor pătratice modulo m, de forma $a + QR_m$. Aceste

mulțimi sunt foarte utile în criptografie datorită faptului că se pot crea scheme criptografice pornind de la acestea [12, 8, 31].

Rezultatele lui Perron [54] relativ la distribuția reziduurilor și non-reziduurilor pătratice în mulțimi de forma $a + QR_m$ se concentrează doar asupra modulilor primi. Noi am extins aceste rezultate la cazul modulilor RSA (produs de două numere prime). De asemenea am generalizat cazul $a + QR_m$ studiind mulțimi e forma $a+X$, unde X poate fi una dintre mulțimile $\mathbf{Z}_m$, $\mathbf{Z}_m^*$, QR_m, QNR_m, iar modulul este fie un număr prim, fie un întreg RSA. În cazul din urmă, când m este de forma $p \cdot q$, pentru două numere prime distincte p and q, X poate fi de asemenea fi $J_m^{\pm}$ sau $J_m^{\mp}$. Pentru toate aceste mulțimi $a+X$ am prezentat nu doar cardinalii acestora, ci și numărul exact de elemente al tuturor șabloanelor Jacobi aplicate asupra acestor mulțimi. Secțiunea 3.2 arată cum să calculăm probabilități peste aceste mulțimi, de exemplu, probabilitatea ca un element x să fie în J_n^-, când este extras uniform și aleator din mulțimea $a + \mathbf{Z}_n^*$, a se vedea Secțiunea 3.2.1.

În Capitolul 4 am detaliat câteva aplicații ale rezultatelor din Capitolul 3 și o combinare interesantă a schemei IBE a lui Cocks cu un protocol de autentificare mutuală continuă pentru a obține un rezultat securizat, devenit rezistent la atacuri la care, în versiunea inițială, era vulnerabil.

În Secțiunea 4.1 am analizat în profunzime schema IBE a lui Cocks și structura criptotextelor acesteia, pentru a putea calcula probabilitatea exactă ca un criptotext dat să fi fost criptat pentru o anumită identitate, a se vedea Secțiunea 4.1.2. Astfel, în Secțiunea 4.1.1, am studiat modul în care sunt criptate mesajele și cum arată mulțimea de criptotexte pe care le produce schema. Așadar, calculele din Secțiunea 4.1.2 au fost făcute folosind rezultatele obținute în Capitolul 3 și cardinalii din Secțiunea 4.1.1. Apoi am arătat în Secțiunea 4.1.3 cum se pot obține criptotexte Cocks anonimizate, într-un mod eficient și ca un proces independent, plecând de la variantele lor neanonimizate. O astfel de schemă universal anonimă se datorează lui G.A. Schipor [61]. Imediat după prezentarea acestei scheme, în Secțiunea 4.1.3, am arătat cât de ușor poate fi

descrisă varianta anonimă a schemei IBE a lui Cocks creată de Joye [40], fără a folosi polinoame ciclotomice și torușii algebrici, după cum este prezentat în lucrarea noastră [51].

Schema IBE a lui Cocks, în pofida eleganței și a simplității ei, generează criptotexte destul de mari, $2log_n$ biți per bit de text în clar. Secțiunea 4.2 descrie o soluție propusă în 2007 de Boneh și colab., schema *BasicIBE* (prescurtată aici cu BGH) care generează criptotexte scurte cu prețul creșterii complexității timp, devenind cuartică în parametrul de securitate. Această schemă are demonstrația de securitate care certifică nivelul de securitate ca fiind IND-ID-CPA sub presupunerea reziduozității pătratice pentru generatorul *Gen* în modelul cu oracol aleator (ROM), după cum putem vedea în Secțiunea 4.2.2. Am obținut o mărginire superioară pentru demonstrația de securitate a schemei BGH, descrisă în Secțiunea 4.2.3 și publicate în [62].

Pornind de la [8] Jhanwar și Barua au încercat să obțină o variantă mai rapidă a proceselor de criptare și de decriptare (schema lor o vom prescurta JB), dar vom vedea în Secțiunea 4.3.1 că, din păcate, această versiune își pierde securitatea din cauza metodei de combinare a soluțiilor aleasă de ei. După cum a arătat A. Schipor, variantele prezentate de Elashry, Mu și Susilo în [23], precum și [21] sunt vulnerabile la același atac. Astfel, în acest moment schemele IBE bazate pe QR care rămân sigure și pot fi utilizate sunt schema lui Cocks, BGH și variantele lor anonime, după cum am detaliat în [74].

Cauza principală a creșterii complexității timp în schema propusă de Boneh și colab. o reprezintă algoritmul determinist de rezolvare a Ecuației 4.2, pagina 40. În [39], aceiași doi cercetători, Jhanwar și Barua, au găsit un algoritm probabilist foarte util pentru a găsi soluții ale Ecuației 4.2, în locul celui determinist al lui Boneh și colab.

O importantă contribuție a tezei este și în problema autentificării mutuale continue. Când două entități doresc să comunice în mod securizat (ambii) vor dori să se asigure, pe tot parcursul comunicării, că la celălalt capăt este chiar persoana care cu care

ei doresc să comunice, și nu o terță parte, un atacator. Pentru a reuși acest lucru se va folosi (mutuală) continuă. Dar ce se întâmplă dacă, la un moment dat, un intrus reușește să decodifice comunicarea? Există vreo posibilitate ca procesul comunicării să redevină securizat? Dacă da, care ar fi costurile? Comunicarea actuală va trebui oprită și reluată? S-ar putea oare resecuriza comunicarea fără a întrerupe procesul? Această proprietate a fost definită prima dată de de către Elashry și colab. în [22]. Ei au numit-o *reziliență*. Noi am găsit o cale de a atinge acestă proprietate făcând uz de schema IBE a lui Cocks, care se pliază perfect pe protocolul RPM. Acest rezultat este descris în Secțiunea 4.4.

La finalul Capitolului 4 vom vedea cum se pot crea generatori pseudo-aleatori folosind reziduurile pătratice, care este o altă aplicație utilă a QR în criptografie.

Astfel, în Capitolul 5 am evidențiat cele mai importante rezultate dezvoltate în ceea ce privește schemele KP-ABE schemes bazate pe aplicații biliniare și partajarea secretelor. Am concluzionat că, pentru securitate, aplicațiile multiliniare pe niveluri trebuie evitate. În orice caz, soluțiile existente pentru circuitele Booleene bazate pe aplicații biliniare nu sunt eficiente, iar a găsi un echilibru aici rămâne încă o problemă deschisă.

Capitolul 6 conturează concluziile și prezintă câteva idei de a extinde stadiul curent al cercetării și rezultatele obținute de noi în ariile atinse în această lucrare.

Lista de publicații

1. F. L. Ţiplea, S. Iftene, G. Teşeleanu, and A.-M. Nica. *On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography.* **Applied Mathematics and Computation**, vol. 372, May 2020 (Journal impact factor: 3.092), available on-line, `doi.org/10.1016/j.amc.2019.124993`.

2. A.-M. Nica, *Continuous mutual authentication and data security.* **International Journal of Computer Science and Information Security** (IJCSIS), vol. 17, February 2019 (Journal impact factor: 0.702).

3. A.-M. Nica și F. L. Ţiplea. *On anonymization of Cocks' identity-based encryption scheme* (extended version of the conference paper). In **Computer Science Journal of Moldova**, vol.27, no.3(81), pp.283-298, 2019 `http://www.math.md/publications/csjm/issues/v27-n3/13001/` (Journal indexed in Web of Science).

4. A.-M. Nica and F. L. Ţiplea. *On anonymization of Cocks' identity-based encryption scheme.* În Proceedings of the **5th Conference on Mathematical Foundations of Informatics**, MFOI 2019, Iași, România, July 3-6, 2019, Editura Universității Alexandru Ioan Cuza din Iași, pages 75-85, 2019.

5. G. Teşeleanu, F. L. Ţiplea, S. Iftene și A.-M. Nica. *Boneh-*

Gentry-Hamburg's identity-based encryption schemes revisited. În Proceedings of the **5th Conference on Mathematical Foundations of Informatics**, MFOI2019, July 3-6, 2019, Iași, România, pages 45 – 58, 2019.

6. F. L. Ţiplea, C. C. Drăgan și A.-M. Nica, *Key-policy attribute-based encryption from bilinear maps*, in Innovative Security Solutions for Information Technology and Communications - 10th International Conference, SecITC 2017, București, România, June 8-9, 2017, Revised Selected Papers, **Lecture Notes in Computer Science** 10543, pp. 28–42, 2017.

7. F. L. Ţiplea, S. Iftene, G. Teşeleanu și A.-M. Nica, *Security of identity-based encryption schemes from quadratic residues*, în Innovative Security Solutions for Information Technology and Communications - 9th International Conference, SecITC 2016, București, România, June 9-10, 2016, Revised Selected Papers, **Lecture Notes in Computer Science** 10006, pp. 63–77, 2016.

8. G. Teşeleanu, F. L. Ţiplea, S. Iftene și A.-M. Nica. *Boneh-Gentry-Hamburg's identity-based encryption schemes revisited*, **IET Information Security** (under review)

Capitolul 1

Introducere în criptografie și reziduuri pătratice

Încă din cele mai vechi timpuri criptologia a jucat un rol important în special în domeniul militar, făcând posibilă printre altele asigurarea confidențialității și integrității datelor. Mai târziu oamenii au fost interesați și de spargerea acestor cifruri, luând naștere criptanaliza. Steganografia, ascunderea datelor sensibile în mesaje ,,inocente", este o altă metodă de ascundere a informațiilor.

La începuturile criptografiei erau utilizate doar *cifruri simetrice* pentru asigurarea confidențialității, integrității și autentificării. Acest tip de criptare utilizează aceeași cheie atât pentru criptare cât și pentru decriptare. *Criptarea asimetrică* a apărut pe la mijlocul secolului al douăzecilea. În acest caz expeditorul criptează cu cheia publică a destinatarului care, pentru a decripta, folosește cheia secretă corespunzătoare celei publice și obține mesajul original. *Criptografia cu chei publice* (PKE) este mai costisitoare decât cea simetrică. Astăzi ele se completează reciproc, în practică utilizându-se o schemă asimetrică pentru transmiterea cheii secrete a unui criptosistem simetric, cu care se va cripta toată conversația propriu-zisă, deoarece acesta este mai rapid. Certificarea cheilor publice în PKE implică un lanț de încredere și un complicat management al cheilor.

În 1984 Adi Shamir a propus Criptarea Bazată pe Identitate (IBE), un nou tip de PKE ce elimină infrastructura cheilor publice. În acest model, cheia publică este reprezentată de un șir de caractere ce identifică în mod unic destinatarul, cum ar fi numărul de telefon sau emailul etc.

Au trecut 17 ani până la primele implementări concrete [7, 12]. Schemele IBE se bazează în principal pe aplicații biliniare pe curbe eliptice [58, 7], reziduuri pătratice (QR) [12, 8, 39] și pe latici [28, 20]. Schemele IBE ce folosesc aplicațiile biliniare au criptotexte foarte scurte și complexitate timp foarte bună, dar utilizează anumite probleme matematice care nu sunt înțelese și stăpânite pe deplin. Schemele bazate pe latici sunt de mare interes deoarece sunt rezistente calculului cuantic dar inconvenientul lor este dimensiunea mare a cheilor publice. QR, pe de altă parte, sunt instrumente matematice simple, elegante și bine înțelese. Actualmente este o efervescență în căutarea balansului optim între complexitățile timp și spațiu. Pionierul utilizării QR în IBE a fost Clifford Cocks. Schema sa din 2001 [12][1] are mare impact în PKE și IBE. Acest criptosistem prezintă un interes special în teza noastră și va fi detaliat în Capitolul 4.

Dacă destinatarul unor informații criptate este un grup de oameni cu anumite caracteristici comune („atribute“), dacă avem mai mulți destinatari a căror identitate poate fi necunoscută, sau dacă mai târziu alți utilizatori noi vor dori să se alăture sistemului, atunci este potrivită criptarea bazată pe atribute (ABE), care generalizează IBE și este esențială în controlul accesului de granulație fină și cloud.

Secretul perfect [63] este dificil de atins datorită lungimii cheii și problemei schimbului de cheie. Astfel vom avea nevoie de alte niveluri de securitate cum ar fi securitatea semantică, indistingibilitatea sau non-maleabilitatea. Cele mai întâlnite modele sunt COA (atacul de criptotext cunoscut), KPA (atacul de text în clar

[1] Se pare că C. Cocks a inventat-o în 1998 pentru serviciile secrete britanice, unde lucra el, dar a rămas clasificată până în 2001. A se vedea https://royalsociety.org/people/clifford-cocks-11242/.

cunoscut), CPA (atacul de text în clar ales), și CCA1/2 (atacul de criptotext ales non-/adaptive).

Capitolul 2

Noțiuni preliminare

În acest capitol vom stabili notația pe care o vom folosi și vom prezenta succint câteva noțiuni utile din teoria numerelor, probabilități, complexitate și reziduuri pătratice.

Fie $\mathbf{Z}$ mulțimea întregilor și $a, b \in \mathbf{Z}$, prin (a, b) vom înțelege cel mai mare divizor comun al lor. Fie m un întreg pozitiv, $\mathbf{Z}_m$ va desemna mulțimea claselor de echivalență induse de echivalența modulo m, adică $\{0, 1, 2, \cdots, m-1\}$, iar $\mathbf{Z}_m^*$ va reprezenta mulțimea întregilor $x \in \mathbf{Z}_m$ cu $(x, m) = 1$. Vom spune că a și b sunt *congruente modulo* m și vom nota aceasta prin $a \equiv b \bmod m$ sau prin $a \equiv_m b$, dacă m divide $a - b$. Restul împărțirii întregului a la m, cu $m \neq 0$, îl notăm cu $(a)_m$ iar câtul aceleiași împărțiri va fi a div m. Întregilor pozitivi $n = pq$ care sunt produs de două numere prime distincte p și q le vom zice *întregi RSA* sau *moduli RSA*.

Un număr întreg a co-prime cu m este *reziduu pătratic modulo* m dacă $a \equiv_m x^2$, pentru un anumit întreg x; întregul $x \in SQRT_p(a)$ va fi numit *rădăcină pătrată* a lui a modulo m. Mulțimea tuturor rădăcinilor pătrate modulo m ale elementelor din mulțimea A va fi notată cu $SQRT_p(A)$. Pe parcursul lucrării când vom spune *reziduu*, ne vom referi la reziduu pătratic.

Fie p un număr prime, *simbolul Legendre* al unui întreg a modulo p, notat cu $\left(\frac{a}{p}\right)$ sau cu $(a|p)$, este 1 dacă a este reziduu pătratic modulo p, 0 dacă p divide a, și -1 altfel. *Simbo-*

lul Jacobi extinde simbolul Legendre la moduli compuși. Dacă $n = p_1^{e_1} \cdots p_m^{e_m}$ este descompunerea în factori primi a întregului pozitiv n, atunci simbolul Jacobi al lui a modulo n va fi $\left(\frac{a}{n}\right) = \left(\frac{p_1}{a}\right)^{e_1} \cdots \left(\frac{p_m}{a}\right)^{e_m}$. Pentru simplitate vom folosi numirea de *simbol Jacobi* în ambele cazuri (moduli primi și compuși).

Dat un număr întreg pozitiv n și o submulțime $A \subseteq \mathbf{Z}_n^*$, $QR_n(A)$ ($QNR_n(A)$, $J_n^+(A)$, $J_n^-(A)$) va reprezenta mulțimea reziduurilor (respectiv a nereziduurilor, a întregilor cu simbolul Jacobi 1, a întregilor cu simbolul Jacobi -1) modulo n din A. Când $A = \mathbf{Z}_n^*$, notația va fi simplificată: QR_n (respectiv QNR_n, J_n^+, J_n^-). Pentru cazul modulilor RSA $n = pq$, unde $p < q$ sunt numere prime impare, vom nota cu $J_n^{\pm}$ sau J_n^{+-} pentru mulțimea întregilor din $\mathbf{Z}_n$ care au simbolul Jacobi 1 modulo p, și -1 modulo q . Vice versa, pentru $x \in \mathbf{Z}_n$ cu $(x|p) = -1$ și $(x|q) = +1$ vom folosi notația $J_n^{\mp}$, sau câteodată J_n^{-+}. Prin J_n^{++} (J_n^{--}) vom nota mulțimea întregilor din $\mathbf{Z}_n$ care sunt reziduuri pătratice (respectiv nereziduuri) atât modulo p cât și modulo q. Când n este un număr prim, $QR_n(A) = J_n^+(A)$ și $QNR_n(A) = J_n^-(A)$.

Faptul că a este ales aleator și uniform din mulțimea A este notat $a \leftarrow A$. Dacă $\mathcal{A}$ este un algoritm probabilist, atunci $a \leftarrow \mathcal{A}$ înseamnă că a este rezultatul lui $\mathcal{A}$ pentru o anumită intrare.

Abordarea asimptotică a securității face uz de parametrul de securitate, notat aici cu λ. O funcție pozitivă $f(\lambda)$ se numește *neglijabilă* dacă, pentru orice polinom pozitiv $poly(\lambda)$ există n_0 astfel încât $f(\lambda) < 1/poly(\lambda)$, oricare ar fi $\lambda \geq n_0$.

Fie $Gen(\lambda)$ un algoritm probabilist în timp polinomial (PPT). Primind la intrare un parametru de securitate λ, generează ca ieșire un triplet (n, p, q), unde $n = pq$ este un modul RSA. *Presupunerea reziduozității pătratice* (QRA) are loc pentru generatorul $Gen(\lambda)$ dacă distanța

$$|P(\mathcal{D}(a,n) = 1 \ : \ (n,p,q) \leftarrow Gen(\lambda),\ a \leftarrow QR_n) - P(\mathcal{D}(a,n) = 1 \ : \ (n,p,q) \leftarrow Gen(\lambda),\ a \leftarrow J_n \setminus QR_n)|,$$

ca funcție după λ, este neglijabilă oricare ar fi $\mathcal{D}$ un algoritm PPT.

Capitolul 3

Despre distribuția reziduurilor pătratice

Ne concentrăm asupra reziduurilor pătratice datorită eleganței, simplității și importanței lor atât în matematică, cât și în criptografie. Problemele dificile din teoria numerelor pe care le ridică reziduurile pătratice sunt bine înțelese de comunitatea criptografică [11] și utilizate în scheme criptografice din criptografia cu chei publice (PKE), în cea bazată pe identitate (IBE) - a se vedea remarcabilul criptosistem al lui Cocks [12] - și chiar în criptografia bazată pe atribute (ABE), la crearea de generatori pseudo-aleatori de numere (PRNG-uri) sau de biți (PRBG-uri), în scheme de semnare digitală și așa mai departe [55, 31, 5].

Schema lui Cocks a reprezentat un punct de pornire în multe studii individuale [8, 39, 1, 38, 4, 40, 45]. Așa cum se preciza în [25, 8], această schemă nu are proprietatea de a păstra anonimatul celui care recepționează mesajul criptat. Acest fapt a dus la apariția mai multor variante anonime ale schemei lui Cocks (a se vedea Secțiunea 4.1.3). Pentru a face analiza anonimatului în cadrul acestei scheme a lui Cocks, am elaborat un studiu concret asupra mulțimilor $\mathrm{Y}(a+X)$, unde $Y \in \{QR_m, J_m^+ \backslash QR_m, J_m^{\pm}, J_m^{\mp}, QNR_m\}$ iar X este o submulțime de elemente din $\mathbf{Z}_n$ care au anumite specificații în ceea ce privește simbolurile Jacobi (numite *șabloane*

Jacobi).

Studiul asupra mulțimilor de tipul $a + QR_p$ unde a este un întreg iar p un număr prim, a început demult, cel puțin de pe la începutul anilor '50, prin munca lui Perron [54]. Damgård [16] și Peralta [53] s-au orientat asupra seriilor de simboluri $\left(\frac{a+i}{p}\right)$, $\left(\frac{a+i+1}{p}\right), \cdots$ dat fiind caracterul lor aleator și, ca urmare, utilitatea lor în obținerea numerelor/biților aleatori. Mai târziu, Benjamin Justus a întreprins câteva studii asupra reziduurilor și non-reziduurilor pătratice în contextul Goldwasser-Micali [42]. Tot el a studiat distribuția reziduurilor și non-reziduurilor pătratice în progresii aritmetice în cazul modulilor primi mari [41].

Cazul modulilor compuși este foarte util de studiat datorită faptului că multe scheme criptografice utilizează contextul grupurilor ciclice în care modulul este un întreg RSA. Aceste distribuții prezintă un interes ridicat de asemenea în asigurarea securității bazate pe reziduuri pătratice, după cum vom vedea în Capitolul 4. Aceste rezultate au fost obținute împreună cu F.L. Ţiplea, S. Iftene, și G. Teşeleanu, fiind publicate în [1].

3.1 Numărarea reziduurilor și non-reziduuri pătratice în mulțimea $a + X$

În această secțiune analizăm distribuția reziduurilor și non-reziduurilor pătratice în mulțimile de forma $(a + X)$, unde $a \in \mathbf{Z}_m^*$, X este una din mulțimile $\mathbf{Z}_m, \mathbf{Z}_m^*, QR_m$ or QNR_m, iar modulul m este fie un număr prim impar, în Secțiunea 3.1.1, fie un întreg RSA, în Secțiunea 3.1.2.

Am început studiul cu cazul în care modulul m este un număr prim.

3.1.1 Cazul modulilor primi

Ca punct de pornire menționăm un rezultat bine cunoscut ce poate fi găsit în aproape orice carte despre teoria numerelor, cum ar fi [13, p.27], [64, 65] sau [49]. Dat p un număr prim, în mulțimea $\mathbf{Z}_p^*$ exact jumătate din elemente sunt reziduuri și jumătate sunt non-reziduuri pătratice. Când modulul este un număr prim, submulțimea de reziduuri coincide cu submulțimea elementelor care au simbolul Jacobi egal cu 1, în timp ce submulțimea non-reziduurilor coincide cu submulțimea elementelor ce au simbolul Legendre și Jacobi egal cu -1. În cazul modulilor RSA, ne putem face o imagine despre proporțiile elementelor ce au anumite șabloane Jacobi prin Figura 3.1 de la pagina 20.

Propoziția 3.1.1. *Dat p un număr prim impar și a un întreg co-prim cu p, au loc următoarele proprietăți:*

a) $a + \mathbf{Z}_p = \mathbf{Z}_p$ *și* $|(a + \mathbf{Z}_p)^*| = |\mathbf{Z}_p^*| = p - 1$*;*

b) $a + \mathbf{Z}_p^* = \mathbf{Z}_p \setminus \{a\}$ *și* $|(a + \mathbf{Z}_p^*)^*| = p - 2$*.*

În acest moment suntem interesați în calculul cardinalității mulțimilor de forma $a + QR_p$ și $a + QNR_p$. Când avem în vedere mulțimile de forma $a + QR_p$, respectiv $a + QNR_p$, vom avea în vedere că $-a \bmod p$ le influențează cardinalitatea. Astfel, în mulțimea $a + X$, când $(-a)_p \in X$ vom avea $a + (-a) \equiv_p 0$. În ceea ce privește mulțimea de reziduuri din $QR_p(A)$, când A este de forma $(a + QR_p^*)^*$, spre deosebire de rezultatele lui Perron din 1952 [54], noi nu vom include 0 în mulțimea de reziduuri. Acest lucru duce la următoarele rezultate.

Corolarul 3.1.1. *Fie p un număr prim impar și $a \in \mathbf{Z}_p^*$. Când $a \in QR_p$, vom avea*

$$|QR_p(a + \mathbf{Z}_p^*)| = \frac{p-3}{2} \quad \text{și} \quad |QNR_p(a + \mathbf{Z}_p^*)| = \frac{p-1}{2},$$

dar când $a \in QNR_p$*, atunci*

$$|QR_p(a + \mathbf{Z}_p^*)| = \frac{p-1}{2} \quad \text{și} \quad |QNR_p(a + \mathbf{Z}_p^*)| = \frac{p-3}{2}.$$

Propoziția 3.1.2. *Fie* p *un număr prim impar și* $a \in \mathbf{Z}_p^*$*. Când* $-a \in QR_p$*, atunci*

$$|(a + QR_p)^*| = \frac{p-3}{2} \quad \text{și} \quad |(a + QNR_p)^*| = \frac{p-1}{2}$$

iar când $-a \in QNR_p$*, atunci*

$$|(a + QR_p)^*| = \frac{p-1}{2} \quad \text{și} \quad |(a + QNR_p)^*| = \frac{p-3}{2}$$

Este important să atragem atenția asupra următoarelor proprietăți. Când adunăm un reziduu cu un întreg fixat a, vom obține $a+QR_p$. Pentru a obține un reziduu prin adunarea reziduului r cu a, unde $r \in QR_p$, dacă considerăm s o rădăcină pătratică r și t o rădăcină pătratică a sumei $a+r$, atunci vom avea două reziduuri, r și $a+r$. Așadar, $a + r \equiv_p a + s^2 \equiv_p t^2$. Începând de aici, Perron [54] a obținut o caracterizare foarte importantă a reziduurilor din mulțimea $a + QR_p$, exprimată prin următoarea lemă.

Lema 3.1.1 ([54])**.** *Fie* p *un număr prim impar,* a *un întreg din* $\mathbf{Z}_p^*$ *și* r *un reziduu modulo* p*. Atunci,* $a+r$ *este reziduu pătratic în* $\mathbf{Z}_p^*$ *dacă și numai dacă* r *se poate scrie ca* $r \equiv_p \frac{1}{4}\,(u - \frac{a}{u})^2$*, unde* $u \in \mathbf{Z}_p^*$ *și* $u \notin SQRT_p(\pm a)$*.*

Astfel, așa cum observa Perron în [54], pentru a număra reziduurile de forma $a + r$, unde r este reziduu, se pot număra reziduurile incongruente din $\mathbf{Z}_p^*$ care pot fi scrise ca $(u - a/u)^2$, cu restricțiile de mai sus pentru u.

Când $p \equiv_4 3$, pentru un întreg $a \in \mathbf{Z}_p^*$, ori a ori $-a$ este reziduu modulo p; dacă $a \in QR_p$ atunci $-a \in QNR_p$ și vice versa. Pe când, dacă $p \equiv_4 1$, când a este reziduu, asta implică faptul că $-a$ este tot un reziduu și similar pentru cazul în care a este

non-reziduu, asta înseamnă că $-a$ este tot non-reziduu. Pe baza acestor proprietăți, urmează imediat teorema.

Teorema 3.1.1. *Fie p un număr prim impar și a un întreg coprim cu p, atunci*

$$|QR_p(a + QR_p)| = \frac{|\mathbf{Z}_p^* \backslash SQRT_p(\pm a)|}{4}.$$

Corolarul 3.1.2. *Când p este un număr prim impar, $p = 4k + i$, iar când $i \in \{1, 3\}$ și $a \in \mathbf{Z}_p^*$, atunci*

$$|QR_p(a + QR_p)| = \begin{cases} k - 1, & \text{după } a \in QR_p \text{ și } i = 1 \\ k, & \text{altfel} \end{cases}$$

și

$$|QNR_p(a + QR_p)| = \begin{cases} k + 1, & \text{după } a \in QR_p \text{ și } i = 3 \\ k, & \text{altfel.} \end{cases}$$

Pentru mulțimile $QR_p(a + QNR_p)$ și $QNR_p(a + QNR_p)$ avem următoarele rezultate.

Corolarul 3.1.3. *Fie $p \equiv_4 i$ un număr prim impar, cu $i \in \{1, 3\}$ și $a \in \mathbf{Z}_p^*$, atunci*

$$|QR_p(a + QNR_p)| = \begin{cases} \dfrac{p-3}{4} + 1, & \text{dacă } i = 3 \text{ și } a \in QNR_p \\ \dfrac{p-i}{4}, & \text{altfel} \end{cases}$$

și

$$|QNR_p(a + QNR_p)| = \begin{cases} \dfrac{p-1}{4} - 1, & \text{dacă } i = 1 \text{ și } a \in QNR_p \\ \dfrac{p-i}{4}, & \text{altfel.} \end{cases}$$

3.1.2 Cazul modulilor RSA

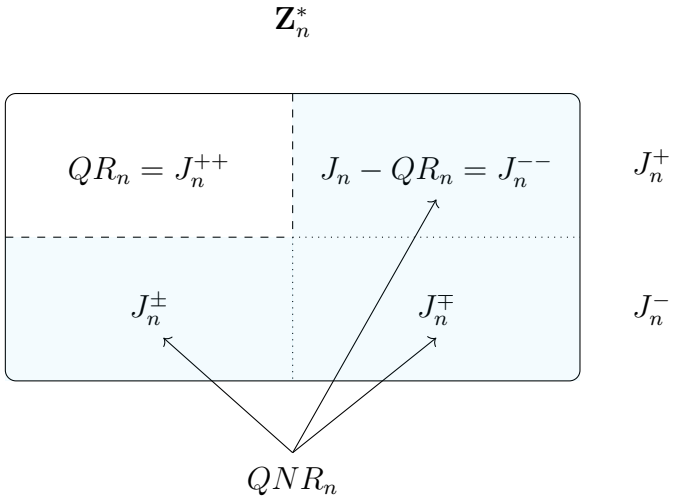


Figura 3.1: Mulțimea $\mathbf{Z}_n^*$

Destul de frecvent se folosesc în criptografie modulii RSA (produsul a două numere prime impare). Obiectivul nostru este de a calcula cardinalii unor mulțimi ce au un anumit șablon Jacobi specificat. Distribuția reziduurilor și a non-reziduurilor pătratice în mulțimea $\mathbf{Z}_n^*$ va fi folosită în crearea sau analizarea criptosistemelor, în construirea generatorilor pseudo-aleatori și așa mai departe. Identificarea unor distribuții de probabilitate care să fie imposibil de distins statistic unele de altele, pot reprezenta un instrument matematic important cu potențial în demonstrațiile de securitate a schemelor criptografice sau a anumitor proprietăți ale acestora, cu am fi anonimatul.

Dacă avem un întreg x din $\mathbf{Z}_n^*$, putem obține valorile corespunzătoare acestuia din $\mathbf{Z}_p^*$ și $\mathbf{Z}_q^*$ prin reducerea lui x modulo p, respectiv modulo q, obținând valori unice. Acest lucru este valabil și invers, plecând de la $(x)_p$ și $(x)_q$ și ajungând la un unic $(x)_n$, datorită teoremei chinezești a resturilor (CRT) și a binecunoscutului izomorfism f de la $\mathbf{Z}_n^*$ la $\mathbf{Z}_p^* \times \mathbf{Z}_q^*$, unde $f(x) =$

$(x \bmod p, x \bmod q), \forall x \in \mathbf{Z}_n^*$. Deși este un rezultat simplu, el are foarte multe aplicații importante și îl vom folosi adesea pe parcursul acestei secțiuni pentru a obține noi rezultate prin combinarea unor mulțimi și pentru a le calcula cardinalitatea, după cum putem observa în următoarea teoremă.

Teorema 3.1.2. *Fie n un modul RSA, $n = pq$, $a \in \mathbf{Z}_p^*$ și bijecția $f : \mathbf{Z}_n^* \to \mathbf{Z}_p^* \times \mathbf{Z}_q^*$, dată de $f(x) = ((x)_p, (x)_q)$, atunci f va pune în corespondență următoarele mulțimi după cum urmează:*

1. $(a + \mathbf{Z}_n^*)^*$ *în* $((a)_p + \mathbf{Z}_p^*)^* \times ((a)_q + \mathbf{Z}_q^*)^*$;
2. $(a + QR_n)^*$ *în* $((a)_p + QR_p)^* \times ((a)_q + QR_q)^*$;
3. $(a + J_n^+ \backslash QR_n)^*$ *în* $((a)_p + QNR_p)^* \times ((a)_q + QNR_q)^*$;
4. $(a + J_n^\pm)^*$ *în* $((a)_p + QR_p)^* \times ((a)_q + QNR_q)^*$;
5. $(a + J_n^\mp)^*$ *în* $((a)_p + QNR_p)^* \times ((a)_q + QR_q)^*$.

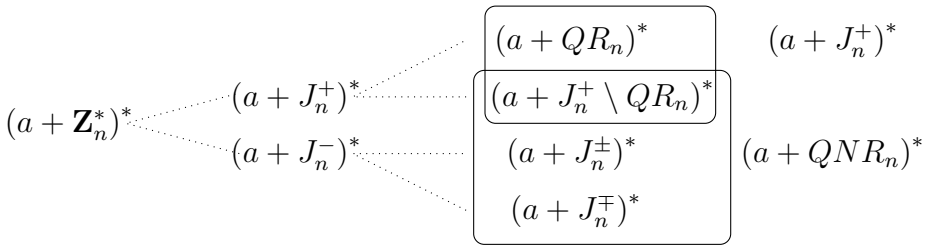


Figura 3.2: Șabloanele Jacobi ale mulțimii $(a + \mathbf{Z}_n^*)^*$

Acum putem număra elementele din Teorema 3.1.2.

Corolarul 3.1.4. *Fie p, q două numere prime impare, $n = pq$ și $a \in \mathbf{Z}_n^*$, atunci*

1. $|(a + \mathbf{Z}_n^*)^*| = (p-2)(q-2)$;
2. $|(a + QR_n)^*| = \dfrac{(p - 2 - (-a|p))(q - 2 - (-a|q))}{4}$;

3. $|(a + J_n^+ \backslash QR_n)^*| = \dfrac{(p-2+(-a|p))(q-2+(-a|q))}{4}$;

4. $|(a + J_n^\pm)^*| = \dfrac{(p-2-(-a|p))(q-2+(-a|q))}{4}$;

5. $|(a + J_n^\mp)^*| = \dfrac{(p-2+(-a|p))(q-2-(-a|q))}{4}$;

6. $|(a + J_n^+)^*| = \dfrac{(p-2)(q-2)+(-a|p)(-a|q)}{2}$;

7. $|(a + J_n^-)^*| = \dfrac{(p-2)(q-2)-(-a|p)(-a|q)}{2}$;

8. $|(a + QNR_n)^*| = \dfrac{3(p-2)(q-2)+(-a|p)(q-2)}{4} + \dfrac{(-a|q)(p-2)-(-a|p)(-a|q)}{4}$.

Un alt rezultat care ajută la partiționarea mulțimii $(a + \mathbf{Z}_n^*)^*$ este de asemenea obținut prin punerea în corespondență pe care o face bijecția f.

Teorema 3.1.3. *Fie n un modul RSA, produs a două numere prime p și q, și $a \in \mathbf{Z}_n^*$, atunci bijecția f din Teorema 3.1.2 pune în corespondență următoarele mulțimi după cum urmează:*

a) $QR_n(a + \mathbf{Z}_n^*)$ *în* $QR_p((a)_p + \mathbf{Z}_p^*) \times QR_q((a)_q + \mathbf{Z}_q^*)$;

b) $(J_n^+ \backslash QR_n)(a + \mathbf{Z}_n^*)$ *în* $QNR_p((a)_p + \mathbf{Z}_p^*) \times QNR_q((a)_q + \mathbf{Z}_q^*)$;

c) $J_n^\pm(a + \mathbf{Z}_n^*)$ *în* $QR_p((a)_p + \mathbf{Z}_p^*) \times QNR_q((a)_q + \mathbf{Z}_q^*)$;

d) $J_n^\mp(a + \mathbf{Z}_n^*)$ *în* $QNR_p((a)_p + \mathbf{Z}_p^*) \times QR_q((a)_q + \mathbf{Z}_q^*)$.

Acum putem calcula cardinalii mulțimilor puse în corespondență prin teorema de mai sus, după cum este expus în corolarul următor.

Corolarul 3.1.5. *Fie $p < q$ două numere prime impare, $n = pq$ și $a \in \mathbf{Z}_n^*$, atunci*

1. $|QR_n(a + \mathbf{Z}_n^*)| = \dfrac{(p-2-(a|p))(q-2-(a|q))}{4}$;

2. $|(J_n^+ \backslash QR_n)(a + \mathbf{Z}_n^*)| = \dfrac{(p-2+(a|p))(q-2+(a|q))}{4}$;

3. $|J_n^{\pm}(a + \mathbf{Z}_n^*)| = \dfrac{(p-2-(a|p))(q-2+(a|q))}{4}$;

4. $|J_n^{\mp}(a + \mathbf{Z}_n^*)| = \dfrac{(p-2+(a|p))(q-2-(a|q))}{4}$;

5. $|J_n^{+}(a + \mathbf{Z}_n^*)| = \dfrac{(p-2)(q-2)+(a|p)(a|q)}{2}$;

6. $|J_n^{-}(a + \mathbf{Z}_n^*)| = \dfrac{(p-2)(q-2)-(a|p)(a|q)}{2}$;

7. $|QNR_n(a + \mathbf{Z}_n^*)| = \dfrac{3(p-2)(q-2)+(a|p)(q-2)}{4} + \dfrac{(a|q)(p-2)-(a|p)(a|q)}{4}$.

Următoarea mulțime asupra căreia ne vom concentra este $A = (a + QR_n)$, mai precis asupra submulțimilor acesteia: $QR_n(A)$, $(J_n^+ \backslash QR_n)(A)$, $J_n^{\pm}(A)$ și $J_n^{\mp}(A)$. Datorită aceluiași izomorfism f din Teorema 3.1.2 aceste mulțimi sunt puse în corespondență după cum se poate vedea în teorema de mai jos.

Teorema 3.1.4. *Fie $n = pq$ un modul RSA și $a \in \mathbf{Z}_n^*$, atunci funcția f din Teorema 3.1.2 pune în corespondență partițiile lui $A = (a + QR_n)$ după cum urmează:*

a) $QR_n(A)$ *în* $QR_p((a)_p + QR_p) \times QR_q((a)_q + QR_q)$;

b) $(J_n^+ \backslash QR_n)(A)$ *în* $QNR_p((a)_p + QR_p) \times QNR_q((a)_q + QR_q)$;

c) $J_n^{\pm}(A)$ *în* $QR_p((a)_p + QR_p) \times QNR_q((a)_q + QR_q)$;

d) $J_n^{\mp}(A)$ *în* $QNR_p((a)_p + QR_p) \times QR_q((a)_q + QR_q)$.

Putem stabili acum câte elemente are fiecare mulțime discutată mai sus prin următorul corolar. Pentru a reduce numărul de cazuri, vom folosi notația stabilită în articolul [1].

Notația 3.1.1 ([1]). *Fie p un număr prim impar, a un întreg co-prim cu p, și $i = p \bmod 4 \in \{1, 3\}$, atunci vom defini:*

$$\tau_{p,a}^{i} = \begin{cases} 1, & \text{dacă } (p)_4 = i \text{ și } (a)_p \in QR_p \\ 0, & \text{altfel} \end{cases}$$

și

$$\bar{\tau}_{p,a}^{i} = \begin{cases} 1, & \text{dacă } (p)_4 = i \text{ și } (a)_p \in QNR_p \\ 0, & \text{altfel.} \end{cases}$$

Corolarul 3.1.6. *Dat un modul RSA $n = pq$, cu $s = p \text{ div } 4$, $t = q \text{ div } 4$, și un întreg $a \in \mathbf{Z}_n^*$, atunci*

1. $|QR_n(a + QR_n)| = (s - \tau_{p,a}^1)(t - \tau_{q,a}^1)$;
2. $|(J_n^+ \backslash QR_n)(a + QR_n)| = (s + \tau_{p,a}^3)(t + \tau_{q,a}^3)$;
3. $|J_n^{\pm}(a + QR_n)| = (s - \tau_{p,a}^1)(t + \tau_{q,a}^3)$;
4. $|J_n^{\mp}(a + QR_n)| = (s + \tau_{p,a}^3)(t - \tau_{q,a}^1)$;
5. $|J_n^+(a + QR_n)| = 2st + s(\tau_{q,a}^3 - \tau_{q,a}^1) + t(\tau_{p,a}^3 - \tau_{p,a}^1) + \tau_{p,a}^1\tau_{q,a}^1 + \tau_{p,a}^3\tau_{q,a}^3$;
6. $|J_n^-(a + QR_n)| = 2st + s(\tau_{q,a}^3 - \tau_{q,a}^1) + t(\tau_{p,a}^3 - \tau_{p,a}^1) - \tau_{p,a}^1\tau_{q,a}^3 - \tau_{p,a}^3\tau_{q,a}^1$;
7. $|QNR_n(a + QR_n)| = 3st + s(2\tau_{q,a}^3 - \tau_{q,a}^1) + t(2\tau_{p,a}^3 - \tau_{p,a}^1) - \tau_{p,a}^1\tau_{q,a}^3 - \tau_{p,a}^3\tau_{q,a}^1 + \tau_{p,a}^3\tau_{q,a}^3$.

Vom partiționa mulțimea $(a + J_n^+ \backslash QR_n)$ după cum vedem în teorema următoare.

Teorema 3.1.5. *Fie n un modul RSA cu $n = pq$, $a \in \mathbf{Z}_n^*$ și mulțimea $A = (a + J_n^+ \backslash QR_n)$, atunci bijecția din Teorema 3.1.2 pune în corespondență următoarele patru mulțimi astfel:*

a) $QR_n(A)$ *în* $QR_p((a)_p + QNR_p) \times QR_q((a)_q + QNR_q)$;

b) $(J_n^+ \backslash QR_n)(A)$ *în* $QNR_p((a)_p + QNR_p) \times QNR_q((a)_q + QNR_q)$;

c) $J_n^{\pm}(A)$ *în* $QR_p((a)_p + QNR_p) \times QNR_q((a)_q + QNR_q)$;

d) $J_n^{\mp}(A)$ *în* $QNR_p((a)_p + QNR_p) \times QR_q((a)_q + QNR_q)$.

Cardinalii corespunzători mulțimilor din Teorema 3.1.5 sunt detaliați în corolarul de mai jos.

Corolarul 3.1.7. *Fie p și q numere prime impare, $n = pq$ un modul RSA, $s = p \ div \ 4$, $t = q \ div \ 4$, $a \in \mathbf{Z}_n^*$, și $A = (a + J_n^+ \backslash QR_n)$, atunci*

1. $|QR_n(A)| = (s + \bar{\tau}_{p,a}^3)(t + \bar{\tau}_{q,a}^3)$;
2. $|(J_n^+ \backslash QR_n)(A)| = (s - \bar{\tau}_{p,a}^1)(t - \bar{\tau}_{q,a}^1)$
3. $|J_n^{\pm}(A)| = (s + \bar{\tau}_{p,a}^3)(t - \bar{\tau}_{q,a}^1)$;
4. $|J_n^{\mp}(A)| = (s - \bar{\tau}_{p,a}^1)(t + \bar{\tau}_{q,a}^3)$;
5. $|J_n^+(A)| = 2st + s(\bar{\tau}_{q,a}^3 - \bar{\tau}_{q,a}^1) + t(\bar{\tau}_{p,a}^3 - \bar{\tau}_{p,a}^1) + \bar{\tau}_{p,a}^3\bar{\tau}_{q,a}^3 + \bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^1$;
6. $|J_n^-(A)| = 2st + s(\bar{\tau}_{q,a}^3 - \bar{\tau}_{q,a}^1) + t(\bar{\tau}_{p,a}^3 - \bar{\tau}_{p,a}^1) - \bar{\tau}_{p,a}^3\bar{\tau}_{q,a}^1 - \bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^3$;
7. $|QNR_n(A)| = 3st + s(\bar{\tau}_{q,a}^3 - 2\bar{\tau}_{q,a}^1) + t(\bar{\tau}_{p,a}^3 - 2\bar{\tau}_{p,a}^1) - \bar{\tau}_{p,a}^3\bar{\tau}_{q,a}^1 - \bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^3 + \bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^1$.

Următoarele rezultare partiționează mulțimea $a + J^{\pm}$.

Teorema 3.1.6. *Fie $p < q$ două numere prime impare, $n = pq$ un modul RSA, $a \in \mathbf{Z}_n^*$ și $A = (a + J_n^{\pm})$. Atunci izomorfismul f din Teorema 3.1.2 pune în corespondență următoarele mulțimi după cum putem vedea mai jos:*

a) $QR_n(A)$ *în* $QR_p((a)_p + QR_p) \times QR_q((a)_q + QNR_q)$;

b) $(J_n^+ \backslash QR_n)(A)$ *în* $QNR_p((a)_p + QR_p) \times QNR_q((a)_q + QNR_q)$;

c) $J_n^{\pm}(A)$ *în* $QR_p((a)_p + QR_p) \times QNR_q((a)_q + QNR_q)$;

d) $J_n^{\mp}(A)$ *în* $QNR_p((a)_p + QR_p) \times QR_q((a)_q + QNR_q)$.

Numărul de întregi ai mulțimilor din teorema de mai sus sunt exprimate de următorul corolar.

Corolarul 3.1.8. *Fie* $n = pq$ *un modul RSA,* $s = p \text{ div } 4$, $t = q \text{ div } 4$, $a \in \mathbf{Z}_n^*$, *și* $A = (a + J_n^{\pm})$, *atunci*

1. $|QR_n(A)| = (s - \tau_{p,a}^1)(t + \bar{\tau}_{q,a}^3)$;
2. $|(J_n^+ \backslash QR_n)(A)| = (s + \tau_{p,a}^3)(t - \bar{\tau}_{q,a}^1)$;
3. $|J_n^{\pm}(A)| = (s - \tau_{p,a}^1)(t - \bar{\tau}_{q,a}^1)$;
4. $|J_n^{\mp}(A)| = (s + \tau_{p,a}^3)(t + \bar{\tau}_{q,a}^3)$;
5. $|J_n^+(A)| = 2st + s(\bar{\tau}_{q,a}^3 - \bar{\tau}_{q,a}^1) + t(\tau_{p,a}^3 - \tau_{p,a}^1) - \tau_{p,a}^1 \bar{\tau}_{q,a}^3 - \tau_{p,a}^3 \bar{\tau}_{q,a}^1$;
6. $|J_n^-(A)| = 2st + s(\bar{\tau}_{q,a}^3 - \bar{\tau}_{q,a}^1) + t(\tau_{p,a}^3 - \tau_{p,a}^1) + \tau_{p,a}^1 \bar{\tau}_{q,a}^1 + \tau_{p,a}^3 \bar{\tau}_{q,a}^3$;
7. $|QNR_n(A)| = 3st + s(\bar{\tau}_{q,a}^3 - 2\bar{\tau}_{q,a}^1) + t(2\tau_{p,a}^3 - \tau_{p,a}^1) + \tau_{p,a}^1 \bar{\tau}_{q,a}^1 + \tau_{p,a}^3 \bar{\tau}_{q,a}^3 - \tau_{p,a}^3 \bar{\tau}_{q,a}^1$.

Ultima mulțime care ne-a mai rămas să o discutăm în această secțiune este $(a + J_n^{\mp})$.

Teorema 3.1.7. *Fie* $n = pq$ *un modul RSA și* $a \in \mathbf{Z}_n^*$. *Atunci bijecția* f *din Teorema 3.1.2 pune în corespondență mulțimile care partiționează* $A = (a + J_n^{\mp})$ *după cum urmează:*

a) $QR_n(A)$ *în* $QR_p((a)_p + QNR_p) \times QR_q((a)_q + QR_q)$;

b) $(J_n^+ \backslash QR_n)(A)$ *în* $QNR_p((a)_p + QNR_p) \times QNR_q((a)_q + QR_q)$;

c) $J_n^{\pm}(A)$ *în* $QR_p((a)_p + QNR_p) \times QNR_q((a)_q + QR_q)$;

d) $J_n^{\mp}(A)$ *în* $QNR_p((a)_p + QNR_p) \times QR_q((a)_q + QR_q)$.

Corolarul 3.1.9. *Fie* $n = pq$, $s = p \ div\ 4$, $t = q \ div\ 4$, $a \in \mathbf{Z}_n^*$, *și* $A = (a + J_n^{\mp})$, *atunci*

1. $|QR_n(A)| = (s + \bar{\tau}_{p,a}^3)(t - \tau_{q,a}^1)$;
2. $|(J_n^+ \backslash QR_n)(A)| = (s - \bar{\tau}_{p,a}^1)(t + \tau_{q,a}^3)$
3. $|J_n^{\pm}(A)| = (s + \bar{\tau}_{p,a}^3)(t + \tau_{q,a}^3)$;
4. $|J_n^{\mp}(A)| = (s - \bar{\tau}_{p,a}^1)(t - \tau_{q,a}^1)$;
5. $|J_n^+(A)| = 2st + s(\tau_{q,a}^3 - \tau_{q,a}^1) + t(\bar{\tau}_{p,a}^3 - \bar{\tau}_{p,a}^1) - \bar{\tau}_{p,a}^3\tau_{q,a}^1 - \bar{\tau}_{p,a}^1\tau_{q,a}^3$;
6. $|J_n^-(A)| = 2st + s(\tau_{q,a}^3 - \tau_{q,a}^1) + t(\bar{\tau}_{p,a}^3 - \bar{\tau}_{p,a}^1) + \bar{\tau}_{p,a}^3\tau_{q,a}^3 + \bar{\tau}_{p,a}^1\tau_{q,a}^1$;
7. $|QNR_n(A)| = 3st + s(2\tau_{q,a}^3 - \tau_{q,a}^1) + t(\bar{\tau}_{p,a}^3 - 2\bar{\tau}_{p,a}^1) + \\ + \bar{\tau}_{p,a}^3\tau_{q,a}^3 + \bar{\tau}_{p,a}^1\tau_{q,a}^1 - \bar{\tau}_{p,a}^1\tau_{q,a}^3$.

Dat fiind faptul că am finalizat calculele tuturor cardinalilor mulțimilor ce partiționează $(a + \mathbf{Z}_n^*)^*$ și totodată și mulțimile cu diferite șabloane Jacobi modulo p și q, acum putem arăta, în următoarea secțiune, cum se poate calcula o probabilitate ce depinde de mulțimile menționate mai sus. Pentru o imagine vizuală asupra acestor partiționări, a se vedea Figura 3.3.

3.2 Calculul probabilităților peste mulțimile de forma Y$(a + X)$

QR sunt importante în special în matematică dar și în alte domenii precum criptografia. De obicei „definim securitatea și analiza schemelor utilizând experimente probabilistice ce implică algoritmi ce fac alegeri aleatoare“ [43, p.25]. Astfel crește interesul în a afla cum putem calcula probabilități peste mulțimi cu diverse șabloane Jacobi. În această secțiune vom da câteva exemple de calcul a unor astfel de probabilități, urmând ca în următorul capitol să le utilizăm.

$(a + \mathbf{Z}_n^*)^*$

$a + QR_n$	$a + (J_n^+ \setminus QR_n)$
$a + J_n^{\pm}$	$a + J_n^{\mp}$

$\Downarrow$

$QR_n(a + QR_n)$	$(J_n^+ \setminus QR_n)(a + QR_n)$	$QR_n(a + J_n^+ \setminus QR_n)$	$(J_n^+ \setminus QR_n)(a + J_n^+ \setminus QR_n)$
$J_n^{\pm}(a + QR_n)$	$J_n^{\mp}(a + QR_n)$	$J_n^{\pm}(a + J_n \setminus QR_n)$	$J_n^{\mp}(a + J_n \setminus QR_n)$
$QR_n(a + J_n^{\pm})$	$(J_n^+ \setminus QR_n)(a + J_n^{\pm})$	$QR_n(a + J_n^{\mp})$	$(J_n^+ \setminus QR_n)(a + J_n^{\mp})$
$J_n^{\pm}(a + J_n^{\pm})$	$J_n^{\mp}(a + J_n^{\pm})$	$J_n^{\pm}(a + J_n^{\mp})$	$J_n^{\mp}(a + J_n^{\mp})$

Figura 3.3: Mulțimile ce partiționează $(a + \mathbf{Z}_n^*)^*$

Corolarul 3.2.1. *Fie $n = pq$ un modul RSA și $a \in \mathbf{Z}_n^*$. Atunci:*

(1) $P\left(x \in QR_n \,:\, x \leftarrow (a + \mathbf{Z}_n^*)^*\right) = \begin{cases} \frac{1}{4} + \mathcal{O}\left(\frac{1}{n}\right), & \text{dacă } a \in J_n^+ \setminus QR_n \\ \frac{1}{4} - \mathcal{O}\left(\frac{1}{n}\right), & \text{altfel.} \end{cases}$

(2) $P(x \in J_n^+ \setminus QR_n \,:\, x \leftarrow (a + \mathbf{Z}_n^*)^*) = \begin{cases} \frac{1}{4} + \mathcal{O}\left(\frac{1}{n}\right), & \text{dacă } a \in J_n^+ \setminus QR_n \\ \frac{1}{4} - \mathcal{O}\left(\frac{1}{n}\right), & \text{altfel.} \end{cases}$

(3) $P(x \in J_n^{\pm} \,:\, x \leftarrow (a + \mathbf{Z}_n^*)^*) = \begin{cases} \frac{1}{4} + \mathcal{O}\left(\frac{1}{n}\right), & \text{dacă } a \in J_n^{\mp} \\ \frac{1}{4} - \mathcal{O}\left(\frac{1}{n}\right), & \text{altfel.} \end{cases}$

Distribuția diverselor șabloane Jacobi, mai ales în cazul modulilor RSA - produs de două numere prime - este de mare interes nu doar în matematică ci și în criptografie, așa cum menționam mai sus. În următorul capitol vom vedea cum putem folosi rezultatele din capitolul acesta pentru a demonstra anumite proprietăți și chiar cum putem evita presupunerea reziduozității pătratice și obține rezultate mai bune în demonstrații legate de securitatea anumitor scheme.

Capitolul 4

Aplicații ale reziduurilor pătratice în criptarea bazată de identitate

O schemă generală IBE, după cum este prezentat în [7], are patru algoritmi probabiliști de complexitate timp polinomială (PPT). Primul este $\textsc{Setup}(\lambda)$, care, primind la intrare un parametru de securitate λ, returnează parametrii publici, PP, și cheia secretă master, msk. Algoritmul $\textsc{KeyGen}(PP, msk, ID)$ calculează cheia secretă, sk_{ID}, corespunzătoare unei identități date, ID. Următorii doi algoritmi sunt $\textsc{Encryption}(PP, m)$ și $\textsc{Decryption}(sk_{ID}, c)$. Aceștia criptează un mesaj m pentru o anumită identitate, ID, obținând criptotextul c și, respectiv decriptează criptotextul c utilizând cheia secretă ce corespunde aceleiași identități, cea a destinatarului, și anume ID.

Vom prezenta, în cele ce urmează, prima schema IBE ce folosește reziduurile pătratice, schemă ce se datorează lui Cocks [12].

4.1 Schema IBE a lui Cocks

Construcția lui Cocks, algoritmul 1 de la pagina 31, criptează un bit odată și funcționează bine pentru mesaje scurte [12]. Deși are

un timp de rulare excelent, dezavantajul acesteia este reprezentat de expansiunea criptotextului, $\mathcal{O}(2\ log\ n)$ - un bit din textul în clar, plaintext, este criptat prin doi întregi din $\mathbf{Z}_n$. Securitatea schemei este exprimată prin următoarea teoremă.

Teorema 4.1.1 ([12, 30])**.** *Schema IBE a lui Cocks este sigură IND-ID-CPA în modelul cu oracol aleator, ROM, presupunând că QRA are loc pentru generatorul Gen.*

Criptotextele rezultate din criptarea cu schema lui Cocks sunt de forma: $t+at^{-1}$, unde $a, t \in \mathbf{Z}_n^*$. În cele ce urmează vom analiza mulțimea de întregi ce pot fi criptotexte Cocks, cu scopul de a înțelege de ce acest criptosistem nu asigură anonimatul destinatarului sau, mai pe scurt, nu este anonimă, și cum de funcționează testul lui Galbraith (GT).

4.1.1 Criptotextele schemei Cocks IBE

Fie un modul n și $a \in J_n^+$, știm despre criptotextele Cocks că sunt de forma aceasta: $t + at^{-1} \bmod n$. Vom nota mai departe mulțimea elementelor de acest fel prin $C_n(a)$.

Dacă rescriem un criptotext Cocks pentru valor fixate ale lui a și c în $\mathbf{Z}_n^*$, vom obține forma generală a unei ecuații de gradul doi, în necunoscuta t, adică $c \equiv_n t + at^{-1} / \cdot t \quad \Leftrightarrow ct \equiv_n t^2 + a$, care este echivalent cu:

$$t^2 - ct + a = 0 \bmod n \tag{4.1}$$

Teorema 4.1.2. *Fie $a \in J_n^+$, $c \in \mathbf{Z}_n$ și $C_n(a) = \{t + at^{-1} \bmod n | t \in \mathbf{Z}_n^*\}$. Atunci $c \in C_n(a)$ dacă și numai dacă discriminantul ecuației 4.1, notat cu Δ, este fie 0, fie un reziduu pătratic în $\mathbf{Z}_n^*$. Mai mult, c poate fi 0 și totuși în $C_n(a)$ dacă și numai dacă $-a$ este reziduu pătratic.*

Această teoremă va fi utilă în calculele ce urmează în Secțiunea 4.1.2, unde, în plus, vom avea nevoie de cardinalul precis al mulțimii

Algorithm 1 Schema IBE a lui Cocks

procedure Setup(λ)
  $(p, q) \leftarrow Gen(\lambda)$; ▷ astfel încât $p \equiv_4 q \equiv_4 3$
  $n = pq$;
  $e \leftarrow J_n^+ \setminus QR_n$; ▷ de exemplu $e \equiv_n -1$
  $h : \{0,1\}^* \leftarrow J_n^+$; ▷ funcție hash ce pune în corespondență identitățile cu elemente din J_n^+
  $PP = (n, e, h)$;
  $msk = (p, q)$;
  return (PP, msk).
end procedure

procedure KeyGen(msk, ID)
  $a = h(ID)$;
  if $a \in QNR_n$ **then**
    $a = ea$;
    $r = a^{(n+5-(p+q))/8}$; ▷ $r \leftarrow SQRT_n(a)$
  end if
  return r.
end procedure

procedure Encrypt(PP, ID, m) ▷ unde $m \in \{\pm 1\}$
  $a = h(ID)$;
  $t_1, t_2 \leftarrow \mathbf{Z}_n^*$ astfel încât $(t_1|n) = (t_2|n) = (m|n)$
  $c_1 = t_1 + at_1^{-1}$;
  $c_2 = t_2 + eat_2^{-1}$;
  return (c_1, c_2).
end procedure

procedure Decrypt($PP, r, (c_1, c_2)$)
  if $r^2 \equiv_n h(ID)$ **then**
    $c = c_1$;
  else $c = c_2$;
  end if
  $m = \left(\frac{c+2r}{n}\right)$;
  return m.
end procedure

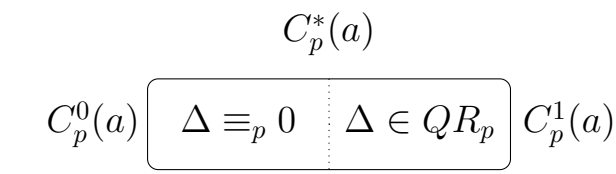


Figura 4.1: Mulțimea C_p^*, unde $\Delta = c^2 - 4a$ din Ecuația 4.1

de criptotexte Cocks. Astfel, pentru a-l obține, am calculat cardinalul acesta pentru cazul modulilor primi p, $C_p(a)$, folosind rezultatele din Capitolul 3, și am calculat apoi cardinalul aceleiași mulțimi pentru cazul $C_n(a)$, unde n este un modul RSA obținut cu ajutorul bijecției f din Teorema 3.1.2.

Dacă analizăm mulțimea $C_p^*(a) = C_p(a) \cap \mathbf{Z}_p^*$ prin prisma Teoremei 4.1.2, pentru un modul prim p, putem exprima partiționarea acestei mulțimi după cum se vede în Figura 4.1 și este exprimată mai jos.

$$\Delta \equiv_p 0: \qquad C_p^0(a) = \{c \in \mathbf{Z}_n^* | (c^2 - 4a | n) = 0\}$$

$$\Delta \in QR_p: \qquad C_p^1(a) = \{c \in \mathbf{Z}_n^* | (c^2 - 4a | n) = 1\}$$

Astfel, pentru ca un întreg c să fie în $C_p^0(a)$, este nevoie de un element $a \in QR_p$. Acum putem purcede la calculul cardinalilor acestor mulțimi: $|C_p^0(a)|$, $|C_p^1(a)|$, al reuniunii acestora, $|C_p^*(a)|$ și al mulțimi ce îl conține și pe $c \equiv_p 0$, adică mulțimea $C_p(a)$.

Corolarul 4.1.1. *Fie $C_p^0(a)$, $C_p^1(a)$, $C_p^*(a)$ și $C_p(a)$ definit ca mai sus, p un număr prim impar, $a \in \mathbf{Z}_n^*$ și $k = p$ div 4. Atunci*

1. $|C_p^0(a)| = 2(\tau_{p,a}^1 + \tau_{p,a}^3)$
2. $|C_p^1(a)| = 2|QR_p(a + QR_p)| = 2(k - \tau_{p,a}^1)$
3. $|C_p^*(a)| = 2(k + \tau_{p,a}^3)$
4. $|C_p(a)| = 2(k + \tau_{p,a}^3) + \tau_{p,a}^1 + \bar{\tau}_{p,a}^3$.

În cazul modulilor RSA n, pentru un întreg fixat $a \in \mathbf{Z}_n^*$, vom folosi funcția f din Teorema 3.1.2 pentru a analiza mulțimea $C_n^*(a)$. Fie Δ determinantul din Ecuația 4.1 și mulțimile $C_n^{i,j}(a) =$

$\{c \in \mathbf{Z}_n^* | ((\Delta)_p|p) = i,\ ((\Delta)_q|q) = j\}$, putem ușor ajunge de la două numere prime impare p și q la modulul RSA $n = pq$ prin f, ca în teorema de mai jos.

Teorema 4.1.3. *Fie p, q două numere prime impare distincte, $n = pq$ un modul RSA și $a \in \mathbf{Z}_n^*$. Atunci izomorfismul f din Teorema 3.1.2 va duce la următoarele corespondențe:*

a) $C_n^*(a)$ *onto* $C_p^*((a)_p) \times C_q^*((a)_q)$;

b) $C_n^{0,0}(a)$ *în* $C_p^0((a)_p) \times C_q^0((a)_q)$;

c) $C_n^{0,1}(a)$ *în* $C_p^0((a)_p) \times C_q^1((a)_q)$;

d) $C_n^{1,0}(a)$ *în* $C_p^1((a)_p) \times C_q^0((a)_q)$;

e) $C_n^{1,1}(a)$ *în* $C_p^1((a)_p) \times C_q^1((a)_q)$;

f) $C_n(a)$ *în* $C_p((a)_p) \times C_q((a)_q)$.

Corolarul 4.1.2. *Fie n un modul RSA și $a \in \mathbf{Z}_n^*$. Atunci mulțimea $C_n^*(a)$ este reuniunea mulțimilor $C_n^{0,0}, C_n^{1,0}, C_n^{0,1}$ și $C_n^{1,1}$.*

cum vom putea calcula cardinalul fiecărei mulțimi din Teorema 4.1.3.

Corolarul 4.1.3. *Fie p, q două numere prime impare, $n = pq$ modul RSA, $a \in \mathbf{Z}_n^*$, $k_1 = p \ div\ 4$, și $k_2 = q \ div\ 4$. Atunci,*

1. $|C_n^*(a)| = |C_p^*((a)_p)| \cdot |C_q^*((a)_q)|$;
2. $|C_n^{0,0}(a)| = 4(\tau_{p,a}^1 + \tau_{p,a}^3)(\tau_{q,a}^1 + \tau_{q,a}^3)$;
3. $|C_n^{0,1}(a)| = 4(\tau_{p,a}^1 + \tau_{p,a}^3)(k_2 - \tau_{q,a}^1)$;
4. $|C_n^{1,0}(a)| = 4(\tau_{q,a}^1 + \tau_{q,a}^3)(k_1 - \tau_{p,a}^1)$;
5. $|C_n^{1,1}(a)| = 4|QR_n(a + QR_n)| = 4(k_1 - \tau_{p,a}^1)(k_2 - \tau_{q,a}^1)$;
6. $|C_n(a)| = |C_p((a)_p)| \cdot |C_q((a)_q)|$.

Odată ce avem aceste rezultate, le putem folosi pentru a verifica anonimatul criptotextelor rezultate din schema IBE a lui Cocks.

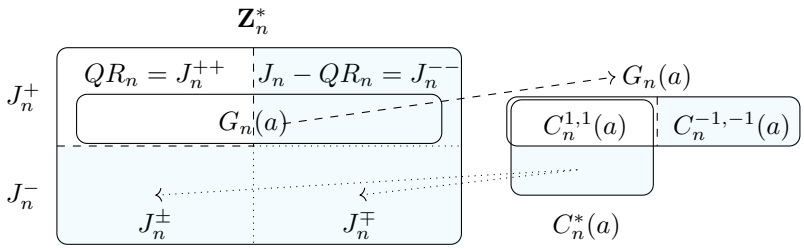


Figura 4.2: Partițiile mulțimii $G_n(a)$

4.1.2 Testul Galbraith

Când cineva criptează un mesaj printr-o schemă IBE, se utilizează o identitate, cea a destinatarului. Câteodată este important să nu se poată ști pentru cine criptăm, astfel încât destinatarul să rămână anonim. Fie $ID_1, ID_2 \in J_n^+$ identitățile a doi destinatari. Spunem că o schemă IBE este anonimă (cu sensul din [2]) dacă, în momentul în care intervine o a treia entitate și analizează criptotextele obținute pentru una din aceste două identități, ID_1 sau ID_2, aceasta nu va putea spune că destinatarul a fost ID_1 sau ID_2 decât cu o probabilitate neglijabilă.

Din 2004, de când se preciza în [25, 6] că, prin testul Galbraith se poate descoperi destinatarul criptotextelor Cocks, au fost propuse mai multe variante de anonimizare a acestei scheme, mai mult sau mai puțin eficiente [14, 1, 61, 11, 40]. Boneh și colab. au prezentat GT în [6]. Acest test ajută în a stabili, cu probabilitate foarte mare, dacă destinatarul unui criptotext are o anumită identitate sau nu. În această secțiune am folosit rezultatele din Capitolul 3 pentru a demonstra riguros GT. Algoritmul GT, după cum a fost prezentat în [1], primește la intrare un modul n, un criptotext c și o identitate a, returnând ± 1 cu următorul înțeles:

$$\begin{cases} +1: & c \text{ este un criptotext Cocks și, cu o probablilitate} \\ & \text{de } 1/2 \text{ el a fost criptat pentru identitatea } a; \\ -1: & c \text{ nu a fost criptat pentru identitatea } a \text{ (cu siguranță).} \end{cases}$$

Am demonstrat amănunțit cum este posibilă această identifi-

care, și am prezentat cardinalii exacți care sunt implicați în acest calcul.

Teorema 4.1.4. *Fie $n = p \cdot q$ un modul RSA, iar p, q numere prime impare și $a \in \mathbf{Z}_n^*$. Atunci mulțimea $G_n(a)$, partiționată de mulțimile $C_n^{1,1}(a)$ și $C_n^{-1,-1}(a)$, are cardinalul $4|QR_n(a + J_n^+)|$.*

Așadar, îl putem verifica pe c prin prisma lui a pentru a afla dacă $c \in C_n^*(a)$ făcând uz de testul Galbraith, descris în Algoritmul 2 și putem calcula exact probabilitatea ca $c \in C_n^*(a)$, când $(\Delta|n) = +1$, folosind rezultatele din secțiunea anterioară astfel:

$$P(c \in C_n^*(a) : c \leftarrow G_n(a)) = \frac{|C_n^{1,1}(a)|}{|G_n(a)|} = \frac{1}{2} - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right).$$

Algorithm 2 : Testul Galbraith

Input: (a, c, n) ▷ $a \in J_n^+$, $n \leftarrow Gen(\lambda)$, c - `criptotext Cocks`

Output: *yes* `sau` *no*

$\Delta = c^2 - 4a$;

if $\left(\frac{\Delta}{n}\right) = 1$ `sau dacă` $\left(\frac{\Delta}{n}\right) = 0$ **then**

  return `yes` ▷ `cu înțelesul:` $P[c \in C_n(a)] = 1/2$

else

  return `no` ▷ `cu înțelesul:` $c \notin C_n(a)$, în mod cert

end if

Pentru a stabili identitatea unei mulțimi de criptotexte al căror destinatar este același, se repetă GT pentru fiecare criptotext din această mulțime, pentru a crește probabilitatea unui răspuns corect. Având în vedere că schema IBE a lui Cocks criptează doar

câte un bit odată și că un expeditor, în general, trimite mai mulți biți și nu doar unul singur, se va obține o mulțime de criptotexte Cocks criptate folosind aceeași identitate, iar această mulțime va fi analizată pentru a se stabili identitatea destinatarului.

4.1.3 Variantele anonime ale schemei lui Cocks

În 2005, Hayashi și Tanaka au extins sensul anonimatului, descris în Secțiunea 4.1.2, la un caz generalizat, numit *anonimat universal* [35]. Această proprietate permite oricui deține cheia publică a destinatarului să anonimizeze un criptotext, și nu doar expeditorului. În acest caz procesul de anonimizare este separat de criptare, fiind o acțiune de sine stătătoare.

Schema lui Cocks nu este anonimă [6], dar au fost propuse anumite variante anonime de către mai mulți cercetători. G. Di Crescenzo și V. Saraswat [14] în 2007, G. Ateniese și P. Gasti [1] în 2009, M. Clear, H. Tewari și C. McGoldrick [11], ca și G.A. Schipor [61], în 2014, iar M. Joye [40] în 2016.

Schema IBE a lui Joye

Cea mai eficientă variantă anonimă a schemei IBE a lui Cocks este cea propusă de Joye [40]. În această secțiune prezentăm schema acestuia într-o formă mult simplificată [51], folosindu-ne de analiza criptotextelor Cocks făcută anterior și de rezultatele din Capitolul 3.

Pe baza secțiunii 4.1.1 și ținând cont de faptul că majoritatea criptotextelor Cocks fac parte din mulțimea $C_n^{1,1}(a)$, ne putem da seama că, dacă expeditorul ar modifica ușor câteva criptotexte, alegând în mod aleator pe care să le modifice și pe care nu, și dacă am găsi o metodă prin care destinatarul să fie singurul care să poată identifica criptotextele modificate, și să poată să le deanonimizeze, atunci vom obține o schemă anonimă. Astfel, dat un element $c \in C_n^{1,1}(a)$, expeditorul va putea să îl transforme într-un c' astfel încât $GT_{n,a}(c') = \pm 1$ fixând un d astfel încât $GT_{n,a}(d) = -1$

și folosind apoi o operație binară $\circ$ pe $\mathbf{Z}_n^*$ astfel încât

$$GT_{n,a}(c \circ d) = GT_{n,a}(c) \cdot GT_{n,a}(d).$$

Astfel criptotextul modificat ar fi $c' = c \circ d$. Acum vom căuta o metodă astfel încât doar expeditorul și destinatarul să poată ști care criptotexte trebuie deanonimizate și care nu. În acest scop va fi folosit testul Galbraith după cum vom vedea mai jos.

Vom nota prin $\circ$ următoarea operație:

$$u \circ v = \frac{uv + 4a}{u + v} \bmod n,$$

oricare ar fi $u, v \in \mathbf{Z}_n^*$ cu $(u + v, n) = 1$.

Această operație are anumite proprietăți ce sunt prezentate în propoziția următoare și asigură corectitudinea schemei.

Propoziția 4.1.1. *Fie $u, v, w \in \mathbf{Z}_n^*$ și $a \in J_n^+$. Atunci:*

1. *Operația $\circ$ este asociativă atunci când este definită, deci $u \circ (v \circ w) = (u \circ v) \circ w$.*

2. *Chiar dacă $v \circ (-v)$ nu este definită, avem $(u \circ v) \circ (-v) = u$ când $(u + v, n) = 1$ și $(v^2 - 4a, n) = 1$.*

3. *Când $u \circ v$ este definită, $GT_{n,a}(u \circ v) = GT_{n,a}(u) \cdot GT_{n,a}(v)$.*

4. *$u \circ u \in G_n(a)$.*

Pentru a identifica dacă un criptotext c^* a fost modificat sau nu, vom folosi Propoziția 4.1.1(4), care spune că $u \circ u$ va trece întotdeauna testul Galbraith și Propoziția 4.1.1(3) care, presupunând că $u \circ v$ este definită, stabilește că $u \circ v$ trece testul Galbraith dacă și numai dacă testul Galbraith dă același rezultat atât pentru u cât și pentru v.

Folosind această operație, împreună cu proprietățile de mai sus, avem tot ce ne trebuie pentru a descrie schema anonimă, așa cum putem vedea în Algoritmul 3.

În ceea ce privește securitatea schemei, avem următoarea teoremă.

Teorema 4.1.5 ([51]). *Schema AnonIBE a lui Cocks este sigură ANON-IND-ID-CPA în modelul cu oracol aleator sub QRA.*

4.2 Schema BGH

Există un rezultat remarcabil din 2007, al cărui obiectiv a fost obținerea unor criptotexte mai mici pornind de la schema lui Cocks [12] - schema lui Boneh, Gentry și Hamburg (BGH) [8]. Ei și-au îndeplinit scopul dar schema lor rămâne totuși nefezabilă în practică din cauza complexității, care devine cuartică în parametrul de securitate.

Ei criptează un bit de text în clar prin multiplicarea acestuia printr-un simbol Jacobi a cărui valoare poate fi calculată doar de expeditor, deoarece doar el cunoaște anumiți parametri pe care i-a ales.

Procesul de decriptare este foarte inovativ. Fără a ști parametrii aleși de expeditor, destinatarul calculează o anumită cantitate, pe baza cheii sale secrete, care are același simbol Jacobi cu cel calculat de expeditor. Cum poate fi posibil?

Ne-ar trebui o metodă prin care să putem obține aceeași valoare atât la expeditor cât și la destinatar folosindu-și fiecare parametrii pe care îi cunoaște. O astfel de metodă ar putea folosi o pereche de polinoame f și g și câteva condiții. Astfel, considerând că destinatarul are cheia secretă r și expeditorul are propriul parametru, cunoscut doar de el, s, destinatarul va folosi $f(r)$ la decriptare iar expeditorul va folosi $g(s)$ pentru a cripta, cu condiția ca simbolul lor Jacobi să fie egal modulo n, unde n este public. Mai precis, $(f(r)|n) = (g(s)|n)$. Aceasta este ideea folosită de Boneh și colab. în schema propusă de ei [8]. Concept este foarte frumos, interesant și bine gândit.

Ideea lor a fost de a stabili câțiva parametri utilizați la criptare și decriptare pe care îi obțin prin calcularea unor soluții pentru

Algorithm 3 Schema AnonIBE a lui Cocks [40]

procedure SETUP(λ):
$PP = (n, e, d, h)$
▷ unde n și e sunt ca în schema IBE a lui Cocks
$d \leftarrow \mathbf{Z}_n^*$ și $h : \{0,1\}^* \to J_n^+$ sunt aleși astfel încât $GT_{n,a}(d) = -1 = GT_{n,ea}(d)$, pentru orice ieșire a a funcției h
$msk = (p, q)$
return (PP, msk).
end procedure

procedure EXT(msk, ID):
$a = h(ID)$;
return r ▷ (cheia secretă) răd. pătr. aleatoare a lui a sau ea
end procedure

procedure ENC(PP, ID, m):
$a = h(ID)$;
$t_0, t_1 \leftarrow \mathbf{Z}_n^*$ cu $J_n(t_0) = m = J_n(t_1)$;
$c_0 \leftarrow \{u, u \circ d\}$ unde $u = t_0 + at_0^{-1} \bmod n$;
$c_1 \leftarrow \{v, v \circ d\}$ unde $v = t_1 + eat_1^{-1} \bmod n$;
return (c_0, c_1).
end procedure

procedure DEC($(c_0, c_1), r$):
set $b \in \{0,1\}$ astfel încât $e^b a \equiv_n r^2 \bmod n$;
return $m = \begin{cases} J_n(c_b + 2r), & \text{dacă } GT_{n,e^b a}(c_b) = 1 \\ J_n(c_b \circ (-d) + 2r), & \text{altfel} \end{cases}$
end procedure

ecuația congruențială notată prin $QC_n(a, S)$ și dată de

$$ax^2 + Sy^2 \equiv_n 1 \tag{4.2}$$

unde n este un modul RSA și $a, S \in \mathbf{Z}_n^*$. Astfel, dacă considerăm (x, y) o soluție pentru Ecuația 4.2, atunci cele două polinoame vor fi calculate astfel:

$$f(r) = xr + 1 \bmod n,$$

$$g(s) = 2(ys + 1) \bmod n.$$

Procesul prin care se găsesc aceste soluții (x, y) reprezintă partea care crește complexitatea schemei BGH și este detaliat în Secțiunea 4 din [8], arătând totodată cum pot fi găsite două astfel de *polinoame asociate* f și g. Acum să vedem concret ce proprietăți trebuie să îndeplinească acestea.

4.2.1 Polinoame asociate

Definiția 4.2.1 ([74, 62])**.** *Fie $n \in \mathbf{N}$, $a, S \in \mathbf{Z}_n^*$ și $f, g \in \mathbf{Z}_n^*[x]$, atunci, dacă următoarele două condiții sunt îndeplinite, spunem că f și g sunt două* polinoame asociate (a,S)*:*

1. *$f(r)g(s) \in QR_n$ ori de câte ori $a, S \in QR_n$, $\forall r \in SQRT_n(a)$ și $\forall s \in SQRT_n(S)$.*
2. *$f(r)f(-r)S \in QR_n$ ori $a \in QR_n, \forall r \in SQRT_n(a)$. În acest caz spunem că f este* a-sigur*.*

Remarca 4.2.1. *Când $S \in J_n^+ \setminus QR_n$, Condiția (2) este echivalent cu a zice că $\left(\frac{f(r)}{n}\right)$ este uniform distribuit în $\{\pm 1\}$ când r este uniform ales din $SQRT_n(a)$, ori de câte ori a este a reziduu modulo n (vezi Lema 3.3 din [8]). Această proprietate va fi exploatată în Secțiunea 4.2.3.*

Corectitudinea decriptării este asigurată de (1), iar (2) este utilizată în a demonstra securitatea, după cum vom vedea în Jocul 6 din demonstrația de securitate a schemei BGH.

Definiția 4.2.2 ([8]). *Dacă $\mathcal{Q}$ este un algoritm determinist care, primind la intrare n, a, S calculează două polinoame asociate (a, S), atunci $\mathcal{Q}$ se numește algoritm* compatibil IBE.

S-a evidențiat în [8, Lema 3.3.] că, dacă $n = pq$ este un modul RSA, $a \in QR_n$ iar polinomul f satisface (1) din Definiția 4.2.1 și $S \in J_n^+$, atunci, când S este reziduu, pentru toate valorile lui r din $SQRT_n(a)$, $(f(r)|n)$ are aceeași valoare, iar când $S \in J_n^+ \backslash QR_n$, $(f(r)|n)$ este $+1$ sau -1 cu egală probabilitate, deci $(f(r)|n)$ este uniform distribuit în $\{\pm 1\}$. Acest ultim caz are loc datorită celor patru valori posibile din $SQRT_n(a)$, obținute prin combinarea valorilor lui $r \in \mathbf{Z}_p^*$ și ale lui $r \in \mathbf{Z}_q^*$ prin CRT. Această proprietate se utilizează în ultimul joc din demonstrația de securitate.

4.2.2 Schema BGH și securitatea acesteia

Schema abstractă *BasicIBE* a fost propusă de Boneh și colab. în [8], iar securitatea acesteia (discutată în articolul nostru [62]) va fi analizată mai jos, având ca punct de pornire teorema de mai jos.

Teorema 4.2.1 ([8]). *Fie h, din schema BasicIBE, modelată ca oracol aleator și F o funcție PRF. Presupunând că QRA are loc pentru generatorul Gen, atunci schema BasicIBE este sigură IND-ID-CPA și avantajul unui adversar eficient $\mathcal{A}$ împotriva acestei scheme va fi*

$$\text{IBEAdv}_{\mathcal{A},BasicIBE}(\lambda) \leq \text{PRFAdv}_{\mathcal{B}_1,F}(\lambda) + 2 \cdot \text{QRAdv}_{\mathcal{B}_2,Gen}(\lambda)$$

pentru algoritmii eficienți $\mathcal{B}_1$ și $\mathcal{B}_2$, al căror timp de execuție este aproximativ același cu cel al lui $\mathcal{A}$.

Pentru a reduce numărul de soluții ale ecuațiilor de forma Ecuației 4.2, la criptare, de la $2l$ la $l + 1$, Boneh și colab. au propus următoarea formă de combinare a soluțiilor:

Lema 4.2.1 ([8]). *Fie (x_i, y_i) o soluție a ecuației $a_i x^2 + Sy^2 = 1$, unde $i \in \{1, 2\}$, atunci (x_3, y_3) este o soluție pentru ecuația*

$$a_1 a_2 \cdot x^2 + S \cdot y^2 = 1 \tag{4.3}$$

unde $x_3 = \dfrac{x_1x_2}{Sy_1y_2+1}$ *și* $y_3 = \dfrac{y_1+y_2}{Sy_1y_2+1}$.

Această formulă va fi folosită pentru a combina soluțiile ecuațiilor $ax^2+Sy^2 \equiv_n 1$ și $ex^2+Sy^2 \equiv_n 1$ și a obține o soluție pentru ecuația $eax^2 + Sy^2 \equiv_n 1$.

În Secțiunea 4.3.1 vom vedea cum a fost modificată această lemă și de ce rezultatul nu a fost cel așteptat, ducând, în schimb, la pierderea securității schemei.

4.2.3 O nouă analiză de securitate pentru schema $BasicIBE$

Datorită faptului că $QC_n(a,S)$ este simetric, folosind Remarca 4.2.1, extindem Definiția 4.2.1 cu o a treia condiție după cum urmează.

Definiția 4.2.3 ([62]). *Fie* $n \in \mathbf{N}$, $a, S \in \mathbf{Z}_n^*$ *și fie* $\mathcal{Q}(n,a,S)$ *un algoritm determinist ce generează două polinoame* $f, g \in \mathbf{Z}_n[x]$. *Spunem că* $\mathcal{Q}$ *este* compatibil-extins IBE *dacă este* compatibil IBE *și este îndeplinită următoarea condiție*

3. $\left(\frac{g(s)}{n}\right)$ *este uniform distribuit în* $\{\pm 1\}$ *ori de câte ori* $a \in J_n^+ \setminus QR_n$ *și* $S \in QR_n$, *unde* $s \in_R SQRT_n(S)$.

Cu ajutorul unui algoritm compatibil-extins IBE vom putea obține o mărginire superioară mai precisă decât cea din Teorema 4.2.1, modificând puțin demonstrația de securitate a schemei BGH. Acest rezultat este concentrat în teorema următoare.

Teorema 4.2.2. *Fie* h *din schema BasicIBE modelată ca un oracol aleator, și* F *o funcție PRF. Presupunând că are loc QRA pentru generatorul* Gen, *atunci schema BasicIBE este sigură IND-ID-CPA iar avantajul unui adversar eficient, adică PPT,* $\mathcal{A}$ *împotriva acesteia va fi*

$$\mathrm{IBEAdv}_{A,BasicIBE}(\lambda) \leq \mathrm{PRFAdv}_{B_1,F}(\lambda) + \mathrm{QRAdv}_{B_2,Gen}(\lambda).$$

pentru algoritmii eficienți $\mathcal{B}_1$ și $\mathcal{B}_2$, al căror timp de rulare este aproximativ același cu cel al algoritmului $\mathcal{A}$.

4.3 Schemele IBE nesigure bazate pe QR

Modalitatea de combinare a soluțiilor în scopul reducerii numărului de ecuații de rezolvat poate duce la pierderea securității, deci vom avea o schemă nesigură, așa cum vom vedea în această secțiune. Vom începe cu schema lui Jhanwar și Barua, care au venit cu ideea de a modifica lema de combinare din [8, Lema 5.1]. Dorim să evidențiem aici că, în pofida faptului că articolul lor nu oferă o variantă sigură a schemei BGH, autorii vin cu un rezultat foarte util: un algoritm rapid de rezolvare a ecuației congruențiale de forma Ecuației 4.2.

4.3.1 Schema lui Jhanwar și Barua

În [39] (JB), Jhanwar și Barua au înlocuit algoritmul determinist de găsire de soluții pentru Ecuația 4.2 printr-unul probabilist. În calculul unei soluții folosind acest algoritm propus de ei, este nevoie de numai o inversiune modulară în $\mathbf{Z}_n$ iar cea mai mare îmbunătățire față de BGH este că nu necesită generarea de numere prime, care este un proces costisitor.

Ei folosesc o formulă diferită de cea din [8] pentru a combina soluții ale Ecuației 4.2. Scopul este obținerea unei scheme mai rapide.

Lema 4.3.1. *Fie (x_i, y_i) o soluție a ecuației $ax^2 + S_i y^2 = 1$, unde $i \in \{1, 2\}$, atunci perechea (x_3, y_3) obținută prin*

$$x_3 = \frac{x_1 + x_2}{ax_1x_2 + 1}, \quad y_3 = \frac{y_1y_2}{ax_1x_2 + 1}$$

este o soluție a ecuației $ax^2 + S_1S_2y^2 = 1$.

Din nefericire, utilizând această combinare survine pierderea securității schemei, care nu va mai fi sigură IND-ID-CPA [60].

4.3.2 Alte scheme IBE nesigure bazate pe QR

JB-REVIZUIT DE SUSILO ȘI COLAB.
În [21], Elashri, Mu și Susilo au notificat o pierdere de securitate din [39], diferită de cea menționată în [60]. Ei au arătat totodată cu se poate evita această pierdere dar, în pofida acestui fapt, versiunea lor „remediată“ a variantei JB rămâne vulnerabilă în fața atacului prezentat de Adrian Schipor în [60]. Elashri și colab. spun că versiunea lor este la fel de sigură ca și schema BGH dar, din păcate, datorită faptului că ei folosesc aceeași combinare ca și Jhanwar și Barua [39], pierderea securității menționată de Schipor în [60] are loc și în acest caz.

Dat fiind faptul că variantele propuse de Susilo și colab. nu sunt sigure, rămâne loc pentru îmbunătățiri și pentru versiuni mai rapide ale schemei BGH.

4.4 Autentificarea mutuală continuă

În anumite contexte cum ar fi domeniul militar sau alte asemenea nișe importante, comunicarea prin canale nesigure necesită ca, în orice moment al conversației, ambele părți implicate autentificate [34]. Acest concept se numește *autentificare mutuală continuă* (CMA) [50, 47, 48].

4.4.1 Real privacy management

*Real Privacy Managemen*t (RPM) este o metodă pentru CMA ce a fost patentată în 2008 de Paul McGough (a se vedea [47] și [48]). Aceasta generează și manageriază cheile, asigurând totodată secretizarea informațiilor. Oferă de asemenea o soluție de securitate în timp real pentru comunicarea în rețea în general.

Prin *pas de comunicare* vom înțelege operațiile efectuate pentru a transmite și a primi un singur mesaj m dintr-o parte în alta într-un mod sigur și autentificat. Mai mulți pași de comunicare vor forma o *sesiune*.

Protocolul RPM asigură secret perfect iar securitatea acestuia constă într-o autentificare robustă (atât construcție cât și transmisie) și o criptare sigură.

Dacă un atacator, la un anumit moment, captează credențialele (datele de autentificare), el va avea acces la tot restul comunicării. În cazul unui astfel de atac, pentru a opri intrusul de la accesarea informației ce va fi transmisă după atacul cu succes, ne-am putea gândi să reînnoim credențialele, dar rămâne întrebarea: „Cum am putea transmite noii parametri *ack* evitând ca atacatorul care înțelege deja comunicarea să îi capteze?". Aceasta este principala problemă a protocolului RPM ce a motivat studiul nostru. Astfel propunem în cele ce urmează o nouă metodă de autentificare ce previne acest atac [50]. Ideea principală este ca metoda de actualizare să fie diferită de cea utilizată în RPM.

4.4.2 Descrierea RPM

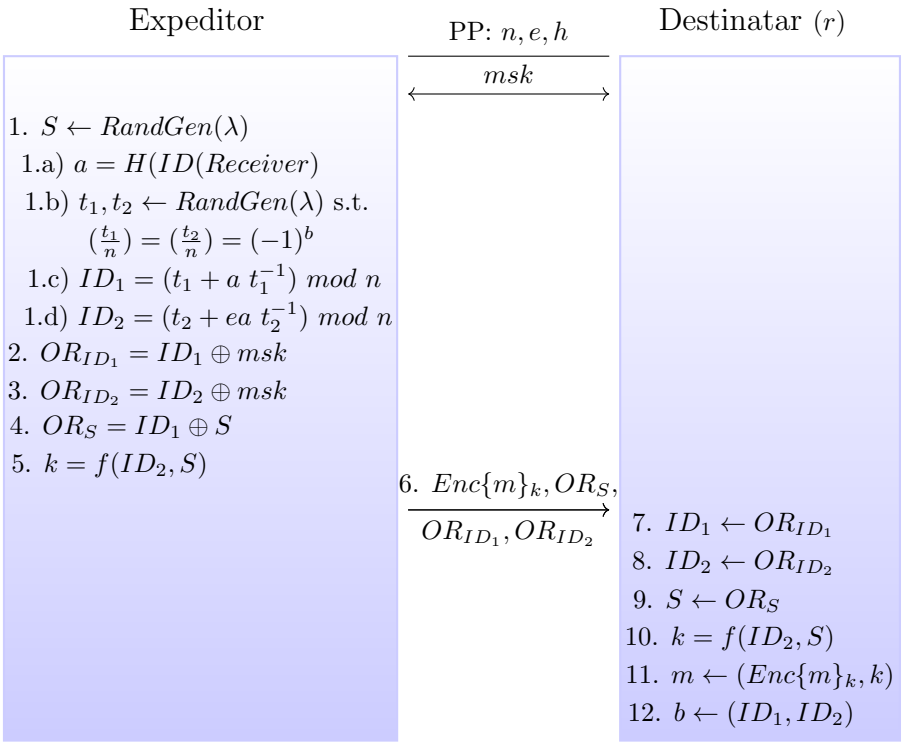
RPM este un protocol ce asigură o transmisie autentificată și sigură de transmitere a mesajelor prin metodele sale de generare și management al cheilor. Există patru configurații ale RPM ce combină anumite funcții pentru a asigura securitatea informațiilor și autentificarea mutuală continuă, după cum putem vedea în [71]: PDAF de bază, PDAF de rețea, CE de bază și CE de rețea. Toate cele patru configurații asigură autentificarea (continuă) și securitatea informațiilor, precum și stabilirea cheii și metoda de schimb de cheie. Am putea observa că, dacă la un moment dat cheia secretă k este descoperită, fără altă informație secretă, duce la decriptarea mesajului din pasul de comunicare curent, dar nici mesajele precedente, nici cele viitoare nu pot fi decriptate.

4.4.3 Autentificare mutuală continuă și securitatea datelor

Metodele cunoscute și folosite la ora actuală pentru pasul inițial sunt departe de a fi eficiente sau flexibile. Acest lucru ne-a determinat să căutăm o metodă ce ar putea asigura securitate, eficiență și flexibilitate. Rezultatul nostru [50] poate fi folosit atât la transmiterea datelor inițiale de autentificare, *ack*-urile inițiale, cât și pentru reînnoirea acestora în orice moment (din timpul sesiunilor sau după fiecare sesiune). Astfel vom obține confidențialitatea comunicării într-un mod autentificat, fără a o întrerupe.

Metoda cu care venim noi are la bază schema IBE a lui Cocks (Secțiunea 4.1). Principala îmbunătățire pe care am adus-o în acest proces de transmitere a informațiilor constă în aceea că rezolvă vulnerabilitățile fără a adăuga pași suplimentari. Pentru aceasta folosim schema lui Cocks, care este foarte rapidă și elegantă. Ea criptează un singur bit o dată, ceea ce, în acest context, este de folos deoarece credențialele (noi) vor fi trimise în mai mult de un pas de sesiune, fără a putea fi identificate de un atacator. Costul său computațional este mai mic decât o exponențiere modulară, așadar reprezintă o alternativă excelentă din punct de vedere al complexității timp, pentru a trimite credențialele de (re)autentificare (în mod continuu) oricând pe parcursul comunicării. Aceasta este ilustrată în Figura 4.3.

Schema va funcționa în astfel: cele două entități care comunică vor utiliza anumiți parametri publici, $(n,\ e,\ h)$, și o cheie master secretă msk (care permite schimbul de cheie), în timp ce *Destinatarul* va folosi o cheie secretă corespunzătoare identității sale a. *Expeditorul* generează un parametru aleator S, apoi calculează identitatea folosind o funcție hash H pe ID, unde ID este un parametru public ce identifică *Destinatarul* în mod unic, cum ar fi numărul lui de telefon sau adresa sa de e-mail. Atunci, *Expeditorul* generează aleator doi întregi din $\mathbf{Z}_n^*$, astfel încât simbolul lor Jacobi să fie egal cu bitul ce se dorește a fi transmis (pus în corespondență cu ± 1). Apoi cei doi parametri ID_1 și ID_2 vor fi calculați exact



Unde PP sunt parametrii publici, $r \in SQRT_n(a)$ și $a = ID(Destinatar)$

Figura 4.3: Configurația PDAF de rețea combinată cu schema lui Cocks [50]

ca în schema lui Cocks, $ID_i = (t_i + e^{(i+1) \bmod 2}\ at_i^{-1})_n$, $i \in \{1, 2\}$. Apoi va calcula cheia secretă k cu ajutorul funcției f aplicată pe ID_2 și S. În final va ascunde S, ID_1 și ID_2 folosind funcția OR și msk prin parametrii OR_S, OR_{ID_1}, respectiv OR_{ID_2} și va trimite aceste tei valori, împreună cu mesajul criptat $Enc\{m\}_k$ *Destinatarului*. Folosind msk, *Destinatarul* recuperează S, ID_1 și ID_2 din OR_S, OR_{ID_1}, respectiv OR_{ID_2}, calculează cheia de criptare k, după care, folosind funcția f peste ID_2 și S, recuperează mesajul inițial din criptotext. În final mai recuperează și bitul suplimentar ce i-a fost transmis.

Așadar putem observa că aceasta este o modalitate excelentă de a rezolva problema schimbului de credențiale *ack*. Acest lucru se poate realiza în fiecare pas de comunicare, rând pe rând, fără a necesita pași sau mesaje suplimentare. Astfel, dacă părțile comunicante stabilesc, extern protocolului în sine, când își vor transmite biții suplimentari, mesajele trimise între cele două entități când se trimite bitul din noile credențiale și când nu se trimite, vor părea identice din perspectiva unui adversar ce interceptează aceste mesaje și, deci, nu va putea afla noua cheie. Credențialele vor putea fi transmise fără a modifica sau întrerupe comunicarea obișnuită. Pașii necesitați de distribuirea noilor credențiale nu afectează în mod considerabil complexitatea timp și pot fi făcuți doar atunci când cele două părți au stabilit schimbarea *ack*-ului

În ceea ce privește securitatea, protocolul rămâne protejat de randomitatea criptotextelor Cocks, așadar, cei doi parametri ce sunt calculați în cadrul schemei Cocks IBE, ID_1 și ID_2 sunt nu se diferențiază față de niște parametri aleși aleator (dacă considerăm că QRA este adevărată).

4.5 Generatori pseudo-aleatori

Generatorii pseudo-aleatori (PRG) reprezintă algoritmi determiniști ce primesc la intrare o *sămânță* și la ieșire generează numere (PRNGs) sau biți (PRBGs) simulând un comportament aleator.

Aceștia au o *perioadă* care constituie distanța dintre începutul unei secvențe generate și apariția din nou a aceleiași secvențe [29, 17, 24]. Scopul PRG-urilor este să nu se poată distinge, cel puțin din punct de vedere computațional, dacă nu chiar statistic, între ceea ce este generat de ele și o secvență cu adevărat aleatoare, în primul rând, iar în al doilea rând, o astfel de secvență să fie cât mai lungă, dar primul obiectiv să rămână îndeplinit.

Cercetătorii au considerat reziduurile pătratice un bun material pentru construcția unor astfel de generatori pseudo-aleatori. Anumite rezultate în această direcție se datorează lui unor personalități cum ar fi Damgard [16], Perron [54], Peralta [53], Tarakanov [68], ca să enumerăm numai câțiva. Un exemplu de PRG bazat pe QR este generatorul Blum-Blum-Shub [5]. Acesta întrunește cerințele menționate anterior, sub presupunerea QRA. Un alt exemplu ar fi [59], în care autorii descriu o modalitate de a crea o familie de secvențe binare; de asemenea ei prezintă și un PRBG ce generează astfel de secvențe folosind QR.

Capitolul 5

De la criptarea bazată pe identitate la criptarea bazată pe atribute

5.1 Introducere

Criptarea bazată pe atribute (ABE)[1] este o generalizare a IBE ce permite comunicarea criptată „de la unul la mai mulți“, și definește identitățile ca fiind mulțimi de atribute ce caracterizează grupul de destinatari [57]. Așadar, pentru a decripta un mesaj, este necesară o combinație validă (acceptată) de atribute, pe care o vom numi *structură de acces*. ABE este implementat actualmente folosind instrumente matematice cum ar fi aplicații biliniare [36, 18], latici [46, 15] sau QR [10].

Structurile de acces, în funcție de complexitatea lor, pot fi exprimate prin formule Booleene pentru circuite Booleene (non-/monotone) sau prin circuite Booleene generale.

Circuitele Booleene cu două fire de intrare, adică fan-in doi, cu porți `AND` și `OR` dar fără porți `NOT` se numesc *monotone*. Ne vom orienta atenția asupra schemelor KP-ABE (ABE cu politică

[1] Prezentăm în acest capitol studiul realizat de noi în lucrarea [73].

de cheie). Primele astfel de scheme apărute funcționează pentru structuri de acces simple, ce pot fi exprimate prin formule Booleene, pentru circuite Booleene monotone [33], sau ne-monotone [52]. Unele structuri de acces sunt mai complexe, cum ar fi cele multi-nivel [69, 70], și nu pot fi exprimate prin formule Booleene ci prin circuite Booleene generale.

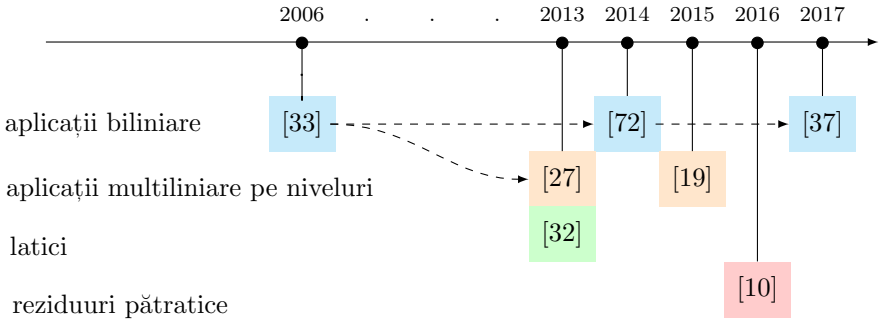


Figura 5.1: Linia timpului pentru KP-ABE

Goyal și colab. au introdus în [33] conceptul de KP-ABE și prima schemă ce permite criptarea „unul-la-mai-mulți“. Aceștia au folosit partajarea secretelor și o reconstrucție a unie informații de jos în sus cu ajutorul unei aplicații biliniare pentru a obține posibilitatea partajării de granulație fină a datelor criptate. Aceasta funcționează pentru structurile de acces simple deoarece poate suporta doar arbori Booleeni și nu circuite Booleene generale. Abia în 2013 a fost propusă o primă soluție pentru circuite Booleene generale prin [27]. Această schemă este o extensie a celei din [33] ce folosește aplicații multiliniare pe niveluri, așadar este mai puțin eficientă decât [33], dar are capacitatea de a exprima structuri de acces mai complexe. În același an a fost propusă și o soluție bazată pe latici [32]. Toate aceste scheme sunt sigure în modelul standard.

A folosi doar aplicații biliniare și totodată a obține o schemă rezistentă la atacul de backtracking este o provocare și o problemă

deschisă la ora actuală pentru modelul KP-ABE. Din 2014 au fost câteva încercări în această direcție.

Țiplea și Drăgan au extins [33] de la cazul arborilor Booleeni la circuite Booleene (monotone) în [72], schemă ce este mult mai eficientă. Aceasta folosește partajarea secretelor și o singură aplicație biliniară, oferind același nivel de securitate ca și schema originală. O mică îmbunătățire a acestei scheme a fost făcută în 2017 de către Hu și Gao în [37] și obține chei de decriptare mai scurte, păstrând nivelul de securitate.

Soluția 2015 [19] este o schemă KP-ABE ce acceptă structuri de acces exprimate prin circuite Booleene generale, cum este și [27], dar este de departe mai eficientă deoarece folosește *aplicați multiliniare înlănțuite* - care reprezintă un tip de aplicații multiliniare simplificat - și tehnici de partajarea secretelor, păstrând același nivel de securitate.

5.2 ABE și atacul backtracking

Vom da acum câteva definiții și vom stabili notația utilizată în acest capitol.

Structurile de acces [67] sunt în general reprezentate prin circuite Booleene [3]. Un circuit are fire de intrare și de ieșire (unele din acestea nu sunt fire de intrare, în timp ce altele nu sunt nu sunt fire de ieșire); de asemenea, anumite porți care pot fi porți `AND` (ȘI), `OR` (SAU) și `NOT` (NEGAȚIE). Vizual, firele de intrare se găsesc sub porți și le vom număra prin *fan-in*, în vreme ce firele de ieșire sunt poziționate deasupra porților și le vom contoriza prin *fan-out*. Vor fi două fire de intrare pentru fiecare poartă `AND` sau `OR`, în vreme ce porțile `NOT` vor avea un singur fie de intrare. Fiecare dintre acestea vor avea ca ieșire cel puțin un fir. Prin *circuite* vom înțelege *circuite Booleene*, dacă nu este specificat altfel. *Formulele Booleene* sunt acele circuite în care toate porțile au fan-out unu. Amintim că un circuit *monoton* nu are porți `NOT`. În acest capitol vom avea de-a face doar cu circuite monotone monotone ce

au exact un fir de ieșire, dar asta nu pierde din generalitate, după cum se explică în [27].

Fie $\mathcal{U}$ o mulțime de atribute, A o submulțime a lui $\mathcal{U}$, iar $\mathcal{C}$ un circuit. Dacă elementele din A pot fi mapate (puse în corespondență) astfel încât să corespundă unu-la-unu cu firele de intrare ale circuitului, atunci $\mathcal{C}$ este considerat un circuit Boolean peste mulțimea $\mathcal{U}$. Circuitul $\mathcal{C}$ va fi evaluat la 1 sau la 0, pentru o submulțime de atribute A, punând valoarea 1, respectiv 0, la toate firele de intrare corespunzătoare din A. Intrarea uni circuit este formată din valori 1 și 0; fiecare din aceste valori fiind transmisă de la nivelul cel mai de jos către vârf, prin porți, în mod standard. Rezultatul evaluării circuitului $\mathcal{C}$ pentru A va fi notat cu $\mathcal{C}(A)$. Structurile de acces definite de $\mathcal{C}$ reprezintă acele mulțimi A cu $\mathcal{C}(A) = 1$.

Fie $\mathcal{U}$ o mulțime de atribute, atunci tuplul $(\overline{a}, \overline{\mathcal{U}}, \mathcal{S})$ se va numi *structură de acces disjunctivă multinivel* [66] peste $\mathcal{U}$, unde $\overline{a} = (a_1, \ldots, a_k)$ și $a_i \in \mathbf{N}$, astfel încât $0 < a_1 < \cdots < a_k$, $\overline{\mathcal{U}}$ partiționează $\mathcal{U}$ prin $= (\mathcal{U}_1, \ldots, \mathcal{U}_k)$ și $\mathcal{S} = \{A \subseteq \mathcal{U} | (\exists i \in \{1, \ldots, k\})(|A \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq a_i)\}$. Dacă alegem $\mathcal{S}$ astfel încât expresia de mai sus să fie validă oricare ar fi $i \in \{1, \ldots, k\}$ asta va defini cazul *conjunctiv* al structurilor de acces multinivel [69].

O schemă KP-ABE are patru algoritmi PPT [33]: algoritmul *Setup*, care generează cheia master (secretă) msk pornind de la parametrul de securitate λ și de la parametrii publici PP. Algoritmul de criptare $Enc(m, A, PP)$, care utilizează la intrare mesajul m, o submulțime de atribute $A \subseteq \mathcal{U}$ și parametrii publici PP pentru a crea criptotextul E. Cheia secretă sk este obținută cu ajutorul algoritmului $KeyGen(\mathcal{C}, msk)$ folosind un circuit Boolean $\mathcal{C}$ și msk. În final, mesajul m este decriptat prin algoritmul $Dec(E, sk)$ dacă se utilizează o cheie validă sk și un criptotext c.

Proprietatea de corectitudine: pentru o pereche formată din parametrii publici și cheia master secretă, obținute cu algoritmul *Setup*, un circuit oarecare $\mathcal{C}$ pentru o mulțime stabilită de atribute, $\mathcal{U}$, și o submulțime A a lui $\mathcal{U}$, fie m un mesaj din spațiul de mesaje și E, criptarea lui m folosind parametrii publici PP și

submulțimea A. Dacă circuitul este evaluat la 1 pentru A, adică $\mathcal{C}(A) = 1$ atunci decriptarea lui E, $Dec(E, sk)$, va returna m, pentru toate cheile secrete sk generate de $KeyGen(\mathcal{C}, msk)$. Această proprietate trebuie îndeplinită de toate schemele KP-ABE.

Prima schemă KP-ABE creată [33] nu poate funcționa pentru circuite ci doar pentru formule Booleene datorită faptului că valoarea unui fir ce intră într-o poartă `OR` se poate ajunge la celelalte fire de intrare, datorită procedurii de partajare a secretelor, în această situație, dacă aceeași valoare de intrare este folosită de o altă poartă, așa cum este în cazul circuitelor, atunci această „scăpare“ de informații nu poate fi evitată. Acesta se numește *atacul de backtracking*, care este posibil numai în contextul unui circuit. Când vorbim de formule Booleene, situația se schimbă iar un astfel de atac nu este posibil deoarece un fir de intrare într-o poartă `OR` nu este niciodată folosit de o altă poartă (a se vedea [72] pentru o a se observa grafic acest atac).

5.2.1 Schema sigură KP-ABE_Scheme_1

Schema este descrisă în teză și în articolul [18]. Corectitudinea sa rezultă în urma uni calcul simplu, iar teorema de mai jos stabilește nivelul de securitate pe care îl asigură aceasta.

Teorema 5.2.1 ([18])**.** *Schema KP-ABE_Scheme_1 este sigură în modelul selectiv, sub presupunerea Diffie-Hellman biliniară decizională.*

Schema KP-ABE_Scheme_1 nu este este eficientă când există multe porți `FO` conectate dar această schemă poate fi mai eficientă decât schema din [27] când porțile `FO` sunt în partea de jos a circuitului și când doar o parte din ele au o cale într ele. Ca un exemplu o vom aplica pe structurile de acces multinivel din [66, 69].

E ușor a se vedea că formulele Booleene nu sunt suficient de complexe pentru a exprima structurile de acces multinivel conjunctive și disjunctive (a se vedea [18] pentru demonstrație), așadar

Algorithm 4 : KP-ABE_Scheme_1

procedure SETUP(λ, n)
se alege un număr prim p; stabilim G_1 și G_2;
▷ două grupuri multiplicative de ordin prim p
set g; ▷ un generator al lui G_1
set $e : G_1 \times G_1 \to G_2$; ▷ o aplicație biliniară
$\mathcal{U} \leftarrow \{1, \ldots, n\}$; ▷ mulțimea de atribute
$y \in \mathbf{Z}_p$ și $t_i \in \mathbf{Z}_p, \forall i \in \mathcal{U}$;
$PP \leftarrow (p, G_1, G_2, g, e, n, Y = e(g, g)^y, (T_i = g^{t_i} | i \in \mathcal{U}))$;
$msk \leftarrow (y, t_1, \ldots, t_n)$;
return (PP, msk)
end procedure
procedure ENCRYPT(m, A, PP)
$m \in G_2$ și $s \leftarrow \mathbf{Z}_p$;
$A \subseteq \mathcal{U}$; ▷ o mulțime nevidă de atribute
$E \leftarrow (A, E' = mY^s, (E_i = T_i^s = g^{t_i s} | i \in A), g^s)$;
return E
end procedure
procedure KEYGEN($\mathcal{C}, msk$)
$(S, P) \leftarrow$ SHARE($y, \mathcal{C}$);
foreach $i \in \mathcal{U}$ **do**
$D(i) = (g^{S(i,j)/t_i} | 1 \leq j \leq |S(i)|)$;
$D \leftarrow ((D(i) | i \in \mathcal{U}), P)$
end foreach
return D
end procedure
procedure DECRYPT(E,D)
$R \leftarrow$ RECON($\mathcal{C}, P, V_A, g^s$);
foreach $i \in \mathcal{U}$ și $1 \leq j \leq |S(i)|$ **do**
if $i \in A$ **then**
$V_A(i, j) \leftarrow e(E_i, D(i, j)) = e(g^{t_i s}, g^{S(i,j)/t_i}) = e(g, g)^{S(i,j)s}$;
else $V_A(i, j) \leftarrow \perp$; $m \leftarrow E'/R(o, 1)$;
end if
end foreach
return m
end procedure

pentru astfel de structuri se vor folosi circuitele Booleene. Acum, pentru o reprezentare ușoară și clară a structurilor, circuitele e care le vom folosi vor fi îmbunătățite cu *porți cu prag*-(a, b) [33], unde $b \geq 2$ și $1 \leq a \leq b$. Aceste porți vor avea un număr de b fire de intrare și un singur fir de ieșire. Dacă evaluăm ieșirea unei astfel de porți, aceasta va fi 1, adică adevărat, când este îndeplinit pragul, adică un număr de a fire de intrare să aibă valoarea 1. Așadar putem spune că pragul este 1 în cazul porților `OR`, (și vom nota aceasta prin porți cu prag-$(1, 2)$) și va fi 2 pentru porțile `AND` (numite porți cu prag-$(2, 2)$).

Folosind o partajare a secretelor liniară și probabilistă KP-ABE_Scheme_1 poate fi natural extinsă astfel încât varianta nouă să conțină, în plus, și porți cu prag. Putem remarca faptul că schema KP-ABE_Scheme_1 este mai rapidă decât cea a lui Garg și colab. [27] (a se vedea [72] pentru mai multe detalii).

5.3 KP-ABE pentru circuite Booleene folosind partajarea secretelor și aplicații multiliniare

Garg și colab. au fost primii care au creat o schemă KP-ABE ce poate fi folosită pentru formule Booleene generale. În [27] ei au au renunțat să folosească partajarea secretelor și în locul acesteia au implementat o tehnică ce trece de jos în sus prin circuit, utilizând aplicații multiliniare pe niveluri, schimbând generatorul la fiecare nivel. În afară de firul de ieșire al circuitului, toate celelalte fire vor avea între două și patru chei.

În cele ce urmează vom prezenta rezultatul lui Drăgan și Țiplea din [19], care nu a renunțat la utilizarea partajării secretelor, dar au protejat schema de atacul de backtracking utilizând aplicații multiliniare pe niveluri. Această variantă obține o soluție mai bună decât schema [27]. Pentru o descriere completă alte detalii a se consulta [19].

5.3.1 Schema sigură KP-ABE_Scheme_2

În [19] Drăgan și Țiplea utilizează o formă simplificată de aplicații multilineare pe niveluri, numite aplicații multilineare înlănțuite. Fie p un număr prim, $G_1, \ldots, G_{k+1}$ grupuri multiplicative de ordin p, atunci vom numi *aplicații multiliniare înlănțuite* secvența de aplicații biliniare $(e_i : G_i \times G_1 \to G_{i+1} | 1 \leq i \leq k)$ astfel încât, dacă $g_1 \in G_1$ este un generator al lui G_1, atunci, oricare ar fi $i \in \{1, \ldots, k\}$, un generator g_{i+1} pentru fiecare grup G_{i+1} poate fi definit recursiv prin $g_{i+1} = e_i(g_i, g_1)$ (datorită faptului că e_i este o aplicație biliniară). Astfel, $(e_i | 1 \leq i \leq k)$ este de asemenea o formă de aplicații multiliniare pe nivelului, dar una mai simplă. Acum vom vedea cum sunt folosite aceste construcții în [19].

Fie $\mathcal{C}$ un circuit Boolean, vom nota cu r numărul total de niveluri FO iar cu $(e_i | 1 \leq i \leq r+1)$ o aplicație multiliniară înlănțuită, așa cum au fost descrise mai sus. În etapa de setup se alege un întreg aleator $y \in_R \mathbf{Z}$. Algoritmul de criptare pornește de la un mesaj $m \in G_{r+2}$, alege un întreg aleator $s \in_R \mathbf{Z}$ și obține criptotextul: mg_{r+2}^{ys}. Algoritmul de decriptare va folosi două proceduri, una pentru a partaja un secret iar alta pentru refacerea acestuia ulterioară, adică pentru a ajunge din nou la g_{r+2}^{ys}, cantitate ce va fi utilizată pentru a ajunge la mesajul inițial.

Schema [19] este descrisă în Algoritmul 5. Corectitudinea schemei KP-ABE_Scheme_2 reiese dintr-un calcul simplu. În ceea ce privește securitatea schemei, avem următorul rezultat important.

Teorema 5.3.1 ([19])**.** *Schema KP-ABE_Scheme_2 este sigură în modelul selectiv sub presupunerea Diffie-Hellman multilineară decisională.*

Translarea la sisteme de codare multinivel (graded encoding systems [26]), presupunând că aplicațiile multiliniare pe niveluri chiar există, poate fi aplicată, în aceeași manieră în care s-a arătat în [27], și schemei KP-ABE_Scheme_2.

Schema poate fi îmbunătățită pentru a accepta circuite ce au porți cu trei sau mai multe fire de intrare, păstrând totodată dimensiunea cheii de decriptare. În ceea ce privește limitarea nive-

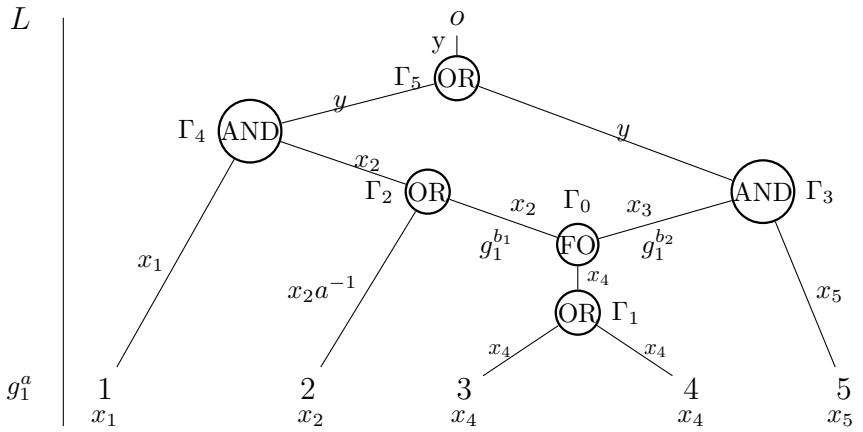
Algorithm 5 : KP-ABE_Scheme_2

procedure SETUP(λ, n, r)
se alege un număr prim p;
set $G_1, \ldots, G_{r+2}$; ▷ grupuri multiplicative de ordin prim p
set $g_1 \in G_1$; ▷ un generator
set $(e_i : G_i \times G_1 \to G_{i+1} | 1 \leq i \leq r+1)$; ▷ o aplicație biliniară
$g_{i+1} = e_i(g_i, g_1)$, oricare ar fi $1 \leq i \leq r+1$;
$\mathcal{U} = \{1, \ldots, n\}$; ▷ mulțimea de atribute
foreach $i \in \mathcal{U}$ **do**
$y \leftarrow \mathbf{Z}_p$ și $t_i \leftarrow \mathbf{Z}_p$;
end foreach
$PP \leftarrow (n, r, p, G_1, \ldots, G_{r+2}, g_1, e_1, \ldots, e_{r+1}, Y = g_{r+2}^y, (T_i = g_1^{t_i} | i \in \mathcal{U}))$;
$msk \leftarrow (y, t_1, \ldots, t_n)$;
return (PP, msk).
end procedure

procedure ENCRYPT(m, A, PP)
$m \in G_{r+2}, s \leftarrow \mathbf{Z}_p$ și $A \subseteq \mathcal{U}$; ▷ unde A este nevidă
foreach $i \in A$ **do**
$E \leftarrow (A, E' = mY^s, (E_i = T_i^s = g_1^{t_i s}))$;
end foreach
return E.
end procedure

procedure KEYGEN($\mathcal{C}, msk$)
$(S, P, L) \leftarrow$ SHARE$(y, \mathcal{C})$;
foreach $i \in \mathcal{U}$ **do**
$D(i) = g_1^{S(i)/t_i}$ și $D \leftarrow ((D(i) | i \in \mathcal{U}), P, L)$
end foreach
return D.
end procedure

procedure DECRYPT(E,D)
$R \leftarrow$ RECON$(\mathcal{C}, P, L, A, V_A)$;
foreach $i \in \mathcal{U}$ **do**
if $i \in A$ **then** $V_A(i) \leftarrow e_1(E_i, D(i)) = e_1(g_1^{t_i s}, g_1^{S(i)/t_i}) = g_2^{S(i)s}$;
else $V_A(i) \leftarrow \perp$ și $m \leftarrow E'/R(o)$;
end if
end foreach
return m or $\perp$.
end procedure



$x_1a + x_2 \equiv y \bmod p,\ x_3 + x_5a \equiv y \bmod p,\ x_4b_1 \equiv x_2 \bmod p,\ x_4b_2 \equiv x_3 \bmod p$

Figura 5.2: SHARE$(y, \mathcal{C})$

lurilor FO, schema este flexibilă, putând fi extinsă la o versiune ne limitată, cu costul de a crește numărul de chei al nivelurilor FO. Cantitatea de elemente ce țin de cheile de decriptare poate de asemenea fi micșorată prin reutilizarea cheii de la fiecare nivel FO la unul din firele de ieșire al fiecărei (câtorva) porți aflate la același nivel.

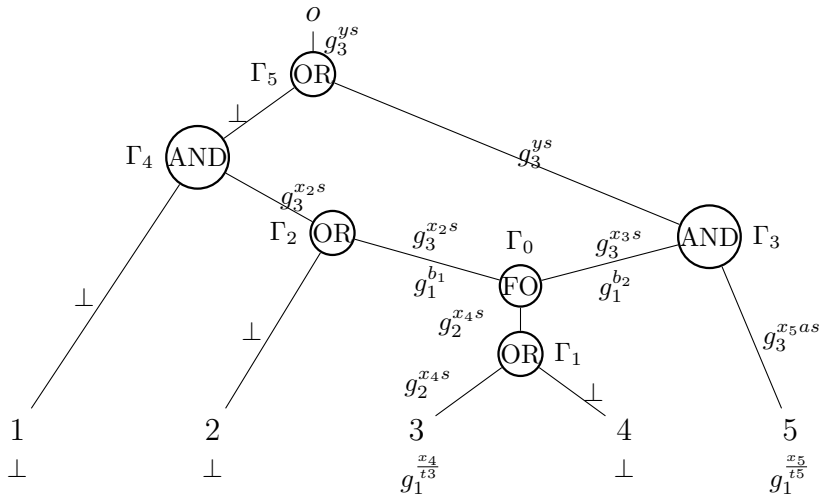


Figura 5.3: Recon$(\mathcal{C}, P, L, A, V_A)$ unde $A = \{3, 5\}$

Capitolul 6

Concluzii și probleme deschise

După un studiu de aproape șase ani asupra QR, putem spune că acestea reprezintă un instrument foarte puternic în multe arii, cum ar fi matematica, informatica și altele. Datorită simplității și eleganței lor, QR sunt bine înțelese de comunitatea criptografică și sunt preferabile altor instrumente matematice.

Partea matematică ce ține de QR a fost studiată în Capitolul 3, unde am calculat anumite cardinalități ale mulțimilor de forma $a + QR_m$, ce au diverse șabloane Jacobi, unde m este fie un număr prim, fie un modul RSA, apoi am arătat cum se calculează anumite probabilități ce vor fi aplicate ulterior în Capitolul 4. Rezultatele obținute în Capitolul anterior reprezintă fundamentul aplicațiilor prezentate în Capitolul 4, în care analizăm în profunzime schema lui Cocks [12] și criptotextele ei, studiu ce a ajutat la demonstrarea riguroasă a testului Galbraith și la descrierea unei variante anonime a acestei scheme [40] într-o manieră mult simplificată, prezentată în lucrarea noastră [51]. Urmează o contribuție la mărginirea superioară a demonstrației de securitate a schemei BGH în Secțiunea 4.2. În lucrul cu QR este nevoie de multă atenție, și am tras un semnal de atenție asupra metodelor ce au încercat să „optimizeze“ schemele [8] și [40] dar care au pierdut

securitatea, ne putând fi folosite. Capitolul se finalizează cu o aplicație a schemei Cocks în autentificarea mutuală continuă folosind RPM, Secțiunea 4.4.3, și cu câteva exemple de PRBG-uri bazate pe QR, Secțiunea 4.5.

În ultima parte a tezei am analizat criptarea bazată pe atribute (ABE) și atacul de backtracking, [27]. În prezentarea cronologică din Figura 5.1 se pot vedea cu ușurință principalele instrumente utilizate în crearea schemelor ABE și stadiul cercetării în ceea ce privește KP-ABE. Mai departe am prezentat două scheme KP-ABE [18, 19] rezistente la atacul de backtracking și care sunt probabil cele mai eficiente la momentul actual, acestea sunt însoțite și de demonstrațiile lor de securitate. Stadiul cercetării în ABE, (Secțiunea 5.1) arată că rezultatele curente se bazează în principal pe aplicații biliniare, apoi pe latici și există abia un început în ABE bazat pe QR. Ca o direcție viitoare suntem interesați în a analiza cât de potrivite sunt QR în crearea de scheme ABE.

Open problems and further work

Chiar dacă a durat șase ani finalizarea tezei, acesta este abia începutul unui următor nivel mai profund de cercetare. Sunt interesată atât de dezvoltarea ideilor la care lucrăm în grupul nostru de cercetare cât și în găsirea de noi problematici în care QR, sau poate reziduuri de ordin înalt pot fi de folos.

Dacă ar fi să enumerăm câteva dintre problemele deschise, una dintre ele ar fi să descoperim reguli ale șabloanelor Jacobi aplicate peste alte șabloane Jacobi în submulțimi ale lui $\mathbf{Z}_n^*$, cum ar fi mulțimile de forma $QR_n(a + \cdots QR_n(a + QR_n) \cdots)$, dezvoltând astfel studiul nostru. Acest rezultat ar putea valida (sau nu) pseudo-randomitatea (caracterul aleator al) reziduurilor.

Un subiect de asemenea interesant de cercetat ar fi extinderea schemei lui Cocks astfel încât să putem cripta mai mulți biți odată. Câteva probleme de rezolvat ar fi și cele legate de schema BGH [8], cum ar fi găsirea unei metode eficiente și sigure de combinare a soluțiilor pentru Ecuația 4.2. O altă ramură ce așteaptă a fi

exploatată ar fi găsirea altor utilizări ale rezultatelor noastre legate de distribuția QR, sau extinderea lor în aplicații tipul VoIP, în cloud, big data (ABE) [10] și așa mai departe.

Ne mai gândim de asemenea dacă ar fi posibilă utilizarea QR combinate cu aplicațiile biliniare sau laticile, pentru a oferi rezistență și la calculul cuantic[56, 9, 44].

Bibliografie

[1] Giuseppe Ateniese and Paolo Gasti. Universally anonymous IBE based on the quadratic residuosity assumption. In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology*, CT-RSA '09, pages 32–47, Berlin, Heidelberg, 2009. Springer-Verlag.

[2] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '01, pages 566–582, London, UK, 2001. Springer-Verlag.

[3] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 784–796, New York, NY, USA, 2012. ACM.

[4] Sergey Bezzateev and Daeyoub Kim. Threshold encryption scheme based on Cocks' IBE scheme. In *The KIPS Transactions: Part C*, volume 19C, pages 225–230, Aug 2012.

[5] Lenore Blum, Manuel Blum, and Mike Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on Computing*, 15(2):364–383, 1986.

[6] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 506–522. Springer, 2004.

[7] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *The 21st Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, California, USA, August 19–23, 2001. Proceedings*, CRYPTO '01, pages 213–229. Springer Berlin Heidelberg, Berlin, Heidelberg, Aug 2001.

[8] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryption without pairings. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), October 20-23, 2007, Providence, RI, USA, Proceedings*, pages 647–657, 2007.

[9] J. Buchmann, K. Lauter, and M. Mosca. Postquantum cryptography – state of the art. *IEEE Security Privacy*, 15(4):12–13, 2017.

[10] Balaji Chandrasekaran and Ramadoss Balakrishnan. Attribute based encryption using quadratic residue for the big data in cloud environment. In *Proceedings of the International Conference on Informatics and Analytics*, ICIA-16, pages 19:1–19:4, New York, NY, USA, 2016. ACM.

[11] Michael Clear, Hitesh Tewari, and Ciaran McGoldrick. Anonymous IBE from quadratic residuosity with improved performance. In *Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, pages 377–397, 2014.

[12] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363, London, UK, Dec 2001. Springer-Verlag.

[13] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Heidelberg, 1993.

[14] Giovanni Di Crescenzo and Vishal Saraswat. Public key encryption with searchable keywords based on Jacobi symbols. In *Progress in Cryptology - INDOCRYPT 2007, 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007, Proceedings*, pages 282–296, 2007.

[15] Wei Dai, Yarkın Doröz, Yuriy Polyakov, Kurt Rohloff, Hadi Sajjadpour, Erkay Savaş, and Berk Sunar. Implementation and evaluation of a lattice-based key-policy ABE scheme. *IEEE Transactions on Information Forensics and Security*, 13(5):1169–1184, 2018.

[16] Ivan Bjerre Damgård. On the randomness of Legendre and Jacobi sequences. In Shafi Goldwasser, editor, *Advances in Cryptology — CRYPTO' 88*, pages 163–172, New York, NY, 1990. Springer New York.

[17] Hans Delfs and Helmut Knebl. Public-key cryptography. In *Introduction to Cryptography*, volume 10.1007/3-540-49244-5 of *Information Security and Cryptography*, pages 33–80. 2015.

[18] Constantin Cătălin Drăgan and Ferucio Laurenţiu Ţiplea. Efficient key-policy attribute-based encryption for general Boolean circuits from multilinear maps. Preprint on IACR Cryptology ePrint Archive. Report 2014/462, 2014.

[19] Constantin Cătălin Drăgan and Ferucio Laurentiu Ţiplea. Key-policy attribute-based encryption for general boolean circuits from secret sharing and multi-linear maps. In Enes Pasalic and Lars R. Knudsen, editors, *Cryptography and Information Security in the Balkans: Second International Conference, BalkanCryptSec 2015, Koper, Slovenia, September 3-4, 2015, Revised Selected Papers*, pages 112–133. Springer International Publishing, 2016.

[20] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. Efficient identity-based encryption over NTRU lattices. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014*, pages 22–41, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[21] Ibrahim Elashry, Yi Mu, and Willy Susilo. Jhanwar-Barua's identity-based encryption revisited. In ManHo Au, Barbara Carminati, and C.-C.Jay Kuo, editors, *Network and System Security*, volume 8792 of *Lecture Notes in Computer Science*, pages 271–284. Springer International Publishing, 2014.

[22] Ibrahim Elashry, Yi Mu, and Willy Susilo. A resilient identity-based authenticated key exchange protocol. *Security and Communication Networks*, 8(13):2279–2290, 2015.

[23] Ibrahim F. Elashry, Yi Mu, and Willy Susilo. An efficient variant of Boneh-Gentry-Hamburg's identity-based encryption without pairing. In *Information Security Applications - 15th International Workshop, WISA 2014, Jeju Island, Korea, August 25-27, 2014. Revised Selected Papers*, pages 257–268, 2014.

[24] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. Introduction to cryptography. In *Cryptography Engineering (Design Principles and Practical Applications)*, volume 10.1002/9781118722367, pages 23–39, 2015.

[25] S. Galbraith. Personal communication.

[26] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 1–17, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[27] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, volume 8043 of *Lecture Notes in Computer Science*, pages 479–499. Springer Berlin Heidelberg, 2013.

[28] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM Symposium on Theory of Computing (STOC)*, pages 197–206, 2008.

[29] Oded Goldreich. *Studies in Complexity and Cryptography*, volume 6650 of *Lecture Notes in Computer Science*. Springer-Verlag Berlin Heidelberg, 1st edition, 2011. In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman.

[30] Shafi Goldwasser. Lecture 3: Cock's IBE scheme. Course 6.876: Advanced Cryptography, Sep 2004.

[31] Shafi Goldwasser and Silvio Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing, May 5-7, 1982, San Francisco, California, USA*, pages 365–377, 1982.

[32] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *STOC*, pages 545–554. ACM, 2013.

[33] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 89–98, New York, NY, USA, 2006. ACM.

[34] Jabeom Gu, Sehyun Park, Ohyoung Song, Jaeil Lee, Jaehoon Nah, and Sungwon Sohn. Mobile PKI: A PKI-based authentication framework for the next generation mobile communications. In Rei Safavi-Naini and Jennifer Seberry, editors, *Information Security and Privacy*, pages 180–191, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[35] Ryotaro Hayashi and Keisuke Tanaka. Universally anonymizable public-key encryption. In *Proceedings of the 11th international conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT '05, pages 293–312, Berlin, Heidelberg, Dec 2005. Springer-Verlag.

[36] Susan Hohenberger and Brent Waters. Attribute-based encryption with fast decryption. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography – PKC 2013*, pages 162–179, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[37] Peng Hu and Haiying Gao. A key-policy attribute-based encryption scheme for general circuit from bilinear maps. *International Journal of Network Security*, 19(5):704–710, 2017.

[38] Mahabir Prasad Jhanwar. *Studies on Public Key and Identity-based Cryptographic Primitives*. PhD thesis, Kolkata, 2010. Thesis under the supervision of Prof. Rana Barua.

[39] Mahabir Prasad Jhanwar and Rana Barua. A variant of Boneh-Gentry-Hamburg's pairing-free identity based encryption scheme. In *Information Security and Cryptology, 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers*, pages 314–331, Berlin, Heidelberg, 2008. Springer.

[40] Marc Joye. Identity-based cryptosystems and quadratic residuosity. In *Proceedings, Part I, of the 19th IACR International Conference on Public-Key Cryptography — PKC 2016 - Volume 9614*, pages 225–254, Berlin, Heidelberg, 2016. Springer-Verlag.

[41] Benjamin Justus. The distribution of quadratic residues and non-residues in arithmetic progressions. *Lithuanian Mathematical Journal*, 54(2):142–149, Apr 2014.

[42] Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser-Micali type of cryptosystem. *Journal of Mathematical Cryptology*, 8(2):115–140, Jan 2014.

[43] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Cryptography and Network Security. CRC Press, Boca Raton, London, New York, second edition, 2015.

[44] Tanja Lange and Rainer Steinwandt. *Post-Quantum Cryptography*, volume 10786 of *Lecture Notes in Computer Science*. Springer International Publishing, 1st edition, 2018.

[45] Rio LaVigne. Simple homomorphisms of Cocks IBE and applications. Preprint on IACR Cryptology ePrint Archive. Report 2016/1150, 2016.

[46] Yuan Liu, Licheng Wang, Lixiang Li, and Xixi Yan. Secure and efficient multi-authority attribute-based encryption scheme from lattices. *IEEE Access*, 2018.

[47] Paul McGough. Real privacy management authentication system, Jul 31, 2008. US Patent 2008/0184031 A1, Centreville, VA, (US).

[48] Paul McGough. Real privacy management authentication system, Mar 1, 2011. US Patent 2011/7899185 B2, Centreville, VA, (US).

[49] Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Springer, New York, 2000.

[50] Anca-Maria Nica. Continuous mutual authentication and data security. *International Journal of Computer Science and Information Security (IJCSIS)*, 17(2), Feb 2019.

[51] Anca-Maria Nica and Ferucio Laurenţiu Ţiplea. On anonymization of Cocks' identity-based encryption scheme. In *Proceedings of the 5th Conference on Mathematical Foundations of Informatics*, MFOI 2019, pages 75 – 85, Iaşi, România, 2019. Editura Universităţii „Alexandru Ioan Cuza" from Iaşi.

[52] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In *ACM Conference on Computer and Communications Security*, pages 195–203. ACM, 2007.

[53] René Peralta. On the distribution of quadratic residues and non-residues modulo a prime number. *Mathematics of Computation*, 58:433–440, Jan 1992.

[54] Oskar Perron. Bemerkungen über die Verteilung der quadratischen Reste. *Mathematische Zeitschrift*, 56:122–130, 1952.

[55] Michael O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, Massachusetts Institute of Technology, Cambridge, MA, USA, Jan 1979.

[56] Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, editors. *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Lecture Notes in Computer Science 9100. Springer-Verlag Berlin Heidelberg, 1 edition, 2016.

[57] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT '05, pages 457–473, Berlin, Heidelberg, 2005. Springer-Verlag.

[58] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. *2000 Symposium on Cryptography and Information Security - C20*, pages 26–28, Jan 2000.

[59] András Sárközy and C.L. Stewart. On pseudorandomness in families of sequences derived from the Legendre symbol. *Periodica Mathematica Hungarica*, 54(2):163–173, Jun 2007.

[60] Adrian G. Schipor. On the security of Jhanwar-Barua identity-based encryption scheme, 2018.

[61] Gheorghe A. Schipor. On the anonymization of Cocks IBE scheme. In *Cryptography and Information Security in the Balkans - First International Conference, Istanbul, Turkey, October 16-17, 2014, Revised Selected Papers*, BalkanCryptSec 2014, pages 194–202, 2014.

[62] George Teşeleanu, Ferucio Laurenţiu Ţiplea, Sorin Iftene, and Anca-Maria Nica. Boneh-Gentry-Hamburg's identity-based encryption schemes revisited. In *Proceedings of the Conference on Mathematical Foundations of Informatics MFOI2019, July 3-6, 2019, Iasi, Romania*, pages 45 – 58, 2019. An extended version will appear in *The Computer Journal*.

[63] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[64] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, New York, NY, USA, 2005.

[65] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, New York, NY, USA, 2nd edition, 2009.

[66] Gustavus J. Simmons. How to (really) share a secret. In Shafi Goldwasser, editor, *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology (CRYPT '88)*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer, 1988.

[67] D.R. Stinson. *Cryptography: Theory and Practice*. Chapman and Hall/CRC, 3rd edition, 2005.

[68] V. E. Tarakanov. An application of the Gauss lemma to the study of pseudorandom sequences based on quadratic residues. *Mathematical Notes*, 73(3-4):562–570, Mar 2003.

[69] Tamir Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264, 2007.

[70] Tamir Tassa and N. Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology*, 22(2):227–258, 2008.

[71] Telcordia. Cryptography assesment of RS corps Real Privacy Management (RPM) System. Extended summary. Apr 2011.

[72] Ferucio Laurenţiu Ţiplea and Constantin Cătălin Drăgan. Key-policy attribute-based encryption for boolean circuits from bilinear maps. Preprint on IACR Cryptology ePrint Archive. Report 2014/608, 2014.

[73] Ferucio Laurenţiu Ţiplea, Constantin Cătălin Drăgan, and Anca-Maria Nica. Key-policy attribute-based encryption from bilinear maps. In *Innovative Security Solutions for Information Technology and Communications - 10th International Conference, SecITC 2017, Bucharest, Romania, June 8-9, 2017, Revised Selected Papers*, pages 28–42, 2017.

[74] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica. Security of identity-based encryption schemes from quadratic residues. In *Innovative Security Solutions for Information Technology and Communications - 9th International Conference, SECITC 2016, Bucharest, Romania, June 9-10, 2016, Revised Selected Papers*, pages 63–77, 2016.