Referat Științific

24 februarie 2012

Universitatea din Craiova, Facultatea de Matematică și Informatică

Titlu Proiect

Analiza Sistemelor de Autentificare

Titlu Raport Cercetare

Titlu Raport Stiințific
De la: 01.01.2008 **la:** 01.06.2008

Beneficiar

Microsoft

Coordonator Stiintific

dr. Ion Ionescu

Membrii Echipei de Cercetare

Dan Marmura

Mihai Daniel

Cuprins

Listă de figuri

Listă de tabele

Listă de algoritmi

Partea I

Introducere

Capitolul 1

Generalitați

1.1 Titlu Secțiunea 1

1.1.1 Titlu Secțiunea 1.1

1.2 Titlu Secțiunea 2

Capitolul 2

Descrierea Domeniului

2.1 Titlu Secțiunea 1

2.1.1 Titlu Secțiunea 1.1

2.2 Titlu Secțiunea 2

Partea II

Descriere Model. Studiu de caz

Capitolul 3

Model Matematic

3.1 Titlu Secțiunea 1

3.1.1 Titlu Secțiunea 1.1

Capitolul 4

Model Algoritmic

4.1 Titlu Secțiunea 2

Capitolul 5

Implementări

Partea III

Concluzii

Capitolul 6

Rezultate

Capitolul 7

Studii viitoare

Anexa A

Modele matematice folosite

Anexa B

Standarde in vigoare

Bibliografie

[1] I.F. BLAKE, G. SEROUSSI, N.P. SMART, *Elliptic Curves in Cryptography*, Cambridge University Press, 2002

[2] R. CRANDALL, *Method and apparatus for public key exchange in a cryptographic system*, U. S. Patent Number 5159632

[3] R. LERCIER and F. MORAIN, *Counting points in elliptic curves over F_{p^n} using Couveignes algorithm*, Rapport de Recherche LIX/RR/95/09.1995

[4] R. LERCIER, *Computing isogenies in F_{2^n}*, White Paper, 197–212

[5] J.H. VAN LINT, *Introduction to Coding Theory*, Springer-Verlag, 1982

[6] P.L. MONTGOMERY, *Modular multiplication without trial division*, Math. Comp., **44**, 519–521, 1985

[7] G. C. POHLIG and M. E. HELLMAN, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic signifiance*, IEEE Trans. Info. Theory, **24**, 1978, 106–110.

[8] N.P. SMART, *Elliptic curves over small fields of odd characteristic*, Journal of Cryptography, **12**, 141–151, 1999

[9] J.A. SOLINAS, *An improved algorithm for arithmetic on a family of elliptic curves*, Springer-Verlag, 1997

[10] DOUGLAS R. STINSON, *Cryptography - Theory and Practice*, CRC Press, 2002

[11] CERTICOM WHITE PAPER, *The elliptic curve cryptosystem for smart card*, Published: May 1998.

[12] G. AGNEW, R. MULLIN, S. VANSTONE, *An implementation of elliptic curve cryptosystem over $F_{2^{155}}$*, IEEE Journal on Selected Areas in Communications, **11** (1993), 804–813.

[13] SHUHONG GAO, JOACHIM VON ZUR GATHEN, DANIEL PANARIO, VICTOR SHOUP, *Algorithms for Exponentiation in Finite Fields*, Journal of Symbolic Computation 2000, **29**, 879–889.

[14] C. LIM, P. LEE, *A key recovery attack on discrete log-based schemes using a prime order subgroup*, Advances in Cryptography 1997, **1294** (1997), Springer-Verlag, Lecture Notes in Computer Science, 275–288.

[15] PAUL C. VAN OORSCHOT, MICHAEL J. WIENER, *Parallel Collision Search with Cryptanalytic Applications*, Journal of Cryptology, **12** (1999) , Springer - Verlag, 1–28.