Raport științific și tehnic in extenso pentru proiectul *Modele avansate de proiectare și evaluare a sistemelor criptografice moderne – ADECS*

Etapa I

Analiza mecanismelor de securitate pentru smartphone-uri.

Analiza și proiectarea testării și a procedurilor de evaluare.

Cuprins

Introducere

Proiectul Modele avansate de proiectare și evaluare a sistemelor criptografice moderne – ADECS (Advanced models for the design and evaluation of modern cryptographic systems) își propune să dezvolte capabilități în domeniul cercetării privind mecanismele de securitate privind protecția informațiilor pe dispozitive mobile, smartphones și tablete, și a evaluării și certificării produselor de securitate informatică. Etapele proiectului cuprind:

1. Analiza mecanismelor de securitate pentru dispozitive mobile, smartphones și tablete, precum și analiza și proiectarea testării și evaluării produselor de securitate informatică
2. Elaborarea de soluții pentru protecția informațiilor pe dispozitive mobile
3. Implementarea soluțiilor de protecție a informațiilor clasificate și a unui sistem de testare și evaluare
4. Testarea implementării
5. Diseminarea rezultatelor

În proiect sunt implicate companii private, institute de cercetare și mediul academic. Coordonatorul consorțiului este certSIGN SA, companie din România cu tradiție în dezvoltarea aplicațiilor de securitate informatică ce utilizează mecanisme bazate pe criptografia cu chei publice. Ca parteneri participă: Academia Tehnică Militară (ATM), Agenția de Cercetare pentru Tehnică și Tehnologii Militare (ACTTM) și UTI Grup SA.

Descrierea etapei și a activităților

Prima etapă a proiectului cuprinde Analiza mecanismelor de securitate pentru smartphone-uri și Analiza și proiectarea testării și a procedurilor de evaluare. Etapa a cuprins 6 activități și livrabilele aferente:

1. Activitatea I.1 Elaborarea unui studiu detaliat pentru mecanismele existente de criptare cu aplicabilitate în domeniul de echipamente mobile, cu livrabilele:
    a. Studiu privind mecanismele de securitate pe dispozitivele mobile
    b. Articol privind mecanismele de securitate pe dispozitivele mobile. Articolul urmează a fi prezentat la conferința internațională SECITC organizată de către ATM în 2013 (www.secitc.eu).
2. Activitatea I.2 Realizarea analizei cu privire la punerea în aplicare a unor algoritmi bazati pe curbe eliptice în hardware, folosind tehnologia FPGA, cu livrabilul:
    a. Studiu privind implementarea algoritmilor criptografici bazați pe curbe eliptice utilizând tehnologia FPGA
3. Activitatea I.3 Realizarea analizei funcţionale pentru soluţia de criptare a comunicaţiilor de voce, cu livrabilele:
    a. Cerințe privind criptarea de voce pe dispozitive mobile
    b. Articol privind criptarea de voce pe dispozitivele mobile. Articolul urmează a fi prezentat la conferința internațională SECITC organizată de către ATM în 2013 (www.secitc.eu).
4. Activitatea I.4 Fundamentarea tehnico-ştiinţifică a proiectului, cu livrabilul:
    a. Documentarea tehnico-științifică a proiectului

5. Activitatea I.5 Proiectarea unui model experimental a algoritmilor de criptare pentru evaluarea platformei de testare, cu livrabilele:
    a. Documente de proiectare a platformei de testare-evaluare a algoritmilor criptografici
    b. Articol privind platforma de testare-evaluare a algoritmilor criptografici. Articolul urmează a fi prezentat la conferința internațională organizată de cptre ACTTM
6. Activitatea I.6 Proiectarea platformei de evaluare a securitatii pentru produse IT, în conformitate cu standardele FIPS 140-2, cu livrabilul:
    a. Proiectarea platformei de testare - evaluare pentru produse de securitate IT în conformitate cu standardul FIPS 140-2/Common Criteria

Activitatea I.1 Elaborarea unui studiu detaliat pentru mecanismele existente de criptare cu aplicabilitate în domeniul de echipamente mobile

În cadrul activității I.1 a fost realizat un studiu cu privire la cerințele de securitate în ceea ce privește protecția datelor pe dispozitivele mobile și a mecanismelor de criptare existente. Studiul a avut în vedere sistemele de operare cele mai răspândite și a considerat că, indiferent de tipul dispozitivului, smartphone sau tabletă, cerințele și metodele de protecție sunt similare.

Din punct de vedere al cerințelor de securitate, acestea includ: stocarea datelor pe dispozitiv, autentificare utilizatorului pentru a accesa dispozitivul, E-mail, SMS, voce, interfațare cu alte dispozitive, ștergere date, Data Lost Prevention (DLP), ștergere datelor la distanță, Utilizarea tehnologiei NFC (NerField Communication).

În acest moment piața dispozitivelor mobile este neomogenă, incluzând o serie de producători majori pentru sistemele de operare care sunt instalate pe echipamente: Google Android, Apple iOS, BlackBerry OS, Symbian, Microsoft Windows și alți producători mai mici.

Cota de piață cea mai mare este ocupată de dispozitivele care ruleaza sistemele de operare Android și iOS, acestea fiind folosite atât de persoane particulare cât și de mediul de afaceri, acolo unde BlackBerry a deținut în trecut o poziție importantă. Au fost analizate mecanismele de protecție atât din punct de vedere al funcționalităților oferite nativ de fiecare producător cât și din perspectiva posibilității de a dezvolta aplicații care să ruleze pe aceste echipamente. Astfel, există posibilitatea de autentificare a utilizatorilor pentru acces la telefon, ștergerea la distanță a datelor sau criptarea conținutului. Niciunul dintre sistemele de operare nu oferă funcționalități de criptare a vocii, singurul mecanism de protecție fiind, de fapt, criptarea oferită de standardul GSM și de implementarea acestuia de către operatorul de telefonie mobilă unde sunt folosite Gaussian Minimum Shift Keying (GMSK) modularea digitala și Time Division Multiple Access (TDMA). Aceste mecanisme de securitate sunt vulnearbile iar criptarea GSM a fost spartă.

Mecanismele necesare pentru protecția datelor pe dispozitivele mobile trebuie să utilizeze algoritmi criptografici puternici, care să garanteze sigurnața informațiilor. A fost analizată posibilitatea implementării algoritmilor criptografici "clasici" fața de implementarea algortitmilor care utilizează curbe eliptice, mecanismele de generare și distribuție a cheilor precum și cel de gestiune a dispozitivelor mobile și a cheilor criptografice.

Din perspectiva implementării mecanismelor de securitate, a fost realizată o comparație între sistemele de operare Android și iOS. Pentru ambele sisteme de operare procesele și aplicațiile rulează într-un sandbox, creând în acest fel un mediu de lucru izolat, care previne accesul la resursele deținute de sistemul de operare sau de alte aplicații. Acest lucru poate îngreuna lucrul dezvoltatorilor software iar abordarea impusă de producătorul sistemului de operare trebuie urmată. Distribuția aplicațiilor se realizează, în cazul Android, direct pe telefon, prin intermediul Google Play sau al altor directoare de aplicații on-line. Controlul asupra aplicațiilor nu este strict, prin urmare au existat situații în care aplicațiile publicate pe aceste directoare de aplicații conțineau viruși.

În cazul iOS aplicațiile sunt instalate exclusiv prin intermediul App Store. Pentru a fi publicată aici fiecare aplicație trece printr-un proces riguros de verificare desfășurat de Apple, astfel că utilizarea anumitor bibliteci, ca de exemplu biblioteci criptografice externe, sau a anumitor resurse poate să fie interzisă. Rezultatul este faptul că Apple a reușit să împiedice publicarea virușilor, creând un mediu mai sigur pentru utilizatori, dar, în același timp, dezvoltarea unor aplicații cu cerințe speciale este mai dificilă.

Un alt element important îl reprezintă interoperabilitatea și posibilitatea de a transmite informații într-un format standard între dispozitive mobile pe care rulează sisteme de operare diferite sau între dispozitivele mobile și calculatoare.

Au fost analizate următoarele direcții majore:

- Protecția e-mail și SMS: politica iOS este ca ori de câte ori o aplicație utilizează un serviciu pentru care utilizatorul este taxat de către operatorul de telefonie, de exemplu pentru transmiterea unui SMS sau MMS, utilizatorul trebuie să dea explicit acceptul pentru realizarea acelei operațiuni. Astfel, utilizatorul trebuie să parcurgă mai mulți pași pentru a utiliza o aplicație a unui terț.Android are o politică mai permisivă din acest punct de vedere.
- Implementarea mecanismelor criptografice este posibilă prin mai multe abordări:
    - Utilizarea API de securitate ai sistemului de operare: abordare fezabilă atunci când sunt dezvoltate aplicații pentru un singur sistem de operare
    - Utilizarea bibliotecilor openSSL: fezabil atunci când sunt dezvoltate aplicații pentru cel mult două sisteme d eoperare. Este ușor de păstrat compatibilitatea între fișiere, SMS și e-mail.
    - Utilizarea bibliotecilor openSSL împreună cu un wrapper deaspura acestora: permite dezvoltarea aplicațiilor pentru toate sistemele de operare, wrapperul asigurând interoperabilitatea.
- Interoperabilitatea între mai multe platforme: utilizarea openSSL oferă o fundație puternică, pentru care există garanții privind securitatea, și permite atât compilarea și integrarea bibliotecilor pe Android și iOS cât și interoperabilitatea cu alte oluții ce utilizează openSSL. Nu există însă un build openSSL standard de la care să se obțină direct bibliotecile pentru Andriod și iOS, este necesar un efor suplimentar pentru adaptarea fișierelor de configurare și chiar a codului sursă. Rezultatele obținute trebuie testate.
- Crearea semnăturilor electronice pe mobil: nu există standarde iar cadrul legal îngreunează crearea semnăturilor electronice cu valoare legală utilizând dispozitivele mobile.

Din punct al vedere al performanțelor sistemele de operare sunt similare, fără diferențe sesizabile pentru operațiuni punctuale realizate de un utilizator. În cazul realizării unor baterii de teste cu un număr mare de operațiuni pot exista diferențe date de platforma hardware pe care rulează sistemul de operare respectiv.

Activitatea I.2 Realizarea analizei cu privire la punerea în aplicare a unor algoritmi bazati pe curbe eliptice în hardware, folosind tehnologia FPGA

In cadrul activitatii I.2 s-a realizat un studiu analitic cu privire la metodele de implementare practica a algoritmilor criptografici bazati pe curbe eliptice (ECC – *Eliptic Curve Cryptography*), a posibilitatilor de aplicare a acestora in practica, dar si din punctul de vedere al avantajelor obtinute prin implementarea acestora folosind tehnologii hardware de tip FPGA. In cadrul studiului s-au avut in vedere aspecte cum ar fi matematica curbelor eliptice aplicabile in criptografie, schemele notabile ale criptografiei cu chei publice bazata pe curbe eliptice, rezultatele obtinute in cadrul implementarilor realizate dealungul timpului in literatura de specialitate (*state of the art*), algoritmii de calcul si mecanismele principale folosite in cadrul acestor implementari, securitatea si vulnerabilitatile schemelor de tip ECC.

Sistemele criptografice bazate pe matematica curbelor eliptice (ECC) fac parte din familia sistemelor de criptare cu chei publice, aflandu-se in acest moment in plin proces de dezvoltare si maturizare. Studiile facute pana acum in literatura de specialitate arata faptul ca folosirea schemelor de tip ECC pot conduce la obtinerea celor mai eficiente sisteme de criptare cu chei publice. In comparatie cu sistemele criptografice clasice precum RSA, sistemele ECC permit obţinerea unui nivel de securitate echivalent folosind chei de dimensiuni mult reduse (aproximativ cu un ordin de marime mai mici) ceea ce duce la creşterea performanţelor sistemului prin scurtarea timpilor de execuţie şi reducerea spaţiului de memorare, a benzii de reţea şi a puterii consumate. S-a demonstrat faptul că pentru a obţine un anumit nivel de securitate, de exemplu RSA/DSA necesită chei de 1024 biţi pe când în cazul ECC sunt suficienţi doar 160 biţi. Pe măsură ce nivelul de securitate creşte adica dimensiunea cheilor se mareste raportul privind dimensiunile cheilor respective si implicit al performantelor amintite este net în favoarea ECC. Implementările optimizate, software sau hardware ale acestor sisteme au demonstrat faptul că generarea de semnături electronice este cu un ordin de mărime mai rapidă în cazul ECC faţă de RSA sau DSA. Timpii de verificare a semnăturilor sunt însă comparativi ca valoare. Aceste elemente plaseaza schemele ECC ca fiind cele mai potrivite in a fi folosite in contextul urmatoarelor tipuri de aplicatii:

- Aplicaţii ce folosesc în mod intensiv operaţii criptografice cu chei publice. Sistemele electronice de plată şi în general aplicaţiile de comerţ electronic se încadrează în această categorie.

- Aplicaţii în care puterea de calcul, capacitatea de memorare sau banda de reţea sunt limitate. Cel mai elocvent exemplu de astfel de aplicaţii sunt cele în care se folosesc dispozitive wireless, smart card-uri criptografice sau **dispozitive de calcul mobile** (telefoane inteligente, tablete, etc).

Operatia de baza in criptografia pe curbe eliptice este cea de multiplicare a unui punct de pe curba eliptica cu un scalar adica, calculul lui $Q = kP$ unde k este un scalar (numar intreg mare), iar P este un punct al curbei folosite. Calculul lui $Q = kP$ este realizat in general printr-o secventa de adunari de doua puncte si de dublari a unui punct, operatiile de baza necesare la nivelul curbei eliptice. Aplicabilitatea curbelor eliptice in criptografie si relevanta operatiei de multiplicare a unui punct cu un scalar se bazeaza pe **dificultatea rezolvarii problemei logaritmului discret pe curba eliptica**. Mai concret, fiind date un scalar k si un punct de pe

curba *P*, rezolvarea calculului $Q = kP$, din punct de vedere al complexitatii calculelor se poate face in timp polinomial, insa obtinerea lui *k* cand sunt date punctele *P* si *Q* (unde $Q = kP$) implica complexitati de calcul mult mai mari. In aceste conditii, unul din obiectivele principale urmarite in implementarile schemelor de tip ECC este acela de a obtine metode cat mai optime de calcul pentru $Q = kP$.

Una din problemele avute in vedere in aceasta etapa a proiectului a fost aceea de a studia si sintetiza principalele metode si algoritmi de calcul pentru operatia de multiplicare a unui punct al curbei eliptice cu un scalar. Din acest punct de vedere am constatat ca exista o multime de astfel de metode propuse insa doar cateva sunt folosite in practica datorita avantajelor oferite: complexitatea cat mai scazuta, necesarul de spatiu de stocare si binenteles performantele de viteza. Metoda cel mai des folosita este cea de tipul *dubleaza şi aduna*. Ea este bazata pe reprezentarea binara a lui k. Astfel, dacă $k = \sum_{i=0}^{l-1} k_i 2^i$, unde $k_i \in \{0,1\}$, atunci kP poate fi calculat astfel:

$$kP = \sum_{i=0}^{l-1} k_i 2^i P = k_{l-1} 2^{l-1} P + k_{l-2} 2^{l-2} P + \ldots + k_1 2^1 P + k_0 P$$

Densitatea medie de biţi diferiţi de zero ai reprezentării în formă binară a lui *k* este aproximativ egală cu $l/2 \approx m/2$. Prin urmare, această metodă necesită aproximativ $m/2$ adunări şi *m* dublări de puncte, timpul total de execuţie fiind aproximativ egal cu $(1/2)mA + mD$ unde *A* reprezintă timpul necesar adunării a două puncte distincte iar *D* timpul necesar dublării unui punct. Pentru a reduce numărul de adunări din cadrul algoritmului de mai sus, se poate folosi reprezentarea lui *k* în *forma non-adiacentă*, $k = \sum_{i=0}^{l-1} k_i 2^i$, unde $k_i \in \{-1,0,1\}$, care are proprietatea că oricare ar fi doi biţi consecutivi k_i numai unul singur este diferit de zero. Forma non-adiacentă de lungime ω este o generalizare a acestei reprezentări în care fiecare digit k_i este impar, $|k_i| < 2^{\omega-1}$, şi oricare ar fi ω digiţi consecutivi k_i numai unul singur este diferit de zero. Orice număr întreg *k* are o reprezentare unică în formă non-adiacentă, notată $NAF_\omega(k) = (k_{l-1} \ldots k_1 k_0)$, de lungime cu cel mult un digit mai mare decât reprezentarea binară. Densitatea medie de digiţi diferiţi de zero ai reprezentării în formă non-adiacentă a lui *k* este aproximativ egală cu $1/(\omega+1)$. Timpul total de execuţie al algoritmului *NAFω* este de aproximativ $(1D + (2^{\omega-2} - 1)A) + (m/(\omega+1)A + mD)$. Dacă punctul *P* este fixat, timpul de înmulţire a acestuia cu un scalar poate fi redus prin calcularea în avans şi memorarea unor valori care depind de *P*. De exemplu, dacă se calculează în avans şi se memorează valorile $P, 2P, 2^2 P, \ldots, 2^{l-1} P$ atunci se pot elimina toate operaţiile de dublare de puncte din algoritmii de tip *dubleaza si aduna*. În cazul în care *m=163*, ar trebui memorate 163 puncte. Ţinând cont pentru a memora un punct sunt necesari *21+21=42* octeţi, asta înseamnă un total de 6.846 octeţi. Această abordare nu poate fi folosită direct pentru dispozitive cu capcitate redusa de memorare (cum ar fi smart card-urile) având în vedere spaţiul de memorare limitat al acestora.

O solutie alternativa o constituie metodele de tipul înjumătăţire şi adunare. In acest sens, cea mai importantă optimizare pentru înmulţirea cu un scalar a unui punct a fost realizată de E. Knudsen care a propus înlocuirea operaţiilor de dublare de puncte cu operaţii mai rapide de înjumătăţire a punctelor. Tabelul de mai jos sintetizeaza cateva metrici privind costul unei

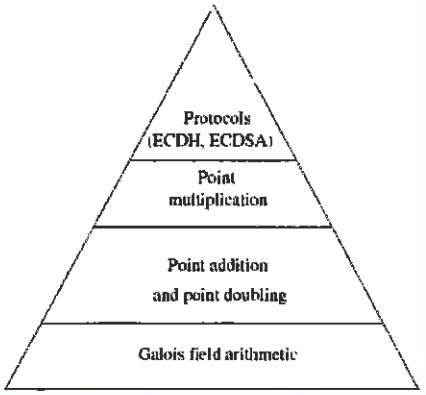
operaţii de înmulţire cu un scalar a unui punct pentru curbele eliptice de tip $E(F_{2^{163}})$ folosind diverse pentru multiplicare diverse metode analizate in studiu:

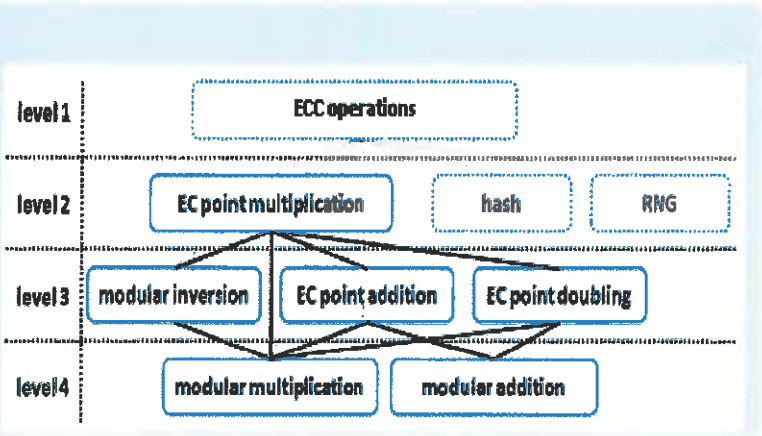
Metoda	**Memorie necesară (octeţi)**	**Nr. de operaţii asupra punctelor de pe curba eliptică**	**Nr. de operaţii în corpul binar** $F_{2^{163}}$ *(I=8M)*
Dublare şi adunare	0	$(163/2)A+163D$	2445*M*
Înjumătăţire şi adunare	81·21+21+21 (1743 octeţi)	$(163/2)A'+163H$	1060*M*
Dublare şi adunare (NAF, $\omega=4$*)*	0	$(1D+3A)+(163/5A+163$	1996*M*
Înjumătăţire şi adunare (NAF, $\omega=4$*)*	81·21+21+21 (1743 octeţi)	$(1D+3A)+(163/5A'+163$	725*M*

Un alt aspect observat pe timpul analizei facute este acela ca modelul matematic specific criptografiei pe curbe eliptice este unul de tip cascada: operatiile necesare pentru implementarea schemelor de criptare si decriptare ECC sunt implementate pe baza operaţiei de multiplicare realizate asupra punctelor de pe curba eliptica astfel:

- **inmulţirea cu un scalar a unui punct** de pe curba eliptică. Aceasta operatie se bazează mai departe pe operatii de
    - **adunare a două puncte**, de **dublare a unui punct** si de **inversare a unui punct** de pe curba eliptica. Acestea, la randul lor sunt realizate prin
        - **adunarea modulara, scăderea modulara, multiplicarea modulara** si **inversarea modulara**, operatii fundamentale realizate in campul finit utilizat F(p) sau F(2^m).

Această ierarhie a operaţiilor criptografiei pe curbe eliptice poate fi reprezentată sub forma unei stive cu patru nivele, în care fiecare nivel depinde de implementarea nivelului de mai jos.





Un element important folosit in algoritmii de calcul ECC este metoda de reprezentare a coordonatelor punctelor. Metoda traditionala (cunoscuta sub denumirea de reprezentare afina) foloseste sistemul cartezian clasic cu doua coordonate (x, y). S-a constatat insa ca exista metode de reprezentare mai performante ce folosesc 3 valori pentru reprezentarea unui punct (X, Y, Z). Acestea sunt numite coordonate proiective iar avantajul obtinut este dat de faptul ca in cadrul operatiilor aritmetice realizate asupra punctelor se pot elimina anumite operatii costisitoare cum ar fi inversarea unui punct de pe curba sau in campul finit de lucru. Adunarea a două puncte în coordonate afine foloseşte o inversare. În general, inversarea peste un câmp este o operaţie foarte costisitoare din punct de vedere al complexităţii. Astfel, multiplicarea scalară a unui punct în coordonate afine va folosi foarte multe inversări, ceea ce nu este avantajos din punct de vedere al eficienţei. Multiplicarea scalară a unui punct în coordonate proiective foloseşte o singură inversare, la sfârşitul operaţiei de multiplicare, in acest sens fiind preferată acest tip de reprezentare. Utilizarea coordonatelor proiective necesită o conversie initiala a coordonatelor afine în coordonate proiective, efectuarea calculelor in coordonate proiective, iar apoi la final, conversia coordonatelor proiective ale punctului obtinut la coordonatele sale afine.

Principalul obiectiv al activitatii I.2 a fost acela de a studia posibilitatile de implementare a algoritmilor criptografici bazati pe curbe eliptice pe tehnologia hardware de tip FPGA. Flexibilitatea tehnologiei FPGA corelata cu posibilitatile acesteia de paralelizare si calcul distribuit confera acesteia un avantaj major in fata implementarilor software pe de o parte dar si in raport cu alte tehnologii hardware cum ar fi ASIC –urile (acestea din urma fiind mult mai putin permisive la nevoile continue de modificare). In acest sens in cadrul activitatii de cercetare s-au analizat o serie consistenta de materiale ce prezinta diverse tipuri de implementari recente (state of the art) de scheme criptografice de tip ECC in FPGA, majoritatea lor fiind realizate cu precadere in ultimii ani. Analiza facuta s-a concentrat pe tipurile de mecanisme folosite in cadrul implementarilor respective si a performantelor obtinute. Din analiza facuta am observat ca in cazul acestui tip de implementari exista doua tipuri de provocari majore:

- Reducerea suprafeţei FPGA ocupate de implementare. Reducerea gradului de ocupare la nivelul circuitelor FPGA, de implementarile realizate, se poate obtine in general numai în defavoarea vitezei de procesare. Exista insa aplicatii in care aspectul dimensiunii este mai important decât cel al vitezei:
    - Atunci când funcţionalitatea criptografică nu face parte din funcţiile de bază, şi prin urmare influenţa ei asupra vitezei totale este mică.
    - Atunci când comunicarea cu exteriorul se face rar, de exemplu în cazul reţelelor de senzori
    - Atunci cand schemele/protocoalele ce utilizeaza implementarea hardware din FPGA sunt paralelizabile, gradul mic de ocupare poate conduce la duplicarea unitatilor de calcul din FPGA si automat la obtinerea unor performante de calculelor imbunatatite prin paralelizarea operatiilor realizate.
- Cresterea vitezei de procesare pentru schemele implementate. În general majoritatea implementărilor realizate au ca scop direct sau indirect cresterea vitezei de realizare a operatiilor specifice. Reducand problema la nivelul cel mai de jos (calculele la nivelul campului finit) putem spune asadar ca eficienţa unei implementări hardware de tip FPGA in ceea ce priveste aritmetica necesara la nivelul câmpurilor finite de lucru este determinată pe baza a două criterii: complexitatea în spaţiu (cantitatea totală de resurse hardware

necesare pentru a implementa circuitul) şi complexitatea în timp (întârzierea totală a circuitului respectiv).

Din analiza facuta cadrul proiectului putem afirma ca modelul general de diagrama bloc pentru un coprocesor criptografic de tip ECC implementat in FPGA poate fi format din urmatoarele componente (se pot vedea si grafic in figura):

a) **Interface block** – controlează comunicaţia dintre procesorul principal (sistemul gazda) şi coprocesorul criptografic.

b) **Parameter generation block** – calculează anumiţi parametri importanţi folosiţi in criptografia ECC (cum ar fi de exemplu cheia publică), şi se ocupă de conversia mesajului text primit în punctul corespunzător de pe curba eliptică.

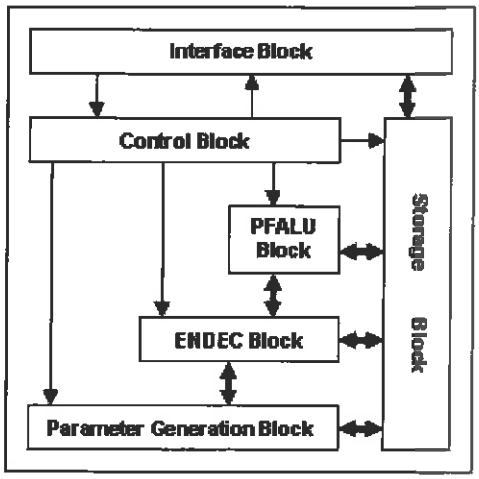
c)**Prime/Binary field arithmetic logic unic block** – implementează operaţiile fundamentale peste câmpul finit (adunarea, scăderea inversarea si multiplicarea modulară – pentru câmpurile GF(p), şi respectiv adunarea, scăderea, multiplicarea, inversarea şi ridicarea la pătrat pentru câmpurile GF(2^n)), precum şi operaţiile de bază pentru curba eliptică (adunarea, scăderea punctelor, dublarea punctelor, multiplicarea scalară a punctelor).

d) **Encryption/Decryption block** – realizează primitivele de criptare sau decriptare ale schemei ECC implementate.

e) **Control block** – controlează modul de operare ale celorlalte blocuri funcţionale ale coprocesorului şi permite configurarea coprocesorului astfel încât să realizeze operaţii peste câmpul finit şi/sau operaţii peste curba eliptică.

f) **Storage block** – memorează valorile de intrare, de ieşire şi cele intermediare.

Un aspect important pe care l-am observat in implementarile hardware analizate este selectarea metodelor de calcul ce pot optimiza calculele la nivelul campului finit de lucru, in functie de tipul acestuia. Astfel, alegerea corecta a algoritmilor poate conduce la imbunatatirea semnificativa a performantelor de calcul la nivelul intregului sistem criptografic.



De exemplu, in cazul campurilor binare GF (2^m), adunarea a două elemente a şi b reprezentate polinomial şi constă de fapt în adunarea celor două polinoame a(x) şi b(x), a căror coeficienţi sunt adunaţi în GF(2). Prin urmare adunarea constă într-o operaţie XOR între vectorii a şi b, operatie extrem de simplu de realizat hardware. Circuitul care realizează adunarea a două elemente peste GF(2m) este in general implementat sub forma unui circuit XOR pentru două registre de lungime m. Ieşirea poate fi asigurată într-un registru, într-un singur ciclu de ceas.

Pentru a putea realiza multiplicarea a două elemente a şi b din GF(2m) este nevoie de un polinom ireductibil de grad m, p(x). Este evident că alegerea unui polinom sau a altuia va duce la reprezentări diferite ale câmpului finit. Multiplicarea peste GF(2^m) poate fi implementată în mai multe moduri, circuitul multiplicator putand fi implementat şi el prin mai multe arhitecturi:

- Printr-o arhitectură de vector sistolic
- Printr-o matrice course-grained de unităţi modulare
- Prin utilizarea blocurilor multiplicatoare de pe FPGA
- Prin utilizarea blocurilor DSP de pe FPGA

In acest moment exista o serie de algoritmi de multiplicare modula, algoritmi folositi in majoritatea implementarilor FPGA intalnite: algoritmul de multiplicare Montgomery (circuit implementat sub forma unui vector sistolic de lungime variabila m si de lungime variabila a cuvantului w si care permite ca frecventa ceasului sa fie dependenta numai de lungimea cuvantului w, nu si de lungimea m), algoritmul Karatsuba-Ofman (are complexitate sub O(m^2), dar impune o serie de restricţii asupra lui m), cu diverse variante (Karatsuba-Ofman binar si Karatsuba-Ofman hibrid), multiplicatorul Massey-Omura (multiplicator serial la nivel de biţi), etc.

Tipul câmpului	**Număr biţi**	**Platformă**	**Tip multiplicator**	**Paralelizare**	**Durată execuţie Multiplicare scalară (microSecunde)**	**Referinţă (vezi raportul extins)**
GF(2^n)	163	Altera EPF10K200SBC600-1	Standard dublează şi aduna	Nu	14900	[19]
GF(2^n)	160	Xilinx Virtex XCV800-4-HQ240	Montgomery	Nu	3810	[54]
GF(2^n)	283	Xilinx Virtex 4 XC4VFX140-FF1517-11	Montgomery	Nu	3040	[8]
GF(2^n)	191	Xilinx XCV2600E	Karatsuba-Ofman binar, parallel	Da	63	[52]
GF(2^n)	11	Actel IGLOO AGLN250V2-VQFP100 **Nano**	Massey-Omura	Nu	62.08333	[21]
GF(p)	192	Altera Cyclone II EP2C70F896C8	nu este specificat	Nu	59.93	[53]
GF(2^n)	163	Stratix IV GX EP4SGX230KF40C2	Multiplicare window pe curbe Koblitz cu utilizarea endomorfismului	Da	8.3	[57], [59]

			Forbenius			
GF(2^n)	233	Xilinx Virtex 4	Karatsuba-Ofman hibrid	Nu	0.877	[61]

Un aspect important analizat a fost bineinteles cel al performantelor de viteza. Tabelul urmator prezinta un set de rezultate intalnite si sintetizate pe parcursul implementarilor studiate. Performantele de viteza depind intotdeauna in primul rand de dimensiunea cheilor (dimensiunea campului finit pe care se lucreaza) dar si de tipul de camp, de faptul ca exista sau nu paralelizare la nivelul implementarii dar si de platforma hardware unde s-a testat implementarea (familia sau generatia de circuit FPGA). Performantele de viteza sunt in general contorizate ca numar de ciclii de ceas sau ca timp efectiv de calul. Frcventa maxima la care pot rula unitatile de calcul constituie un aspect important in stabilirea performantei unei implementari de ECC in FPGA. Tabelul urmator prezinta doar o parte din rezultatele analizate si exprima performanta ca si timp de executie (microsec).

Un ultim aspect analizat in aceasta activitate a fost cea legata de securitatea si vulnerabilitatile schemelor de tip ECC. Au fost parcurse o serie de atacuri documentate in literatura de specialitate: atacul Pohlig – Hellman, atacul BSGS (Baby-Step / Giant-Step), atacul Pollard-Rho, atacul MOV, Atacul Smart. Acestea au fost punctate mai pe larg in raportul tehnic extins. Concluzia este aceea ca prin alegerea unei curbe eliptice neadecvate, problema ECDLP poate deveni ușor de rezolvat. Acest fapt poate conduce la scăderea drastică a securității sistemului criptografic de tip ECC bazat pe schema/curba respectiva. In urma analizei acestor tipuri de atacuri reies asadar cateva conditii necesare in alegerea curbelor eliptice. Acestea ar trebui sa satisfaca cumulativ cel putin urmatoarele proprietati:

- Numărul de puncte ale curbei eliptice (îi spunem $card(E(F_q))$)nu trebuie să aibă divizori primi mici;
- Curbele nu trebuie să fie definite peste corpuri de forma F_q, unde q este o putere netrivială a caracteristicii și $n > 1$;
- Cel mai mic număr n asa incat $card(E(F_q)) / q^n - 1$ trebuie să fie suficient de mare pentru ca problema logaritmului discret în F_2^n să fie dificilă;

Nu trebuie folosite curbe a.î. $E(F_q) \neq q$ (curbe eliptice cu urma Frobenius egală cu 1).

Activitatea I.3 Realizarea analizei funcţionale pentru soluţia de criptare a comunicaţiilor de voce

În cadrul activității I.4 a fost realizată analiza pentru stabilirea funcționalităților ce trebuie asigurate de soluția de criptare a comunicațiilor de voce.

A fost stabilit faptul că nu se vor utiliza tehnologiile de criptare ale standardului GSM deoarece acestea prezintă vulnerabilități. De asemenea, pentru a simplifica procesul de realizare a soluției, fără a fi necesară realizare unui echipament hardware dedicat care să cripteze comunicația înainte de a fi transmisă peste comunicația GSM, s-a stabilit faptul că funcționalitățile vor fi oferite prin intermediul unei aplicații care va realiza transmisia utilizând conexiunea de date disponibilă pe telefon.

Aplicația realizată va permite atât criptarea apelurilor de voce cât și realizarea unui sistem de mesagerie instant criptată.

A fost stabilită o arhitectură de tip stea, cu componentă centrală, care să gestioneze utilizatorii, cheile criptografice și conexiunile și componente distribuite, respectiv dispozitivele mobile, care sunt utilizate pentru schimbul de informații de către utilizatori.

Componenta centrală poate fi implementată de un operator și oferită ca un serviciu clienților săi sau poate fi implementată în cadrul unei organizații care să gestioneze utilizatorii proprii.

Pentru criptarea comunicației se vor avea în vedere două mecanisme: utilizarea criptografiei cu chei publice (PKI), unde fiecare utilizator deține un certificat digital pe care îl utilizează pentru criptarea comunicației de voce și date, și criptografia simetrică, unde sunt utilizate chei de criptare simetrice, gestionate centralizat și distribuite utilizatorilor pe suport de stocare extern.

Activitatea I.4 Fundamentarea tehnico-ştiinţifică a proiectului

În cadrul activității I.4 a fost realizată documentarea tehnico științifică a proiectului, atât din punctul de vedere al implementării mecanismelor de criptare cât și în ceea ce privește importanța testării și evaluării produselor și sistemelor informatice.

Au fost astfel identificate mecanismele tehnologice de implementare a securității dispozitivelor mobile în ceea ce privește transmisia de date și de voce în mod protejat. S-au stabilit cerințele tehnice privind aplicațiile care să realizeze aceste operații, cerințe utilizator privind funcționalitățile și ergonomia aplicațiilor.

Importanța testării - evaluării produselor de securitate IT

Divulgarea, modificarea, distrugerea sau deturnarea neautorizată a informaţiilor duc la prejudicii care pot induce consecinţe nefaste pentru cel are este deţinătorul de drept al acelor informaţiilor. De aceea primul obiectiv al unui produs sau sistem de securitate IT trebuie să fie acela de a reduce la un nivel acceptabil pentru organizaţia interesată, riscurile asociate. Acest obiectiv se atinge prin alegerea caracteristicilor şi funcţiilor de securitate pentru sistemul IT care minimalizează riscurile.

La îndeplinirea obiectivului de securitate a produselor sau sistemelor IT contribuie diverse procese. Acestea sunt ilustrate în figura 1. Această figură prezintă contextul ideal în care se înscrie evaluarea securităţii IT. Săgeţile indică faptul că fiecare proces furnizează datele pentru prelucrarea ulterioară de către celălalt proces. Procesele pot să se suprapună parţial. Înlănţuirea prelucrărilor este cel mai frecvent ciclică şi iterativă.

În cursul procesului de dezvoltare, este construit un sistem sau un produs IT. Acesta este examinat după criterii bine definite de evaluare a securităţii în cursul procesului de evaluare. Rezultatele evaluării şi aplicarea corectă a criteriilor de evaluare sunt confirmate în cursul procesului de certificare. Procesul de omologare a sistemului permite să se confirme că utilizarea unui sistem IT este acceptabilă într-un mediu particular şi într-un scop particular. În procesul de exploatare sigură, un sistem omologat este exploatat conform procedurilor

agreate, dar schimbările aduse mediului pot antrena nevoia modificării sistemului care se repercutează asupra procesului de dezvoltare.

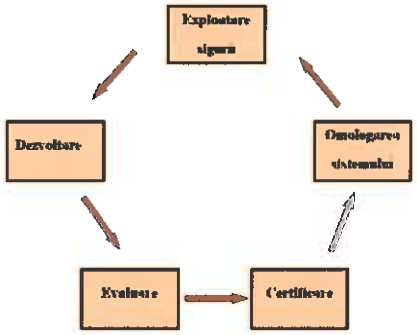


Figura 1 Procesele care se înscriu în cadrul securității IT

În consecinţă, securitatea a devenit un aspect esenţial al IT. Majoritatea utilizatorilor însă nu au cunoştinţele sau resursele necesare pentru a judeca cât de sigure din punct de vedere al securităţii sunt aceste produse sau sisteme IT. Aceştia vor să cunoască gradul de încredere pe care ei îl pot avea în securitatea oferită de produselor sau sistemelor IT. Acest grad de încredere poate fi obţinut printr-o estimare a securităţii produsului sau sistemului în raport cu criteriile de securitate stabilite şi recunoscute la nivel naţional şi internaţional.

Evaluarea securității IT reprezintă o apreciere independentă a unei ținte de evaluare (TOE) constând din analiză și testare cu scopul de a se asigura că TOE nu are vulnerabilități exploatabile. Scopul unei evaluării a securității IT este acela de a determina dacă contramăsurile pe care le implementează TOE sunt eficiente în combaterea amenințărilor identificate la adresa activelor ce necesită protecție. Rezultatele unei evaluări pot ajuta dezvoltatorii IT să își îmbunătățească produsele și utilizatorii să determine dacă un anumit produs sau sistem IT îndeplinește cerintele lor de securitate.

De evaluarea proprietăţilor de securitate a produselor şi sistemelor IT sunt interesaţi atât utilizatorii cât şi dezvoltatorii de produse IT, astfel de-a lungul timpului s-a acordat o atenţie sporită acestui subiet încercându-se elaborarea unor criterii de securitate care să fie recunoscute la nivel internaţional.

Procesul de testare - evaluare a produselor de securitate IT

Evaluarea securității IT conform unor anumite criterii cuprinde un examen aprofundat al unui produs pentru cercetarea vulnerabilităților și vizează determinarea în ce măsură specificaţiile de securitate ale produsului evaluat sunt satisfăcute de realizarea lor.

Evaluarea corespunde unei estimări a securităţii oferite de un anumit produs sub următoarele două aspecte:

- **conformitate**: se estimează dacă funcţiile şi **mecanismele dedicate securităţii** furnizate de produs sunt realizate corect,
- **eficacitate**:

- se estimează dacă funcţiile şi mecanismele dedicate securităţii furnizate de produs satisfac efectiv obiectivele de securitate declarate;
- se estimează capacitatea mecanismelor dedicate securităţii de a rezista atacurilor directe.

Evaluarea este realizată de către experţi în securitate, în raport cu criterii de securitate stabilite şi conforme cu un anumit standard. De evaluarea proprietăţilor de securitate a produselor şi sistemelor IT sunt interesate trei grupuri: utilizatorii TOE, dezvoltatorii TOE şi evaluatorii TOE. Pentru buna desfăşurare a acestui proces este necesar un parteneriat între cele trei grupuri.

Obiectivul procesului de evaluare este de a permite evaluatorului să pregătească un raport imparţial care să indice dacă sistemul sau produsul IT satisface sau nu ţinta sa de securitate cu gradul de încredere precizat prin nivelul de evaluare declarat.

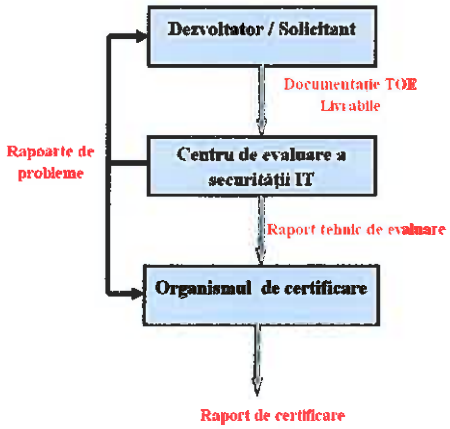


Figura 2 Procesul de evaluare şi certificare

Procesul de evaluare este guvernat de criteriile de evaluare (ex: FIPS, ITSEC şi CC), metodologiile de evaluare (ex: DTR pentru FIPS, ITSEM şi CEM) şi de schemele naţionale de evaluare.

Criteriile de evaluare reprezintă baremul faţă de care poate fi măsurată securitatea unui produs sau sistem IT, pentru evaluarea, dezvoltarea sau achiziţia sa. Acestea definesc ceea ce trebuie să fie evaluat. **Metodologiile de evaluare** definesc modul de executare de către evaluator a sarcinilor cerute prin criteriile de evaluare. **Schemele naţionale** furnizează regulile de organizare care se aplică procesului de evaluare, de certificare şi de acreditare a laboratoarelor în termeni de rol, proceduri, drepturi şi obligaţii.

Orice organism de certificare naţional impune respectarea celor patru principii în schema naţională de certificare. Acest organism de certificare trebuie, în particular, să vegheze ca repetabilitatea şi reproductibilitatea rezultatelor testelor să fie acoperită de verdictul global al evaluării.

Procesul de evaluare cuprinde trei faze:

a) Faza I Pregătirea evalării;

b) Faza II Desfăşurarea evaluării;

c) Faza III Concluzia evaluării.

Prima fază a evaluării „Pregătirea evaluării" prezintă modul în care sunt furnizate resursele şi cum este manageriată evaluarea.

În faza a doua „Desfăşurarea evaluării" este realizată evaluarea propriu zisă a produsului de către evaluator pe baza criteriilor stabilite. Toate testele efectuate de evaluator, rezultatele obținute și recomandările propuse de evaluator sunt descrise în Raportul Tehnic de Evaluare. Acest raport va constitui baza pe care organismul de certificare va lua decizia cu privire la certificare.

Procesul de evaluare se încheie cu faza a treia "Concluzia evaluării" în care organismul de certificare examinează Raportul Tehnic de Evaluare în scopul de a determina dacă ţinta de evaluare satisface ţinta de securitate ţinând cont de toţi factorii exteriori din domeniul aplicării evaluării. Organismul de certificare fiind implicat în proces este capabil să atribuie un nivel de evaluare şi o rezistenţă minimă a mecanismelor. Concluziile sale sunt înregistrate în Raportul de certificare / Certificat care este un document public.

Activitatea I.5 Proiectarea unui model experimental a algoritmilor de criptare pentru evaluarea platformei de testare

În cadrul activității I.5 a fost realizată proiectarea platformei de testare-evaluare a algoritmilor criptografici.

Algoritmii criptografici reprezintă nucleul produselor de securitate IT. De aceea evaluarea acestora pe o platformă unitară și cu rezultate reproductibile este esențială. Platforma care va evalua algoritmii criptografici va fi dezvolta urmărind fluxul de lucru din figura de mai jos.

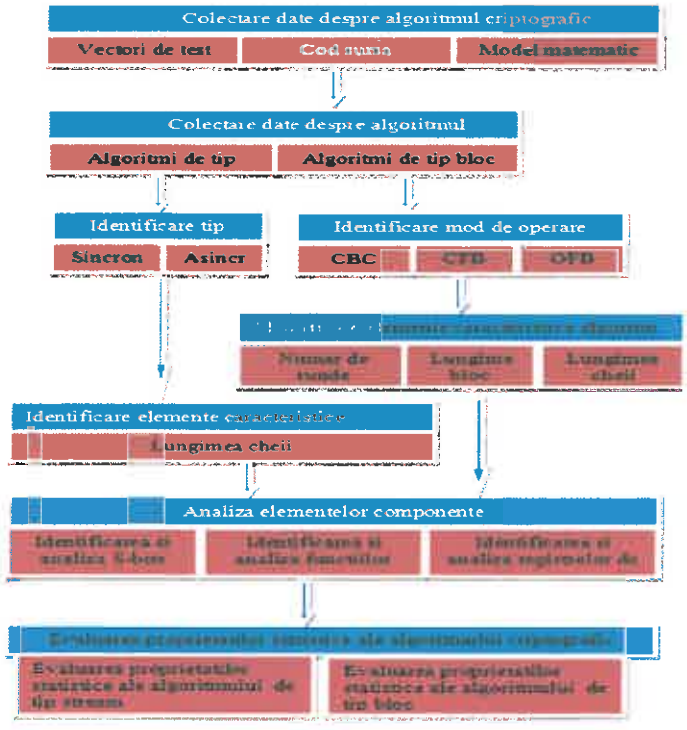


Figura 3 Fluxul evaluării algoritmilor criptografici

Testarea algoritmilor de tip stream si a celor de tip bloc se va realiza utilizând metodologia NIST prezentată în documentul SP 800-22. Bateria de teste statistice NIST constă din 16 teste statistice care au fost dezvoltate pentru a verifica aleatorismul unor secvenţe binare (de lungime arbitrară) generate în scopuri criptografice, cu ajutorul generatoarelor de numere aleatoare. Testele din cadrul bateriei NIST sunt:

1. Testul de frecvenţă (Monobit)
2. Testul de frecvenţă (bloc)
3. Testul secvenţial
4. Testul pentru secvenţa maximă de valori unu într-un bloc
5. Testul rangului matricelor binare aleatoare
6. Testul spectral al transformării Fourier discretă
7. Testul de potrivire a şablonului (neperiodic)
8. Testul de potrivire a şablonului (periodic)
9. Maurer's "Universal Statistical" Test
10. Testul de compresie Lempel-Ziv
11. Testul de complexitate liniară
12. Testul serial
13. Testul entropiei aproximate
14. Testul sumelor cumulative
15. Testul parcurgerilor aleatoare
16. Testul varianţei parcurgerilor aleatoare

Etapele necesare testării sunt:

- Generarea secvenţelor de test
- Testarea secvenţelor cu bateria NIST

Generarea secvenţelor de test

Testarea aleatorismului cifrurilor bloc cu bateria NIST implică construcţia a opt tipuri de date specifice fiecărui test în parte. Acestea sunt prezentate în continuare:

- ***Plaintext Avalanche***: utilizat pentru a examina sensibilitatea unui algoritm la modificările unui text clar.
- ***Key Avalanche***: utilizat pentru a examina sensibilitatea unui algoritm la modificările unei chei de 128biţi
- ***Plaintext/Ciphertext Correlation***: utilizat în scopul studierii corelaţiei perechilor text clar / text cifrat.
- ***Cipher Block Chaining Mode***: utilizat în scopul studierii textului cifrat obţinut utilizând prin criptarea în modul CBC.
- ***Low Density Plaintext:*** utilizat în scopul studierii algoritmului în cazul în care se foloseşte text clar cu densitate redusă (având aproape toţi biţii ‚0').
- ***Low Density Keys:*** în scopul studierii algoritmului în cazul în care se foloseşte cheie cu densitate redusă (având aproape toţi biţii ‚0').
- ***High Density Plaintext:*** utilizat în scopul studierii algoritmului în cazul în care se foloseşte text clar cu densitate mare (având aproape toţi biţii ‚1').
- ***High Density Keys:*** utilizat în scopul studierii algoritmului în cazul în care se foloseşte cheie cu densitate mare (având aproape toţi biţii ‚1').

Testarea secvenţelor cu bateria NIST

Pentru eficientizarea testării se va proiecta o aplicație server client. Aceasta va rula pe o rețea de calculatoare formată dintr-un server și N stații de lucru.

Un sistem pentru testarea statistică a algoritmilor va trebui să îndeplinească urmatoarele funcții: Generarea datelor de test, Distributia datelor de test, Testarea datelor și Generarea rapoartelor

Generarea datelor de test se poate realiza pe server, sau poate fi distribuită pe stațiile client. În modul de generare distribuit, fiecare stație client va genera date indepenent, care vor fi apoi concatenate pe server prin intercalare.
Distribuția datelor de test se va realiza de la server către stațiile de lucru astfel încât toate stațiile de lucru vor avea acces la aceleași date de test.
Fie N numarul de stații client. Fiecare stație client conține M_i procesoare.

Rețeaua de testare statistică va avea în total $C = \sum_{i=1}^{N} M_i$ procesoare

N_t este numărul de tipuri de date ce va fi testat. În mod uzual N_t este egal cu 8 pentru algoritmii de tip bloc și 1 pentru algoritmii de tip stream. Fiecare tip de dată va conține N_s secvențe ce vor fi testate, rezultând în total

$$N_{st} = N_t * N_s \quad \text{secvențe}$$

Astfel fiecare procesor din rețea de la 1 la M-1 va avea de procesat fiecare $trunc(N_{st} / C)$ secvențe și procesorul M va avea de procesat $N_{st} - (M-1) * trunc(N_{st} / C)$ secvente.

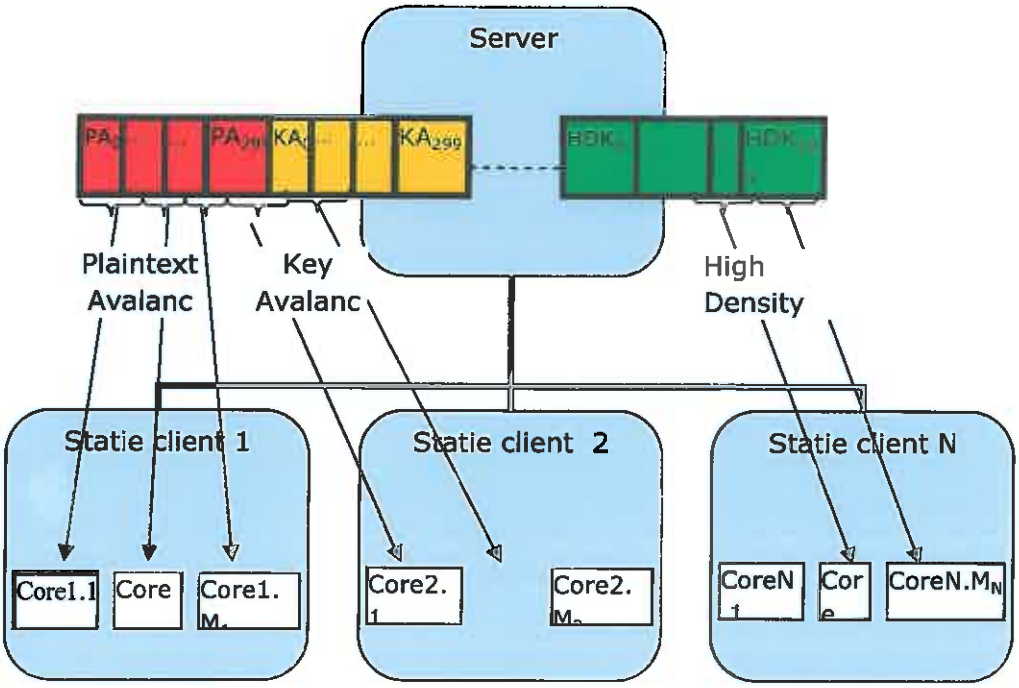


Figura 4. Distribuția datelor de server la stațiile client

Generarea rapoartelor partiale, integrarea acestora in raportul general si luarea decizie

După finalizarea testelor fiecare stație client va genera un raport parțial ce va fi transmis serverului. Serverul va concatena rapoartele parțiale într-un rapoart general. În funcție de rezultatele raportului general se va lua decizia dacă rezultatele testelor statistice aplicate secvențelor binare provenite de la algoritmul analizat, depășesc pragul admis.

Activitatea I.6 Proiectarea platformei de evaluare a securitatii pentru produse IT, în conformitate cu standardele FIPS 140-2.

În cadrul activității I.6 a fost realizată Proiectarea platformei de testare - evaluare pentru produse de securitate IT în conformitate cu standardul FIPS 140-2/Common Criteria.

Pentru a susține procesul de testare-evaluare se va crea o platformă software alcătuită dintr-o suită de aplicații care vor ușura activitatea evaluatorilor și va implementa un management coerent al activității de testare-evaluare.

Avantajul principal al utilizării acestei platforme este acela că sprijină evaluatorul în activitatea de evaluare acoperind întregul proces de testare evaluare evaluare a soluțiilor IT de securitate. Modul în care platforma de testare răspunde diferitelor etape ale procesului de testare evaluare este arătat în figura următoare.

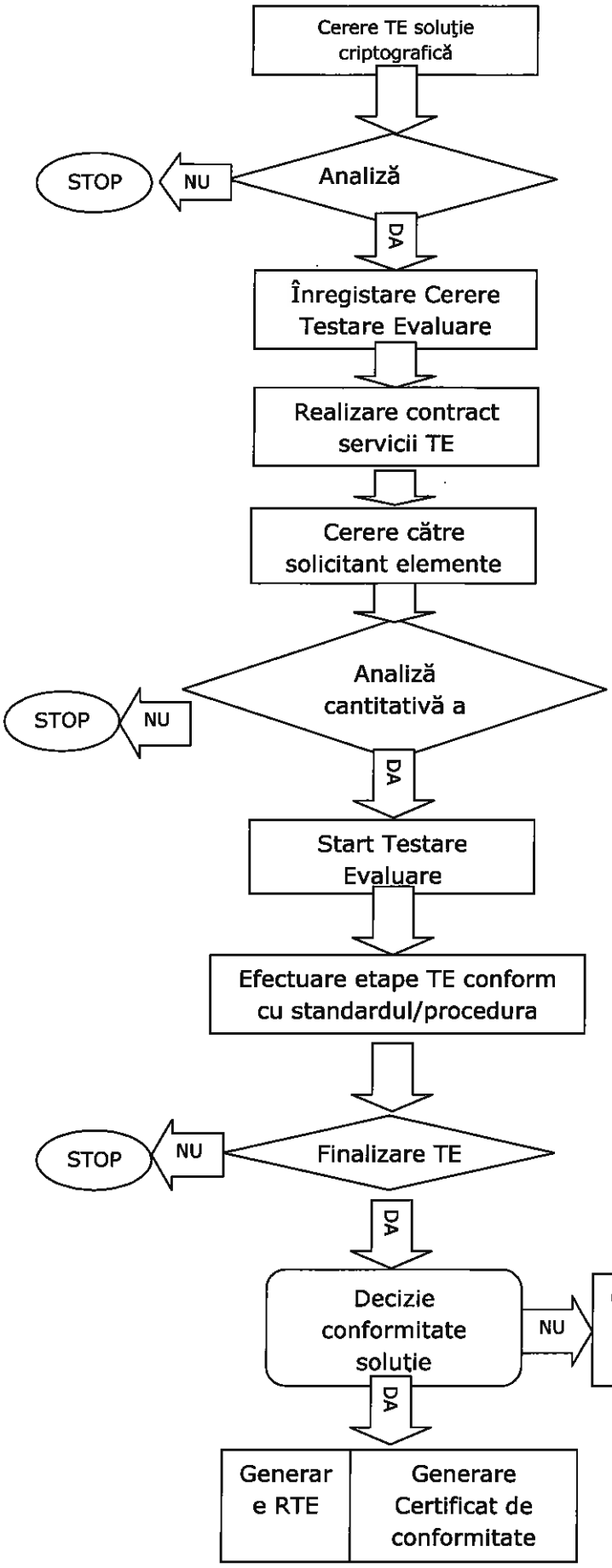
În proiectarea platformei software s-a ținut cont de faptul că modulele criptografice sunt evaluate conform cerințelor de securitate din standardul FIPS PUB 140-2 iar produsele și sistemele de securitate conform cerințelor de asigurare din standardul Common Criteria. În acest sens platforma software permite evaluarea modulelor criptografice folosind criteriile de evaluare specificate în FIPS PUB 140-2 și a sistemelor criptografice folosind criteriile CC.

Principalele funcționalități ale aplicației suport a procesului de testare-evaluare sunt:

- posibilitatea de logare la aplicație pe două roluri: rol de șef de laborator și rol de evaluator;
- acceptarea existenței mai multor proiecte de testare - evaluare simultan
- rolul de șef de laborator oferă următoarele funcționalități:
    - crearea de roluri de evaluator;
    - crearea de proiecte de testare evaluare noi;
    - introducerea datelor referitoare la documentația sistemului (tipul, numele, număr de înregistrare și versiunea documentului);
    - generarea unor statistici ale evaluării;
    - generarea diferitelor tipuri de rapoarte;
- rolul de evaluator oferă următoarele funcționalități:
    - evaluarea unui sistem sau produs conform standardului ales (FIPS PUB 140-2 sau CC);
    - hotărăște ce decizie (trecut/picat) trebuie luată pentru fiecare test efectuat;

- generarea fișelor de măsurători după terminarea testelor unui domeniu din FIPS sau a unei clase de asigurări din Common Criteria, etapă de testare pentru algoritmi.

Flux proces testare-evaluare



Aplicaţia SuportTE

- Generare cerere în format tipizat

- Deschidere comanda TE
- Înregistrare date cerere

- Înregistrare date/termeni din contract
  - Data finalizare TE
  - Perioade derulare proces TE

- Generare cerere în format tipizat (în funcţie de informaţiile introduce în cererea de TE a soluţiei criptografice)

- Înregistrare dată începere proces TE

- Suport pentru efectuarea testelor, luarea deciziei şi înregistrarea datelor

- Suport pentru luarea deciziei de conformitate a soluţiei criptografice prin interogarea bazei de date cu deciziile preliminare

- Generare RTE şi Certificat în format tipizat utilizând date înregistrate în timpul procesului de testare-evaluare

Platforma permite existența mai multor proiecte de testare - evaluare simultan, fiecare din aceste proiecte fiind identificat de un set de date de identificare. Acesta este format din următoarele date:

- Nume produs evaluat;
- Versiune produs evaluat;
- Tip produs evaluat: modul criptografic, produs criptografic, sistem criptografic, profil de protecșie, algoritm criptografic;
- Standard utilizat pentru testare - evaluare : FIPS PUB 140-2, CC sau alte standarde;
- Nivel de securitate/încredere solicitat;
- Date despre solicitantul evaluării: nume, adresă, telefon/fax;
- Date despre dezvoltatorul produsului: nume, adresă, telefon/fax.

Platforma generează statistici referitoare la rezultatele testelor efectuate sau a unor statistici care indică procentul de acoperire al unei evaluări.

Platforma permite de asemenea generarea a două tipuri de rapoarte pe parcursul efectuării unei evaluări. Aceste rapoarte pot fi: raport de observații și raport de testare - evaluare final. Rapoartele de observații conțin informații despre rezultatele parțiale ale evaluării și sunt create ori de câte ori apare o problemă pe parcursul unei evaluări sau trebuie analizat stadiul în care se află evaluarea respectivă. Acestea pot preciza printre altele stadiul în care se află o evaluare, care din testele efectuate nu au trecut, din ce motive și ce măsuri trebuie luate pentru continuarea evaluării. Aceste rapoarte se trimit solicitantului care pe baza lui trebuie să decidă ce trebuie să facă (să modifice produsul, să completeze documentația, etc) pentru a se putea continua procesul evaluare.