Security Level of Cryptography- EPOC

1 Cryptographic Primitive

Name: EPOC

Category: Asymmetric Cryptographic Schemes

Security Function: Confidentiality

2 Evaluation

2.1 The Underlying Number Theoretic Problem

The scheme is based on one of the most remarkable advances in public key encryption, namely the Okamoto-Uchiyama scheme. The scheme is based on a new type of trapdoor. It and its modification by Pailler are very interesting new developments in cryptography in the last few years.

The scheme is actually three schemes,

EPOC-1,-2 and -3.

Some of the schemes are directed towards the hybrid encryption mode.

GENERAL REMARK RR: It is recommended that a general encryption for both the direct encryption and "envelope method" (hybrid asymmetric/symmetric scheme) be developed for each scheme.

GENERAL REMARK LL: It is recommended that in any collection of schemes, the symmetric system used will be based on an encryption method which is secure against forgery (authenticated encryption) including MAC and encryption (see Katz-Yung FSE 2000 and Bellare-Namprempre Asiacrypt 2000). This scheme should be the same everywhere (and be correlated with the symmetric scheme chosen by other part of CRYPTEC).

The scheme is based on a composite number of the form $N = QP^2$. The designer suggest minimal size of primes so that N is hard to factor. Given the state of the art, such a number should not be larger than an N which is a multiple of two primes only. This is

correct, though the EC method can take advantage of the size, it is not as efficient in practice as the best methods. Nevertheless, since special methods exist, and the special method may improve, I would suggest some caution perhaps: e.g. take a number which is 20not a definite measure, since algorithmic advances in factoring is hard to predict. The added size is acceptable assuming the scheme is used mainly for key distribution.

EPOC-1 is based on the p-subgroup assumption, a reasonable new assumption, related to residuosity. EPOC-2 is based on the factoring problem, and EPOC-3 on a gap-factoring.

2.2 Semantic security evaluation

Under the respective assumptions, the schemes are semantically secure (against passive adversary).

2.3 Complexity Theory and Security against active attacks

The scheme employs auxiliary functions like hash function (idealized as random oracle) for the preprocessing (the Okamoto Pointcheval preprocessing of messages).

This preprocessing is very good among the known one. It should be pursued as a general method (replacing OAEP). It gives security against active attacks similar to that of the passive attack in strength.

GENERAL REMARK SS: The auxiliary primitives (hash and pseudo-random-gem.) for preprocessing a message as a materialization of a random oracle accesses should be chosen the same, for any scheme used, in case more than one scheme is chosen. The choice of primitives should depend on the best choice of random-functions in the entire project.

GENERAL REMARK TT: The auxiliary primitives need a "truly random source" a primitive which usually is missing from overall system design. It is recommended to have a "true random generator" which will be used throughout. (It can take up to three sources and exor them together: user generated randomness, system generated randomness, and cryptographic device generated randomness.) This

assures that if one or two components are missing there is still a way to generate randomness (which can later be processed by a pseudo random gen.).

Assuming the random oracle, preprocessing the schemes are proven secure against the strongest attack (adaptive chosen attack).

2.4 Other problems, issues and considerations

I agree with the authors comparisons with other schemes. EPOC-2 seems to be the one which is reduced to the most basic problem (factoring) both for the direct and the hybrid methods. The other assumptions are also reasonable. The performance does not change fundamentally between the schemes.

The schemes can be viewed as two results: the basic encryption function (the new fundamental trapdoor), and preprocessing methods.

The preprocessing method for both the direct and the hybrid encryption schemes should be the method of choice by the best analysis and the fact the in general OAEP applies to non-adaptive CCA (as is known now).

The public key typically specifies a composite, two generators, size parameters and auxiliary schemes (hashing, encryption, etc.). Some of theese parameters should be determined in a standard and may be out of the choice of an individual key. Maintaining what is the parameters associated with a chosen scheme, is required in many other schemes (any preprocessing requires some size determination). In practice such issues generate some procedural requirements that should be solved.

GENERAL REMARK UU: the level of proofs in all the recent papers is as an extended abstract level. It is suggested the journal paper style papers will be written for the suggested schemes. This type of careful writing enables a reviewer to follow the proofs more carefully. It may be a required scrutiny when provable security is a criterion. The example of the notion of security of OAEP (which after careful analysis shows gap) demonstrates the dangers of relying on a collection of extended abstracts in assuming proofs. (On the other hand, I especially looked at the EPOC proofs before and now, and the schemes look valid to me for the current systems).

The choice of the specific trapdoor should be compared to related alternatives, which I believe are in the composite based cryptography, namely Rabin and RSA.

CLOSET ALTERNATIVES AND COMPARISON:

Under the same preprocessing, RSA, Rabin and even the off spring of the current trapdoor (the Pailler scheme) all have similar properties.

The advantage of the current scheme is in the fact that it was designed in Japan, in case there is an advantage on a national level in using a Japanese design. It indeed represents one of the many novel ideas that have come from japan in the last few years in the area of cryptography.

The other alternatives though also have merits. For example RSA (under the suggested preprocessing) can be easily used inside and outside government. I believe the new preprocessing should be pursued in the RSA global standard forum. Thus, with a small change of preprocessing the usage within the government can inter-operate globally. Of course, RSA was not shown provably equivalent to factoring, though it has been around many years and is considered safe in the commercial word.

the suggested preprocessing applies to ElGamal encryption nicely as shown in the submission.