【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成19年8月23日(2007.8.23)

【公開番号】特開2005-27358(P2005-27358A)
【公開日】平成17年1月27日(2005.1.27)
【年通号数】公開・登録公報2005-004
【出願番号】特願2004-309002(P2004-309002)
【国際特許分類】
　Ｈ０４Ｌ　9/20　(2006.01)
【ＦＩ】
　Ｈ０４Ｌ　9/00　６５３

【手続補正書】
【提出日】平成19年7月5日(2007.7.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　共通鍵暗号方法であって，
　冗長データとメッセージとからなる平文を特定の長さで区切った複数の平文ブロックを生成し，
　秘密鍵から，乱数列を生成し，前記乱数列から前記平文ブロックに対応する乱数ブロックを生成し，
　前記平文ブロックと前記乱数ブロックとを演算して得た他の前記平文ブロックへのフィードバック値を出力し，
　前記平文ブロックと，前記乱数ブロックと，他の平文ブロックの演算から得られるフィードバック値とを用いて暗号文ブロックを暗号演算する共通鍵暗号方法。