各ページ内での各項目の記入スペースの配分は応募者の任意とする

受付番号	

暗号技術概要説明書

１．暗号名：Hierocrypt-L1

分類：　共通鍵暗号

詳細分類		
	公開鍵暗号	
	共通鍵暗号	６４ｂｉｔブロック暗号

２．暗号の概要

２．１ 設計方針：

・主要な共通鍵暗号攻撃法に対して十分強く、主要なプラットフォーム上で高速で動作し、実装サイズもコンパクトになることを目標とした。
・計算効率と安全性の両立を高めるため、データ攪拌部にはSPN構造を再帰的に利用した入れ子型SPN構造を採用した。
・入れ子型SPN構造は非常に簡潔であり、十分な安全性を維持しつつ、構成要素もある程度独立に設計できる。さらに、ブロック長の変化にも柔軟に対応できる。
・S-boxは、ガロア体上のべき乗関数を基本とし、差分／線形解読法に対する耐性に関する最適化を行なった。さらに、べき乗関数をビット置換とアフィン変換で挟んで代数的攻撃法の適用を困難にした。
・拡散層は、符号理論を用いて活性S-box数の下限が大きな値を取るものを多数生成して候補とし、安全性と実装効率の条件で絞り込んだ。
・鍵スケジュール部は、64ビットFeistel型構造を基本構造とし、中間出力を組み合わせて拡大鍵を生成する。復号時にもon-the-flyでの鍵設定の初期遅延が小さくなるよう、中間鍵列が途中で逆転して戻ってくる折り返し型の構造を採用した。

２．２ 想定するアプリケーション：

・電子政府で利用されるアプリケーション一般。

・電子商取引に利用されるミドルウェアやＬＳＩへの実装。

・システム・インテグレーション事業。

各ページ内での各項目の記入スペースの配分は応募者の任意とする	受付番号	

２．３ ベースとして用いる理論、技術：

・差分解読法および線形解読法の理論[1,2]。
・SPN型暗号を差分解読法および線形解読法に強くするための設計法[3]。
・SPN型暗号の差分解読法および線形解読法に対する証明可能安全性の定理[4]。
・SPN型暗号に対するSQUARE攻撃法[5]。
・truncated差分解読法の理論[6]。

利用実績・参考文献等：

学会発表

A) **大熊・村谷・佐野・川村**, "Specification and Assessment of the block cipher Hierocrypt", **電子情報通信学会技術研究報告** IT99-102,ISEC99-141,SST99-150, 2000.
B) K.Ohkuma, H.Muratani, F.Sano, and S.Kawamura, `"The block cipher Hierocrypt", SAC2000, 2000. (**掲載予定**).

参考文献

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, and E.DcWin,"The Cipher SHARK,"Fast Software Encryption, Third International Workshop,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. (To be published)
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, and T.A.Berson, "Truncated Differentials of SAFER," Fast SoftWare Encryption, Third International Workshop, LNCS 1039, pp.15-25, 1996.