Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.

Receipt Number	

Cryptographic Techniques Overview

1. Name of Cryptographic Technique

Hierocrypt-L1

Categories 2.Symmetric Ciphers

Security Functions of Asymmetric Cryptographic Schemes

1.confidentiality 2. Authentication 3. signature 4. key- sharing

Subcategories of Symmetric Ciphers

2. 64-bits block ciphers

2. Cryptographic Techniques Overview

2.1 Design policy

- The algorithm was designed to be sufficiently secure against major cryptanalytical attacks, fast in major platforms, and compact in implementation.
- In order to achieve both a high calculational efficiency and a high security, the nested SPN structure is applied to the data randomizing part, which is a recusive version of SPN structure.
- The nested SPN strucure is very simple and makes it possible to achieve a sufficient security and to design algorithmic components independently to some extent.
- The S-box is designed based on the power function over the Galois field GF(2^8), which is the most secure agaist the differential/linear cryptanalysis.
- The diffusion layers are chosen from many candidates with the maximum branch number by criteria on security and performance.
- The fundamental structure of key scheduling part is a 64-bit Feistel network and an iterative 64-bit linear transformation.
- The round key is generated as a linear combination of their intermediate states. A round-trip structure is applied to the fundamental structure, where an intermediate state sequence turn back halfway, so that an initial delay is short for decryption in the on-the-fly implementation.

2.2 Intended applications

- General applications utilized by the electrical government
- Implementation into middleware and LSI utilized by electronic commerce
- System integration business

Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.

Receipt Number	

2.3 Basic theory and techniques

- Theory of the differential/linear cryptanalysis.[1,2)]
- The design rationale to make an SPN-type block cipher which is secure against the differential/linear attack.[3)]
- The theory on provable security of SPN-type block cipher against the differential/linear attack.[4])
- The theory of SQUARE-dedicated attack.[5)]
- The theory of truncated differential cryptanalysis.[6)]

References

1) E.Biham and A.Shamir, “Differential cryptanalysis of DES-like cryptosystems,” Journal of Cryptology, 4, No.1, pp.3-72, 1991.

2) M.Matsui, “Linear cryptanalysis method for DES cipher,” Eurocrypt'93, LNCS 765, pp.386-397, 1994.

3) V.Rijmen, J.Daemen, B.Preneel, A.Bosselaers, E.DcWin, “The Cipher SHARK,” Fast Software Encryption, LNCS 1039, pp.99-112, 1996.

4) S.Hong, S.Lee, J.Lim, J.Sung, and D.Cheon, “Provable Security against Differencial and Linear Cryptanalysis for the SPN Structure,” FSE2000, 2000

5) J.Daemen, L.R.Knudsen, V.Rijmen, “The block cipher Square,” Fast Software Encryption, LNCS 1267, pp.149-165, 1997.

6) L.R.Knudsen, T.A.Berson, “Truncated Differentials of SAFER,” FSE, LNCS 1039, pp.15-25, 1996.

References of submission

A) K.Ohkuma, H.Muratani, F.Sano, and S.Kawamura, “Specification and Assessment of the block cipher Hierocrypt,” IEICE Technical report, ISEC99-141, 2000.

B) K.Ohkuma, H.Muratani, F.Sano, and S.Kawamura, “The block cipher Hierocrypt”, SAC2000, 2000. (To be published).

Previous use

In preparation