Security Level of Cryptography- ECAES

1 Cryptographic Primitive

Name: ECAES (Elliptic Curve Augmented Encryption Scheme)
Category: Asymmetric Cryptographic Schemes
Security Function: Confidentiality

2 Evaluation

2.1 The Underlying Number Theoretic Problem

The scheme is based on one of the the hardness of the equivalent of Diffie-Hellman (D-H and cofactor D-H) problem (related to disc. log.) over elliptic curves.

The background and material presented are in quite an advanced stage of documents for standards and includes many issues (like string representation conversions) that other submissions do not have. This is due to the fact that it seems to be a document sent to various standard bodies earlier. The suggested scheme is part of a larger standard.

The problem is known to be hard and due to its current hardness, the size of the key and the size of encryptions is small. This may become a most desirable alternative when RSA like systems would reach 4k size for their security. The strength of the system is that unlike the arithmetic case, the disc. log. finding algorithms for d.log. over EC known for the general case are generic methods (whose state of the art is correctly described in the mathematical commentary part). (Of course one has to avoid special cases known to be easy, but the random choice seems to be good enough).

One popular view is that EC methods are too young, however they have been around for a while and there is slow progress in understanding the easy cases. It is true that there are not enough people in cryptanalysis who understand EC as well as they understand other areas of number theory. However, EC D. Log. seems to

be a hard problem. One can take precautions and increase the size of the suggested scheme by 20-40 bits (over the 160 bit long suggestion) to assure certain added security on a national level. Note that it is hard to predict real advancement in any number theoretic area (be it ECC or elementary number-theoretic cryptography).

The scheme suggested is actually two schemes: EC over a prime order field and another one over GF(2^n). Both are hard problems of the

Methods for validation of the parameters and the curves are supplied (this is a necessary requirement which is done right).

The methods can be the D-H, or the cofactor D-H. The defenses of the two methods are explained in the mathematical commentary part.

2.2 Semantic security evaluation

Like the regular discrete log, under decisional Diffie-Hellman (the randomness of the resulting combined value), semantic security can be assured. It is explained briefly in B.2.3 of the SEC1 document. commentary. The security under the decisional problem is directly related to the assumption (no reduction in security).

2.3 Complexity Theory and Security against active attacks

The scheme does not provide measures against active attacks and need preprocessing augmentations to enable such security in he random oracle model. Such augmentations seem possible and are actually dealt with in another submission.

2.4 Other problems, issues and considerations

The schemes present a few crucial issues. One is that key generation (finding the right element of the correct order) requires a lot of preprocessing work.

The scheme therefore comes with an appendix (SEC2) of suggested curves and points, generated pseudo-randomly by the authors.

Such schemes as far as the state of key generation stays as it is (and I do not see any improvement, soon), will require maintaining such tables of suggested public curves and points for people to use.

One can trust the designers, but for a national level standard, generating further and incrementally adding more parameters is required. The maintenance board of the standard should be in charge of calculating alternatives for usage, so that not all choices are going to fall on one curves or one field. This adds operational over-head in maintaining and advancing the standard.

GENERAL REMARK AA: I believe that for a method based on suggested public number theoretic parameters, a national body should maintain the parameters and update them.

ALTERNATIVES: For the size parameters of ECC, the only recent alternative is perhaps Lenstra and Verhul's XTR (which may also be represented as an EC problem). If size is not an issue then traditional ElGamal/D-H methods are the alternative.

Another point of consideration is that much research on ECC is being conducted in Japan, having some ECC alternative and maintaining and reviewing progress in the field may be advantageous if done in Japan under some maintenance agency.

SIZE ISSUE and Multi Block Encryption: Since the encryption block may be too small, one needs a "mode" of encryption to concatenate related plaintexts. Merely putting two pieces together will not be enough and will open the door to potential attacks. One better build on "block chaining" practices, and apply them to the encryption. For example, one needs to send an encryption and MAC keys and need to put them in two blocks, these blocks should be uniquely connected, to prevent attacks.