Performance of Elliptic Curve Cryptosystems

Julio López *Ricardo Dahab*

Relatório Técnico IC–00-08

Maio de 2000

Performance of Elliptic Curve Cryptosystems

Julio López[*] Ricardo Dahab[†]

Institute of Computing
State University of Campinas
Campinas, 13081-970 São Paulo, Brazil
{julioher,rdahab}@dcc.unicamp.br
May 22, 2000

Abstract

In recent years, several studies have been conducted on software implementation of elliptic curve cryptosystems (ECC). In this note we have collected several details of reported software implementations of these cryptosystems. For each implementation considered, we include, if available, the platform used, and running times for: finite field operations, scalar multiplications, and protocols such as the ECDSA. This compilation is organized in five sections: performance of ECC over $\mathbb{F}_{2^m}$, performance of ECC over $\mathbb{F}_p$, performance of ECC over $\mathbb{F}_{p^m}$, implementations comparing $\mathbb{F}_{2^m}$ and $\mathbb{F}_p$, and implementations comparing ECC with other public-key systems such as RSA and DL.

1 Performance of ECC over $\mathbb{F}_{2^m}$

- "Fast key exchange with elliptic curve system" [22]
  - **Author:** R. Schroeppel *et al*, 1995
  - **Platform:** SPARC 25MHz; language: C
  - **Representation:** Trinomial basis for $\mathbb{F}_{2^{155}}$
  - **Curves:** Random curves
  - **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. AIA[1](μsec)	kP (msec)
155	8	112	280	92

[*]Institute of Computing, State University of Campinas, 13081-970 Campinas, SP, Brazil, and Dept. of Computer Science, University of Valle, Cali, Colombia.

[†]Institute of Computing, State University of Campinas, 13081-970 Campinas, SP, Brazil. Research partially supported by a Pronex-Finep grant 107/97.

[1]Almost Inverse Algorithm [22].

- "A fast software implementation for arithmetic operations in $\mathbb{F}_{2^m}$" [9]
  - **Author:** E. De Win *et al*, 1996
  - **Platform:** Pentium 133 MHz; language: C++
  - **Representation:** Subfield basis for $\mathbb{F}_{(2^{16})^{11}}$ and trinomial basis for $\mathbb{F}_{2^{177}}$
  - **Curves:** Random curves
  - **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. (μsec)	kP (msec)
176	5.9	68	160 (EEA[2])	72
177	2.7	80	225 (AIA)	96

- "Efficient algorithms for elliptic curve cryptosystems" [13]
  - **Author:** Jorge Guajardo and Christof Paar, 1998
  - **Platform:** DEC Alpha 3000, 175 (64 bits), 175 MHz; laguage: C++
  - **Representation:** Subfield basis for $\mathbb{F}_{(2^{16})^{11}}$
  - **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. (μsec)	kP (msec)
176	4.23	38.56	158.73	68

- "On the performance of signatures schemes based on elliptic curves" [10]
  - **Author:** E. De Win *et al*, 1998
  - **Platform** Pentium Pro 200 MHz; languages: C, C++
  - **Representation:** Trinomial basis for $\mathbb{F}_{2^{191}}$
  - **Curves:** Random curves over $\mathbb{F}_{2^{191}}$
  - **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. AIA(μsec)	kP (msec)
191	2.6	39	126	50

- "Implementing network security protocols based on elliptic curve cryptography" [1]
  - **Author:** M. Aydos, E. Savas, and, Ç. K. Koç, 1999
  - **Platform:** Pentium II 300-MHz, M. Visual C++, V. 5.0
  - **Representation:** Subfields basis (optimal normal basis for $\mathbb{F}_{2^{16}}$ and polynomial basis for $\mathbb{F}_{(2^{16})^{11}}$)

[2]Extended Euclidean Algorithm [9].

- **Curves:** Random curves over $\mathbb{F}_{2^{176}}$
- **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. (μsec)	kP (msec)
176	1.5	12	60	25

- "Improved algorithms for elliptic curve arithmetic in $GF(2^m)$" [18]
  - **Author:** Julio Lopez and Ricardo Dahab, 1999
  - **Platform** UltraSPARC 300MHz, LiDIA system, C++
  - **Representation:** Polynomial basis
  - **Curves:** Random curves over $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{191}}$ and $\mathbb{F}_{2^{239}}$
  - **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. EEA(μsec)	kP (msec)
163	2.3	10.5	96.2	13.5
191	2.0	10.9	118.1	16.0
239	2.6	14.6	162.8	25.6

- "Elliptic curve cryptosystems on embedded microprocessors" [3]
  - **Author:** Bogdan Antonescu, Master Thesis, 1999
  - **Platforms** MC68302, 25MHz, Pentium 200 MHz, optimized C and assembly
  - **Representation:** Polynomial basis
  - **Curves:** Random curves over $\mathbb{F}_{2^{167}}$ and $\mathbb{F}_{2^{191}}$
  - **Timings:**

Pentium 200 MHz

m	Language	Mul. (μsec)	Inv. AIA (μsec)	kP (msec)
167	C	37.00	200.00	-
191	C	51.00	260.00	96.4

MC68302, 25 MHz

m	Language	Mul. (msec)	Inv. AIA (msec)	kP (sec)
167	Assembly	6	40	12
167	C	7	60	13

2 Performance of ECC over $\mathbb{F}_p$

- "Efficient elliptic curve exponentiation using mixed coordinates"[7]
  - **Author:** Henri Cohen *et al*, 1998
  - **Platform:** UltraSPARC 143MHz, GMP library; languages: C and assembly
  - **Curves**: Random curves over $\mathbb{F}_{p_{160}}$, $\mathbb{F}_{p_{192}}$ and $\mathbb{F}_{p_{224}}$
  - **Timings:**

p size	Sqr. (μsec)	Mul. (μsec)	Inv. (μsec)	kP (msec)
160	5.35	6.50	166	16.17
192	7.22	8.93	213	24.93
224	9.01	12.00	261	35.73

- "On the performance of signatures schemes based on elliptic curves" [10]
  - **Author:** E. De Win *et al*, 1998
  - **Platform** Pentium Pro 200 MHz; languages: C, assembly
  - **Curves:** Random curves
  - **Timings:**

m	Sqr. (μsec)	Mul. (μsec)	Inv. (μsec)	kP (msec)
192	7.6	7.8	180	21.1

3 Performance of ECC over $\mathbb{F}_{p^m}$

- "Inversion in optimal extension fields" [5]
  - **Author:** Daniel Bailey and Christof Paar
  - **Platform** Pentium/MMX 233 MHz (C++), Alpha 600 MHz (assembly)
  - **Curves:** Random curves over $\mathbb{F}_{(2^{31}-1)^6}$ and $\mathbb{F}_{(2^{61}-1)^3}$
  - **Timings:**

Field	Language	Mul. (μsec)	Inv. (μsec)	kP (msec)
$\mathbb{F}_{(2^{61}-1)^3}$	Assembly	0.37	2.94	1.09
$\mathbb{F}_{(2^{31}-1)^6}$	C++	5.82	30.0	13.1

- "Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic" [16]
  - **Author:** Tetsutaro Kobayashi *et al*, 1999

- **Platform** DEC Alpha 500 MHz, Pentium II 400 MHz; language: assembly
- **Curves:** Frobenius map $\mathbb{F}_{(2^{31}-1)^6}$ and $\mathbb{F}_{(2^{61}-1)^3}$
- **Timings:** Milliseconds

Field	Machine	kP
$\mathbb{F}_{(2^{61}-1)^3}$	Alpha 500	0.994
$\mathbb{F}_{(2^{31}-1)^6}$	PII 400	1.95

4 ECC-$\mathbb{F}_{2^m}$ vs ECC-$\mathbb{F}_p$

- "On the performance of hyperelliptic cryptosystems" [23]
  - **Author:** Nigel P. Smart, 1999
  - **Platform:** Pentium Pro 334MHz, Microsoft Visual C++
  - **Curves:** Random curves over $\mathbb{F}_{2^{161}}$ and $\mathbb{F}_{p_{160}}$
  - **Timings:** Milliseconds

System	Signature	Verification
ECDSA-$\mathbb{F}_{2^{161}}$	4	19
ECDSA-$\mathbb{F}_{p_{160}}$	3	17

- "High-Speed implementation of an ECC-base wireless authentication protocol on an ARM processor" [2]
  - **Author:** M. Aydo, T. Yanik, and C. K. Koc, 1999
  - **Platform:** 32-bit ARM7TDMI processor, 80 MHz
  - **Curves:** Random curves over $\mathbb{F}_{p_{160}}$
  - **Timings:** Milliseconds

System	Signature	Verification
ECDSA-$\mathbb{F}_{p_{160}}$	46	94

5 ECC vs RSA and DL

- "On the performance of signatures schemes based on elliptic curves" [10]
  - **Author:** Eric De Win *el al*, 1998
  - **Platform:** Pentium Pro 200 MHz; languages: C, C++, assembly
  - **Curves:** Random curves over $\mathbb{F}_{2^{191}}$ and $\mathbb{F}_{p_{192}}$
  - **Timings:** Milliseconds

System	Key generation	Signature	Verification
ECDSA-$\mathbb{F}_{2^{191}}$	11.7	11.3	60
ECDSA-$\mathbb{F}_{p_{192}}$	5.5	6.3	26
RSA-1024	1 sec	43.3	0.65
DSA-1024	22.7	23.6	28.3

- "The Koran certificate-based digital signature algorithm" [15]
  - **Author:** KCDSA, Task Force Team, 1998
  - **Platform:** Pentium Pro 200 MHz; languages: C, assembly
  - **Curves:** Random curves over $\mathbb{F}_{p_{160}}$
  - **Timings:** Milliseconds

System	Signature	Verification
KCDSA	3.3	20.9
RSA-1024	33.1	1.7
DSA-1024	3.9	21.7

- "The elliptic curve cryptosystem for smart cards" [6]
  - **Author:** Certicom, white paper, 1998
  - **Platform:** UltraSPARC 167 MHz; language: C
  - **Curves:** Koblitz curves over $\mathbb{F}_{2^{163}}$
  - **Timings:** Milliseconds (BS v. 1.2 vs BSAFE v. 3.0)

System	Key generation	Signature	Verification
ECDSA-163	3.0	3.8	10.7
RSA-1024	4.7 sec	228.4	12.7

- "A practical implementation of elliptic curve cryptosystems over $\mathbb{F}_p$ on a 16-bit microprocessor" [14]
  - **Author:** Toshio Hasegawa *et al*, 1998
  - **Platform:** M16C (Mitsubishi Electric Coorporation) 10 MHz; assembly
  - **Curves:** Random curves over $\mathbb{F}_{p_{160}}$
  - **Timings:** Milliseconds

System	Signature	Verification
ECDSA	150	630
RSA-1024	10 (sec)	400

- "Experimenting with electronic commerce on the PalmPilot" [8]
  - **Author:** Neil Daswani and Dan Boneh, 1998
  - **Platform:** Motorola Dragon Ball 15 MHz; language C
  - **Curves:** Koblitz curves over $\mathbb{F}_{2^{163}}$
  - **Timings:** Milliseconds

System	Key generation	Signature	Verification
ECDSA	590	800	2340
RSA-512	360 (sec)	5100	310

- "Elliptic-Curve cryptography" [11]
  - **Author:** Andrew Fernandez, 1999
  - **Platform:** Celeron 450 MHz GnuPG V 0.9.5 (hand-optimized assembler code)
  - **Curves:** Special curve over $\mathbb{F}_p$, $p = 2^{255} + 95$ (complex multiplication)
  - **Timings:** Milliseconds

System	Signature	Verification
ECDSA	35.63	76.09
DSA-1024	28.44	43.28
DSA-2048	109.69	219.38

- "Fast implementation of public-key cryptography on a DSP TMS320C6201" [12]
  - **Author:** Kouichi Itoh *et al*, 1999
  - **Platform:** DSP TMS320C6201 200 MHz, (assembly language for the finite field arithmetic)
  - **Curves:** Random curve over $\mathbb{F}_{p_{160}}$, $\mathbb{F}_{p_{192}}$ and $\mathbb{F}_{p_{239}}$.
  - **Timings:**Milliseconds

System	Signature	Verification
ECDSA-160	1.13	3.97
ECDSA-192	1.67	6.28
ECDSA-239	2.85	11.2
DSA-512	2.93	5.14
DSA-1024	7.44	14.5
RSA-1024	11.7	1.2
RSA-2048	84.6	4.5

- "PGP in constrained wireless devices" [4]
  - **Author:** Michael Brown *et al*, 2000
  - **Platform:** Pager RIM 10 MHz, Pentium II 400 MHz; language: C
  - **Curves:** NIST [21] curves over $\mathbb{F}_{2^m}$, $m = 163, 233, 283$
  - **Protocols:** Elliptic curve digital signature algorithm (ECDSA) and elliptic curve authenticated encryption scheme (ECAES).
  - **Timings:** Milliseconds

Timings on the Pager

Koblitz curves

System	Key Generation	Signature	Verification
ECDSA-163	751	1,011	1,826
ECDSA-233	1,552	1,910	3,701
ECDSA-283	2,369	2,760	5,485

Koblitz curves

System	Encryption	Decryption
ECAES-163	1,759	1,065
ECAES-233	3,475	2,000
ECAES-283	5,227	2,932

Random curves

System	Key Generation	Signature	Verification
ECDSA-163	1,085	1,335	3,243
ECDSA-233	2,478	3,066	7,321
ECDSA-283	3,857	4,264	11,587

Random curves

System	Encryption	Decryption
ECAES-163	3,132	2,114
ECAES-233	6,914	4,593
ECAES-283	11,264	7,498

RSA ($e = 2^{16} + 1$) and DSA

System	Key Generation	Signature	Verification
RSA-1024	580,405	15,889	1,008
RSA-2048	-	111,956	3,608
DSA-768	-	6,031	11,594
DSA-1024	-	9,529	18,566

ElGamal

System	Key Generation	Encryption	Decryption
ElGamal-768	-	16,078	26,958
ElGamal-1024	-	26,558	57,248

Timings on the Pentium II

Koblitz curves

System	Key Generation	Signature	Verification
ECDSA-163	1.47	2.11	4.09
ECDSA-233	3.11	4.03	7.87
ECDSA-283	4.50	5.64	11.46

Koblitz curves

System	Encryption	Decryption
ECAES-163	4.37	2.85
ECAES-233	7.83	4.85
ECAES-283	11.02	6.78

Random curves

System	Key Generation	Signature	Verification
ECDSA-163	2.12	2.64	6.46
ECDSA-233	4.58	5.52	14.08
ECDSA-283	6.88	8.08	21.15

Random curves

System	Encryption	Decryption
ECAES-163	6.67	4.69
ECAES-233	13.99	9.55
ECAES-283	20.86	13.88

RSA ($e = 2^{16} + 1$) and DSA

System	Key Generation	Signature	Verification
RSA-1024	2,740.87	66.56	3.86
RSA-2048	26,442.04	440.69	13.45
DSA-768	14,735	15.55	26.13
DSA-1024	54,674	24.28	47.23

ElGamal

System	Key Generation	Encryption	Decryption
ElGamal-768	219,820	35.91	59.53
ElGamal-1024	1,200,157	67.78	144.73

References

[1] M. Aydos, E. Savas, and Ç. K. Koç, "Implementing network security protocols based on elliptic curve cryptography", *Proceedings of the Fourth Symposium on Computer Networks*, pp. 130-139, Istanbul, Turkey, May 20-21, 1999.

[2] M. Aydo, T. Yanik, and C. Koc, "High-Speed implementation of an ECC-base wireless authentication protocol on an ARM processor", submitted for publication, `http://www.security.ece.ort.edu`, December 1999.

[3] Bogdan Antonescu, *Elliptic curve cryptosystems on embedded microprocessors*, Master's thesis, ECE Dept., Worcester Polytechnic Institute, Worcester, USA, May 1999.

[4] Michael Brown, Donny Cheung, Darrel Hankerson, Julio Lopez Hernandez, Michael Kirkup, and Alfred Menezes, "PGP in constrained wireless devices", *Proceedings of the 9th USENIX Security Symposium*, 2000, to appear.

[5] Daniel Bailey and Christof Paar, "Inversion in optimal extension fields", *Proceedings of the Conference on The Mathematics of Public Key Cryptography*, Toronto, Canada, June 12-17, 1999.

[6] Certicom, The elliptic curve cryptosystem for smart cards", white paper, 1998. `http://www.certicom.com`

[7] H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates", In *Asiacrypt'98*, LNCS **1514**, pp. 51-65, Springer-Verlag, 1998.

[8] Neil Daswani and Dan Boneth, "Experimenting with electronic commerce on the PalmPilot". In *Proceedings Eurocrypt'99*, LNCS **1648**, pp. 1-16, Springer-Verlag, 1999.

[9] E. De Win, A. Bosselaers, S. Vanderberghe, P. De Gersem and J. Vandewalle, "A fast software implementation for arithmetic operations in $GF(2^n)$," *Advances in Cryptology, Proc. Asiacrypt'96*, LNCS **1163**, pp. 65-76, Springer-Verlag, 1996.

[10] E. De Win, S. Mister, B. Prennel and M. Wiener, "On the performance of signature based on elliptic curves". In *Algorithmic Number Theory, Proceedings Third Intern. Symp.*, ANTS-III, LNCS **1423**, pp. 252-266, Springer-Verlag, 1998.

[11] Andrew Fernandez, "Elliptic-Curve cryptography", Dr. Dobb's Journal, December, 1999.

[12] K. Itoh, M. Takenaka, N. Torii, S. Temma, and Y. Kurihara, "Fast implementation of public-key cryptography on a DSP TMS320C6201", In *Proceedings of the First Workshop on Cryptographic Hardware and Embedded Systems (CHES'99)*, LNCS **1717**, pp. 61-72, Springer-Verlag, 1999.

[13] J. Guajardo and C. Paar, "Efficient algorithms for elliptic curve cryptosystems", *Advances in Cryptology, Proc. Crypto'97*, LNCS **1294**, pp. 342-356, 1997.

[14] T. Hasegawa, J. Nakajima and M. Matsui, "A practical implementation of elliptic curve cryptosystems over $\mathbb{F}_p$ on a 16-bit microcomputer", *Public Key Cryptography - Proceedings of PKC'98*, LNCS **1431**, pp. 182-194, 1998.

[15] KCDSA, Task Force Team, "The Korean certificate-based digital signature algorithm", 1998.

[16] Tetsutaro Kobayashi, Hikara Morita, Kunio Kobayashi, and Fumikata Hoshio, "Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic",*Eurocrypt'99*, LNCS **1592**, pp. 176-189, 1999.

[17] LiDIA Group **LiDIA v1.3**- *A library for computational number theory*. TH-Darmstadt, 1998.

[18] J. Lopez and R. Dahab, "Improved algorithms for elliptic curve arithmetic in $GF(2^n)$", *SAC'98*, LNCS **1556**, pp. 201-212, Springer-Verlag, 1998.

[19] J. Lopez and R. Dahab, "Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation", *CHES'99*, LNCS **1717**, pp. 316-327, Springer-Verlag, 1999.

[20] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[21] National Institute of Standards and Technology, "Digital signature standard", FIPS Publication 186-2, February 2000. Available at `http://csrc.nist.gov/fips`

[22] R. Schroeppel, H. Orman, S. O'Malley and O. Spatscheck, "Fast key exchange with elliptic curve systems," *Advances in Cryptology, Proc. Crypto'95*, LNCS **963**, pp. 43-56, Springer-Verlag, 1995.

[23] Nigel P. Smart, "On the performance of hyperelliptic cryptosystems", Eurocrypt'99, LNCS **1592**, pp. 165-175, 1999.

[24] J. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves", *Advances in Cryptology -Crypto'97*, LNCS **1294**, Springer-Verlag, 357-371, 1997.

[25] J. Solinas, "Efficient arithmetic on Koblitz curves", *Designs, Codes and Cryptography*, **19**, pp. 195-249, 2000.