

【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 21 年 7 月 9 日 (2009.7.9)

【公開番号】特開 2009-118529 (P2009-118529A)

【公開日】平成 21 年 5 月 28 日 (2009.5.28)

【年通号数】公開・登録公報 2009-021

【出願番号】特願 2009-42235 (P2009-42235)

【国際特許分類】

H 0 4 L 9/08 (2006.01)

H 0 4 L 9/14 (2006.01)

H 0 4 N 7/167 (2006.01)

【F I】

H 0 4 L 9/00 6 0 1 B

H 0 4 L 9/00 6 4 1

H 0 4 N 7/167 Z

【手続補正書】

【提出日】平成 21 年 4 月 24 日 (2009.4.24)

【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】

共通キーにより保護された少なくとも 1 つのシステムを無許可のユーザから保護する方法であって、前記システムは、最低位階層レベルと前記最低位階層レベルよりも高位の少なくとも 1 つの階層レベルとを有する暗号キーの階層を生成する中央装置を備えるものであり、前記方法は、

a) 最低位階層レベルにて各システムユーザに個別暗号キーを割り当てるステップと、

b) 前記個別暗号キーを前記システムと関連する中央記憶装置に保存するステップと、

c) 所定時間に、前記中央装置において、前記個別暗号キーを新たに組み合わせて前記最低位階層レベルよりも高位の暗号キーの新たな複数のサブセットを形成するステップと

、

d) 前記中央装置において、前記新たな複数のサブセットと以前に形成された複数のサブセットとを交差させて、前記個別暗号キーのうちの所定の個別暗号キーを決定すること  
を特徴とする方法。

【請求項 2】

請求項 1 に記載の方法において、前記サブセットへの暗号キーの組合せは有限幾何構造により決定されることを特徴とする方法。

【請求項 3】

請求項 2 に記載の方法において、前記幾何構造はボディ  $GF(q)$  上の  $d$  次元有限アフィン空間  $AG(d, q)$  であることを特徴とする方法。

【請求項 4】

請求項 2 に記載の方法において、前記幾何構造はボディ  $GF(q)$  上の  $d$  次元有限射影空間  $PG(d, q)$  であることを特徴とする方法。