(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4729258号
(P4729258)

(45)発行日　平成23年7月20日(2011.7.20)　(24)登録日　平成23年4月22日(2011.4.22)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
H04N	5/44	(2011.01)	H04N	5/44	Z

請求項の数 6　(全 10 頁)

(21)出願番号	特願2003-585394 (P2003-585394)
(86)(22)出願日	平成15年4月11日 (2003.4.11)
(65)公表番号	特表2005-522947 (P2005-522947A)
(43)公表日	平成17年7月28日 (2005.7.28)
(86)国際出願番号	PCT/FR2003/001169
(87)国際公開番号	WO2003/088612
(87)国際公開日	平成15年10月23日 (2003.10.23)
審査請求日	平成18年4月10日 (2006.4.10)
(31)優先権主張番号	02/04840
(32)優先日	平成14年4月12日 (2002.4.12)
(33)優先権主張国	フランス(FR)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】データ送信者の匿名認証方法

(57)【特許請求の範囲】

【請求項１】

受信機により受信されるデータが信頼される第三者により権限を与えられた匿名の送信機により送信されたものであるということを検証する方法であって、

前記送信機と前記受信機とは、デジタルネットワークに接続され、前記送信機により送信されたデータに識別子が関連付けされ、

当該方法は、

（ａ）乱数を生成するステップと、

（ｂ）前記ネットワーク上に前記乱数と前記識別子とを配信するステップと、

（ｃ）前記乱数と前記識別子とに第１関数を適用することにより計算されるレスポンスを前記送信機から受信するステップと、

（ｄ）前記受信したレスポンス、前記乱数及び前記識別子に第２関数を適用することにより前記受信したレスポンスを検証するステップとを前記受信機が実行することからなり、

前記第１関数は前記信頼される第三者により前記送信機に以前に送信され、

前記第２関数は前記信頼される第三者により前記受信機に以前に送信され、前記第１関数の結果を検証する関数であることを特徴とする方法。

【請求項２】

請求項１記載の方法であって、

前記受信機は、前記ステップ（ｃ）において受信したレスポンスが正しくない場合、あるいは前記乱数の送信から所定時間経過した後でもレスポンスが受信されない場合、前記

データにアクセスしないことを特徴とする方法。
【請求項３】
請求項１又は２記載の方法であって、
前記第１関数は、秘密鍵を利用する公開関数であることを特徴とする方法。
【請求項４】
請求項１乃至３何れか一項記載の方法であって、
前記第１関数は秘密関数であることを特徴とする方法。
【請求項５】
請求項１乃至４何れか一項記載の方法であって、
前記第１関数は、秘密鍵を利用した署名生成のための公開関数であることを特徴とする方法。
【請求項６】
請求項５記載の方法であって、
前記第２関数は、前記第１関数により利用される秘密鍵に対応する公開鍵を利用した署名生成のための公開関数であることを特徴とする方法。
【発明の詳細な説明】
【発明の詳細な説明】
【０００１】
［発明の属する技術分野］
本発明は、各種装置をリンクさせたネットワーク上での安全なデータ交換及びネットワークを介し送信されるデータのデータソースの認証に関する。
［背景技術］
ある場合には、データ受信装置は、データまたは媒介装置により中継される可能性のあるデータを送信した送信者が、信頼される第三者によりデータ送信を行う権限を与えられているということをデータ受信者に送信者の身元を知らせることなく確認する必要がある。
［発明の概要］
本発明の１つの目的は、データの送信者が信頼される第三者によりデータ送信を行う権限が与えられているということをデータの受信者に送信者の身元を明かすことなく証明することができる方法を提案することである。
【０００２】
従って、本発明は、デジタルネットワークに接続された送信者と受信者間において、受信者によって受信されたデータが信頼される第三者により権限を与えられた送信者により送信されたものであるということを確認する方法に関する。本発明によると、送信者から送信されるデータに識別子が関連付けされ、本発明による方法は、受信者に対して、
（ａ）乱数を生成するステップと、
（ｂ）前記乱数をネットワークを介し配信するステップと、
（ｃ）第１関数を前記乱数と前記識別子に適用することにより計算される応答を前記送信者から受信するステップと、
（ｄ）第２関数を前記受信した応答、前記乱数及び前記識別子に適用することにより前記受信した応答を確認するステップとからなり、前記第１関数は信頼される第三者により前記送信者に以前に送られ、前記第２関数は前記第三者により前記受信者に以前に送られ、前記第１関数の結果を確認するための関数であることを特徴とする。
【０００３】
前記送信者は、前記ネットワークの前記データの初期的送信者であってもよいし、あるいは前記初期的送信者と受信者との間において、例えば、前記初期的送信者により送信されたデータを格納する媒介装置であってもよい。
【０００４】
本発明の一変形によると、前記ステップ（ｂ）は、前記乱数を前記送信者に送信するステップにより置き換えられる。

【０００５】
本発明の一実施例によると、前記受信者は、前記ステップ（ｃ）で受信した応答が正しくない場合、あるいは前記乱数の送信から所定時間経過した後も応答が受信されない場合、前記データへのアクセスを禁止する。
【０００６】
前記送信者により送信されるデータに関連付けされる識別子は、好ましくは、前記ネットワークのデータの初期的送信者により生成され、前記初期的送信者により前記データに添付される乱数である。当然のことながら、前記識別子は、前記送信者の身元に関する情報を与えるものでない。
【０００７】
本発明はまた、デジタルネットワークに接続される送信者と受信者間において、前記受信者に送信されたデータが信頼される第三者により権限を与えられた前記送信者により送信されたものであるということを証明する方法に関する。本発明の前記特徴によると、識別子が前記送信者により送信されるデータに関連付けされ、本発明による方法は、前記送信者に対して、
（ａ）前記受信者から乱数を受信するステップと、
（ｂ）第１関数を前記乱数と前記識別子に適用することにより応答を計算するステップと、
（ｃ）前記応答を前記受信者に送信するステップとからなることを特徴とする。
【０００８】
前記応答は、第２関数を前記受信した応答、前記乱数及び前記識別子に適用することにより前記受信者によりおそらく確認され、前記第１関数は信頼される第三者により前記送信者に以前に送られ、前記第２関数は前記信頼される第三者により前記受信者に以前に送られ、前記第１関数の結果を確認するための関数である。
【０００９】
本発明の原理によると、信頼される第三者が、ネットワークの初期的あるいは媒介送信者となりうるすべての装置に、上記方法における応答の計算に使用される第１関数を送信する。信頼される第三者はまた、前記ネットワークの受信者となるうるすべての装置に、前記第１関数を利用して計算された応答を確認するための第２関数を送信する。
［発明の実施例の詳細な説明］
上記説明された本発明の原理に基づき、いくつかのシナリオが可能である。
【００１０】
第１のシナリオによると、アリスと呼ばれる第１送信者とチャーリーと呼ばれる第２送信者が、ボブと呼ばれる受信者が接続されるネットワークを介してそれぞれM_AとM_Cと呼ばれるメッセージを送信する。アリスは、メッセージM_Aと共にメッセージM_Aを特定する識別子$IdEvent_A$を送信し、チャーリーは、メッセージM_Cと共にメッセージM_Cを特定する識別子$IdEvent_C$を送信する。
【００１１】
ネットワークに共に接続されたアリスとチャーリーは、当該ネットワークの各自の他方の送信者により送信されるメッセージM_CとM_Aをそれぞれ受信するが、これらのメッセージを保持はしない。ボブはまた、これら２つのメッセージを受信し、メッセージM_Aのみを保持することを所望していると仮定する。M_Aが信頼される第三者により権限を与えられた送信元から送られてきたものであるということを確認するため、ボブは以下の方法によりチャレンジ/レスポンス（ｃｈａｌｌｅｎｇｅ/ｒｅｓｐｏｎｓｅ）プロトコルを開始する。ボブは、乱数Ｃ（チャレンジ）を生成し、ネットワーク上に配信する。アリスとチャーリーは共にこのチャレンジＣを受信する。
【００１２】
これより以前に、信頼される第三者はアリスとチャーリーにレスポンス計算関数Ｇを送信し、ボブに対応するレスポンス検証関数Ｈを送信している。この関数Ｈは、レスポンスが正しくない場合には０を返し、レスポンスが正しい場合には１を返す。

【００１３】
アリスとチャーリーがボブにより送信されたチャレンジＣを受信すると、アリスとチャーリーはそれぞれのレスポンスR_AとR_Cを以下のように、すなわち、
アリス：$R_A = G(IdEvent_A, C)$；
チャーリー：$R_C = G(IdEvent_C, C)$；
として計算し、その後、レスポンスR_AとR_Cをそれぞれボブに送信する。
【００１４】
その後、ボブは、$H(C, R_X, IdEvent_X)$（ただしＸ＝Ａ，Ｃ）を計算することにより各レスポンスを検証する。関数Ｈにより返される結果のすべてがゼロである場合、ボブは、安全な送信元から送信されたものでないとみなし、メッセージM_Aを保持しない。他方、Ｈにより返される結果の少なくとも１つが１である場合（この例で、それは$H(C, R_A, IdEvent_A)$となるであろう）、ボブは、メッセージM_Aが信頼される第三者により権限を与えられた送信者から送られたものであると確信し、それを受け付ける。
【００１５】
第２のシナリオによると、送信者であるアリスは、識別子$IdEvent_A$と共にメッセージM_Aを、受信者であるボブとデボラと呼ばれる媒介者が接続されるネットワーク上に配信する。初期的には、ボブはメッセージM_Aに関心はなく、それを保持しないと仮定される。しかしながら、デボラは、メッセージM_Aとそれの識別子$IdEvent_A$を保持する。
【００１６】
以降において、アリスがもはやメッセージを配信しなくなると、デボラは保持しているメッセージM_Aとそれの識別子$IdEvent_A$をネットワーク上に配信する。アリスは、単なる送信者であり、M_Aを保持していない。ボブは、M_Aを受信し、それの保持を所望する。メッセージM_Aが信頼される第三者により権限を与えられた送信元から送信されたものであるということを保証するため、ボブは、以下の方法でチャレンジ/レスポンスプロトコルを開始する。ボブは、乱数Ｃ（チャレンジ）を生成し、ネットワーク上に配信する。
【００１７】
これより以前に、信頼される第三者はアリスとデボラにレスポンス計算関数Ｇを送信し、ボブに対応するレスポンス検証関数Ｈを送信している。この関数Ｈは、レスポンスが正しくない場合には０を返し、レスポンスが正しい場合には１を返す。
【００１８】
アリスとデボラは、チャレンジＣを受信する。アリスはメッセージを送信していないため、チャレンジＣを考慮することはない。しかしながら、デボラはレスポンス$R_D = G(IdEvent_A, C)$を計算し、このレスポンスをボブに送信する。その後、ボブは、$H(C, R_D, IdEvent_A)$を計算することによりこのレスポンスを検証する。関数Ｈが１を返す場合、ボブはメッセージM_Aが権限を与えられた送信元から送信されたものとみなし、それを受け付ける。
【００１９】
ここで、上記２つのシナリオでは、受信者ボブは、メッセージの送信元に応答することが可能ではあるが、受信したメッセージが送信者（アリスのような）から送信されたものであるのか、あるいは媒介装置（デボラのような）から送信されたものであるのか知らず、結局ボブはメッセージM_Aの送信者の身元を知らない。
【００２０】
図１を参照して、本発明のより具体的な実施例が説明される。図１において、ＳＴＢ（セットトップボックス）デコーダ１、ＤＴＶ（デジタルテレビ）受信機２及びＳＵ（記憶ユニット）３が表されている。
【００２１】
このネットワークを介して配信されるデータは、ＩＳＯ／ＩＥＣ１３８１８－１規格「

情報技術－動画及び関連する音声情報の汎用的符号化：システム」に規定されるようなデータトランスポートストリームで搬送される音声映像ビットストリームからなるオーディオビジュアルプログラムを表していると仮定される。

【００２２】

デコーダ１は、ネットワークを介したデータの送信者を表し、例えば、衛星アンテナやケーブル接続から受信するデータを送信する。デジタルテレビ２は、ネットワークを介したデータの受信者を表す。記憶ユニット３は、ネットワークの他の送信機から受信したデータをネットワークを介して再送することが可能な媒介装置を表す。

【００２３】

これら３つの装置は、例えば、ＩＥＥＥ１３９４規格に従うデジタルバス４に接続され、従ってデジタルホームネットワークを形成している。ネットワークを介し送信されるメッセージは、バス４の同期チャンネルを介し送信され、アドレス指定されたメッセージはバス４の非同期チャンネルを介し送信される。

【００２４】

チャレンジ/レスポンスプロトコルに対するレスポンスを計算する関数Ｇをネットワークの送信者あるいは媒介装置（本例では、デコーダ１と記憶ユニット３）に送信し、レスポンス検証関数Ｈをネットワークの受信装置（本例では、デジタルテレビ２）に送信する信頼される第三者は、例えば、これら装置の製造業者である。

【００２５】

関数ＧとＨの選択に関して、３つの実施例が考えられる。

【００２６】

第１の好適な実施例によると、関数Ｇは、チャレンジＣ及び識別子ＩｄＥｖｅｎｔ（すなわち、$R = G_K(C, IdEvent)$）に基づきレスポンスＲを計算するため、秘密鍵Ｋを使用する公開関数である。送信者あるいは媒介装置が準拠した装置であり、信頼され第三者により権限を与えられていることを保証するため、秘密鍵Ｋはこれらの装置の以降におけるアクセスが許可されていない安全な記憶領域（例えば、安全なプロセッサでは、特にスマートカードに含まれる）に挿入されている。

【００２７】

この場合、関数Ｈは、秘密鍵Ｋによる関数Ｇを適用することにより、チャレンジＣと識別子ＩｄＥｖｅｎｔに基づきレスポンスＲ’を計算し、結果Ｒ’と受信したレスポンスＲを比較する関数である。Ｈはブール関数であり、Ｒ’とＲが異なる場合には「０」を返し、Ｒ’とＲが一致する場合には「１」を返す。この場合、秘密鍵Ｋはまた、信頼される第三者により受信装置に以前に挿入されていなければならない。

【００２８】

上記定義に対応する関数Ｇは、特に、以下のインターネットアドレス「http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf」で入手可能な「ＦＩＰＳ１９７：アドバンス暗号化規格（ＡＥＳ）仕様書－２００１年１１月２６日」に記載されているＡＥＳ関数のような暗号化関数であってもよい。また、関数Ｇは、特に、以下のインターネットアドレス「http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf」で入手可能な「ＦＩＰＳ刊行物１９８：鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）、ナショナルインスティテュートオブスタンダードアンドテクノロジー、２００１」に記載されるＨＭＡＣ－ＳＨＡ１関数のようなハッシュ関数であってもよい。

【００２９】

第２実施例では、関数Ｇは、準拠しているとみなされる送信者あるいは媒介装置に送信され、信頼される第三者により権限を与えられている秘密関数である。好ましくは、関数Ｇは、それを有する製品を解析することによる検出を困難にするよう選ばれなければならない。さらに、関数Ｇは、適応的に選択される平文攻撃に抵抗力を有するものである必要がある。

【００３０】

第１実施例と同様に、この場合、関数Ｈは、秘密関数Ｇを適用することにより、チャレ

ンジＣと識別子ＩｄＥｖｅｎｔに基づきレスポンスＲ’を計算し、結果Ｒ’と受信したレスポンスＲを比較し、Ｒ’とＲが異なる場合には「０」を返し、Ｒ’とＲが一致する場合には「１」を返すブール関数である。従って、本実施例では、秘密関数Ｇは、信頼される第三者により受信装置に以前に挿入されている必要がある。

【００３１】

第３実施例では、関数Ｇ及びＨは、非対称鍵のペア（秘密鍵/公開鍵）を利用した公開関数である。例えば、関数Ｇは、秘密鍵により署名を生成する関数であり、関数Ｇは、対応する公開鍵により署名を検証する関数である。

【００３２】

例えば、ＲＳＡ（Ｒｉｖｅｓｔ、Ｓｈａｍｉｒ及びＡｄｌｅｍａｎ）署名関数は以下のように、すなわち、

Ｒ＝Ｇ（Ｃ，ＩｄＥｖｅｎｔ）＝ＲＳＡＳｉｇｎ$_{ＫＰＲＩ}$（Ｃ，ＩｄＥｖｅｎｔ）；

Ｈ（Ｃ，Ｒ，ＩｄＥｖｅｎｔ）＝ＲＳＡＶｅｒｉｆ$_{ＫＰＵＢ}$（Ｃ，Ｒ，ＩｄＥｖｅｎｔ）；

（ただし、ＫＰＲＩ及びＫＰＵＢは、秘密鍵と公開鍵であり、ＲＳＡ鍵の同一のペアである）のように利用される。

【００３３】

この場合、秘密鍵は、信頼される第三者によりネットワークの送信者あるいは媒介装置に挿入され、公開鍵は、ネットワークの受信装置に挿入される。

【００３４】

ここで、第１実施例では、関数ＧはＨＭＡＣ－ＳＨＡ１関数であり、秘密鍵Ｋはデコーダ ＳＴＢ１、デジタルテレビ受信機ＤＴＶ２及び記憶ユニットＳＵ３の不揮発性記憶領域に含まれると仮定される。

［第１のシナリオ：ＳＴＢによるプログラムのＤＴＶへの直接的な送信］

図２に示されるように、デコーダＳＴＢ１のユーザが新たなプログラムをネットワークに配信するため選ぶと、ＳＴＢは、好ましくは１２８ビットからなるプログラム識別子ＩｄＥｖｅｎｔをランダムに生成し（ステップ２０）、この識別子を当該プログラムを表すデータを搬送するパケットに含まれるメッセージに挿入する。その後、データトランスポートストリームは、ステップ２１においてネットワーク上（バス４の同期チャンネル上）に配信される。データトランスポートストリームは、最終的にこの識別子ＩｄＥｖｅｎｔを抽出するため、受信したデータパケットから識別子を含むメッセージを抽出するデジタルテレビＤＴＶ２により受け取られる（ステップ２２）。

【００３５】

その後、ステップ２３において、ＤＴＶは、好ましくは１２８ビットの乱数からなるチャレンジＣを生成し、ステップ２４において、このチャレンジＣをネットワーク上に配信する。ＳＴＢがチャレンジＣを受信すると、ステップ２５においてレスポンスを以下のように、すなわち、

Ｒ＝Ｇ（Ｃ，ＩｄＥｖｅｎｔ）あるいはより正確には、：

$Ｒ_{ＳＴＢ}$＝ＨＭＡＣ－ＳＨＡ$１_{Ｋ}$（Ｃ，ＩｄＥｖｅｎｔ）

のように計算し、バス４の非同期チャンネルを介しＤＴＶにこのレスポンスをアドレス指定する（ステップ２６）。

【００３６】

記憶ユニットＳＵ３はまた、チャレンジＣを受信するが、それはデータ送信プロセスにはないため、応答しない。

【００３７】

ＤＴＶがＳＴＢからレスポンス$Ｒ＝Ｒ_{ＳＴＢ}$を受け取ると、関数Ｈ（Ｒ，Ｃ，ＩｄＥｖｅｎｔ）を適用して、$Ｒ_{ＤＴＶ}$＝ＨＭＡＣ－ＳＨＡ$１_{Ｋ}$（Ｃ，ＩｄＥｖｅｎｔ）を計算し、この結果を受信したレスポンス$Ｒ_{ＳＴＢ}$と比較することを意味するレスポンスＲを検証する（ステップ２７）。これら２つの値が同一である場合、ＤＴＶは、受信したプログラムが信頼される第三者により権限が与えられている送信者から送信されたものであるとみ

なし、ユーザに提供することができる。そうでない場合には、ＤＴＶは受信したプログラムをユーザに表示しない。チャレンジＣがネットワーク上に送信されてから所定期間経過した後でもレスポンスを受信しできない場合、ＤＴＶはまた、受信したプログラムの表示をブロックする。

【００３８】

プロトコルの終了時、チャレンジＣと識別子ＩｄＥｖｅｎｔはＳＴＢとＤＴＶのメモリから消去される。

［第２のシナリオ：ＤＴＶに以降に送信するＳＵにより保持されるプログラムのＳＴＢによる送信］

このシナリオは図３により示される。

【００３９】

初期的に、ＳＴＢのユーザは新たなプログラムを選択すると仮定される。その後、ＳＴＢは、前述の第１のシナリオと同様に、識別子ＩｄＥｖｅｎｔを生成し（ステップ３０）、ネットワーク上へのデータトランスポートストリームの配信前に、当該プログラムを表すデータトランスポートパケットに含まれるメッセージにこの識別子を挿入する（ステップ３１）。

【００４０】

その後、ＳＵは、当該プログラムを表すデータストリームを保持する。例えば、ユーザは、デコーダにより配信されたプログラムをすぐには閲覧しないことを選び、以降に再生するためそれを保持することを所望する。

【００４１】

次に、ユーザが記憶されているプログラムの再生を所望する。ＳＵは、ステップ３２において、ネットワーク上に当該プログラムを配信する。ＤＴＶは、このデータパケットを受信し、ステップ３３において、このデータパケットから識別子ＩｄＥｖｅｎｔを含むメッセージを抽出する。

【００４２】

その後、ＤＴＶは、第１のシナリオと同様に、チャレンジＣを生成し（ステップ３４）、ネットワーク上に配信する（ステップ３５、３５’）。

【００４３】

ＳＵは、このチャレンジＣを受信し、ステップ３６において以下のように、すなわち、

Ｒ＝Ｇ（Ｃ，ＩｄＥｖｅｎｔ）あるいはより正確には、：

R_{SU}＝ＨＭＡＣ－ＳＨＡ１$_{K}$（Ｃ，ＩｄＥｖｅｎｔ）

のように計算し、バス４の非同期チャンネルを介しＤＴＶにこのレスポンスをアドレス指定する（ステップ３７）。

【００４４】

データ配信プロセスにないＳＴＢは、受信したチャレンジＣに対して応答しない。

【００４５】

ＤＴＶがＳＵからレスポンスＲ＝R_{SU}を受信すると、関数Ｈを適用して、R_{DTV}＝ＨＭＡＣ－ＳＨＡ１$_{K}$（Ｃ，ＩｄＥｖｅｎｔ）を計算し、この結果を受信したレスポンスR_{SU}と比較することに関するレスポンスＲを検証する（ステップ３８）。これら２つの値が同一である場合、ＤＴＶは、受信したプログラムが信頼される第三者により権限が与えられている送信者から送信されたものであるとみなし、ユーザに提供することができる。そうでない場合、あるいはチャレンジＣがＤＴＶにより送信されてから所定期間経過してもレスポンスが受信されなかった場合には、ＤＴＶは受信したプログラムをユーザに表示しない。

【００４６】

ここで、ＳＴＢが初期的にプログラムの送信を完了すると、その後メモリから識別子ＩｄＥｖｅｎｔは消去される。

【００４７】

プロトコルの終了時、チャレンジＣと識別子ＩｄＥｖｅｎｔはまたＳＵとＤＴＶのメモ

リから消去される。

【００４８】

本発明の変形例では、特に上述の２つのシナリオでは、ＤＴＶにより計算されたチャレンジＣをネットワーク上に配信するステップをチャレンジＣをデータの送信者（第１シナリオではＳＴＢ、第２シナリオではＳＵ）に送信するステップと置き換えることが可能である。この場合、データ送信者のみがチャレンジＣを受信する。具体的には、既存のデジタルネットワーク管理プロトコルにより、データの受信者はデータソースの身元を知ることなく応答することが可能となる。

【００４９】

他の変形例では、データの受信者は、チャレンジＣに加えて、受信したデータに関連付けされている識別子をネットワーク上に配信する（例えば、図２のステップ２４、あるいは図３のステップ３５、３５’において）。チャレンジＣと識別子ＩｄＥｖｅｎｔを受信した各送信ネットワーク装置は、受信した識別子ＩｄＥｖｅｎｔとデータを配信するのに生成したものとを比較することによりこのチャレンジに応答すべきか検証する。送信者は、チャレンジと共に受信した識別子がそれの現在の識別子ＩｄＥｖｅｎｔに一致する場合にのみ応答する。これにより、チャレンジＣが受信者により送信されるとき、ネットワークにデータを配信しているすべての送信者が応答するのを回避することができる。

【００５０】

本発明は、特に以下の効果を有する。

【００５１】

複数の送信者あるいは媒介装置がネットワークに接続されていても、信頼される第三者により権限を与えられ、データを送信したもののみが、データの受信者によるチャレンジ/レスポンスプロトコルに応答することができる。

【００５２】

プロトコルは、送信者に関する情報を受信者に明らかにしない。これにより、送信装置の匿名認証という目的が達成される。

【００５３】

プロトコルはアプリケーションレイヤにのみ基づくものであり、データトランスポートレイヤに関する特別な特徴を必要としない。

【図面の簡単な説明】

【００５４】

【図１】図１は、本発明が実施されるドメスティックなデジタルネットワークを表す。

【図２】図２は、本発明の一実施例を示す。

【図３】図３は、本発明の他の実施例を示す。

【図１】

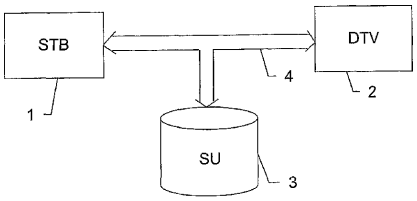
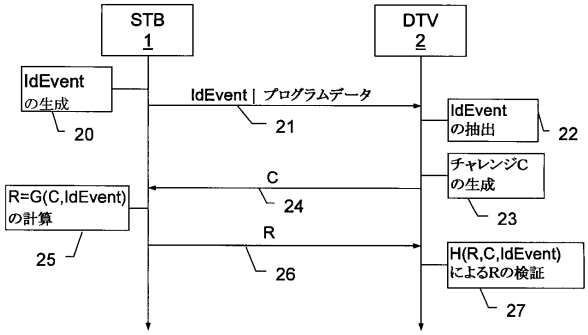
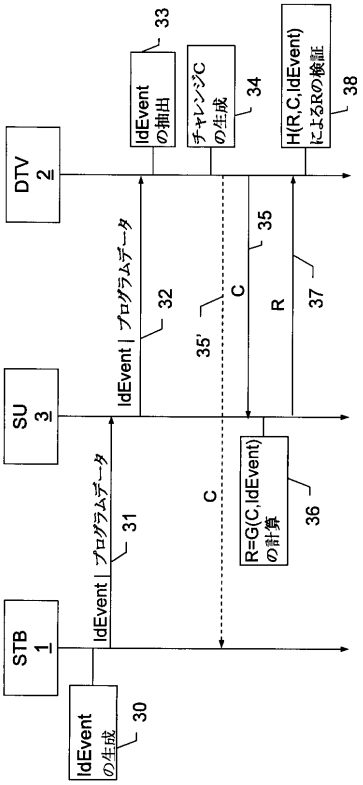

STB
DTV
SU
1
2
3
4

Fig. 1

【図２】


STB 1
DTV 2
IdEvent の生成
20
IdEvent | プログラムデータ
21
IdEvent の抽出
22
チャレンジC の生成
23
C
24
R=G(C,IdEvent) の計算
25
R
26
H(R,C,IdEvent) によるRの検証
27

【図３】


DTV 2
SU 3
STB 1
IdEvent の抽出
33
チャレンジC の生成
34
H(R,C,IdEvent) によるRの検証
38
IdEvent | プログラムデータ
32
C
35'
35
R
37
IdEvent | プログラムデータ
31
C
R=G(C,IdEvent) の計算
36
IdEvent の生成
30

フロントページの続き

(72)発明者 アンドロー，ジャンーピエール
フランス国，３５０００ レンヌ，リュ・ド・ロルジェリル ２０
(72)発明者 ディエル，エリク
フランス国，３５３４０ リフレ，ラ・ビュザルディエール（番地なし）
(72)発明者 デュラン，アラン
フランス国，３５０００ レンヌ，リュ・ド・ディナン ７９

審査官 新田 亮

(56)参考文献 特開２０００－１０１６４０（ＪＰ，Ａ）
特開２００１－２１１１５２（ＪＰ，Ａ）
栃窪 孝也 KOUYA TOCHIKUBO，リニューアル可能な暗号認証システムの検討 Renewable Authentication and Encryption Systems，情報処理学会論文誌 第４１巻 第８号 IPSJ Journal，日本，社団法人情報処理学会 Information Processing Society of Japan，２０００年 ８月，第41巻，p.2121-2128
稲村 雄 YUU INAMURA，最新の暗号技術によるセキュリティの実現，ＯＰＥＮ ＤＥＳＩＧＮ 第３巻 第３号，日本，ＣＱ出版株式会社，１９９６年 ６月 １日，第3巻，p.90-99

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
H04N 5/44