【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5月14日(2009.5.14)

【公表番号】特表2005-513912(P2005-513912A)
【公表日】平成17年5月12日(2005.5.12)
【年通号数】公開・登録公報2005-018
【出願番号】特願2003-555729(P2003-555729)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ

【誤訳訂正書】
【提出日】平成21年3月30日(2009.3.30)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
受信機のグループ（Ｇ）に属すいくつかの受信機（１）に対して、同一の情報（$Ｋ_{c}$）を利用可能にする方法であって、各受信機が、それに固有の情報（$ＳＡ_{i}$）を格納し、
関係$Ｋ_{c}$＝ｆ（Ｋ，$ｂ_{i}$，$ＳＡ_{i}$）を定義するステップであって、（ｆ）が所与の関数であり、（Ｋ）がすべての受信機に共通の情報であり、（$ｂ_{i}$）が各受信機ごと、および情報（Ｋ）の各値ごとに異なる情報であるステップと、
（$Ｋ_{c}$）を利用可能にする前に、各受信機が情報（$ｂ_{i}$）にアクセスすることを可能にするステップと、
（$Ｋ_{c}$）を利用可能にする直前に、情報（Ｋ）をすべての受信機に送信するステップとを含み、
その結果、各受信機が、前記関係を用いて情報（$Ｋ_{c}$）を計算することができることを特徴とする方法。
【請求項２】
情報（Ｋ）が既知でないとき、関数（ｆ）は、（$ｂ_{i}$）および（$ＳＡ_{i}$）を知っており、現実的な時間で且つ無視できない確率で情報（$Ｋ_{c}$）を取得するのに使うことができるアルゴリズムが知られていないことを特徴とする請求項１に記載の方法。
【請求項３】
関数ｆは、受信機のある特定のサブグループ（Ｇ’）に対する特定の数の（$ｂ_{1}$．．$ｂ_{n}$）を知っており、現在のＫを知る前に、現実的な時間で且つ無視できない確率で、ｉが（Ｇ’）の受信機１．．ｎの１つでない正規の（$ＳＡ_{i}$）で、正当な対（$ｂ_{i}$，$ＳＡ_{i}$）を生じるのに使用されることができるアルゴリズムが知られていない、というようであることを特徴とする請求項１に記載の方法。
【請求項４】
関数ｆが、形式
【数１】

$$\mathbf{f(K, b_i, SA_i) = b_i \oplus E_K(SA_i)}$$

を有し、E_Kが、情報（Ｋ）に依存する関数であり、
【数２】

が、
群の算法を指定することを特徴とする請求項１に記載の方法。
【請求項５】
関数（E_K）は、暗号化関数であり、（Ｋ）が、この関数によって使われる秘密鍵であることを特徴とする請求項４に記載の方法。
【請求項６】
値（b_i）は、受信機のある特定のグループ（Ｇ）の各受信機に固有の鍵（K_i）で暗号化されて送られることを特徴とする請求項１に記載の方法。
【請求項７】
各値（SA_i）は、索引がｉである受信機に既知である秘密の値であることを特徴とする請求項１に記載の方法。
【請求項８】
各（b_i）は、２つの値$b_{1\,i}$および$b_{2\,j}$から構成され、同様に、各受信機に固有の情報が、２つの値SA_iおよびSA_jから構成され、そうすることによって、索引（ｉ，ｊ）の対で識別される各受信機が、対応する値$b_{1\,i}$および$b_{2\,j}$を値SA_iおよびSA_jと組み合わせて、前記関係を使って値$K_{c\,1}$および$K_{c\,2}$を計算し、$K_{c\,1}$および$K_{c\,2}$が、情報K_cにアクセスするために順に組み合わされることを特徴とする請求項１に記載の方法。
【請求項９】
情報K_cは、テレビ画像などのデジタルコンテンツを復号するのに使われる鍵であることを特徴とする請求項１に記載の方法。
【請求項１０】
情報K_cは、受信機によって数分間使うことができ、情報Ｋが、数秒前に送られ、値b_iが、数日前に送信を開始され、定期的に送られることを特徴とする請求項１に記載の方法。
【請求項１１】
特定の受信機は、受信機に事前格納された値のリスト内で、少なくともいくつかのそれらの値b_iを見つけることを特徴とする請求項１に記載の方法。
【請求項１２】
可搬型物体のグループ（Ｇ）に属すとともに情報処理手段（２）および情報格納手段（３、４、５）を備える可搬型の受信物体（１）であって、格納手段が、可搬型物体に固有の情報（SA_i）および所与の関数（ｆ）を格納し、
グループ（Ｇ）の各可搬型物体について、および情報（Ｋ）の各値について異なる情報（b_i）へのアクセス権を取得する手段と、
関係$K_c = f(K, b_i, SA_i)$を使って情報（K_c）を計算する手段であって、Ｋが、すべての可搬型物体に共通の情報であり且つすべての可搬型物体に送信される手段と、を備えることを特徴とする可搬型の受信物体。
【請求項１３】
同一の情報（K_c）を、受信機のグループ（Ｇ）に属すいくつかの受信機（１）に利用可能にする送信装置（１０）であって、各受信機が、その受信機に固有の情報（SA_i）を格納し、
関係$K_c = f(K, b_i, SA_i)$を使って情報（b_i）を計算するように設計された計算手段であって、（ｆ）が所与の関数であり、（Ｋ）がすべての受信機に共通の情報であり、情報（b_i）が、各受信機ごと、および情報（Ｋ）の各値ごとに異なる情報である計算手段（１１）と、
（K_c）を利用可能にする前のある特定の時間に、各受信機に関連づけられた情報（ｂ

$_i$）を、各受信機に送信するように、そして、（K_c）を利用可能にする直前に、すべての受信機に情報（Ｋ）を送信するように設計された送信手段（１５）とを備えることを特徴とする送信装置。

【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】０００８
【訂正方法】変更
【訂正の内容】
【０００８】
有利には、関数ｆは、形式
【数１】

$$f(K, b_i, SA_i) = b_i \oplus E_K(SA_i)$$

を有し、E_Kは、情報（Ｋ）に依存する関数であり、
【数２】

$$\oplus$$

が、群の算法を指定する。

【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００２１
【訂正方法】変更
【訂正の内容】
【００２１】
送信を担当する組織が、秘密鍵Ｋを生成し、次いで、すべての索引ｉに対して、以下の値
【数３】

$$b_i = K_c \oplus E_K(SA_i)$$

を計算する。上式において、Ｅは、鍵Ｋを使う暗号化関数、又はより一般的には一方向関数を指し、
【数４】

$$\oplus$$

は、群の算法（たとえばビットごとのＸＯＲ、またはモジュロ２５６の加算）を指し、送信を担当する組織は、こうしたすべての値b_iを、それぞれ鍵K_iで暗号化して送信する。たとえばこの組織は、すべての値b_iを、数日前に定期的に送信する。

【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００２３
【訂正方法】変更
【訂正の内容】
【００２３】
次いで、鍵K_cが有効になるわずか数秒前に、送信機は、秘密鍵Ｋをすべての受信機に送る。この鍵は非常に短くてよく、たとえば６４ビットでよい。受信機はこの時点で、ｙ＝E_K（SA_i）、次いで

【数５】

$$K_c = b_i \oplus y^{-1}$$

（群の演算がビットごとのＸＯＲである場合、ｙ$^{-1}$＝ｙである）を計算することによって、Ｋ$_c$を計算することができるようになる。

【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００４２
【訂正方法】変更
【訂正の内容】
【００４２】
送信を担当する組織は、２つの秘密の値Ｋ$_{c1}$およびＫ$_{c2}$を生成する。こうした値は次いで、メインの鍵Ｋ$_c$にアクセスするため、またはコンテンツに直接アクセスするために組み合わされる。たとえば、以下の式を実行することができる。
Ｋ$_c$＝Ｋ$_{c1}$＃Ｋ$_{c2}$　＃は、群の算法である。

【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００４３
【訂正方法】変更
【訂正の内容】
【００４３】
次いで、送信担当組織は、鍵Ｋを生成し、すべての値

【数７】

$$b_{1i} = K_{c1} \oplus E_K(SA_i)$$
$$\text{および} b_{2j} = K_{c2} \oplus E_K(SA_j)$$

を計算し、上式において、Ｅは、鍵Ｋを使う暗号化関数、より一般的には一方向関数を指し、

【数８】

$$\oplus$$

は、群の算法を指し、次いで、送信担当組織は、鍵Ｋ$_{1i}$で暗号化されたこうしたすべての値ｂ$_{1i}$、およびＫ$_j$で暗号化されたすべての値ｂ$_{2j}$を送信する。たとえば、すべての値ｂ$_{1i}$およびｂ$_{2j}$を数日前に定期的に送信する。