MECANISME AVANSATE DE SECURITATE IMPLEMENTATE ÎN HARDWARE
Contract nr. 81-038/2007

OBIECTIVE

- **Realizarea unui model experimental de platformă hardware-software** (**MASH**) pentru dezvoltarea ulterioară de aplicații diverse cum ar fi acceleratoare criptografice, criptoare de date, module de securitate, protocoale dedicate, etc. Modelul experimental presupune implementarea de algoritmi criptografici de criptare şi hash şi a unui generator de numere aleatoare, folosind platforme hardware bazate pe tehnologia FPGA.
- **Implementarea unor mecanisme de paralelizare si pipelinizare a fluxului de prelucrare a datelor** care poate fi utilizată într-o gamă largă de proiecte viitoare cum ar fi cele legate in special de domeniul criptanalizei.
- **Integrarea platformei hardware-software propusă**, cu diverse pachete software consacrate existente.
- **Realizarea unei aplicații software de testare a functionalităților platformei hardware-software propusă**. Aplicația va utiliza libraria software propusa pentru a exploata modulul hardware proiectat.

CONSORȚIU

Coordonator:

Agenția de Cercetare Pentru Tehnică şi Tehnologii Militare Bucureşti

Parteneri:

Academia Tehnică Militară Bucureşti
UTI Systems SA
SC CertSign SRL

ETAPE

Etape/Activități	Termene
Etapa 1 Analiză soluție şi elaborare specificație prototip	**15.12.2007**
1. Elaborare studiu de produs	
1.1 Coordonare activitate, elaborare lucrare unitară	
1.2 Studiu tehnic de produs asupra componentelor de modul hardware pe post de accelerator criptografic, generatorul hardware de numere aleatoare şi componenta de paralelizare.	
1.3 Raport de cercetare privind algoritmii criptografici vizați şi modalitățile posibile de integrare a modulului hardware cu biblioteci criptografice open-source.	
2. Stabilirea parametrilor tehnici constructivi pentru prototip MASH	
2.1 Coordonare activitate, elaborare lucrare unitară	
2.2 Stabilirea parametrilor tehnici constructivi pentru modul hardware pe post de accelerator criptografic	
2.3 Stabilirea parametrilor tehnici constructivi pentru componenta de paralelizare si pipelinizare a fluxului de prelucrare a datelor	

Etape/Activităţi	Termene
2.4 Stabilirea parametrilor tehnici constructivi produs pentru modul hardware pe post de generator de numere aleatoare	
Etapa 2 Proiectare prototip MASH	**31.10.2008**
1. Proiectare de detaliu	
1.1. Definirea şi proiectarea elementelor constructive ale modulului hardware pe post de accelerator criptografic	
1.2. Definirea şi proiectarea elementelor constructive ale generatorului de numere aleatoare	
1.3. Definirea şi proiectarea componentei de paralelizare şi pipelinizare a fluxurilor de date	
1.4. Definirea şi proiectarea modulelor software necesare pentru accesul la modulul criptografic	
Etapa 3 Dezvoltare parţială prototip MASH	**31.08.2009**
1. Dezvoltarea parţială a unora din componentele MASH	
1.1.Dezvoltarea componentei de accelerator criptografic	
1.2.Integrarea componentei de accelerator criptografic cu biblioteci open-source consacrate	
1.3.Dezvoltarea componentei de paralelizare	
1.4 Dezvoltarea componentelor software necesare accesării modulului criptografic	
Etapa 4 Realizare, testare prototip MASH, elaborare documentatie şi diseminare cunoştinţe	**15.08.2010**
1. Dezvoltare finală prototip MASH	
1.1 Dezvoltarea componentei de generator de numere aleatoare	
2. Elaborare specificaţie de testare	
2.1. Elaborare specificaţie de testare privind modul hardware pe post de accelerator criptografic	
2.2. Elaborare specificaţie de testare privind generator hardware de numere aleatoare	
2.3. Elaborare specificaţie de testare privind implementarea algoritmilor criptografici în modulul hardware	
2.4. Elaborare specificaţie de testare privind componenta de paralelizare si pipelinizare a fluxului de prelucrare a datelor	
2.5. Elaborare specificaţie de testare privind integrarea modulului hardware cu librarii criptografice opensource	
2.6. Elaborare specificaţie de testare privind aplicaţia software de testare	
3. Elaborare documentaţie de produs	
3.1. Elaborare documentaţie de produs privind modalitatea de paralelizare si pipelinizare a fluxului de prelucrare a datelor	
3.2. Elaborare documentaţie de produs privind generator hardware de numere aleatoare	
3.2. Elaborare documentaţie de produs privind modulul hardware pe post de accelerator criptografic	
3.3. Elaborare documentaţie de produs privind modalitatea de integrare a modulului hardware cu librării criptografice open-source	
3.4. Elaborare documentaţie de produs privind aplicaţia software de testare	
4. Diseminarea pe scară largă a informaţiilor privind produsul şi soluţiile adoptate	
4.1. Organizare unui workshop si CD de prezentare	
4.2. Participări la conferinţe şi sesiuni de comunicare ştiinţifică	

REZULTATE

Etape/Activităţi	Termene	Rezultate
Analiză soluţie şi elaborare specificaţie prototip	15.12.2007	• Studii tehnice • Raport de cercetare • Specificatii de prototip
Proiectare prototip MASH	31.10.2008	• Documentaţie de proiectare
Dezvoltare parţială prototip MASH	31.08.2009	• Demonstrator partial prototip MASH

		• Documentatie de realizare
Realizare, testare prototip MASH, elaborare documentatie şi diseminare cunoştinţe	15.08.2010	• Prototip MASH • Raport de testare • Documentatie de produs • Lucrari, comunicari

CONTACT

Responsabil de proiect:
Cpt.lector.univ. ing. Mihai TOGAN
Academia Tehnică Militară Bucureşti
Telefon: +4021 335 4660
Fax: +4021 335 5763
E-mail: mtogan@mta.ro