RSA SECURITY

PRODUCTS SERVICES TRAINING PARTNERS RSA ONLINE: MEMBERS ONLY

NEWS COMPANY EVENTS RSA Worldwide GO

BUY CONTACT DOWNLOAD SUPPORT SEARCH GO

RSA Security Home > RSA Laboratories > Tech Notes > ECC Recommendations

More About

- Bulletins
- Challenges
- Crypto FAQ
- CryptoBytes
- RSA Algorithm
- PKCS
- Advanced Encryption Standard
- Tech Notes
- Staff & Associates
- Standards

Recommendations on Elliptic Curve Cryptosystems

Burton S. Kaliski Jr., Ph.D.

An RSA Laboratories Technical Note
Revised March 1998

Elliptic curve cryptosystems have recently come into strong consideration, particularly by standards developers, as alternatives to established standard cryptosystems such as the RSA cryptosystem and cryptosystems based on the discrete logarithm problem, including Diffie-Hellman and the Digital Signature Standard. Some are calling elliptic curve cryptosystems "the next generation" of public-key cryptography, providing greater strength, higher speed, and smaller keys than established systems.

Elliptic curve cryptosystems have a number of interesting properties, which may make them appropriate tools for meeting security requirements in some cases, and not in others. RSA Laboratories is currently recommending that *elliptic curve cryptosystems continue to be studied as additional tools in the public-key repertoire*, and that they be considered as near-term solutions in the particular cases where the alternative would be to have no security at all.

The rationale for this recommendation is as follows.

1. From a cryptographic perspective, the primary motivation for development of elliptic curve cryptosystems is that they are based on a different number-theoretic problem than established systems, having a reasonable expectation of security, without significant additional cost. Many public-key cryptosystems have been proposed over the years as additions to the established systems. Quite a few of them have been broken, and others have been found too costly. Elliptic curve cryptosystems appear promising at this point and deserve further analysis.

2. In certain applications, elliptic curve cryptosystems can provide security where other systems currently do not fit. However, the range of applications where they make a significant difference is limited, primarily for the reason that in typical applications of cryptography, public-key operations are employed in combination with other techniques, in a way that gains the benefits of both sets of tools. In particular, public-key operations often represent only a minor overhead in the total processing, whether in storage or in computation time. (Consider the fact that typical standard "certificates" bearing public keys are often 1000 bytes or longer - only 20 percent or so of which are related directly to public-key cryptography.) The availability of cryptographic accelerators also keeps the overhead down, particularly in high-volume servers. A "faster" or "smaller" public-key technique thus may have little overall impact in many applications. Established techniques already "fit" in many applications, and given the development of computing technology, what doesn't fit today is likely to fit in the not-too-distant future.

3. Elliptic curve cryptosystems have, at this point, relatively fewer cryptanalytic results than established systems, an observation that can be interpreted positively or negatively: It could be that the systems are stronger, or it could be that they are just not that well understood. In either case, this is an observation that calls for further study.

The main results to date are a 1991 subexponential-time algorithm for "supersingular" elliptic curves (the "MOV reduction" of Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone), a generalization of this result published in 1994 by Gerhard Frey and Hans-Georg Rück, and a linear-time algorithm for "trace-1" elliptic curves, announced in September 1997 independently by Nigel Smart and by Takakazu Satoh and Kiyomichi Araki. The trace-1 result also appears in a January 1998 *Mathematics of Computation* article by I.A. Semaev.

What is somewhat surprising about the trace-1 result is that it was assumed to be common knowledge by several number theorists before 1997, and thus was not previously published. For instance, Ed Schaefer mentioned the result as a "well known fact" at the West Coast Number Theory Conference in 1996. The fact that the trace-1 case had not been considered in elliptic curve cryptography standards prior to 1997 shows the gap that remains between number theorists and cryptographers in this area.

Meanwhile, Leonard Adleman, Jonathan DeMarrais and Ming-Deh Huang exhibited in 1994 a subexponential-time algorithm for a certain class of so-called "hyperelliptic curves". While this result has no immediate applications to elliptic curves, it is somewhat surprising, at least to one who assumes that "hyperelliptic" somehow suggests greater security. (Hyperelliptic curves have

> also been suggested for cryptographic use.)
>
> By contrast, there is a substantial body of experience, both theoretical and practical, on the security of RSA, or DES to give another example. In particular, there have been numerous implementations of integer factorization techniques for small-key-size RSA systems as part of the RSA Factoring Challenge, as well as a variety of research results on factoring since the introduction of RSA, which combine to give an level of confidence for the RSA cryptosystem. Elliptic curve cryptosystems deserve a similar investment.

The rationale should be contrasted with what is sometimes claimed about elliptic curve systems: that, without qualification, they are stronger and faster than established systems. Since the strength of an established system such as RSA is a function of its key size, it is more accurate to say that elliptic curve systems (at least under the current state of cryptanalysis) appear to be more secure at a given key size. But in absolute terms, either system can be as strong as desired for an application. Speed is also a function of key size, and at a given key size elliptic curve systems are in fact slower than established systems. Adjusting key sizes for equal strength against current techniques, elliptic curve cryptosystems are faster than established systems for many operations. But in absolute terms, both elliptic curve cryptosystems and established systems are often fast enough.

There have been a good number of results on the implementation of elliptic curve cryptosystems, both in performing cryptographic operations and in constructing elliptic curves with a known "order", an operation essential to the setup of an elliptic curve cryptosystem. While there are some open questions related to adapting elliptic curve cryptosystems to certain functions (in particular, encryption of quantities such as keys that may be larger than the elliptic curve key size), solutions are forthcoming.

A number of groups are tracking elliptic curve technology from various perspectives. Research is ongoing at a number of universities, including Royal Holloway College, as well as commercial organizations, including Certicom, and at the National Security Agency. RSA Laboratories has been involved for several years in the standardization of elliptic curve cryptosystems as part of the IEEE P1363 project, "Standard for Public-Key Cryptography" (which also covers established techniques, including RSA). RSA Laboratories is also studying techniques for efficient implementation of elliptic curve cryptosystems (as it studies techniques for established systems). The November 1997 Workshop on the Elliptic Curve Discrete Logarithm Problem, sponsored by University of Waterloo, provided an opportunity for further exchange of information, and other such workshops are expected. Thus, there are a variety of sources from which to draw further assessment of elliptic curve cryptosystems, and, should they continue to withstand scrutiny, from which to provide appropriate tools for security. RSA Laboratories will continue to report on developments on elliptic curve cryptosystems, and appreciates any questions or comments on this note.

A more detailed discussion of elliptic curve cryptosystems can be found in a companion RSA Laboratories technical note by Matthew J.B. Robshaw and Yiqun Lisa Yin, "Elliptic Curve Cryptosystems."

United States: 1-877-RSA-4900 or 781 515 5000, Europe, Middle East, Africa: +44 (0)1344 781000,
Asia/Pacific: +65 733 5400, Japan: +81 3 5222 5200

Home | Contact Us | Search | Terms of Use and Privacy Statement