ACADEMIA ROMÂNĂ

Şcoala de Studii Avansate a Academiei Române

Institutul de Matematică "Simion Stoilow" al Academiei Române

REZUMATUL TEZEI DE DOCTORAT

Studii asupra proprietăților de securitate și confidențialitate ale schemelor RFID în modelul Vaudenay

CONDUCĂTOR DE DOCTORAT:

Prof. Dr. Ferucio Laurenţiu Ţiplea

DOCTORAND:

Nicolae Cristian Hristea

2024

Contents

Prefață

Scopul tezei

Această teză este axată pe studiul securității și confidențialității în domeniul RFID dintr-o perspectivă criptografică. Principalul element de studiu în acest domeniu de cercetare este protocolul de comunicare dintre cititor și tag. Pentru realizarea unui astfel de studiu, este nevoie de un *model* care să ofere definiții riguroase pentru securitate și confidențialitate și pentru capabilitățile adversarului. Modelul ajută cercetătorii să proiecteze protocoale și să producă demonstrații formale de securitate care pot fi verificate cu ușurință și sunt de preferat analizei de tip ad-hoc. Probabil cel mai complet și matur model pentru RFID este modelul lui Vaudenay [30, 37]. În acest model, adversarul poate să creeze tag-uri (atât legitime, cât și nelegitime), să intercepteze și să falsifice mesaje și, în funcție de capabilitățile sale, să corupă tag-uri și să afle rezultatul unei sesiuni de autentificare. Modelul lui Vaudenay clasifică adversarii în opt categorii care, la rândul lor, dau naștere la opt clase de confidențialitate corespunzătoare. Clasa *confidențialitate distructivă* cuprinde protocoale care asigură confidențialitatea împotriva adversarilor care pot afla dacă o sesiune de autentificare este reușită și care pot corupe tag-urile pentru a obține starea lor internă. Singura restricție pentru acest tip de adversar este că un tag este considerat distrus după ce a fost corupt.

Principalul scop al acestei teze este realizarea unui studiu asupra confidențialității distructive în modelul lui Vaudenay. Vom explora modalitățile prin care se poate obține confidențialitatea

distructivă și vom evidenția caracteristicile modelului care pot afecta considerabil nivelul de confidențialitate pe care îl poate atinge un protocol. O astfel de caracteristică este distincția dintre corupere și corupere cu obținerea stării temporare (în a doua situație adversarul obține nu doar starea persistentă, ci și starea temporară rezultată din calculul intern al tag-ului). În acest sens, vom descrie atacuri împotriva protocoalelor și soluțiilor existente pentru obținerea confidențialității distructive în contextul în care adversarul poate obține starea temporară. Pentru fiecare schemă RFID pe care o propunem în această teză vom prezenta demonstrații detaliate de securitate și confidențialitate. Sperăm că aceste demonstrații vor contribui la evoluția domeniului și la o mai bună înțelegere a modelului și a complexității proiectării protocoalelor RFID.

Contribuții

Principalele contribuții ale acestei tezei sunt următoarele:

1. Propunem primul protocol de autentificare mutuală cu demonstrații complete care atinge nivelul de confidențialitate distructivă în modelul lui Vaudenay [17] (preprint [18]) - Capitolul 3.

2. Definim variabilele temporare și rolul pe care acestea îl joacă în obținerea confidențialității în condițiile obținerii stării temporare [17, 35] - Capitolul 4.

3. Propunem o metodă generală de atingere a confidențialității în condițiile în care se obține starea temporară, prin protejarea variabilelor temporare care transportă informație între pașii protocolului [35] - Capitolul 4.

4. Propunem două protocoale RFID, proiectate în conformitate cu abordarea cititorul primul, care ating confidențialitate distructivă cu obținerea stării temporare prin evitarea utilizării variabilelor temporare [36, 38, 39] (preprint [8]) - Capitolul 5.

5. Extindem modelul lui Vaudenay pentru a permite analiza protocoalelor RFID cu identificator constant de tag și proiectăm un protocol care obține confidențialitate distructivă în modelul extins [19] (preprint [20]) - Capitolul 6.

6. Extindem modelul lui Vaudenay pentru a permite analiza schemelor RFID de tip offline și introducem o nouă noțiune de confidențialitate numită confidențialitate offline. Propunem o schemă RFID care obține confidențialitate distructivă și confidențialitate offline [16] - Capitolul 7.

Structură

Structura tezei este axată pe studiul noțiunii de confidențialitate distructivă din modelul de securitate și confidențialitate al lui Vaudenay. Această secțiune detaliază planul tezei.

Capitolul 1 prezintă domeniul RFID și noțiunile de securitate și confidențialitate. Introducem mai întâi tehnologia RFID concentrându-ne pe scopul, beneficiile și componentele sale principale. De asemenea, este prezentată o scurtă evoluție istorică a RFID. În continuare, descriem abordarea criptografică asupra securității și confidențialității RFID, împreună cu o scurtă prezentare a ceea ce reprezintă un model de securitate și confidențialitate și a necesității acestuia. Introducem apoi primitivele PUF, o nouă tehnologie care completează RFID. Capitolul se încheie cu considerente de proiectare pentru protocoalele RFID, în ceea ce privește utilizarea generatoarelor de numere aleatorii, a primitivelor criptografice și a timpilor de identificare din partea cititorului.

Capitolul 2 este axat în jurul modelului de securitate și confidențialitate folosit în teză, și anume modelul lui Vaudenay. Capitolul prezintă definiții generale și specifice sistemelor RFID, care sunt utilizate în restul tezei. Modelul de adversar al lui Vaudenay este prezentat în continuare, împreună cu definițiile de securitate și confidențialitate și experimentele de securitate ale acestora. În continuare, prezentăm principalele rezultate de imposibilitate

pentru model și apoi realizăm o analiză a modelului din perspectiva caracterizării black-box/gray-box/white-box. Încheiem acest capitol cu o descriere generală a modului în care sunt construite demonstrațiile în model și cu câteva remarci metodologice.

Capitolul 3 explorează noțiunea de confidențialitate distructivă. În primul rând, discutăm pe larg despre tehnologia PUF, concentrându-ne pe implicațiile acesteia pentru confidențialitatea distructivă și formalismul pe care îl utilizăm. În continuare, prezentăm primul protocol proiectat pentru a obține confidențialitate distructivă în scenariul de autentificare unilaterală. În continuare vom extinde această construcție pentru a obține confidențialitate distructivă împreună cu autentificarea mutuală. Soluția pe care o propunem se bazează pe primitive PUF și folosește o funcție PRF ca primitivă criptografică principală. Pentru protocol sunt realizate demonstrații detaliate de securitate și confidențialitate.

Capitolul 4 abordează problema realizării confidențialității împotriva adversarilor care pot obține, prin corupere, atât starea persistentă, cât și starea temporară a unui tag. În primul rând, prezentăm un rezultat de imposibilitate care afirmă că, în absența PUF-urilor, confidențialitatea mai mare de nivelul slab nu poate fi realizată în cazul coruperii cu TSD. Discutăm acest rezultat și introducem conceptul de variabile temporare, precum și modul în care poate fi modelată coruperea cu TSD. Sunt descrise două atacuri împotriva schemelor care utilizează tehnica de protecție dublă cu PUF împotriva adversarilor care pot obține variabile temporare din memoria volatilă a tag-urilor. În continuare, introducem o soluție generală, numită protecție cu PUF, care poate fi utilizată pentru a îmbunătăți protocoalele care obțin confidențialitate în modelul lui Vaudenay pentru a atinge același nivel de confidențialitate în modelul lui Vaudenay cu TSD. Rezultatul este însoțit de o demonstrație detaliată. La final, soluția este aplicată pe două protocoale.

Capitolul 5 se ocupă de ordinea de autentificare în protocoalele RFID, tag-ul primul sau cititorul primul. După ce discutăm despre implicațiile fiecărei abordări, proiectăm două protocoale care obțin confidențialitate distructivă în modelul lui Vaudenay cu TSD, utilizând abordarea cititorul primul și evitând utilizarea variabilelor temporare între pașii din protocol. Primul protocol utilizează un PUF și un PRF, în timp ce al doilea utilizează o schemă SKE

împreună cu un PUF. Ambele protocoale sunt mai eficiente, deoarece nu folosesc generatoare de numere aleatorii pe tag. Prezentăm demonstrații detaliate de securitate și confidențialitate pentru aceste protocoale.

Capitolul 6 este adresat clasei de protocoale de autentificare cu identificator constant de tag. În primul rând, presentăm un rezultat general care demonstrează că această clasă de protocoale nu poate atinge niciun nivel de confidențialitate în modelul lui Vaudenay. Analizăm și demonstrăm că modelul Refresh [26], propus pentru analiza acestor protocoale, este limitat la scheme cu autentificare unilaterală. De asemenea, construim un atac împotriva schemei LAST, care însoțește acest model, prin care demonstrăm că schema este nesigură. Continuăm apoi cu transformarea modelului lui Vaudenay pentru a permite studiul acestor protocoale. În final, propunem o schemă RFID care obține confidențialitate distructivă în acest model.

Capitolul 7 se concentrează pe o altă clasă de protocoale care nu pot fi analizate în modelul lui Vaudenay, și anume scheme RFID care permit cititoare multiple în sistem (adică scheme offline). După prezentarea acestor scheme, discutăm propuneri de modele de confidențialitate pentru analiza formală a acestor scheme. Demonstrăm că o astfel de propunere pentru modelul lui Vaudenay, *privacy+*, nu este adaptată la confidențialitatea bazată pe blinder a modelului. Propunem o formulare alternativă denumită *confidențialitate offline*, care se utilizează ca o analiză suplimentară față de securitate și confidențialitate. În cele din urmă, propunem o schemă RFID care obține confidențialitate distructivă și confidențialitate offline și construim demonstrațiile de securitate și confidențialitate aferente schemei.

Capitolul 8 prezintă principalele concluzii care pot fi extrase din această teză și rezumă principalele rezultate care au reieșit din această lucrare.

Capitolul 1

Introducere

1.1 Radio Frequency Identification

Ca tehnologie, Radio Frequency Identification (RFID) furnizează identificarea de la distanță a bunurilor și a persoanelor. Pașapoartele (sau alte tipuri de documente de identificare), transportul public, controlul accesului, logistica lanțului de aprovizionare sau îngrijirea medicală, sunt domenii care beneficiază deja de tehnologia RFID sau ar putea fi îmbunătățite dramatic prin utilizarea acesteia. Câteva dintre avantajele sistemelor RFID față de alte tehnologii ID concurente (cod de bare, OCR, carduri inteligente) sunt rata ridicată de transfer de date, costurile operaționale scăzute, raza de citire crescută și independența față de direcție sau poziție [11]. Elementul central al tehnologiei RFID este un mic dispozitiv numit *tag* care este atașat unui obiect și care facilitează identificarea acestuia. În cele mai multe cazuri, tag-ul nu are sursă de alimentare proprie și se bazează pe un alt dispozitiv, numit *reader* (sau *cititor* [11]), pentru a fi alimentat cu energie (captată cu ajutorul unei antene). Cititorul este un dispozitiv mai puternic al cărui scop principal este să colecteze datele stocate pe tag-uri și fie să le proceseze singur, fie să le transmită unui alt sistem de procesare. Odată ce tag-ul este pornit, cititorul și tag-ul vor începe comunicarea și vor schimba mesaje conform unui *protocol*. Rezultatul final al protocolului este *identificarea*.

Modelul de comunicare RFID este ceea ce îl diferențiază de alte tehnologii. Există trei componente în orice sistem RFID: tag-ul, cititorul și serverul. Tag-ul și cititorul formează nucleul oricărui sistem RFID. Serverul este o entitate cu capacitate standard de calcul care deține (sau are acces la) o bază de date. Cititorul comunică cu serverul printr-un canal care este considerat a fi securizat prin mijloace obișnuite (criptografie standard). Canalul de comunicare dintre cititor și tag (în special protocolul de autentificare) reprezintă elementul de interes pentru această teză.

Atacurile efectuate asupra RFID vizează de obicei interceptarea (sau „spionarea"), furtul identității tag-ului sau cititorului, blocarea serviciului sau încălcări ale confidențialității [11]. Blocarea serviciului este de interes pentru îmbunătățirea securității, atât timp cât vizează protocolul și poate afecta confidențialitatea. În caz contrar, nu există niciun sistem RFID care să se poată apăra împotriva unor astfel de atacuri (de exemplu, blocarea semnalului sau bruiajul tag-ului cu metal, astfel încât să nu poată fi pornit [11]). O altă caracteristică specială a sistemelor RFID este potențialul atacurilor invazive. Aceste atacuri sunt în principal direcționate către tag-uri, dar pot fi îndreptate și asupra cititorului, deși mai rar și în unele cazuri speciale (sisteme RFID cu mai multe cititoare [4]). Discrepanța față de sistemele informatice obișnuite este evidentă în acest aspect. Accesul fizic la un tag este mult mai facil decât la un computer obișnuit, iar tag-urile nu au tehnologie avansată de protecție, cum ar fi stocarea criptată sau mecanismele de detecție a intruziunii. Atacurile fizice pot facilita recuperarea datelor stocate pe tag și permit unui atacator furtul de identitate al tag-ului, pierzându-se astfel esența sistemului RFID (de exemplu, un atacator poate obține acces într-o clădire prin clonarea unui card de acces). De asemenea, atacatorul ar putea folosi datele pentru a descoperi utilizări anterioare ale tag-ului și pentru a compromite confidențialitatea utilizatorului.

În aceste circumstanțe, doar identificarea nu poate rezolva problemele de securitate și confidențialitate ale domeniului RFID. Trebuie concepute protocoale mai puternice care oferă, pe lângă identificare, *autentificare* și care împiedică urmărirea utilizatorilor. Având în vedere domeniul de aplicare al RFID, aceste protocoale trebuie să asigure că costurile de producție pentru tag-uri sunt reduse la minimum, iar costurile de securitate nu împiedică scalarea către

aplicații RFID mari sau creșterea consumului de energie nu depășește capacitatea tag-ului. S-ar putea proiecta cu ușurință protocoale foarte puternice care implică o creștere cu un ordin de mărime a costurilor, energiei sau puterii de procesare a tag-ului, dar nu acesta este scopul. Echilibrul dintre performanță, costuri și securitate se dovedește a fi o provocare semnificativă și o combinație între știință și artă. În ultimele două decenii au fost întreprinse eforturi pentru a proiecta și implementa protocoale care să aducă RFID mai aproape de atingerea potențialului său. Deși înțelegerea domeniului a crescut și au fost propuse protocoale mai adaptate nevoilor, mai este încă un drum lung de urmat.

1.2 Criptografia în RFID

În sistemele RFID, criptografia joacă un rol central în asigurarea utilizatorilor cu privire la amenințările privind securitatea și confidențialitatea, care sunt inerente acestor sisteme. Principalele obiective pe care criptografia le stabilește pentru RFID sunt *securitatea* și *confidențialitatea*. În mod informal, scopul securității este de a garanta că un atacator nu poate fura identitatea unei entități (tag sau cititor), în timp ce scopul confidențialității este de a împiedica un atacator să urmărească un tag.

Protocoale Elementul fundamental într-un sistem RFID, care permite utilizarea tehnologiei, este protocolul de comunicare dintre cititor și tag. Scopul principal al acestui protocol este de a permite cititorului să realizeze identificarea tag-ului. Criptografia ajută la transformarea acestuia într-un protocol de autentificare în care se realizează identificarea, dar părțile sunt convinse de rezultat [29]. Protocoalele de autentificare RFID sunt de obicei cu o singură trecere atunci când doar tag-ul se autentifică la cititor și întotdeauna cu mai multe treceri atunci când atât tag-ul cât și cititorul sunt autentificate. În general, protocoalele de autentificare RFID urmează abordarea „provocare - răspuns” [29], în care tag-ul sau cititorul lansează o provocare la care cealaltă parte răspunde și dovedește cunoașterea unui secret pre-partajat. Aceste protocoale de autentificare se pot baza pe diferite primitive criptografice, cum ar fi criptarea cu chei publice [37], funcțiile hash [1, 24], criptarea cu chei simetrice [36] sau

funcțiile pseudorandom [17, 37]. Deși protocoalele de autentificare asigură că identitatea entităților nu poate fi furată de către un adversar rău intenționat, autentificarea nu protejează identitatea entităților (adică adversarul poate afla în continuare tag-ul care a participat la o anumită sesiune de autentificare). Tot prin intermediul criptografiei este atins obiectivul de confidențialitate al protocoalelor RFID. Protocoalele de autentificare care au confidențialitate sunt capabile să protejeze identitatea tag-ului chiar și atunci când adversarul compromite comunicarea.

Modelul de securitate și confidențialitate Un pas cheie în proiectarea protocoalelor adaptate la cerințele specifice ale sistemelor RFID este dezvoltarea unui model adecvat de securitate și confidențialitate. Un astfel de model încearcă să surprindă esența sistemului real și să o traducă în definiții precise și într-o descriere completă a capacităților adversarului și să formuleze experimentele de securitate care ajută la dezvoltarea demonstrațiilor de securitate. Un model de confidențialitate aduce valoare nu doar prin cele de mai sus, ci și prin oferirea unui cadru de comparație între protocoalele de autentificare și permite, astfel, posibilitatea de îmbunătățire. În ceea ce privește domeniul RFID, au fost propuse diverse modele de confidențialitate, cum ar fi: [5, 7, 9, 14, 15, 23, 30, 37].

Probabil că cel mai notabil model și cel pe care îl urmăm în această teză este cel definit în [30, 37], pe care îl vom numi „modelul lui Vaudenay" sau „modelul Vaudenay". În model, entitățile principale (tag-ul, cititorul și adversarul) sunt modelate ca algoritmi PPT (Probabilistic Polynomial Time). Adversarul interacționează cu tag-ul și cititorul prin intermediul *oracolelor* care îi permit să inițieze sesiuni de protocol, să intercepteze comunicația, să afle dacă sesiunile de protocol se încheie cu succes și să obțină starea internă (inclusiv orice secrete ar putea conține) a tag-ului. Ultima capabilitate se numește *corupere* și atunci când adversarul obține starea tag-ului, spunem că *corupe* tag-ul. Posibilitatea de corupere modelează lipsa de protecție fizică a circuitelor integrate RFID din lumea reală. Deoarece efectuarea atacurilor hardware invasive nu este trivială, modelul face distincție între mai multe tipuri de adversari cu această capacitate. Avem astfel adversari *slabi* (care nu pot corupe un

tag), adversari *forward* (care pot efectua corupere doar la sfârșitul atacurilor), adversari *distructivi* (care distrug tag-ul după corupere) și adversari *puternici* (fără restricții de corupere). Atunci când un protocol este rezistent la o clasă de adversari P, spunem că protocolul atinge $confidențialitate\ P$ (sau este $P\ confidențial$).

Capitolul 2

Modelul de securitate și confidențialitate

2.1 Modelul lui Vaudenay

Cele mai importante cerințe pentru schemele RFID sunt *securitatea* și *confidențialitatea*. Pentru a le formaliza, este nevoie de conceptul de *model al adversarului*. În literatură au fost propuse mai multe modele, dintre care amintim [3, 5, 7, 9, 14, 15, 23, 30, 37]. Modelul pe care îl urmăm în această teză este *modelul lui Vaudenay* [30, 37].

În acest model există un singur cititor care este conectat în permanență la baza de date centrală. Cititorul poate comunica cu mai multe *tag-uri* în același timp (are mai multe sesiuni deschise), dar un tag poate fi implicat într-o singură sesiune. Cititorul, tag-urile și adversarul sunt algoritmi PPT (Probabilistic Polynomial Time).

Baza de date a cititorului, DB, este inițial goală, iar tag-urile sunt adăugate pe măsură ce adversarul solicită crearea lor. Adversarul poate solicita crearea de *tag-uri legitime* sau *tag-uri nelegitime*. Acestea din urmă sunt create printr-un proces similar, dar nu sunt inserate în baza de date a cititorului. Odată creat, un tag poate fi *extras* sau *liber*. Acest lucru modelează caracteristica RFID conform căreia un tag poate fi alimentat pentru o perioadă limitată de timp și numai atunci când cititorul sau adversarul se află în vecinătatea sa. Tag-urile extrase

sunt cele cu care adversarul poate interacționa (ascultă comunicarea, trimite mesaje sau le corupe), în timp ce tag-urile libere sunt considerate în afara accesului adversarului. Adversarul nu interacționează direct cu un tag în funcție de identitatea sa, ci prin intermediul unui identificator temporar unic numit *vtag*. Odată ce un tag devine extras, i se atribuie un vtag pe care adversarul îl folosește pentru a comunica cu tag-ul sau pentru a îl corupe. Dacă tag-ul este eliberat (nu mai este în proximitatea adversarului), vtag-ul nu mai poate fi folosit. Dacă același tag este extras din nou în viitor, i se va atribui un vtag diferit.

În modelul lui Vaudenay, adversarului i se oferă acces la următoarele oracole: $CreateTag$ (pentru crearea tag-ului), $Corrupt$ (pentru obținerea stării interne a unui tag), $SendTag$ și $SendReader$ (pentru comunicare), $Result$ (pentru a afla rezultatul unei sesiuni de autentificare), $Free$ și $DrawTag$ (pentru modelarea interacțiunii cu tag-urile) și $Launch$ (pentru crearea unei noi sesiuni de autentificare).

Modelul oferă granularitate prin crearea diferitelor categorii de adversari cu diferite niveluri de putere. Adversarii din model sunt clasificați în funcție de accesul la oracolele $Corrupt$ și $Result$. În funcție de accesul la oracolul $Corrupt$, obținem adversari care sunt *slabi*, *forward*, *distructivi* și *puternici*, în timp ce bazat pe accesul la $Result$, adversarii pot fi *limitați* sau *extinși*.

Putem combina aceste clase pentru a obține opt categorii de adversari: *limitat slabi*, *limitat forward*, *limitat distructivi*, *limitat puternici*, *extins slabi*, *extins înaintați*, *extins distructivi*, *extins puternici*. În scopul simplității, vom considera că atunci când un adversar este denumit doar ca fiind slab, forward, distructiv sau puternic, este implicit extins.

2.2 Securitate

Securitatea schemelor RFID în modelul lui Vaudenay poate fi descompusă în două proprietăți ale protocolului: *autentificarea tag-ului* și *autentificarea cititorului*. În mod informal, securitatea înseamnă că tag-ul sau cititorul nu pot fi impersonate de către adversar. Din perspectiva

modelului, un adversar care încearcă să compromită această proprietate într-o sesiune de protocol va trebui să creeze anumite mesaje care să convingă cititorul/tag-ul că adversarul este cealaltă entitate.

Proprietățile de autentificare a tag-ului și a cititorului sunt descrise prin intermediul experimentelor de securitate, care sunt construite sub forma unui joc între un adversar puternic și un provocator (*challenger*). Adversarul poate crea câte tag-uri dorește și poate corupe orice tag, cu excepția unui tag țintă ID. În acest joc, obiectivul adversarului este să se prezinte ca fiind tag-ul sau cititorul, astfel încât cealaltă parte să-l autentifice, dar fără a avea o conversație corespunzătoare. Acest lucru înseamnă că, pentru a câștiga, adversarul nu poate doar să transmită mesaje între cititor și tag, ci trebuie să calculeze cel puțin o parte a mesajului.

O schemă RFID $\mathcal{S}$ realizează *autentificarea tag-ului* dacă avantajul lui $\mathcal{A}$ de a câștiga experimentul de autentificare a tag-ului este neglijabil, pentru orice adversar puternic $\mathcal{A}$.

O schemă RFID $\mathcal{S}$ realizează *autentificarea cititorului* dacă avantajul lui $\mathcal{A}$ de a câștiga experimentul de autentificare a cititorului este neglijabil, pentru orice adversar puternic $\mathcal{A}$.

2.3 Confidențialitate

Confidențialitatea în sistemele RFID [30] include anonimatul și imposibilitatea urmăririi. În mod informal, confidențialitatea în acest model înseamnă că un adversar nu poate afla nimic nou interceptând comunicația dintre un tag și cititor. Acest concept este modelat prin utilizarea unui algoritm special numit *blinder*. Această metodă de formalizare a confidențialității este diferită de metoda obișnuită de definire a confidențialității în sistemele RFID [14, 15, 22] bazată pe indistingibilitatea dintre două tag-uri țintă (indistingibilitatea între stânga și dreapta).

Un *blinder* pentru un adversar $\mathcal{A}$ care aparține unei anumite clase P de adversari este un algoritm PPT $\mathcal{B}$ care simulează oracolele $Launch$, $SendReader$, $SendTag$ și $Result$ pentru

$\mathcal{A}$, fără a avea acces la secretele tag-ului și cititorului și care observă pasiv comunicarea dintre $\mathcal{A}$ și celelalte oracole permise pentru clasa P.

Când adversarul $\mathcal{A}$ interacționează cu schema RFID prin intermediul unui blinder $\mathcal{B}$, spunem că $\mathcal{A}$ este *orbit de* $\mathcal{B}$ și notăm acest lucru cu $\mathcal{A}^{\mathcal{B}}$. Subliniem faptul că $\mathcal{A}^{\mathcal{B}}$ are voie să facă interogări către oracolele $Launch$, $SendReader$, $SendTag$ și $Result$ doar prin intermediul lui $\mathcal{B}$; toate celelalte oracole sunt interogate ca de obicei de către adversar.

Confidențialitatea afirmă că un protocol este confidențial în raport cu o clasă de adversari dacă toți adversarii din acea clasă sunt *triviali*. Un adversar trivial este, în principiu, un adversar care nu folosește oracolele pe care blinder-ul le poate simula. În jocul de confidențialitate, adversarul interacționează cu schema RFID și are voie să facă interogări către toate oracolele în funcție de clasa sa. Această fază este denumită *faza de învățare*. La sfârșitul acestei faze, adversarul primește tabela secretă Γ a oracolului $DrawTag$, care conține asocierea dintre identificatorii tag-urilor și vtag-uri. Având această informație suplimentară, adversarul intră într-o *fază de analiză*, în urma căreia decide dacă a interacționat cu blinder-ul sau cu oracolele reale.

O schemă RFID $\mathcal{S}$ obține confidențialitate pentru o clasă V de adversari dacă pentru orice adversar $\mathcal{A} \in V$ există un blinder $\mathcal{B}$ astfel încât avantajul lui $\mathcal{A}$ de a distinge oracolele simulate de blinder de oracolele reale este neglijabil.

Capitolul 3

Confidențialitate distructivă

3.1 Primitive PUF

În comparație cu tehnologia RFID, primitivele PUF (PUF-uri) sunt o tehnologie relativ nouă. Prima descriere a conceptului de PUF, deși sub numele de *funcție fizică aleatoare*, a fost prezentată în [31] la începutul anilor 2000. Prima referință cu terminologia exactă a fost menționată pentru prima dată în [13]. De atunci, domeniul a căpătat amploare, și au fost propuse diverse construcții de PUF-uri. Baza de cunoștințe referitoare la ce reprezintă un PUF și ce proprietăți sunt dorite pentru PUF-uri s-a maturizat, de asemenea.

PUF-urile [6,27,28] sunt construcții hardware capabile să identifice în mod unic dispozitivul pe care sunt implementate. În acest sens, PUF-urile au fost comparate cu caracteristicile biometrice unice ale oamenilor și au fost considerate amprenta unui dispozitiv. Procesul de proiectare al unui PUF vizează potențarea imperfecțiunilor inerente procesului de fabricație pentru a produce o trăsătură unică, diferențiată și consistentă a unui circuit. Acest lucru contravine practicilor obișnuite de fabricație hardware, în care aceste distincții între obiecte sunt minimizate. După cum sugerează și numele, caracteristica principală a unui PUF ar trebui să fie imposibilitatea clonării. Aceasta înseamnă că, chiar și cu cunoștințe extinse

despre designul și comportamentul unui PUF, nu ar trebui să fie fezabil să se producă un alt PUF cu același comportament (să poată fi clonat).

3.2 Autentificare unilaterală și confidențialitate distructivă

Prima utilizare a PUF-urilor în contextul modelului lui Vaudenay a fost introdusă în lucrarea [33,34]. În această lucrare, protocolul slab bazat pe PRF din [37] a fost îmbunătățit cu un PUF pentru a realiza confidențialitate distructivă în modelul lui Vaudenay, care era o problemă deschisă până în acel moment. Acesta este primul protocol care atinge nivelul distructiv, deoarece în [37] nu a fost propus niciun protocol pentru acest nivel de confidențialitate. PUF-ul a fost folosit pe tag ca un generator de chei sigur cu comportament rezistent la intruziuni.

3.3 Confidențialitate distructivă și autentificare mutuală

În această secțiune, facem un pas înainte pentru a obține primul sistem RFID care realizează confidențialitate distructivă și autentificare mutuală în modelul lui Vaudenay [17]. Ideea principală este să pornim de la schema din [33, 34] și să o extindem cu un pas suplimentar pentru a realiza autentificarea mutuală, așa cum s-a făcut în [30]. O modalitate alternativă de a gândi acest sistem este să considerăm că schema cu confidențialitate slabă bazată pe PRF din [30] este îmbunătățită cu un PUF.

Fiecare tag este echipat cu un PUF (unic) P și are capacitatea de a calcula PRF-ul F. Pe tag este necesar și un generator de numere aleatoare. Cititorul menține o bază de date DB cu înregistrări pentru toate tag-urile legitime.

Protocolul este inițiat de cititor, care trimite un număr aleator x către tag. După ce îl primește, tag-ul generează un număr aleator y, calculează $K = P(s)$ și $z = F_K(0, x, y)$ și răspunde cu (y, z). Cititorul verifică baza sa de date pentru o pereche (ID, K) astfel încât $z = F_K(0, x, y)$. Dacă se găsește o astfel de pereche, returnează ID; în caz contrar,

returnează $\perp$ și alege în mod aleator o cheie K. Indiferent de cele două cazuri (dacă K se găsește în baza de date sau este generată în mod aleator), cititorul calculează $w = F_K(1, x, y)$ și îl trimite la tag. După ce îl primește, tag-ul calculează $w' = F_K(1, x, y)$, unde K este cel calculat în cea de-a doua etapă. În cele din urmă, returnează OK sau $\perp$ în funcție de egalitatea dintre w și w'.

Capitolul 4

Confidențialitatea distructivă și obținerea stării temporare

4.1 Imposibilitatea autentificării mutuale

Capacitatea de corupere este fundamentală în toate modelele de securitate și confidențialitate RFID. În acest sens, oracolul $Corrupt$ este proiectat într-un mod specific în fiecare model. În modelul lui Vaudenay, $Corrupt$ dă naștere granularității confidențialității și claselor principale de confidențialitate. Inițial, definiția pentru $Corrupt$ stabilea că acesta returnează starea internă a unui tag, care este stocată în memoria tag-ului. Cu toate acestea, memoria unui tag poate fi clasificată în persistentă și temporară. *Memoria persistentă* stochează date în memoria fizică non-volatilă care persistă între sesiunile de pornire a tag-ului. *Memoria temporară* este folosită pentru a stoca date în memoria fizică volatilă. Datele stocate în această memorie fac parte din calculele tag-ului și nu persistă odată ce tag-ul este oprit.

Vom lua în considerare două scenarii pentru oracolul $Corrupt$:

1. Coruperea returnează doar starea persistentă a tag-ului;
2. Coruperea returnează atât starea persistentă, cât și starea temporară a tag-ului.

4.2 Coruperea cu obținerea stării temporare

Memoria temporară a unui tag poate fi văzută ca un set de *variabile volatile/temporare* utilizate pentru a stoca și efectua calculele necesare protocolului de autentificare. Facem distincție între două tipuri de variabile temporare: - *locale* - variabile temporare utilizate de tag-uri pentru a efectua calcule doar într-un anumit pas al protocolului; - *globale* - variabile temporare care stochează valori dintr-un anumit pas al protocolului și sunt utilizate într-un alt pas al protocolului. Aceste variabile au, prin urmare, o durată de viață mai lungă decât variabilele temporare locale.

4.3 Atacuri împotriva confidențialității distructive

În căutarea confidențialității distructive mai puternice din modelul lui Vaudenay cu obținerea stării temporare, au fost propuse mai multe protocoale [1, 24]. Aceste protocoale folosesc PUF-uri și se bazează pe o tehnică numită *evaluarea dublă a PUF* pentru a depăși rezultatul de imposibilitate din [2]. Aceasta a fost dezvoltată pentru a atenua un atac practic numit *cold boot attack* pentru PUF-uri [25]. Acest atac oferă o metodă de a îngheța starea tag-ului și de a recupera valoarea PUF-ului (dacă a fost calculată înainte de atac). Când este formalizat în modelul lui Vaudenay, acest atac intră în categoria coruperii cu obținerea stării temporare. Esența acestei tehnici constă în evaluarea aceluiași PUF de două ori în diferite etape de calcul. Dacă atacul este aplicat imediat după prima evaluare a PUF-ului, valoarea celei de-a doua evaluări a PUF-ului nu va fi obținută, și vice-versa.

Cu toate că tehnica de evaluare dublă a PUF sugerează că autorii au luat în considerare un scenariu mai puternic pentru protocoalele propuse, în această teză le vom analiza în scenariul în care adversarul nu poate obține valorile PUF decât dacă sunt stocate ca variabile temporare globale, și vom arăta că acestea prezintă vulnerabilități de confidențialitate.

4.4 Soluția de protecție cu PUF

Variabilele temporare nu pot fi protejate cu ajutorul primitivelor criptografice fără cheie sau cu cheia stocată în clar pe tag. Acest lucru se datorează faptului că Teorema 1 din [2] se va aplica și în acest caz (cel puțin pentru schemele RFID care nu conțin PUF-uri). Ca urmare, dacă primitivele criptografice cu cheie sunt folosite pentru a proteja variabilele temporare, atunci cheia trebuie să fie protejată de asemenea. Protecția nu ar trebui să fie de natură criptografică, ci mai degrabă fizică.

Într-un astfel de context, PUF-urile par a fi un candidat excelent. În forma sa actuală, Teorema 1 din [2] nu poate fi în general aplicată tag-urilor cu PUF-uri deoarece coruperea distruge tag-ul și valoarea PUF nu poate fi recuperată (cu presupunerea că valorile PUF nu sunt stocate în memoria internă a tag-urilor). Pe baza acestei observații, ajungem la ideea de a proteja variabilele temporare cu ajutorul PUF-urilor. Acest lucru poate fi realizat astfel: dat fiind un tag T_{ID} și o variabilă temporară v din calculele tag-ului, dotăm tag-ul cu un PUF dedicat P și un seed s_v (dacă tag-ul are deja un PUF, adăugăm doar un seed dedicat ales aleator s_v). Apoi, pentru a proteja v, putem cripta valoarea sa folosind o primitivă criptografică cu cheia $P(s_v)$.

Capitolul 5

Autentificarea de tip cititorul primul

5.1 Ordinea de autentificare în RFID

Proiectarea schemelor RFID cu autentificare mutuală poate fi gândită în două abordări distincte: autentificarea *tag-ul primul* și autentificarea *cititorul primul* [32].

Autentificarea *cititorul primul* [32] necesită ca cititorul să fie primul care este autentificat de către tag. Principalul beneficiu al acestei abordări poate fi considerat limitarea suprafeței de atac pentru un atacator. În acest fel, tag-ul va elibera informații sensibile doar după ce este sigur de identitatea cititorului. Ca urmare, numai în prezența unui cititor valid, adversarul poate obține mesajele tag-ului destinate autentificării. Un alt caz de utilizare interesant pentru această abordarea este în schemele în care tag-ul este proiectat doar pentru un număr limitat de autentificări, deoarece previne o formă de atac de tip blocarea de serviciilor care ar "consuma" toate răspunsurile de autentificare ale tag-ului (uneori numite cupoane [32]). Cu această abordare vine și o provocare, cititorul trebuie să se autentifice la un tag necunoscut. Prin urmare, este nevoie de proiectarea unei metode astfel încât cititorul să poată mai întâi identifica și apoi autentifica tag-ul.

Suntem interesați de o soluție alternativă pentru obținerea confidențialității în modelul lui Vaudenay cu TSD, care să fie mai eficientă decât soluția de protecție cu PUF din Capitolul 4.4. Soluția directă ar fi să evităm utilizarea variabilelor temporare în schemele RFID. Considerăm că abordarea cu autentificare cititorul primul realizează acest lucru într-un mod natural și eficient, eliminând necesitatea variabilelor temporare.

5.2 Confidențialitate distructivă prin PUF-uri și PRF-uri

În această secțiune abordăm problema construirii unei scheme RFID cu autentificare mutuală care realizează confidențialitate distructivă în modelul lui Vaudenay cu obținerea stării temporare. Schema [38, 39] se bazează pe o funcție de calcul pseudorandom (PRF) și este mai eficientă decât schemele care au fost îmbunătățite folosind protecția cu PUF. Scopul principal al acestei scheme este să evite complet utilizarea variabilelor temporare globale (vezi Secțiunea 4.2), care transportă informații de la un pas al protocolului la altul, în loc să le protejeze prin criptare. Schema este proiectată urmând abordarea cu autentificare cititorul primul. Fiecare tag va fi dotat cu un PUF și cu un generator de numere aleatoare. Primitiva criptografică principală folosită în cadrul schemei este un PRF.

5.3 Confidențialitate distructivă cu timp constant de identificare

Schema RFID bazată pe criptografia cu chei publice (PKE) propusă în [30] obține confidențialitate de tip forward și autentificare mutuală. Mai mult, permite identificarea constantă a tag-urilor din baza de date a cititorului. Acest lucru se datorează faptului că cititorul are o cheie publică distribuită tuturor tag-urilor, iar cheia privată este păstrată secretă. Prin urmare, fiecare tag poate trimite în siguranță identitatea sa criptată cu cheia publică a cititorului.

Această abordare are însă un dezavantaj important, deoarece nu poate fi implementată în practică: dimensiunea implementării PKE nu este adecvată pentru majoritatea cipurilor RFID. Pentru a obține aceleași avantaje într-o schemă mai eficientă, ar trebui să o proiectăm folosind primitive simetrice, cum ar fi schemele SKE. Această idee nu poate fi însă pusă în practică doar cu ajutorul SKE, deoarece cheia secretă este folosită atât pentru criptare, cât și pentru decriptare. Partajarea cheii secrete între toate tag-urile și cititor ridică probleme serioase de securitate și confidențialitate: coruperea unui tag dezvăluie cheia secretă și întregul sistem este compromis. Soluția la această problemă este din nou utilizarea PUF-urilor: dacă cheia secretă este protejată de PUF-uri, atunci aceasta va acționa ca o cheie master cunoscută doar de tag-uri și cititor. Încercarea de a extrage cheia din tag prin corupere va distruge tag-ul fără a dezvălui cheia.

Prima încercare de a proiecta o schemă RFID cu autentificare mutuală și confidențialitate distructivă folosind chei secrete protejate cu ajutorul PUF-urilor a fost propusă în [1]. Din păcate, schema din [1] nu realizează confidențialitate distructivă în modelul lui Vaudenay cu obținerea stării temporare. Acest lucru se datorează faptului că schema utilizează variabile temporare pentru a transporta informații cruciale între pașii protocolului, iar aceste informații pot fi obținute prin corupere.

Cu toate acestea, combinarea ideii din [1] de a folosi o cheie secretă protejată cu ajutorul PUF-urilor cu abordarea de proiectare cu autentificare cititorul primul pentru a evita utilizarea variabilelor temporare duce la o schemă RFID care obține confidențialitate distructivă și autentificare mutuală în modelul lui Vaudenay cu TSD, împreună cu identificarea în timp constant a tag-urilor în baza de date.

Capitolul 6

Confidențialitate aleatorizată

6.1 Descriere generală

Creșterea aplicabilității tehnologiei RFID în sistemele de scară mare necesită identificare și autentificare eficiente a tag-urilor. Acest lucru a dus la proiectarea a numeroase scheme RFID cu timp de identificare care variază de la constant la liniar. Cu siguranță, obținerea unui timp mai bun de identificare a tag-urilor se face cu un anumit cost, și de cele mai multe ori cu sacrificiul confidențialității. Găsirea unui echilibru între timpul de identificare a tag-urilor și nivelul de confidențialitate este foarte importantă. Pentru a realiza acest lucru, protocoalele cu identificator constant de tag trebuie să beneficieze de aceeași analiză de securitate și confidențialitate ca și alte tipuri de protocoale RFID.

Scopul acestei secțiuni este de a introduce o clasă de scheme RFID care permite un timp rapid de identificare cu o pierdere rezonabilă de confidențialitate. Aceasta este clasa de *scheme RFID cu identificator constant de tag* [19]. În aceste scheme, primul mesaj trimis de tag are o parte constantă (identificatorul tag-ului) care permite cititorului să identifice eficient tag-ul în baza sa de date. Un identificator de tag nu trebuie neapărat să fie considerat identitatea tag-ului sau un mesaj fix. Poate fi schimbat după procesul de identificare (dar nu înainte).

6.2 Rezultat de imposibilitate

În schemele RFID cu identificator constant de tag, tag-ul își actualizează starea permanentă după ce este identificat sau autentificat de către cititor. Acest decalaj în actualizarea stării tag-ului poate fi exploatat de către un adversar, în special pentru a urmări tag-urile. Adversarul poate deschide o sesiune de protocol cu tag-ul, obține identificatorul și apoi închide sesiunea fără a permite tag-ului să-și actualizeze starea. Având identificatorul, adversarul poate deschide o nouă sesiune de protocol pentru a urmări tag-ul până când acesta reușește autentificarea cu cititorul. Prin urmare, această clasă de scheme RFID pierde confidențialitatea în modelul lui Vaudenay.

6.3 Extensia modelului

Analiza schemelor RFID cu identificator constant propuse până în prezent a fost făcută fie informal, așa cum este cazul în [10], fie în modele restrânse, așa cum este cazul modelului Refresh [26]. Prin urmare, este imposibil să comparăm astfel de scheme în ceea ce privește confidențialitatea. Devine imperativ să avem un model unitar de confidențialitate pentru aceste scheme. Deoarece modelul lui Vaudenay este, probabil, cel mai general și utilizat model de confidențialitate pentru sistemele RFID, este natural să încercăm să-l adaptăm la această clasă de protocoale [19]. Ceea ce trebuie să facem este să verificăm confidențialitatea schemelor cu identificator constant în fața unei clase limitate de adversari, și anume în fața adversarilor care pot extrage un tag cel mult o dată între două sesiuni complete ale protocolului. Acest lucru se datorează faptului că știm deja că schemele nu obțin nici măcar confidențialitate slabă în modelul lui Vaudenay dacă adversarul extrage un tag de mai multe ori între două sesiuni complete ale protocolului.

Cel mai simplu mod de a utiliza modelul lui Vaudenay cu o clasă restrânsă de adversari, așa cum am menționat mai sus, este să modificăm unul dintre oracolele $DrawTag$ sau $Free$: atunci când un tag este extras sau eliberat, starea acestuia este randomizată prin cel puțin

o sesiune completă de protocol. Modelul Refresh implementează o aleatorizare similară primului tip: tag-urile țintă sunt randomizate în primul rând și apoi sunt puse la dispoziția adversarului. Modelul HPVP [15] sugerează o aleatorizare de tipul al doilea pentru a putea analiza schemele RFID cu stare (Secțiunea IV(C) din [15]).

Indiferent dacă modificăm oracolul $DrawTag$ sau $Free$ așa cum am discutat mai sus, această schimbare încorporează ideea că modelul lui Vaudenay este restricționat să considere confidențialitatea doar în fața adversarilor care pot extrage un tag cel mult o dată între două sesiuni complete ale protocolului. Cu toate acestea, pentru a fi în concordanță cu abordările din [15, 21], preferăm să schimbăm oracolul $Free$.

6.4 Confidențialitate distructivă în rVM

În această secțiune proiectăm o schemă RFID cu identificator constant de tag, care oferă autentificare mutuală și confidențialitate distructivă în modelul Vaudenay cu aleatorizare (rVM). Schema este proiectată urmând abordarea cititorul primul.

Fiecare tag este echipat cu un PUF ideal și cu un PRF. În locul unui generator de numere aleatoare, tag-ul va partaja cu cititorul o stare aleatoare aleasă uniform. Atunci când primește o provocare de la cititor, tag-ul va evalua PUF-ul pentru a obține cheia, și apoi va aplica PRF-ul asupra stării și provocării cititorului. Cititorul trebuie să mențină o bază de date cu două versiuni ale stării tag-ului, deoarece poate apărea o desincronizare de cel mult un pas între cititor și tag. Prima etapă în protocol este folosită pentru identificare, astfel încât cititorul să poată găsi perechea corectă de stare și cheie care se potrivește cu răspunsul tag-ului. Când cititorul găsește valoarea corectă, se va resincroniza cu tag-ul și va calcula răspunsul care îl autentifică către tag. Dacă cititorul nu actualizează starea tag-ului din baza de date (pentru că respinge tag-ul), atunci va face acest lucru în cea de-a doua etapă a următoarei sesiuni de protocol (cu același tag). Prin urmare, desincronizarea între cititor și tag poate fi de cel mult un pas.

Capitolul 7

Confidențialitate distructivă offline

7.1 Scheme RFID offline

Schemele RFID descrise în Capitolul 2, pe care le vom numi în continuare scheme online, sunt alcătuite dintr-un cititor, mai multe tag-uri și un server central care furnizează baza de date a sistemului. Pentru a ne concentra asupra protocolului dintre cititor și tag, se presupune că, comunicația între server și cititor este securizată. În plus, această comunicație nu poate avea întreruperi. În astfel de condiții, este natural să considerăm serverul și cititorul ca o entitate unică (de exemplu, cititorul din modelul lui Vaudenay).

Însă această configurație nu este adecvată pentru aplicațiile care necesită mai multe cititoare care pot funcționa deconectate de la baza de date. Aplicații care se încadrează în această descriere sunt sistemele de control al accesului în care multe camere individuale sunt echipate cu încuietori electronice, evenimentele sportive sau transportul public. De exemplu, cititoarele de autobuz se conectează la baza de date centrală doar la sfârșitul zilei. Prin urmare, este natural să luăm în considerare implicațiile privind confidențialitatea atunci când un atacator compromite un cititor și să analizăm securitatea și confidențialitatea în aceste circumstanțe. Schemele RFID offline reprezintă o extensie a schemelor online (adică un sistem online este un sistem offline cu un singur cititor care este întotdeauna conectat la baza de

date). În schemele RFID offline, presupunem că cititorul este conectat la baza de date centrală doar în anumite momente. Pentru că cea mai mare parte sau toată activitatea cititorului trebuie să fie efectuată fără acces la server, cititorul trebuie să aibă o bază de date parțială (sau completă) cu informații despre tag-uri.

7.2 Modificarea modelului

Modelul lui Vaudenay a fost construit pentru a analiza schemele RFID online. În această secțiune, propunem extinderea modelului Vaudenay pentru schemele offline cu modificări inspirate din [24] și [15]. Esența transformării constă în acordarea adversarului capacitatea de a crea mai multe cititoare și de a corupe cititoare. Coruperea va fi modelată similar cu confidențialitatea distructivă: după ce un cititor este corupt, este considerat distrus. Cu toate acestea, vom restrânge aceste capacități la un experiment special de confidențialitate și vom continua să analizăm schema cu experimentele de securitate și confidențialitate definite în Capitolul 2. Astfel, vom modela analiza offline ca o analiză suplimentară a securității și confidențialității. În acest capitol, vom efectua toate analizele sub corupere fără obținere stării temporare.

7.3 Confidențialitate distructivă pentru scheme offline

În această secțiune, ne bazăm pe eforturile din [12, 24] și pe protocolul din Secțiunea 3.3, și propunem o schemă RFID care oferă confidențialitate offline, autentificare mutuală și confidențialitate distructivă. Ideea principală a schemei este de a proiecta un mecanism care permite fiecărui tag să stocheze o singură cheie, partajată doar cu serverul central, și să derive chei specifice cititorului bazate pe această cheie și pe identitatea cititorului. În acest fel, tag-ul nu trebuie actualizat pentru a suporta cititoare suplimentare sau pentru a se recupera confidențialitatea. Pentru a proteja informațiile stocate pe cititor, criptăm fiecare cheie cititor-tag cu o cheie specifică. Pentru protecția acestei chei, folosim PUF-uri.

Capitolul 8

Concluzii

Cercetarea pentru această teză s-a concentrat asupra studiului confidențialității în modelul RFID al lui Vaudenay, mai concret asupra obținerii confidențialității distructive. Modelul lui Vaudenay este unul dintre primele modele de securitate și confidențialitate și poate fi considerat cel mai matur model. Pentru a înțelege mai bine necesitatea confidențialității în sistemele RFID, am efectuat o introducere în domeniul RFID dintr-o perspectivă tehnică și criptografică. De asemenea, am analizat tehnologia PUF, care s-a dovedit a fi un element de bază esențial pentru realizarea confidențialității distructive în modelul lui Vaudenay. Natura PUF de rezistență la atacuri fizice, modelată sub forma primitivei hardware PUF ideal, este foarte adecvată pentru definiția confidențialității distructive.

Confidențialitatea a fost marcată ca o piedică majoră pentru progresul tehnologiei RFID acum mai bine de un deceniu. Între timp, comunitatea științifică a acumulat o înțelegere mai bună a acestui domeniu, iar noi tehnologii promițătoare au apărut (PUF-uri, primitive criptografice lightweight) care pot aduce confidențialitatea mai aproape de practică. Această teză a furnizat o înțelegere mai profundă a confidențialității, așa cum este ea modelată în modelul lui Vaudenay, prin studierea implicării coruperii cu obținerea stării temporare, prin extinderea modelului lui Vaudenay la alte clase de scheme și prin construirea de scheme RFID cu demonstrații detaliate. Cu toate acestea, confidențialitatea continuă să fie o provocare și un subiect central pentru sistemele RFID.

Bibliography

[1] Mete Akgün and M. Ufuk Çaglayan. Providing destructive privacy and scalability in RFID systems using PUFs. *Ad Hoc Netw.*, 32(C):32–42, September 2015.

[2] Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, and Christian Wachsmann. In Marina L. Gavrilova, C. J. Kenneth Tan, and Edward David Moreno, editors, *Transactions on Computational Science XI*, chapter Impossibility Results for RFID Privacy Notions, pages 39–63. Springer-Verlag, Berlin, Heidelberg, 2010.

[3] Gildas Avoine, Iwen Coisel, and Tania Martin. A privacy-restoring mechanism for offline rfid systems. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pages 63–74, 2012.

[4] Gildas Avoine, Cédric Lauradoux, and Tania Martin. When compromised readers meet rfid. In *International Workshop on Information Security Applications*, pages 36–50. Springer, 2009.

[5] Jens-Matthias Bohli and Andreas Pashalidis. Relations among privacy notions. *ACM Trans. Inf. Syst. Secur.*, 14(1):4:1–4:24, June 2011.

[6] Christoph Böhm and Maximilian Hofer. *Physical unclonable functions in theory and practice*. Springer Science & Business Media, 2012.

[7] Sébastien Canard, Iwen Coisel, Jonathan Etrog, and Marc Girault. Privacy-preserving RFID systems: Model and constructions. https://eprint.iacr.org/2010/405.pdf, 2010.

[8] Ferucio Laurenţiu Ţiplea and Cristian Hristea. Privacy and reader-first authentication in Vaudenay's RFID model with temporary state disclosure. Cryptology ePrint Archive, Report 2019/113, 2019. https://eprint.iacr.org/2019/113.

[9] Robert H. Deng, Yingjiu Li, Moti Yung, and Yunlei Zhao. A new framework for RFID privacy. In *Proceedings of the 15th European Conference on Research in Computer Security*, ESORICS'10, pages 1–18, Berlin, Heidelberg, 2010. Springer-Verlag.

[10] Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, pages 59–66, Washington, DC, USA, 2005. IEEE Computer Society.

[11] Klaus Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons, 2010.

[12] Flavio D Garcia and Peter Van Rossum. Modeling privacy for off-line rfid systems. In *International Conference on Smart Card Research and Advanced Applications*, pages 194–208. Springer, 2010.

[13] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[14] Jens Hermans, Frederik Pashalidis, Andreasand Vercauteren, and Bart Preneel. A new RFID privacy model. In Vijay Atluri and Claudia Diaz, editors, *Computer Security – ESORICS 2011*, pages 568–587, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[15] Jens Hermans, Roel Peeters, and Bart Preneel. Proper RFID privacy: Model and protocols. *IEEE Transactions on Mobile Computing*, 13(12):2888–2902, Dec 2014.

[16] Cristian Hristea. Reliable RFID Offline Privacy. In *Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC*

2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers 13, pages 212–226. Springer International Publishing, 2021.

[17] Cristian Hristea and Ferucio Laurenţiu Ţiplea. Destructive privacy and mutual authentication in Vaudenay's RFID model. Cryptology ePrint Archive, Report 2019/073, 2019. https://eprint.iacr.org/2019/073.

[18] Cristian Hristea and Ferucio Laurenţiu Ţiplea. Destructive privacy and mutual authentication in Vaudenay's RFID model. Cryptology ePrint Archive, Report 2019/073, 2019. https://eprint.iacr.org/2019/073.

[19] Cristian Hristea and Ferucio Laurenţiu Ţiplea. Privacy of stateful RFID systems with constant tag identifiers. *IEEE Transactions on Information Forensics and Security*, 15:1920–1934, 2019.

[20] Cristian Hristea and Ferucio Laurentiu Tiplea. Privacy of stateful rfid systems with constant tag identifiers. *Cryptology ePrint Archive*, 2019.

[21] Cristian Hristea and Ferucio LaurenŢiu Ţiplea. A PUF-based destructive private mutual authentication RFID protocol. In Jean-Louis Lanet and Cristian Toma, editors, *Innovative Security Solutions for Information Technology and Communications*, pages 331–343, Cham, 2019. Springer International Publishing.

[22] Ari Juels and Stephen A Weis. Authenticating pervasive devices with human protocols. In *Annual international cryptology conference*, pages 293–308. Springer, 2005.

[23] Ari Juels and Stephen A. Weis. Defining strong privacy for RFID. *ACM Trans. Inf. Syst. Secur.*, 13(1):7:1–7:23, November 2009.

[24] Süleyman Kardaş, Serkan Çelik, Muhammet Yildiz, and Albert Levi. PUF-enhanced offline RFID security and privacy. *J. Netw. Comput. Appl.*, 35(6):2059–2067, November 2012.

[25] Süleyman Kardaş, Mehmet Sabir Kiraz, Muhammed Ali Bingöl, and Hüseyin Demirci. A novel RFID distance bounding protocol based on physically unclonable functions. In

Ari Juels and Christof Paar, editors, *RFID. Security and Privacy*, pages 78–93, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[26] Li Lu, Yunhao Liu, and Xiang-Yang Li. Refresh: Weak privacy model for RFID systems. In *Proceedings of the 29th Conference on Information Communications*, INFOCOM'10, pages 704–712, Piscataway, NJ, USA, 2010. IEEE Press.

[27] Roel Maes. *Physically Unclonable Functions: Constructions, Properties and Applications*. Springer Verlag, 2013.

[28] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. *Towards Hardware-Intrinsic Security: Foundations and Practice*, pages 3–37, 2010.

[29] Tania Martin. *Privacy in RFID systems*. PhD thesis, Ph. D. Thesis. Universite catholique de Louvain, Belgium, 2013.

[30] Radu-Ioan Paise and Serge Vaudenay. Mutual authentication in RFID: Security and privacy. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '08, pages 292–299, New York, NY, USA, 2008. ACM.

[31] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.

[32] Roel Peeters, Jens Hermans, and Junfeng Fan. IBIHOP: Proper privacy preserving mutual RFID authentication. In Changshe Ma and Jian Weng, editors, *The 2013 Workshop on Radio Frequency Identification/Internet of Things Security (RFIDsec'13 Asia)*, volume 11 of *Cryptology and Information Security Series*. IOS Press, 2013.

[33] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. *Enhancing RFID Security and Privacy by Physically Unclonable Functions*, pages 281–305. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[34] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. PUF-enhanced RFID security and privacy. In *Workshop on secure component and system identification (SECSI)*, volume 110, 2010.

[35] Ferucio Laurenţiu Ţiplea and Cristian Hristea. PUF protected variables: a solution to RFID security and privacy under corruption with temporary state disclosure. *IEEE Transactions on Information Forensics and Security*, 16:999–1013, 2020.

[36] Ferucio Laurentiu Tiplea and Cristian Hristea. Practically Efficient RFID Scheme with Constant-time Identification. In *SECRYPT*, pages 495–506, 2021.

[37] Serge Vaudenay. On privacy models for RFID. In *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'07, pages 68–87, Berlin, Heidelberg, 2007. Springer-Verlag.

[38] Ferucio Laurențiu Țiplea, Cristian Hristea, and Rodica Bulai. Privacy and reader-first authentication in Vaudenay's RFID model with temporary state disclosure. *Computer Science Journal of Moldova*, 90(3):335–359, 2022.

[39] Ferucio Laurențiu Țiplea, Cristian Hristea, and Rodica Bulai. Privacy and mutual authentication under temporary state disclosure in RFID Systems. In *Electronics, Communications and Computing*, pages 119–124, 2023.