Security Level of Cryptography- ACE

1 Cryptographic Primitive

Name: ACE (Advanced Cryptographic Schemes)
Category: Asymmetric Cryptographic Schemes
Security Function: Confidentiality

2 Evaluation

2.1 The Underlying Number Theoretic Problem

The scheme is based on a theoretical breakthrough, that using the decision D-H assumption Cramer and Shoup designed a scheme which is secure against CCA, without using random oracle assumptions and while being only somewhat less efficient than existing methods (earlier theoretical schemes like this were known which were not implementable).

The decision D-H is fine assumption which seems possible. The scheme is also secure under the regular D-H assumption but with a Random Oracle (in which case one can use ElGamal with preprocessing).

The biggest question in considering such a scheme is how much weight should be put in practice to the fact that this is a unique scheme that achieves what others do while idealizing hash functions without this assumption.

GENERAL REMARK CC: A random oracle assumption should only be assumed about a component independent of the rest of the scheme which can be replaced by a black-box access to a device. This assures that the idealization is correct and that the actual idealized system can be changed. All the schemes under consideration which use random oracle indeed employ it in this manner.

The authors argue strongly against random oracle assumption, yet they hedge with it against the decisional D-H being not true but the computational D-H being true.

CLOSE ALTERNATIVE: ElGamal scheme with a preprocessing like in Okamoto-Pointcheval.

The main issue is how relevant are these arguments in practice, since the scheme compared to the close alternative is less efficient.

Also, if we choose a family of functions: Composite-based-one, Disc-Log one, and ECC based one. If we take a uniform approach of being relatively efficient and based on the same argument then random oracle arguments and the similar preprocessing can serve us uniformly. Note that ACE can be adapted also in the ECC arena.

The concrete analysis used articulate the security well.

The scheme bundles concrete HAS and Pseudo-random functions based on IBM inventions. There is no need to necessarily have such a bundle, and other auxiliary functions can serve well.

2.2 Semantic security evaluation

Under the Decision D-H, we get semantic security. Similarly if we hash and assume D-H as a one-way function

2.3 Complexity Theory and Security against active attacks

The scheme gives under certain assumptions about the auxiliary functions being secure and the decision D-H, a proof of security against active attackers (CCA-2).

The security reduction is well analyzed, showing the system is secure with concrete reduction of security based on number of queries. The proof is complete.

2.4 Other problems, issues and considerations

The problems are key size and extra computations.

The bundling mentioned should be replaced by a more generic arguments about the auxiliary function (I suggested uniformity of these functions).

This alternative is slower, though (half the speed and even less).

Other auxiliary functions can be used.

Even if this alternative is used, a hybrid method and a chained mode may be needed. The scheme adopted the hybrid method for efficiency.

For the ECC variant one can employ precomputed curves.