(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4133321号
(P4133321)
(45)発行日　平成20年8月13日(2008.8.13)　(24)登録日　平成20年6月6日(2008.6.6)

(51)Int.Cl.　　F I
G07B 17/00 (2006.01)　　G07B 17/00
G09C 1/00 (2006.01)　　G09C 1/00　640D

請求項の数 5　(全 6 頁)

(21)出願番号	特願2002-536971 (P2002-536971)
(86)(22)出願日	平成13年10月16日 (2001.10.16)
(65)公表番号	特表2004-512606 (P2004-512606A)
(43)公表日	平成16年4月22日 (2004.4.22)
(86)国際出願番号	PCT/DE2001/003893
(87)国際公開番号	WO2002/033663
(87)国際公開日	平成14年4月25日 (2002.4.25)
審査請求日	平成16年8月24日 (2004.8.24)
(31)優先権主張番号	100 51 818.4
(32)優先日	平成12年10月18日 (2000.10.18)
(33)優先権主張国	ドイツ(DE)

(73)特許権者　503141732
ドイッチェ・ポスト・アクチェンゲゼルシャフト
ドイツ連邦共和国、５３１１３　ボン、シャルルードーゴールーストラーセ、２０
(74)代理人　100069556
弁理士　江崎　光史
(74)代理人　100092244
弁理士　三原　恒男
(74)代理人　100093919
弁理士　奥村　義道
(74)代理人　100111486
弁理士　鍛冶澤　實

最終頁に続く

(54)【発明の名称】郵便物に貼付された郵便料金支払証を検査する方法

(57)【特許請求の範囲】

【請求項１】

クライアントのシステムが、郵便料金支払証を生成することが可能であり、これらの郵便料金支払証は、監査局の検査装置内で改ざん又は偽造に対して検査され得、この場合、これらの郵便料金支払証は、少なくとも一部が信頼するに足る出所に由来する暗号信頼性要素を含み、この場合、監査局の検査装置だけが、これらの暗号信頼性要素を復号化できるように、認証局の認証装置が、このクライアントのシステム内で郵便料金支払証を生成する前に暗号化された暗号信頼性要素をこのクライアントのシステム内に伝送し、この場合、この監査局の検査装置は、認証局の認証装置側及び監査局の検査装置側で暗号化及び復号化するための対応する鍵を必要とし、この場合、これらの郵便料金支払証は、鍵フェーズ・インディケータと共に郵便物に貼付され、これらの郵便料金支払証は、監査局の検査装置内で検査され、この場合、この監査局の検査装置は、信頼するに足る認証局の認証装置に由来する暗号信頼性要素を復号化する方法において、

この監査局の検査装置は、郵便料金支払証を生成したクライアントのシステムのＩＤ及び出所の正しさを解読し、この場合、さらに鍵フェーズ・インディケータが、１つの郵便料金支払証の中にある状態でこの監査局の検査装置に伝送され得、この監査局の検査装置は、暗号信頼性要素を復号化するための１つの対応する鍵を見つけ出すことができることを特徴とする方法。

【請求項２】

復号化が最も確率の高い鍵によって成功したかどうかが、検査されることを特徴とする

請求項１に記載の方法。
【請求項３】
復号化が失敗した場合は、復号化が、別の鍵によって実施されることを特徴とする請求項２に記載の方法。
【請求項４】
正しさが１つの所定の確率に合わせて達している複数の鍵によって、復号化が失敗した１つの郵便料金支払証は、偽造と認定されることを特徴とする請求項１に記載の方法。
【請求項５】
郵便料金支払証の復号化が複数の鍵によって失敗し、これらの鍵のうちの少なくとも１つの鍵が、少なくとも 95 %の確率で正しいときに、郵便料金支払証が偽造と認定されることを特徴とする請求項１に記載の方法。
【発明の詳細な説明】
【０００１】
本発明は、監査局の検査装置で郵便物に貼付された郵便料金支払証を検査する方法に関する。この場合、監査局の検査装置(Ueberpruefungsstelle)は、信頼するに足る認証局の認証装置(Bescheinigungsstelle)が発行した暗号信頼性要素によって郵便料金支払証を生成するクライアントのシステム(Kundensystem)のＩＤ及び出所の正しさを解読する。
【０００２】
暗号化された固有の郵便料金支払証を貼付した郵便物を管理することが公知である。
【０００３】
これらの鍵は、考慮される暗号化方法で復号化不可能である鍵の長さを有するものの、鍵の構成に関して知らされた狭い範囲の集団の或る構成員が、その鍵に関するこの情報を権限なく利用するか又は他の人に渡すという危険をさらに回避する必要がある。
【０００４】
それ故に、暗号化に対して使用された鍵をシステムの要求時に又は所定の期間の経過後に別のものに交換することが必要である。新しい鍵の個人的な引き渡しは、同時に関連するシステムの経費を考慮すると大量の使用には適していないので、鍵の交換を大幅に自動化する必要がある。
【０００５】
鍵を必要のある場合に交換するという課題の解決手段が、ヨーロッパ特許出願公開第 0 854 444号明細書中に記されている。ポインタを見つけだすためのポインタ・アルゴリズムを利用する。この場合、１つのデータアドレスを指し示す１つのポインタが使用される。このデータアドレスは、交換すべき１つの鍵に関する情報を含む。この方法は、必須要件として一定数の鍵を有する。これらの鍵は、ポインタを選択することによって確定されている。
【０００６】
本発明の課題は、管理の高信頼性を監査局の検査装置での郵便料金支払証の迅速な検査可能性に融合させた郵便物に貼付された郵便料金支払証を検査する方法を提供することにある。
【０００７】
この課題は、１つの鍵が監査局の検査装置に属する手段によって選択され、データが認証局の認証装置内でこの鍵によって暗号化される確率がこの鍵に対して非常に高いことによって解決される。
【０００８】
本発明は、ポインタを使用することなしに郵便料金支払証中に含まれる暗号情報を迅速にかつ確実に解読することを可能にする。
【０００９】
これによって、データの信頼性が何倍にも向上する。一方ではポインタの機能が不正な意図で外部のデータルーチンによって突き止められるかもしれないポインタが存在せず、他方では任意の数の鍵が使用可能である。

【００１０】
郵便料金支払証の全データが使用すべき鍵に関する情報を含まないように、これらの郵便料金支払証の全データが取得されているならば、この方法はとりわけ信頼できる。
【００１１】
特に認証局の認証装置によって暗号鍵を交換する場合、検査すべき鍵に関する情報の他の人への受け渡しが阻止される。
【００１２】
このような鍵の交換がとっさに起きて、多数の鍵の使用期間の一部が重なる場合、クライアントのシステムから郵便料金支払証に送られる付随情報がこの鍵の交換を必ず記録することが阻止され得る。
【００１３】
復号化が最も確率の高い鍵によって成功したかどうかを、監査局の検査装置に属する手段が検査すると特に好ましい。
【００１４】
復号化が成功しなかった場合に対しては、別の鍵による復号化が有効に実施される。
【００１５】
復号化が鍵によって失敗したときに、郵便料金支払証が偽造と認定されることによって、偽造された郵便料金支払証が、本発明の特に簡単でかつ目的に合った実施形で発見される。これらの鍵の信頼性は、所定の確率を同時に得る。
【００１６】
その他の利点，特徴及び目的にあったその他の構成は、従属請求項及び図面に基づく本発明の好適な実施の形態の以下の説明に記されている。
【００１７】
図１中には、鍵検査方法の原理が示されている。鍵の交換が、認証局の認証装置と監査局の検査装置との間で取り決められ得る。特に、この鍵の交換は、この認証局の認証装置とクライアントのシステムとの間で交換されるその他の暗号信頼性要素に関係なく実行される。
【００１８】
以下に、本発明の検査方法の好適な実施の形態を説明する。この場合、１つの鍵が、複数の信頼性要素を復号化する監査局の検査装置内で確認される。この鍵によって暗号化される確率がこの鍵に対して非常に高い。これらの信頼性要素は、認証局の認証装置によって前もって暗号化されて、クライアントのシステムに伝送してある。
【００１９】
クライアントのシステムが郵便料金支払証を生成する立場にあるように、本発明の方法を実施することが特に有益である。これらの郵便料金支払証は、監査局の検査装置内で改ざん又は偽造に対して検査され得る。これらの郵便料金支払証は、少なくとも一部が信頼するに足る出所に由来する暗号信頼性要素を含む必要がある。監査局の検査装置の視点から信頼するに足るこのような出所は認証局の認証装置である。
【００２０】
監査局の検査装置だけが暗号信頼性要素を復号化できるように、認証局の認証装置は、クライアントのシステムが郵便料金支払証を生成する前にこれらの暗号信頼性要素を暗号化する。そのため、認証局の認証装置側と監査局の検査装置側では、対応する鍵が暗号化と復号化のために必要である。
【００２１】
暗号信頼性要素のこの交換と同時に、付随情報が、認証局の認証装置とクライアントのシステムとの間で交換され得る。付随情報は、この付随情報及び場合によっては暗号信頼性要素を生成する時点を示す。この付随情報は、郵便料金支払証の中にある状態で監査局の検査装置にさらに伝送される。監査局の検査装置は、暗号信頼性要素を復号化するための１つの対応する鍵をより高い確率で確認する立場にある。この付随情報は、本発明の方法を実現するにあたって鍵フェーズ・インディケータ(Schluesselphasen-Indikator)と呼

ばれる。

【００２２】

監査局の検査装置内では、暗号信頼性要素を復号化するための考慮の対象になる多数の鍵が用意されることによって、郵便料金支払証の改ざん又は偽造が検査される。郵便料金支払証を自動的に検査するときに不可欠である高い検査速度を保証するため、データが認証局の認証装置内で鍵によって暗号化される確率がこれらの鍵に対して非常に高い複数の鍵が、復号化に対して考慮の対象になる多数の鍵から選択される。

【００２３】

最も確率の高い鍵を突き止めるため、以下に記された連続する方法ステップのうちの少なくとも１つが実施される：

１）

暗号信頼性要素の作成時点が分かる１つの付随情報が、鍵フェーズ・インディケータの形態で郵便料金支払証の中に含まれている場合、この期間内に使用される鍵が、プリセットされた順序にしたがって、例えば時系列順に最も確率の高い鍵として検査のために最初に考慮される。引き続き、隣接した期間中でも隣接した鍵フェーズ・インディケータによって使用されたあまり確率の高くない鍵が検査される。その他の鍵はさらに確率が低くなるので、この検査は、所定の（低い）確率以降はその他の鍵に対して最終的に中止され、郵便料金支払証が無効と判断される。

２）

付随情報を含まない場合、監査局の検査装置は以下のような措置をとる：監査局の検査装置が、１つの鍵フェーズ・インディケータを逆時系列方向に割り当てる、つまり現在使用する鍵フェーズ・インディケータから過去に逆戻りさせる。これによって、対応する鍵の見つけ出しが最適化される。

【００２４】

図２中には、鍵フェーズ・インディケータの期間及び鍵の使用期間の好ましい調整が示されている。特に鍵の交換時の重なった期間（図中では誇張して示されている）も、鍵フェーズ・インディケータを採用することによってカバーできる点が注目に値する。

【００２５】

鍵Ｓ４が、鍵Ｓ５と並んで高い確率でこの期間中に使用され、この鍵Ｓ４が鍵Ｓ５の前に時系列的に使用されるので、鍵フェーズ・インディケータＫＰＩ３を付随情報として含む郵便料金支払証又はこの鍵フェーズ・インディケータを欠陥のある付随情報に基づいて監査局の検査装置によって割り当てられてしまった郵便料金支払証が、最初に鍵Ｓ４によって復号化される。復号化が鍵Ｓ４によって失敗した場合、鍵Ｓ５が使用される。復号化がこの鍵Ｓ５によっても失敗した場合、あまり確率の高くない鍵Ｓ３が復号化のために使用される。これも失敗した場合、復号化が、さらに確率の高くない鍵Ｓ６によって試みられる。引き続き、その他の鍵の使用確率が非常に低いために、復号化が最終的に中止され、郵便料金支払証が無効と判断され、場合によっては偽造と認定される。

【図面の簡単な説明】

【図１】　鍵検査方法の原理図である。

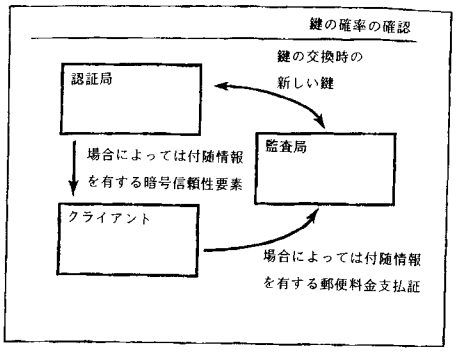
【図２】　本発明の鍵フェーズ・インディケータの使用の時間可能性の原理図である。

【符号の説明】

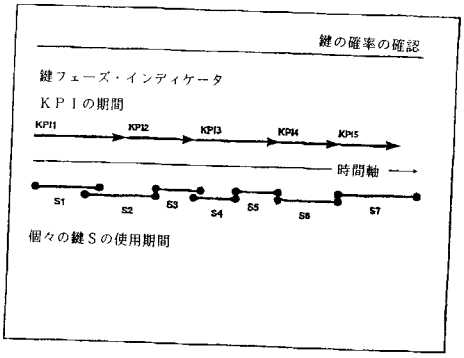
ＫＰＩ１～ＫＰＩ５　　鍵フェーズ・インディケータ

Ｓ１～Ｓ７　　鍵

【図１】


鍵の確率の確認
鍵の交換時の
新しい鍵
認証局
監査局
場合によっては付随情報
を有する暗号信頼性要素
クライアント
場合によっては付随情報
を有する郵便料金支払証

【図２】


鍵の確率の確認
鍵フェーズ・インディケータ
ＫＰＩの期間
KPI1
KPI2
KPI3
KPI4
KPI5
時間軸
S1
S2
S3
S4
S5
S6
S7
個々の鍵Ｓの使用期間

フロントページの続き

(72)発明者　ラング・ユルゲン
ドイツ連邦共和国、ベルギッシュ・グラートバッハ、シャウ・インス・ラント、１５
(72)発明者　マイヤー・ベルント
ドイツ連邦共和国、ケーニヒスヴィンター、ツム・シュテッカーホーフ、２ツェー

審査官　岩田　洋一

(56)参考文献　特開平９－２８２５０６（ＪＰ，Ａ）
特開平１１－３２８４６２（ＪＰ，Ａ）
特開２０００－１０５８４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G07B 17/00
G09C 1/00