REZUMATUL TEZEI DE DOCTORAT

„Eficientizarea caracterului de confidențialitate în sistemele publice de gestiune a informațiilor cu caracter personal”

Autor: ing. Narcis-Florentin ANTONIE

Email: narcis.antonie@yahoo.com, tel: 0744 753 198

Conducător de doctorat: prof.univ.dr.ing. Ciprian Răcuciu

Lucrarea începe cu o parte introductivă în care sunt prezentate câteva elementele de bază în domeniul criptografiei precum și elemente istorice care au dus la evoluția domeniului criptografie.

În **capitolul 1** sunt descrise noțiunile de bază în criptografie, terminologia folosită și sunt prezentate elemente de bază în comunicații cum ar fi stivele de protocoale și necesitatea standardizării acestora. Sunt prezentate elemente generale în domeniul securității comunicațiilor și este detaliată funcționarea câtorva algoritmi de criptare de tip bloc, precum și a algoritmului OTP. La finalul capitolului este descrisă o alternativă în domeniul criptografiei și anume criptografia cuantică.

Capitolul 2 descrie una dintre cele mai populare și implementate suite de protocoale de securitate, și anume IPSec. Capitolul se încheie cu descrierea testelor de laborator executate de autor în vederea determinării performanțelor din punct de vedere al întârzierii introduse de diferiți algoritmi de criptare de tip bloc.

Capitolul 3 introduce noțiunea de structură de calcul distribuită și descrie elemente de securitatea informațiilor în astfel de structuri. Aici sunt prezentate serviciile de stocare în „*cloud*” precum și problemele legate de stocarea datelor în astfel de sisteme. Acest capitol descrie soluțiile pentru a rezolva unele dintre aceste probleme.

Capitolul 4 descrie în detaliu două sisteme publice care gestionează informații cu caracter personal, sistemul electronic național al asigurărilor de sănătate și sistemul electronic național de evidență a populației. Aceste sisteme fiind cele vizate în această lucrare pentru eficientizarea caracterului de confidențialitate prin introducerea de semnături anonime.

În **capitolul 5** se descrie conceptul de semnătură anonimă în contextul diferențierii acesteia de semnăturile digitale standard. Sunt descrise conceptele de semnătură anonimă propuse de alți autori și se descrie aplicabilitatea acestor scheme în practică prin patru exemple concrete de aplicabilitate.

Acest capitolul se încheie prin descrierea a trei variante de scheme de semnături digitale anonime inovative propuse de autorul acestei teze. Aceste variante presupun introducerea în schema de semnătură anonimă a unui algoritm de criptare simetric descris la capitolul 1 al acestei lucrări.

Capitolul 6 reprezintă propunerile efective ale autorului pentru eficientizarea caracterului de confidențialitate al celor două sistemele publice de gestiune a informațiilor cu caracter personal descrise la capitolul 4. Ambele propuneri se bazează pe câte o schemă de semnături anonime concepută de autor în capitolul 5. De asemenea este prezentată o idee de cercetare viitoare pentru introducerea semnăturilor anonime în cadrul unui sistem complex de evidență a populației și management al informațiilor personale ce folosește carduri inteligente și date biometrice.

Capitolul 7 descrie modul de implementare practică al unei semnături anonime descrise la capitolul 5 folosind un card inteligent. Capitolul începe cu o descriere a cardurilor inteligente și continuă cu descrierea algoritmului de implementare practică a soluției. Este descrisă aplicația dezvoltată și modul de funcționare al acesteia cu rezultatele unor scenarii de testare concepute de autor.

Capitolul 8 reprezintă secțiunea de concluzii și rezultate experimentale în care sunt evaluate rezultatele activității depuse pe parcursul scolii doctorale și ca rezultat al activităților de cercetare care se regăsesc în cuprinsul lucrării. Sunt precizate conceptele științifice moderne privitoare la asigurarea confidențialității datelor personale și asigurarea cerințelor impuse de legislația Europeană în vigoare (GDPR – „General Data Protection Regulation).

În finalul capitolului este precizată activitatea publicistică și stagiile de cercetare efectuate de autor, în legătură cu tematica abordată în teza de doctorat. De asemenea sunt descrise posibile direcții de cercetare viitoare și sunt punctate elementele de contribuție personală și originalitate aduse de autor în tematica studiată.

Ultimele secțiuni din structura lucrării reprezintă referințele bibliografice, glosarul de abrevieri, lista cu figuri și tabele și anexele la lucrare care detaliază unele aspecte practice descrise în teză.