A Comparison of Practical Public-Key Cryptosystems based on Integer Factorization and Discrete Logarithms

(extended abstract)

Paul C. van Oorschot †
Bell-Northern Research, Ottawa, Canada

Since its inception in the mid 1970's, public-key cryptography has flourished as a research activity, and significant theoretical advances have been made. In more recent years, many public-key concepts have gained acceptance in the commercial world. Without question, the best-known public-key cryptosystem is the RSA system of Rivest, Shamir and Adleman [28]. Although not as well-known, another public-key cryptosystem of practical interest is that due to ElGamal [11]. The latter system and its variations use a basic extension of Diffie-Hellman key exchange [9] for encryption, together with an accompanying signature scheme. Elliptic curve cryptosystems, introduced by Miller [24] and Koblitz [12], have also recently received much attention as cryptographic alternatives.

The security of the RSA and ElGamal cryptosystems is generally equated to the difficulty of integer factorization and that of the computation of discrete logarithms in finite fields, respectively. Based on the current literature, this survey considers a detailed analysis of a version of the multiple polynomial quadratic sieve integer factorization algorithm [26], and a variation of the Coppersmith algorithm for computing discrete logarithms in $GF(2^n)$ [6]. The analysis is used for a practical security comparison between the RSA cryptosystem and the ElGamal cryptosystem in fields of characteristic two. By "practical" we mean a comparison suitable for dealing with particular problem instances of practical interest, rather than dwelling exclusively on asymptotic complexities. The algorithms analyzed are the best general practical algorithms currently known for the respective problems, for problem sizes of cryptographic interest. Other aspects of the cryptosystems are considered in addition to relative security, including practical efficiency. The security of elliptic curve cryptosystems, which is generally equated to the difficulty of extracting elliptic curve logarithms (the elliptic curve analogue of the discrete logarithm problem), is also discussed and related to that of the previously mentioned cryptosystems. The recent reduction [23] of

†Partial support for this work was provided by the University of Waterloo, Waterloo, Ontario, and by Newbridge Microsystems, Kanata, Ontario.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 576-581, 1991.

prove to be a competitive factoring technique for general integers of sizes of cryptographic interest. Elliptic curve factorization allows extraction of smaller factors (up to 30 or 40 digits) from relatively large numbers (up to 200 digits). The number field sieve applies to a small class of numbers including those of the form $N = r^e \pm s$ for small integers r and s, and runs in heuristic expected time $\exp((c+o(1))(\ln N)^{1/3}(\ln\ln N)^{2/3})$, where $c \approx 1.526$; it has been used to factorize the 155-digit ninth Fermat number, $2^{512}+1$. The generalized number field sieve applies to general integers, and has a running time constant of $c = 3^{2/3} \approx 2.08$; further research is underway to improve upon this constant. While asymptotically significantly faster than all previous general factoring algorithms, the generalized number field sieve is not currently practical for integers of cryptographic interest.

While the elliptic curve method and the number field sieve have been used to factor numbers of special form much larger than can be factored at present using the quadratic sieve, such numbers can be easily avoided in cryptographic applications. The quadratic sieve (in particular, the multiple polynomial version, suggested by Davis and independently by Montgomery) remains the most efficient general purpose factoring algorithm in 1990. Two important new ideas that apply to the quadratic sieve have been demonstrated by A.K. Lenstra and Manasse. The first is the use of electronic mail to coordinate the activities of large networks of "anonymous" workstations [18]; this has changed the rules somewhat regarding what should generally be considered as computationally feasible. The second is the "two large prime" version used for collecting sparse equations [19].

The discrete logarithm problem has also been the subject of much study in recent years. The computation of discrete logarithms in odd prime fields GF(p) is discussed by Coppersmith et al. [7] and by LaMacchia and Odlyzko [15]. The latter paper indicates that in practice the computation of discrete logarithms in GF(p), using the best currently known techniques, is slightly harder than factorization of integers N (where $N \approx p$) via the multiple polynomial quadratic sieve. We restrict attention primarily to fields of characteristic two - these traditionally being of practical interest, as arithmetic in such fields is particularly amenable to efficient hardware implementation. Early work by Blake et al. [3] rendered the field $GF(2^{127})$ totally inadequate for cryptographic security; a key size of 127 bits, which corresponds to 38 digits, is simply insufficient. Subsequent work by Coppersmith [6] and Odlyzko [25] led to further improvements in the index-calculus techniques for computing logarithms in larger fields $GF(2^n)$. There has been a lack of further practical work in fields of characteristic two, although it appears there is renewed interest of late. Recent surveys discussing discrete logarithms include [16], [1], and [21].

Efficient techniques for the solution of large sparse linear systems over finite fields are important in both factoring and extracting discrete logarithms. Progress on this front has been made by Wiedemann [34], and LaMacchia and Odlyzko [14].

The Diffie-Hellman key exchange technique and the related ElGamal cryptosystem can be carried out using the group of points of an elliptic curve over a finite field, resulting in elliptic curve cryptosystems as noted above. The apparent absence of efficient attacks on elliptic curve systems (and efficient general algorithms for computing elliptic curve logarithms) has resulted in the belief that these systems with relatively short keylengths may afford greater security than alternative cryptosystems with larger keylengths. Shorter keylengths imply simpler implementations of arithmetic, and smaller bandwidth and memory requirements - important in smart card applications, among others.

Menezes, Okamoto and Vanstone [23] have recently shown that for certain classes of curves over fields GF(q), the elliptic curve logarithm problem can be reduced to the discrete logarithm problem in an extension field $GF(q^k)$. In general k is exponentially large and the reduction takes exponential time, but for *supersingular* curves, k is small and the reduction is probabilistic polynomial time - yielding a subexponential-time elliptic curve logarithm algorithm. The cryptographic impact of this is that special care must now be taken in the particular choice of elliptic curve, either avoiding the supersingular curves or compensating for the new algorithm by using appropriately larger fields to preserve security. These larger fields in the latter case may still be smaller than those required for equivalent security in other types of cryptosystems, in which case even these elliptic curve systems remain attractive in practice. Ironically, the classes of curves susceptible to the new attack include many of those which have previously been recommended for use, including curves originally suggested by Miller [24], Koblitz [12], Bender and Castagnoli [2], and Menezes and Vanstone [22].

Significant advances have also been made in recent years, in theory and in practice, on techniques for efficient implementation of the cryptosystems in question. For RSA modular exponentiation, these include custom VLSI chips (see Brickell's survey [4]), efficient digital signal processor software implementations (e.g. Dussé and Kaliski [10]), and a Programmable Active Memory implementation by Shand et al. [31]. Custom VLSI chips for arithmetic operations in $GF(2^n)$ are now also available (see Rosati [29]). Schnorr has recently proposed a signature scheme for ElGamal-like cryptosystems resulting in shorter signatures that can be both constructed and verified more efficiently than in ElGamal's original proposal [30]. Implementation of elliptic curve cryptosystems over

fields of characteristic two has recently been studied by Menezes and Vanstone [22] and Koblitz [13].

References

[1] E. Bach, "Intractable problems in number theory", *Advances in Cryptology - Crypto 88*, S. Goldwasser (ed.), *Lecture Notes in Computer Science* 403, Springer-Verlag (1990), 77-93.

[2] A. Bender and G. Castagnoli, "On the implementation of elliptic curve cryptosystems", *Advances in Cryptology - Crypto 89*, G. Brassard (ed.), *Lecture Notes in Computer Science* 435, Springer-Verlag (1990), 186-192.

[3] I.F. Blake, R. Fuji-Hara, R.C. Mullin, and S.A. Vanstone, "Computing logarithms in finite fields of characteristic two", *SIAM J. Alg. Disc. Meth.* 5 (2), June 1984, 276-285.

[4] E.F. Brickell, "A survey of hardware implementations of RSA (abstract)", *Advances in Cryptology - Crypto 89*, G. Brassard (ed.), *Lecture Notes in Computer Science* 435, Springer-Verlag (1990), 368-370.

[5] T.T. Caron and R.D. Silverman, "Parallel Implementation of the quadratic sieve", *J. Supercomput.* 1 (1988), 273-290.

[6] D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two", *IEEE Transactions on Information Theory* IT-30 (4), July 1984, 587-594.

[7] D. Coppersmith, A.M. Odlyzko, and R. Schroeppel, "Discrete logarithms in GF(p)", *Algorithmica* 1 (1), 1986, 1-15.

[8] J.A. Davis, D.B. Holdridge, and G.J. Simmons, "Status report on factoring", *Advances in Cryptology - Eurocrypt 84*, T. Beth, N. Cot, I. Ingemarsson (eds.), *Lecture Notes in Computer Science* 209, Springer-Verlag (1985), 183-215.

[9] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory* IT-22 (6), Nov. 1976, 644-654.

[10] S.R. Dussé and B.S. Kaliski, Jr., "A cryptographic library for the Motorola DSP56000", *Advances in Cryptology - Eurocrypt 90*, I. Damgard (ed.), to appear.

[11] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory* IT-31 (4), July 1985, 469-472.

[12] N. Koblitz, "Elliptic curve cryptosystems", *Math. Comp.* 48 (1987), 203-209.

[13] N. Koblitz, "Constructing elliptic curve cryptosystems in characteristic 2", *Advances in Cryptology - Crypto 90*, S.A. Vanstone (ed.), to appear.

[14] B.A. LaMacchia and A.M. Odlyzko, "Solving large sparse linear systems over finite fields", *Advances in Cryptology - Crypto 90*, S.A. Vanstone (ed.), to appear.

[15] B.A. LaMacchia and A.M. Odlyzko, "Computation of discrete logarithms in prime fields", *Advances in Cryptology - Crypto 90*, S.A. Vanstone (ed.), to appear.

[16] A.K. Lenstra and H.W. Lenstra, Jr., "Algorithms in number theory", in *Handbook of theoretical computer science*, A. Meyer, M. Nivat, M. Paterson, D. Perrin (eds.), North Holland, Amsterdam, to appear.

[17] A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse and J.M. Pollard, "The number field sieve", *Proc. 22nd ACM Symp. Theory of Computing* (1990), 564-572.

[18] A.K. Lenstra and M.S. Manasse, "Factoring by electronic mail", *Advances in Cryptology - Eurocrypt 89,* J.-J. Quisquater and J. Vandewalle (eds.), *Lecture Notes in Computer Science* 434, Springer-Verlag (1990), 355-371.

[19] A.K. Lenstra and M.S. Manasse, "Factoring with two large primes", *Advances in Cryptology - Eurocrypt 90,* I. Damgard (ed.), to appear.

[20] H.W. Lenstra, Jr., "Factoring with elliptic curves", *Ann. of Math.* 126 (1987), 649-673.

[21] K.S. McCurley, "The discrete logarithm problem", in *Cryptography and Computational Number Theory,* C. Pomerance (ed.), *Proc. Symp. Appl. Math.*, Amer. Math. Soc. (1990), to appear.

[22] A. Menezes and S. Vanstone, "The implementation of elliptic curve cryptosystems", *Advances in Cryptology - Auscrypt 90,* J. Seberry and J. Pieprzyk (eds.), *Lecture Notes in Computer Science* 453, Springer-Verlag (1990), 2-13.

[23] A. Menezes, S. Vanstone and T. Okamoto, "Reducing elliptic curve logarithms to logarithms in a finite field", presented at *Crypto 90*; to appear in *Proc. 23rd ACM Symp. Theory of Computing* (1991).

[24] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology - Crypto 85,* H. Williams (ed.), *Lecture Notes in Computer Science* 218, Springer-Verlag (1986), 417-426.

[25] A.M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", *Advances in Cryptology - Eurocrypt 84,* T. Beth, N. Cot, I. Ingemarsson (eds.), *Lecture Notes in Computer Science* 209, Springer-Verlag (1985), 224-314.

[26] C. Pomerance, "Analysis and comparison of some integer factoring algorithms", in *Computational Methods in Number Theory,* H.W. Lenstra, Jr. and R. Tijdeman (eds.), Math. Centrum Tract 154, 1982, 89-139.

[27] C. Pomerance, J.W. Smith and R. Tuler, "A pipeline architecture for factoring large integers with the quadratic sieve algorithm", *SIAM J. Computing* 17 (2), Apr. 1988, 387-403.

[28] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM* 21 (1978), 120-126.

[29] T. Rosati, "A High Speed Data Encryption Processor for Public Key Cryptography", *Proceedings of the IEEE Custom Integrated Circuits Conference*, May 1989.

[30] C.P. Schnorr, "Efficient identification and signatures for smart cards", *Advances in Cryptology - Crypto 89,* G. Brassard (ed.), *Lecture Notes in Computer Science* 435, Springer-Verlag (1990), 239-251.

[31] M. Shand, P. Bertin and J. Vuillemin, "Hardware speedups in long integer multiplication", *Proceedings of the 2nd ACM Symposium on Parallel Algorithms and Architectures*, Crete, July 2-6, 1990, to appear.

[32] R.D. Silverman, "The multiple polynomial quadratic sieve", *Math. Comp.* 48 (1987), 329-339.

[33] G.J. Simmons (ed.), *Contemporary Cryptology: The Science of Information Integrity*, IEEE press, to appear.

[34] D.H. Wiedemann, "Solving sparse linear equations over finite fields", *IEEE Transactions on Information Theory* IT-32 (1), Jan. 1986, 54-62.