Elliptical Curve Cryptography

Ibraim Silva Torres
Segurança e Privacidade em Sistemas de Armazenamento e Transporte de Dados
MSDPA, Univ. do Minho

10 de Junho de 2007

Resumo

Pretende-se, com a apresentação deste documento, apresentar a criptografia de curvas elípticas, como uma das vertentes da criptografia da actualidade, no âmbito da disciplina de Segurança e Privacidade em Sistemas de Armazenamento e Transporte de Dados.

Será apresentado um enquadramento desta matéria na criptografia, salientando as principais capacidades desta área, definido o âmbito de acção e as principais características.

As principais técnicas criptográficas existentes assim como as potencialidades a nível da eficiência e eficácia do seu uso serão brevemente mencionadas, com o intuito de esclarecer as potencialidades do seu uso

Por fim, será indicado as vantagens e desvantagens desta área da criptografia em comparação com outras concorrentes.

Palavras chave: Criptografia com Curvas Elípticas, Criptografia Assimétrica, Certificação Digital, Assinatura Digital, Problema do Logarítmo Discreto, Segurança, Eficiência e Normalização

1 Introdução

Em Criptografia, os sistemas criptográficos têm por base problemas matemáticos que, dado ao elevado nível de trabalho envolvido na sua resolução, tornam mais complexa a sua quebra.

Consequentemente, encontramos segurança no facto de que nosso "adversário"não conseguirá, mesmo contando com as mais modernas ferramentas computacionais, reverter a função de criptografia (na qual o sistema se baseia) e aceder a parâmetros e entradas do nosso sistema num período de tempo aceitável.

Em termos de criptografia computacional, um problema matemático é dito "de difícil solução"quando, mesmo aplicando-se o algoritmo mais eficiente para resolvê-lo, esse leva um longo período para que sua execução termine.

Esse tempo de execução, por sua vez, possui uma relação directa com o tamanho dos dados de entrada do algoritmo utilizado. Cientistas da área defendem o facto de que,

em geral, um problema de fácil solução tem o tempo de execução polinomial, enquanto problemas de difícil solução tem esse tempo em formato exponencial.

Consequentemente, estaremos interessados em saber o quanto um problema se torna difícil (tempo de execução) com o aumento do tamanho de sua entrada e, adicionalmente, em seleccionar problemas que maximizem esse tempo, sempre que quisermos obter um sistema de criptografia mais seguro.

A utilização de curvas elípticas em criptografia foi proposta de modo independente por Neal Koblitz e Victor Miller em 1985.

Utilizaram as curvas elípticas na criptografia como uma forma implementação de um sistema de chave pública em algumas aplicações já existentes.

A principal empresa comercial ligada ao ECC é a Certicom, que possui 130 patentes e outorgou licenças sobre a tecnologia para NSA por 25 milhões de dólares.

A Certicom também patrocinou vários desafios ao algoritmo ECC. O resultado mais complexo até aqui é uma chave de 109 bits que foi quebrada por uma equipa de investigadores no começo de 2003. A equipa que quebrou a chave utilizou um ataque massivo em paralelo baseado no birthday attack.

Para este ataque foram mobilizados mais de 10.000 PCs do tipo Pentium, funcionando continuamente durante 540 dias. Estima-se que a chave de comprimento mínimo recomendado para ECC, de 163 bits, exigira recursos 108 maiores do que aqueles usados para resolver o problema da chave de 109 bits.

2 Enquadramento

Sistemas de criptografia com chave pública (sistemas assimétricos) foram inicialmente propostos por Whitfield Diffie e Martin Hellman em 1976.

Esses sistemas trabalham com duas chaves diferentes, independentes e não facilmente deriváveis: A chave pública, utilizada na codificação de uma mensagem cifrada, e, a chave privada, utilizada na sua descodificação.

2.1 Criptografia Assimétrica

A criptografia assimétrica usa pares de chaves para cada dos utilizadores, tenho n como o número de pares de chaves necessárias. Na situação com 1000 utilizadores, irás obter 1000 pares de chaves.

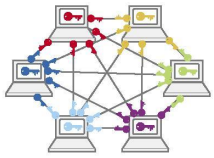

Figura 1: Assinatura Simétrica

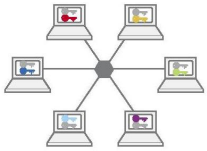

Figura 2: Assinatura Assimétrica

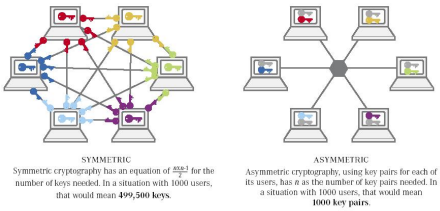

Figura 3: Assinatura Assimétrica vs Assinatura Simétrica

2.2 Assinatura Digital

No caso assinatura digital de uma mensagem, a utilização da chave pública e privada se inverte, ou seja, o remetente "assina"(codifica) a mensagem através de sua chave privada, enquanto o destinatário somente conseguirá descodificar essa mensagem aplicando a chave pública do remetente. A segurança está em poder armazenar a chave privada em segurança e ser computacionalmente impossível obter essa chave a partir da mensagem cifrada e da chave pública correspondente.

Figura 4: Assinatura Digital

2.3 Certificação Digital

Para projectar sistemas criptográficos de chave pública, é necessário também haver um compromisso entre o nível de segurança e o tempo de resposta que se deseja obter. Nesse aspecto, quanto mais desenvolvidos forem as ferramentas e algoritmos utilizados para violação dos sistemas de criptografia existentes, maiores têm que ser os parâmetros (chaves) e, consequentemente, maior o esforço no trabalho de codificação e descodificação dos textos cifrados.

Para reduzir o tempo de resposta, foi criado na criptografia a certificação digital, onde uma terceira entidade certifica o mensagem codificada e os termos da codificação.

3 Definição das Curvas Elípticas

3.1 Curvas Elípticas sobre Números Reais

A forma de "Weierstrass"de uma curva elíptica é:

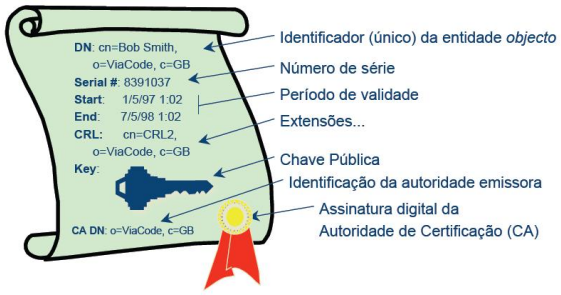

Figura 5: Assinatura Digital

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in \mathbb{F}.$$

Figura 6: Equação

As variáveis x e y situam-se no plano. Na verdade, x e y podem ser complexos, reais, inteiros, base polinomial, base canónica ou qualquer outro tipo de elemento. Mas, iremos considerar números reais sobre o plano dos números reais.

Sendo a forma simplificada da equação: $y^2{=}x^3{+}a_4\mathrm{x}{+}a_6$.

Para definir uma expressão algébrica sobre curvas elípticas devemos encontrar uma maneira de definir "adição"de dois pontos da curva, cuja soma seja outro ponto da curva. Além disso, devemos definir o elemento identidade da soma O, ponto que somado com qualquer outro da curva, resulte no próprio ponto: P + 0 = P.

Este ponto também é conhecido de ponto no infinito.

Para a álgebra funcionar, o negativo do ponto de intersecção é definido como a "soma elíptica". Matematicamente: R = P + Q .

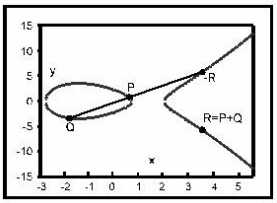

Figura 7: Equação Soma Elíptica

Adição de pontos de uma curva elíptica sobre números reais. Adicionar um ponto a ele mesmo é um caso especial. A linha usada é a tangente à curva no ponto considerado.

3.2 Curvas Elípticas sobre Corpos Finitos Primos

3.2.1 Característica 1

Em criptografia interessa-nos estudar a matemática de curvas elípticas aplicadas a corpos finitos. Analisaremos, inicialmente, corpos finitos gerados por grandes primos. Ou seja, analisaremos curvas elípticas sobre Zp, sendo p primo maior que 3.

Uma curva elíptica E sobre Zp pode ser definida pela mesma equação estudada no item anterior: $y^2{=}x^3{+}a_4\mathrm{x}{+}a_6$.

Onde a_4, a_6 pertencem a Zp e $4{a_4}^3 + 27{a_6}^2$ é diferente a 0. O conjunto E(Zp) é composto, então, por todos os pontos (x,y), x pertencente a Zp, y pertencente a Zp, que satisfazem a equação de definição, juntamente com o ponto no infinito O.

Podemos adicionar dois pontos numa curva elíptica E(Zp) com o intuito de obter um terceiro ponto da curva. Junto com esta operação de adição, o conjunto de pontos E(Zp) forma um grupo, com O servindo como sua identidade. É este grupo que é utilizado na construção de sistemas de criptografia baseados em curvas elípticas. A regra de adição é apresentada abaixo como uma sequência de fórmulas algébricas:

1. $P + O = O + P = P$ para todo $P \in E(Zp)$
2. Se $P = (x, y) \in E(Zp)$, então $(x, y) + (x, -y) = O$. (O ponto $(x, -y)$ é representado por $-P$ e é chamado negativo de P. Observe que $-P$ é, também, um ponto na curva.)
3. Seja $P = (x_1, y_1) \in E(Zp)$ e $Q = (x_2, y_2) \in E(Zp)$, onde $P \neq -Q$. Então $P + Q = (x_3, y_3)$, onde:

$$x^3 = \lambda^2 - x_1 - x_2 \quad (5) \qquad \text{e}$$

$$y^3 = \lambda(x_1 - x_3) - y_1 \quad (6)$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, se\ P \neq Q & (7) \\ \dfrac{3{x_1}^2 + a_4}{2y_1}, se\ P = Q & (8) \end{cases}$$

Figura 8: Equação

3.2.2 Característica 2

Os corpos finitos de característica 2, GF(2m), interessam especialmente, pois permitem implementações eficientes da aritmética de curvas elípticas. Neste caso, as constantes são números de base polinomial ou canónica. Não podemos, neste caso, utilizar a versão simplificada da equação.

Teremos de usar uma das duas versões:

- y^2+y=x^3+a_4x+a_6 : função "supersingular- inútil para a criptografia;
- y^2+xy=x^3+a_2x^2+a_6:a função "nonsupersingular"é considerada uma excelente solução. Contudo, para ser válido, a_6 tem de ser diferente de 0. Contudo, a_2 pode ser igual a 0.

No que diz respeito as equações da forma "nonsupersingular", não existe nenhum método de ataque conhecido de menor complexidade do que exponencial para estas curvas. Certamente, a escolha dos coeficientes é fundamental, a fim de que se obtenha a máxima vantagem da segurança.

3.3 Multiplicação sobre Curvas Elípticas

A multiplicação sobre curvas elípticas refere-se, ao produto de um escalar por um ponto da curva: Q=kP.

Onde Q e P são pontos sobre uma curva elíptica e k é um inteiro. O que a multiplicação realmente significa é a soma de Pa com ele mesmo k vezes.

Como a própria curva elíptica, isto é, os pontos sobre ela, forma um corpo, o inteiro k não deve ser maior que a ordem do ponto P. Caso não se saiba a ordem do ponto, o cálculo não será tão eficiente quanto poderia ser.

Outro método para o cálculo da multiplicação é a expansão balanceada, proposta por Koblitz.

O algoritmo converte uma string de bits "1" em uma string de bits "0" seguido de "-1". Este tipo de cálculo resulta ainda mais eficiente do que o anterior, uma vez que serão efectuadas menos operações.

3.4 Ordem da Curva

O número de pontos de uma curva elíptica sobre um corpo finito deve satisfazer o teorema de Hasse. Dado um campo, GF(q), a ordem da curva N deverá satisfazer esta equação:

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Figura 9: Equação

Ou de outra forma:

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$$

Figura 10: Equação

Então, o número de pontos de uma curva é, aproximadamente, o tamanho do corpo.

3.5 Propriedades de Interesse Criptográfico

O problema do logaritmo discreto das curvas elípticas (conhecido e citado por ECDLP), é uma propriedade das curvas elípticas, tornando o grande desafio para vencer a criptografia para decifrar as mensagens, uma vez que, garante elevados níveis de segurança para os sistemas criptográficos, tornando muito difícil resolver a capacidade de processamento quando o ponto P é um número primo grande.

Os métodos de conhecimento para resolver o ECDLP são:

- The Pohlig-Hellman algorithm;
- Shanks' baby-step-giant-step method;
- Pollard's methods;
- The Menezes-Okamoto-Vanstone;
- The Frey-Rueck attack using the Tate pairing;
- The attacks on anomalous elliptic curves;
- Weil descent (for some special finite fields).

Figura 11: Equação

4 Sistemas Criptográficos com Curvas Elípticas

4.1 Codificação de texto com Criptografia em Curvas Elípticas

Suponhamos que desejamos codificar algum texto com ECC. Podemos seguir um método que insira alguma parte de um texto, arbitrariamente, e o coloque numa curva elíptica, ou seja, representando uma bijecção (uma bijecção é uma função injectiva e sobrejectiva ao mesmo tempo) entre os pontos de uma curva elíptica e de um bloco de texto. Com isto, esboçamos um algoritmo.

1º Passo: Escolhemos um alfabeto com N letras e fixamos o tamanho i de um bloco de texto. Os caracteres do alfabeto são identificados com números de 0 a N-1. Com a seguinte tarefa alcançamos a bijecção entre os bloco de textos W e os números $0<X_w<N^i$.

$$w = (a_0 a_1 \dots a_{l-1}) \mapsto x_w = a_0 N^{l-1} + a_1 N^{l-2} + \cdots + a_{l-2} N + a_{l-1}, \quad 0 \le x_w \le N^l$$

Figura 12: Equação

Para cada X_w não há necessidade de ser um ponto da curva elíptica. Mas é possível encontrar o próximo ponto X_1 perto do X_w eficientemente. Dado um número K, queremos ter uma probabilidade elevada, isto é, P=(1-(1/2)^k para $X_w < X_1 < X_w$ + k.

Passo 2: Escolhemos um K apropriado, ou seja, que a probabilidade é elevada e que o q>kN^i. Para cada j obtemos um elemento de F_q através kX_w+j. Pegamos no primeiro ponto da curva (j>0) P_w com a coordenada X>kX_w, ou seja, P_w=(kX_w+j,*) pertencente E(F_q).

Passo 3: Podemos recuperar o bloco de texto a partir do ponto X_w=[X/k].

4.2 Mudança de chave ECDH

A troca de chave através da curva elíptica de Diffie-Hellman, supõe comunicações de duas partes, com acordo no uso de uma chave que será usada depois para codificar a comunicação em conjunto com uma chave privada de um sistema criptográfico.

Eles primeiros fixam um campo finito F_q, uma curva elíptica E definida sobre essa curva e a ponto base B pertencente a E, com uma ordem superior. Para gerar a chave, primeiro uma das partes escolhe aleatoriamente A pertencente a F_q, que mantém em segredo. Depois calcula B pertencente a E, que é chave pública e envia a outra parte.

A outra parte executa os mesmos passos, ou seja, escolhe aleatóriamente um inteiro b e calcula bB que será enviado de volta. A chave secreta em comum é P=abB pertencente E.

4.3 Analogia ao El-Gamal

Começamos com um campo finito Fq fixado publicamente, uma curva elíptica definida sobre ele e um ponto base B pertencente a E.

Cada utilizador escolhe um inteiro aleatório a, que é tido em segredo e computa o ponto X=aB, que será a chave pública.

Para enviar a mensagem P para o outro utilizador, escolhe um inteiro aleatório k e envia o par de pontos (kB, P+k(bB), onde bB é a chave pública, para o utilizador final.

Para ler a mensagem, basta multiplicar o primeiro ponto no par pela sua chave privada b e subtrair o resultado do segundo ponto: P + k(bB)-b(kB)=P.

4.4 EC Digital Signature Algorithm

É uma analogia ao DAS.

Para executar a assinatura:

1.	Choose a random number k with $k : 1 \leq k \leq n-1$.
2.	Compute $kG = (x_1, y_1)$ and $r = x_1 \bmod n$. If $r = 0$ then go to step 1.
3.	Compute $k^{-1} \bmod n$.
4.	Compute $e = \text{SHA-1}(M)$.
5.	Compute $s = k^{-1}(e + dr) \bmod n$. If $s = 0$ then go to step 1.
6.	Alice signature for the message M is (r, s).

Figura 13: Executar assinatura digital

Para verificar a assinatura:

1.	Verifiy that r, s are integers in the intevall $[1, n-1]$.
2.	Compute $e = \text{SHA-1}(M)$.
3.	Compute $w = s^{-1} \bmod n$.
4.	Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
5.	Compute $X = u_1G + u_2Q$. If $X = \mathcal{O}$ then reject the signature. Otherwise compute $v = x_1 \bmod n$ where $X = (x_1, y_1)$.
6.	Accept the signature if and only if $v = r$.

Figura 14: Executar assinatura digital

4.5 ECM - Factoring Method

O método ECM é a curva elíptica análoga ao método (p-1). Um utiliza uma equação Y^2=X^3+aX+b sobre F_n. O método ECM determina divisores primários para cada pedido de E(F_n) estável. A vantagem deste método é, basicamente, existirem imensas curvas elípticas sobre um campo finito conhecido. Se não podemos usar uma determinada curva elíptica, seguimos para outra. Muitas implementações da actualidade trabalham com centenas de curvas elípticas em paralelo.

5 Normalização

O desenvolvimento de standards para os sistemas criptográficos é muito importante para a utilização dos mesmos, uma vez que, assegura a segurança e a inter operacionalidade dos sistemas criptográficos.

Os standards mais importantes para segurança das tecnologias de informação são:

- ISO:Internacional Standard Organization;
- ANSI:American National Standard Inst.;

- IEEE:Institute of Electrical and Electronic Engenieers;
- FIPS:Federal Information Processing Standards.

O algoritmo mais utilizado ECC, o ECDSA foi aceite em 1998 como ISO14888-3, em 1999 como ANSI X9.62 e em 2000 como IEEE P1363 e FIPS 186-2.

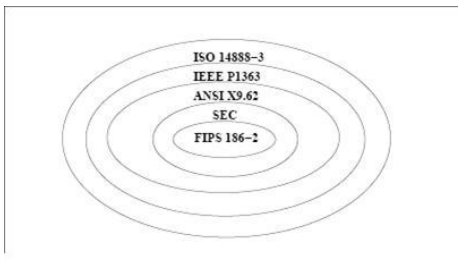

Figura 15: Standards mais importantes

IEEE	1363-2000 • 1363a • 1363.2
CEN	TC331 WG3 (DPM)
NESSIE	ECDSA • "PSEC"
SECG	SEC1 • SEC2
ANSI X9F	X9.24 Key management • X9.37 Check Image Exchange • X9.57 Cert management • X9.59 Payment • X9.62 ECDSA • X9.63 Key establishment • X9.68 Compressed certificates • X9.73 CMS • X9.84 Biometrics • X9.90 IRD • X9.92 ECPVS • X9.95 Time stamps • X9.96 XML CMS
FIPS	FIPS 186-2 Signatures (ECDSA) • SP 800-56 Key establishment • SP 800-57 Key Management
FAA Security	Security • Next generation ATN • Secure ACARS
ISO	14888 • 15946 • 9796 • 18033 •...
IETF	PKIX • S/MIME • IPSec (IKE) • TLS
CE	1394 • Consumer Electronics DTCP
OMA	WTLS • WPKI • WMLScript • ...

Figura 16: Normas em vigor

A normalização em vigor compreende:

- Pode ser usada a mesma chave ECC para ambas assinaturas digitais assinando e codificação;
- Os parâmetros das Curvas Elípticas podem ser dados directamente no certificado ou pode ser referenciado por nome;
- O uso da secção chave para ECDSA incluí digitalSignatures, nonRepudition, keyCertSign e cRLSign;
- O uso da secção chave para ECDH incluí: keyAgreement, encipherOnly, decipherOnly.

6 Conclusão

O uso da criptografia como chave publica baseada em curvas elípticas é uma excelente opção, não somente em termos de nível de segurança, como também em todos os principais pontos relativos à eficiência das operação de codificação.

Dadas suas características, esta técnica pode ser utilizada, principalmente, em sistemas "embutidos" ou sistemas com restrições físicas de espaço e/ou capacidade de processamento.

6.1 Nível de Segurança

Os algoritmos genéricos podem resolver qualquer configuração encontrada em cada um desses problemas, diferindo dos algoritmos específicos, que somente se aplicam a determinadas "classes" de problemas.

Ao avaliar e comparar as opções de sistemas de criptografia com chave pública, os cientistas da área baseiam-se nos algoritmos genéricos e qual a complexidade (número de passos X tamanho da entrada) que cada um deles oferece.

Os problemas de factorização de inteiros e de logaritmos discretos admitem, em geral, algoritmos que executam em tempo sub exponencial.

Esses problemas também são considerados "difíceis", mas não tão difíceis quanto os que necessitam de algoritmos puramente exponenciais.

O melhor algoritmo genérico conhecido para o problema dos logaritmos discretos em curvas elípticas é puramente exponencial.

Consequentemente, podemos constatar que o problema de logaritmos discretos em curvas elípticas é considerado mais "difícil´´ de resolver que os demais. Estudos recentes indicam que, para um nível de segurança razoável (1012 MIPS), enquanto o RSA e o DSA necessitam de 1024 bits, o ECC precisa de somente 160 bits para o tamanho de chave.

Outro dado importante tem a ver com o aumento do nível de segurança (MIPS maior) necessitar de um aumento bem mais expressivo do tamanho das chaves do RSA e DSA, em comparação ao ECC.

Evidencia que o aumento dos actuais parâmetros de segurança, irá exigir um crescimento do tamanho da chave bem mais significativo no caso do RSA e DSA do que no ECC.

6.2 Eficiência

A eficiência de cada um dos sistemas de criptografia considera os seguintes factores: Carga computacional, tamanho de chave e tamanho de banda.

Para uma comparação mais justa, os dados apresentados levam em consideração o mesmo nível de segurança para todas as propostas (ECC, RSA ou DSA).

6.2.1 Carga Computacional

Mede a eficiência com que os algoritmos podem implementar as transformações com as chaves públicas e privadas (sistema em operação). As melhores implementações de cada um dos sistemas indicam que o ECC executa numa ordem de 10 vezes mais rápido que o RSA ou DSA.

6.2.2 Tamanho da Chave

O ECC também apresenta grande vantagem nesse aspecto. Enquanto RSA e DSA apresentam pares de chave (pública, privada) com tamanhos, em bits, RSA(1088,2048) e DSA(1026,160), temos, no caso da implementação de curvas elípticas o par ECC(161,160).

6.2.3 Tamanho de Banda

Corresponde a quantos bits temos que transmitir após codificar ou assinar uma mensagem, em relação a mensagem original. O ECC maximiza a utilização dos sistemas de transmissão de dados.

Se visualizarmos os sistemas de criptografia com chave pública como eficiente ferramenta de troca de chave de secção (usa transformação de mensagens pequenas), essa vantagem do ECC torna-se ainda mais significativa.

6.3 Vantagens

Vantagens da utilização da Criptografia por Curvas Elípticas:

- Grande flexibilidade na escolha do sistema criptográfico;
- Desconhecido o tempo para o ECDLP (Problema Logaritmo Discreto);
- Utilização de chaves mais pequenas, com o mesmo nível de segurança (o tamanho mínimo da chave deve ser para o ECC de 132 bits vs. 952 bits para o RSA);
- Resultado: Grande velocidade de tráfego, menos capacidade de armazenamento necessária;
- Ideal para o uso em smart cards, telemóveis, pagers, etc.

6.4 Vantagens

Desvantagens da utilização da Criptografia por Curvas Elípticas:

- Sistemas criptográficos Hyperelliptic sobre chaves ainda mais pequenas;
- ECC é matematicamente mais subtil do que o RSA e o SDL;
- Dificuldade para demonstrar e justificar ao cliente.

Referências

[Diffie et al, 1976] Diffie, W., Hellman, M., "New Directions on Cryptography´´, IEEE Transactions on Information Theory, 1976.

[Rauscher et al, 1999] Rauscher, R., Bohnsack, F., "Results of na Elliptic-Curve-Approach for Use in Cryptosystems. EUROMICRO Conference´´, Milan, Italy, 1999.

[Gura et al, 2005] Gura, N., Shantz,S., Eberle, H., Gupta,S., Gupta,V., Finchelstein,D., Goupy,E., Stebila, D., "An End-to-End Systems Approach to Elliptic Curve Cryptography´´, Sun Microsystems Laboratories, http://www.research.sun.com, USA, 2005.

[Gura et al, 2005] Gura, N., Shantz,S., Eberle, H., Gupta,S., Gupta,V., Finchelstein,D., Goupy,E., Stebila, D., "An End-to-End Systems Approach to Elliptic Curve Cryptography´´, Sun Microsystems Laboratories, http://www.research.sun.com, USA, 2005.

[Miller et al, 1998] Miller, V., Koblitz, N., "Uses of Elliptic Curves in Cryptography. Advances in Cryptography", Springs Verlag, USA, 1998.

[Certicom, 1997] www.certicom.com, "Current Public-Key Cryptographic Systems´´, A Certicom Tutorial, USA, 1997.

[Certicom, 2004] www.certicom.com, "An intro to Elliptical Curve Cryptography´´, A Certicom Whitepaper, USA, 2004.