【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６部門第２区分
【発行日】平成22年5月6日(2010.5.6)

【公表番号】特表2009-537025(P2009-537025A)
【公表日】平成21年10月22日(2009.10.22)
【年通号数】公開・登録公報2009-042
【出願番号】特願2009-502237(P2009-502237)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　9/28　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｚ
Ｈ０４Ｌ　9/00　６６１

【手続補正書】
【提出日】平成22年3月17日(2010.3.17)
【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】
ｎビットの数｛d_0、d_1、．．．d_{n-1}｝$_2$として表され得る秘密Ｄを必要とし、X^Dに等しい出力要素ＯＵＴを計算するように構成されている暗号化機構にして、Ｘがモノイド｛Ｍ、＊｝の要素であり、当該機構が、第１の変数VAR_0と第２の変数VAR_1とを含み、各ステップMUL_iの間、暗号化装置が$VAR_{1-d_i} * VAR_{d_i}$を計算するように、当該暗号化機構がｎ個のステップ$\{MUL_i\}_{i=n-1..0}$を含み、各ステップSQ_iの間、暗号化装置が$VAR_{d_i} * VAR_{d_i}$を計算するように、当該暗号化機構がｎ個のその他のステップ$\{SQ_i\}_{i=n-1..0}$を含み、各ステップSQ_iが、０とｎ－１の間の任意のｉに関してステップMUL_iの後で実行されており、各ステップMUL_{i-1}が、１とｎ－１の間の任意のｉに関してステップMUL_iの後で実行されている、暗号化機構であって、
ａ．ランダム要素ＭＳＫ＿ＩＮＰＵＴ（Ｒ）を生成するステップと、
ｂ．要素Ｘとランダム要素ＭＳＫ＿ＩＮＰＵＴとを使用することによってマスキングされた要素ＭＡＳＫＥＤ＿Ｘ（VAR_1）を作成するステップと、
ｃ．マスキングされた要素ＭＡＳＫＥＤ＿Ｘを使用して、上述のステップ$\{MUL_i\}_{i=n-1..0}$と$\{SQ_i\}_{i=n-1..0}$とを必要とする、マスキングされた出力要素ＭＡＳＫＥＤ＿ＯＵＴ（VAR_0）を計算するステップと、
ｄ．秘密Ｄを必要とせずに、ランダム要素ＭＳＫ＿ＩＮＰＵＴから出力マスクＭＳＫ＿ＯＵＴＰＵＴ（MSK_0）を計算するステップと、
ｅ．マスキングされた出力要素ＭＡＳＫＥＤ＿ＯＵＴと出力マスクＭＳＫ＿ＯＵＴＰＵＴとを使用して、出力要素ＯＵＴを計算するステップと
を含むことを特徴とし、
ステップｄがステップａとステップｅの間の任意のときに発生し、ステップａ、ｂ、ｃ、ｅが連続的である、暗号化機構。
【請求項２】
ランダム要素ＭＳＫ＿ＩＮＰＵＴ（Ｒ）がモノイド｛Ｍ、＊｝の演算＊に関する逆元（R^{-1}）を有し、逆元が出力マスクＭＳＫ＿ＯＵＴＰＵＴを計算するために使用可能であ

る、請求項１に記載の暗号化機構。
【請求項３】
出力マスクＭＳＫ＿ＯＵＴＰＵＴの計算が、各ステップＲ＿ＳＱ$_{i}$の間、暗号化装置が$MSK_i * MSK_i$を計算するように、ｎ個のステップ$\{R_SQ_i\}_{i=n-1..0}$を含み、MSK_iがモノイド｛Ｍ、＊｝の要素であり、初期値MSK_nがランダム要素ＭＳＫ＿ＩＮＰＵＴの逆元（R^{-1}）から取得されており、最終値MSK_0がマスキングされた出力ＭＡＳＫＥＤ＿ＯＵＴの値からマスキングを取るために使用される出力マスクＭＳＫ＿ＯＵＴＰＵＴである、請求項１または２に記載の暗号化機構。
【請求項４】
MSK_iが、ｎ－１から０までに等しいｉに関して、$MSK_{i+1} * MSK_{i+1}$に等しい、請求項３に記載の暗号化機構。
【請求項５】
マスキングされた要素ＭＡＳＫＥＤ＿ＸがＸ＊Ｒに等しく、出力要素ＯＵＴが$MASKED_OUT * MSK_0$に等しく、MSK_nがＲの逆元に等しく、第１の変数VAR_0の初期値がランダム要素の値（Ｒ）に設定されており、第２の変数VAR_1の初期値がマスキングされた要素ＭＡＳＫＥＤ＿Ｘの値に設定されており、各ステップMUL_iが$VAR_{1-d_i} * VAR_{d_i}$を計算して、結果をVAR_{1-d_i}内に記憶することであり、各ステップSQ_iが$VAR_{d_i} * VAR_{d_i}$を計算して、結果をVAR_{d_i}内に記憶することである、請求項４に記載の暗号化機構。
【請求項６】
請求項１から５のいずれかに記載の暗号化機構を実施することを特徴とする、秘密Ｄを記憶する暗号化装置。
【請求項７】
請求項１から５のいずれかの請求項に記載の暗号化機構を実施することを特徴とする、秘密Ｄを記憶するスマートカード。