(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6173455号
(P6173455)
(45)発行日　平成29年8月2日(2017.8.2)　(24)登録日　平成29年7月14日(2017.7.14)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 620Z
H04L 9/08 (2006.01)　　H04L 9/00 601B

請求項の数 10　(全 18 頁)

(21)出願番号　特願2015-527038(P2015-527038)
(86)(22)出願日　平成25年7月22日(2013.7.22)
(65)公表番号　特表2015-524945(P2015-524945A)
(43)公表日　平成27年8月27日(2015.8.27)
(86)国際出願番号　PCT/IB2013/055995
(87)国際公開番号　WO2014/027263
(87)国際公開日　平成26年2月20日(2014.2.20)
審査請求日　平成28年7月20日(2016.7.20)
(31)優先権主張番号　61/684,216
(32)優先日　平成24年8月17日(2012.8.17)
(33)優先権主張国　米国(US)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
KONINKLIJKE PHILIPS N.V.
オランダ国　5656　アーエー　アインドーフェン　ハイテック　キャンパス　5
High Tech Campus 5, NL-5656 AE Eindhoven
(74)代理人　110001690
特許業務法人M&Sパートナーズ

最終頁に続く

(54)【発明の名称】属性ベース暗号化

(57)【特許請求の範囲】
【請求項１】
メッセージと、属性のセットに関する、複数の要素を含むポリシーとを決定するための入力ユニットと、
前記メッセージの暗号化された表現及び前記複数の要素の暗号化された表現を生成するための第１の暗号ユニットであって、
秘密を生成するための秘密生成器と、
前記秘密に基づいて前記メッセージを暗号化して前記メッセージの前記暗号化された表現を得るためのメッセージ暗号化ユニットと、
前記ポリシーの要素各々を前記秘密に基づいて変換し、各々のポリシー暗号文要素を得るためのポリシー変換ユニットと、
前記秘密を暗号化して暗号化された秘密を得るための秘密暗号化ユニットとを含む、第１の暗号ユニットと
を含む、第１のエンクリプタと、
前記メッセージの前記暗号化された表現及び前記複数の要素の前記暗号化された表現を受信するための受信ユニットと、
前記メッセージの前記暗号化された表現及び前記複数の要素の前記暗号化された表現を、前記ポリシーに関連付けられた属性ベース暗号メッセージに変換するための第２の暗号ユニットであって、
前記暗号化された秘密の解読を可能にしない鍵に基づいて前記暗号化された秘密の複

数の暗号化されたシェアを生成するためのシェア生成ユニットと、
前記ポリシー暗号文要素の各々を前記暗号化された秘密の前記暗号化されたシェアの各々と組み合わせて前記ポリシーの暗号表現を得るための組み合わせユニットとを含む、第２の暗号ユニットと
を含む、第２のエンクリプタと
を含む、属性ベース暗号のためのシステム。
【請求項２】
前記第１のエンクリプタは、モバイル端子の一部として実装され、前記第２のエンクリプタは、前記モバイル端子とは異なるデバイスの一部として実装される、請求項１に記載のシステム。
【請求項３】
前記要素の各々は、各属性に対応する、請求項１に記載のシステム。
【請求項４】
前記組み合わせユニットは、前記暗号化された秘密の前記暗号化されたシェアによって前記ポリシー内の属性間の関係を施行する、請求項４に記載のシステム。
【請求項５】
前記第２の暗号ユニットは、前記秘密を解読することなく、前記暗号化された秘密から前記暗号化されたシェアを直接生成し、前記暗号化されたシェアを解読することなく、前記暗号化されたシェアを組み合わせて前記秘密を得ることはできない、請求項１に記載のシステム。
【請求項６】
前記第１の暗号ユニットは、所定の数字を前記秘密を表す値で累乗することによって前記秘密を暗号化するための秘密暗号化ユニットを含む、請求項５に記載のシステム。
【請求項７】
請求項１に記載のシステムを含む通信システム。
【請求項８】
前記メッセージは、モバイル端末上で動作するデータ入力アプリケーションによって生成される医療情報を含む、請求項７に記載の通信システム。
【請求項９】
前記第２のエンクリプタのための鍵であって、前記第２の暗号ユニットが前記秘密の暗号化されたシェアを生成することを可能にするが、前記第２の暗号ユニットが前記秘密を解読することは可能にしない当該鍵を生成する、請求項１に記載のシステムに使用される鍵生成器。
【請求項１０】
第１のデバイスにおいて、
メッセージと、属性のセットに関する、複数の要素を含むポリシーとを決定するステップと、
前記メッセージの暗号化された表現及び前記複数の要素の暗号化された表現を生成するステップと、
秘密を生成するステップと、
前記秘密に基づいて前記メッセージを暗号化して、前記メッセージの前記暗号化された表現を得るステップと、
前記ポリシーの要素各々を前記秘密に基づいて変換して、各々のポリシー暗号文要素を得るステップと、
前記秘密を暗号化して暗号化された秘密を得るステップと
を含み、
第２のデバイスにおいて、
前記メッセージの前記暗号化された表現及び前記複数の要素の前記暗号化された表現を受信するステップと、
前記メッセージの前記暗号化された表現及び前記複数の要素の前記暗号化された表現を

、前記ポリシーに関連付けられた属性ベース暗号メッセージに変換するステップと、
第２のエンクリプタ秘密鍵に基づいて、前記暗号化された秘密の複数の暗号化されたシェアを生成するステップと、
前記ポリシー暗号文要素の各々を前記暗号化された秘密の前記暗号化されたシェアの各々と組み合わせて、前記ポリシーの暗号表現を得るステップと
を含む、属性ベース暗号化方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、属性ベース暗号化に関する。
【背景技術】
【０００２】
従来のヘルスケアからホームヘルスケア及びウェルネスサービスにわたるケアサイクルに関与する異なるパーティ間でのデータ交換の必要性の増加は、健康／医療データの安全管理を重要な問題にした。他の応用分野においても、安全なデータ伝送及び管理に対する関心の増加が見られている。健康／医療データ管理に対する現行のアプローチは、従来のセキュリティ機構に基づき、物理的手続き及び管理的手続きによって補完されている。この組み合わせの結果、健康情報の利用可能性は限定され、健康記録のやり取りは煩雑になる。デジタルポリシー管理及び施行技術は、（１）異種ネットワークにおけるエンドツーエンドプライバシー及びセキュリティを提供して、データが伝搬するインフラ及び機関的な境界とは無関係にデータを保護し、（２）ヘルスケアアプリケーションにおいて重要である利用制御を属性ベースアクセス制御機構の上に提供し、（３）システムがネットワークにとらわれない態様で展開することを可能にする単純な相互運用可能セキュリティアーキテクチャを提供して、ネットワーク固有のセキュリティ規定の必要性を除去し、よって実装及び保守コストを削減することにより、従来の機構及び手続きを上回る。しかし、安全なデータ交換に必要とされる暗号アルゴリズムは計算的にインテンシブであり得る。
【０００３】
J. Bethencourt、A. Sahai、及びB. Watersによる“Ciphertext-Policy Attribute-Based Encryption”, Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 321-334, 2007は、属性ベース暗号方式（ＡＢＥ）、例えば暗号文ポリシーＡＢＥ方式（ＣＰ－ＡＢＥ）等に基づくデジタルデータセキュリティ管理システムを開示する。この方式では、データはアクセス制御ポリシーとも呼ばれるアクセス構造に従って暗号化され、正しい属性を有するユーザのみがデータを解読できる。データを解読できるよう、ユーザは自身が保持する認証された属性のセットに対応する特定のプライベートキーを信頼機関から得る。
【０００４】
Joseph A. Akinyeleらによる“Self-Protecting Electronic Medical Records Using Attribute-Based Encryption”, http://eprint.iacr.org/2010/565.pdfは、電子医療記録の保護のためにＣＰ－ＡＢＥ方式をポータブルデバイス上に実装することを開示する。
【０００５】
M. Green、S. Hohenberger、B. Watersによる“Outsourcing the Decryption of ABE Ciphertexts”, Proceedings of USENIX Security, 2011は、ユーザがクラウドに単一の変換鍵を供給することを含み、変換鍵は、サーバがユーザのメッセージを読み取り得ることなく、ユーザの属性によって満たされる任意のＡＢＥ暗号文をクラウドがＥｌＧａｍａｌスタイルの暗号文に変換する方法を開示する。得られたＥｌＧａｍａｌスタイルの暗号文はその後ユーザに送信され、ユーザはそれを解読することができる。
【発明の概要】
【発明が解決しようとする課題】
【０００６】

改良された属性ベース暗号化システムを得ることは好適であろう。この課題をより好適に扱うために、本発明の第１の側面は、第１のエンクリプタと第２のエンクリプタとを含むシステムを提供し、
第１のエンクリプタは、
メッセージと、属性のセットに関する、複数の要素を含むポリシーとを決定するための入力ユニットと、
メッセージの暗号化された表現及び複数の要素の暗号化された表現を生成するための第１の暗号ユニットとを含み、
第２のエンクリプタは、
メッセージの暗号化された表現及び複数の要素の暗号化された表現を受信するための受信ユニットと、
メッセージの暗号化された表現及び複数の要素の暗号化された表現を、ポリシーに関連付けられた属性ベース暗号メッセージに変換するための第２の暗号ユニットとを含む。
【０００７】
このスキームは、第１のエンクリプタが、属性ベース暗号化スキームの暗号化ステップより計算的な要求が低い暗号化方法を用いることを可能にする。典型的には、属性ベース暗号化システムの暗号化部分は計算的に高価である。例えば、その計算複雑性は、アクセス制御ポリシー内の属性の数によって測られるアクセス制御ポリシーのサイズと共に線形増加する。第１のエンクリプタによって実行される暗号化は、メッセージ及びポリシーを安全に第２のエンクリプタに伝送することを可能にする。第２のエンクリプタは、メッセージ及びポリシーを、ポリシーに関連付けられた属性ベース暗号メッセージに変換し、これにより、第１のエンクリプタが実行しなければならない計算量を減らす。
【０００８】
（上記で引用する）Ｇｒｅｅｎらは、属性ベース暗号化スキームの解読ステップのアウトソーシングを開示するが、当該文献が開示する方法は属性ベース暗号化スキームの暗号化ステップのアウトソーシングは可能にしない。
【０００９】
第１のエンクリプタはモバイル端末の一部として実装され、第２のエンクリプタはモバイル端末とは異なるデバイスの一部として実装され得る。属性ベース暗号化方法の暗号化ステップの計算負荷が低減されるので、これはモバイル端末上への属性ベース暗号化スキームの効果的な実装を可能にする。
【００１０】
他の側面では、本発明は属性ベース暗号のためのシステムを提供し、システムは、
メッセージと、属性のセットに関する、複数の要素を含むポリシーとを決定するための入力ユニットと、第１の暗号ユニットとを含む第１のエンクリプタを含み、第１の暗号ユニットは、
秘密を生成するための秘密生成器と、
秘密に基づいてメッセージを暗号化してメッセージの暗号化された表現を得るためのメッセージ暗号化ユニットと、
ポリシーの各要素を秘密に基づいて変換し、各ポリシー暗号文要素を得るためのポリシー変換ユニットと、
秘密を暗号化して暗号化された秘密を得るための秘密暗号化ユニットとを含み、
システムは更に、メッセージの暗号化された表現及び複数の要素の暗号化された表現を受信するための受信ユニットと、第２の暗号ユニットとを含む第２のエンクリプタを含み、第２の暗号ユニットは、
暗号化された秘密の解読を可能にしない鍵に基づいて暗号化された秘密の複数の暗号化されたシェアを生成するためのシェア生成ユニットと、
ポリシー暗号文要素の各々を暗号化された秘密の暗号化されたシェアの各々と組み合わせてポリシーの暗号表現を得るための組み合わせユニットとを含む。
【００１１】

このシステムは、後者が属性ベース暗号化スキームの暗号化オペレーションを実行することを望むとき、第１の暗号ユニットに課される計算負荷を低減する。計算負荷が低減するのは、計算の一部が第２の暗号ユニットによって引き受けられるからである。また、秘密がメッセージ及びポリシーの要素を共に保護するので、第１の暗号ユニットと第２の暗号ユニットとの間のデータ通信は安全である。メッセージ暗号化ユニットがメッセージを暗号化するので、メッセージが権限のない者によって解読されることから保護される。また、ポリシー変換ユニットは、第２の暗号ユニットを含む権限のないエンティティが属性等のポリシーの要素を変更できないよう、ポリシーの要素を変換し得る。シェア生成ユニットは暗号化された秘密の暗号化されたシェアを生成できるが、秘密は暗号化されているので、第２の暗号ユニットは秘密を復元することはできない。組み合わせユニットは計算的に比較的高価であり得るステップ、すなわち、ポリシー暗号文要素と暗号化されたシェアとの組み合わせを実行する。このような組み合わせは、スキームを暗号的に安全にするために、計算的に高価である累乗及び乗算ステップを十分に含み得る。これらの計算的に高価な演算は、第１の暗号ユニットによって実行される必要がない。

【００１２】

ポリシーの各要素は、各属性に対応し得る。例えば、ポリシーは複数の属性を含む論理式（logic expression）を含み得る。要素はこれらの属性に対応し得る。論理式内の属性間の関係が、要素内に又は別個のデータ要素として表現され得る。要素は秘密のシェアと結合されるので、メッセージを解読することを望むパーティは、ポリシー内の属性とマッチする適切な属性を含むキーを有さなければならない。したがって、第１のエンクリプタと第２のエンクリプタとの間の通信において、属性を別々の要素としてパッケージすることが比較的効率的であり得る。

【００１３】

組み合わせユニットは、暗号化された秘密の暗号化されたシェアによってポリシー内の属性間の関係を施行するよう構成され得る。ポリシー内の属性の選択は、第１の暗号ユニットによって施行され得る。また、セミ信頼第２の暗号ユニットは、ポリシー内の属性間の関係を施行するよう暗号演算を実行し得る。これは、例えば、メッセージを解読するのに所定の最小数の特定の属性のセットが必要であるよう、秘密のシェアを適用することによって実行され得る。

【００１４】

第２の暗号ユニットは、秘密を解読することなく、暗号化された秘密から暗号化されたシェアを直接生成するよう構成され、ここで、暗号化されたシェアを解読することなく、暗号化されたシェアを組み合わせて秘密を得ることはできない。第２の暗号ユニットはユーザ秘密鍵がなければメッセージを解読することができないので、これはシステムのセキュリティを強化する。

【００１５】

第１の暗号ユニットは、所定の数字を秘密を表す値で累乗することによって秘密を暗号化するための秘密暗号化ユニットを含み得る。これは安全な暗号化方法を提供し得る。また、これは、第２の暗号ユニットが平文で秘密にアクセスする必要なく秘密の暗号化されたシェアを生成することを可能にし得る。

【００１６】

上記システムは通信システム内に含まれ得る。例えば、通信システムは暗号化のために第１の暗号ユニット及び第２の暗号ユニットを含み、また、対応する解読タスクを実行するための追加の暗号ユニットを少なくとも提供し得る。

【００１７】

通信システムは、モバイル端末上で動作する患者データ入力アプリケーションによって生成される医療情報を含むメッセージを伝送するために使用され得る。ハンドヘルドデバイスは、第１の暗号ユニットと、第２の暗号ユニットに生成された暗号化情報を伝送するための伝送ユニットとを含み得る。

【００１８】

他の側面では、本発明は、上記のシステムに使用される鍵生成器を提供する。鍵生成器は、第２のエンクリプタのための鍵であって、第２の暗号ユニットが秘密の暗号化されたシェアを生成することを可能にするが、第２の暗号ユニットが秘密を解読することは可能にしない当該鍵を生成するよう構成され得る。この種の鍵は、第２の暗号ユニットがセミ信頼機関としてタスクを実行することを可能にする。

【００１９】

他の側面では、本発明は、

第１のデバイスにおいて、

メッセージと、属性のセットに関する、複数の要素を含むポリシーとを決定するステップと、

メッセージの暗号化された表現及び複数の要素の暗号化された表現を生成するステップとを含み、

第２のデバイスにおいて、

メッセージの暗号化された表現及び複数の要素の暗号化された表現を受信するステップと、

メッセージの暗号化された表現及び複数の要素の暗号化された表現を、ポリシーに関連付けられた属性ベース暗号メッセージに変換するステップとを含む、属性ベース暗号化方法を提供する。

【００２０】

他の側面では、本発明は、

第１のデバイスにおいて、

メッセージと、属性のセットに関する、複数の要素を含むポリシーとを決定するステップと、

秘密を生成するステップと、

秘密に応じてメッセージを暗号化して、メッセージの暗号化された表現を得るステップと、

ポリシーの各要素を秘密に応じて変換して、各ポリシー暗号文要素を得るステップと、

秘密を暗号化して暗号化された秘密を得るステップとを含み、

第２のデバイスにおいて、

メッセージの暗号化された表現及び複数の要素の暗号化された表現を受信するステップと、

第２のエンクリプタ秘密鍵に応じて、暗号化された秘密の複数の暗号化されたシェアを生成するステップと、

ポリシー暗号文要素の各々を暗号化された秘密の暗号化されたシェアの各々と組み合わせて、ポリシーの暗号表現を得るステップとを含む、属性ベース暗号化方法を提供する。

【００２１】

当業者は、本発明の上記実施形態、実装形態、及び／又は側面の２つ以上が、有用であると考えられる任意の態様で組み合わせられ得ることを理解するであろう。

【００２２】

本明細書に基づき、当業者は、説明されるシステムの改変例及び変形例に対応する、通信システム、システム、方法、及び／又はコンピュータプログラム製品の改変例及び変形例を実施し得る。

【図面の簡単な説明】

【００２３】

本発明の上記及び他の側面は本明細書から明らかであり、本明細書にて図面を参照して説明される。各図を通して、同様のアイテムは同じ参照符号によって示される。

【００２４】

【図１】図１は、暗号化ステップの一部がプロキシにアウトソーシングされる属性ベース暗号のためのシステムのブロック図である。

【図２】図２は、属性ベース暗号システムのブロック図である。

【図３】図３は、暗号処理ステップがプロキシにアウトソーシングされる属性ベース暗号システムのブロック図である。
【図４】図４は、暗号化ステップの一部がプロキシにアウトソーシングされる属性ベース暗号化プロセスのフローチャートである。
【図５】図５は、暗号化ステップの一部がプロキシにアウトソーシングされる属性ベース暗号化プロセスの他の実施形態のフローチャートである。
【発明を実施するための形態】
【００２５】
本明細書が開示するスキームでは、データオーナーとも呼ばれるホストは、プロキシと呼ばれるセミ信頼機関にポリシー作成をアウトソースでき、また、与えられたポリシーに従ってユーザのためにメッセージを暗号化でき、プロキシは、（ａ）暗号文にアクセスできず、（ｂ）ポリシーが指定する属性に基づいてメッセージを暗号化するよう強いられる。このようなアウトソーシングにより、処理能力が抑えられたモバイルデバイスであり得るホストにかかる計算負荷を低減することができる。このような計算負荷の低減は、ＡＢＥ暗号方式の採用を拡大するために有用であり得る。
【００２６】
以下、複数のスキームがより詳細に開示される。しかし、本明細書に開示されるスキームの詳細はあくまで例として見なされるべきことが理解されよう。変形及び付加は、本明細書に基づき当業者の範囲内である。
【００２７】
本明細書に開示されるＡＢＥに関するあるスキームでは、ユーザ（例えば、病院の医療スタッフ）に秘密鍵を発行するための中央鍵権限が準備される。ユーザの鍵はユーザが保持する属性に関連する。中央権限は、プロキシとして機能し得る、例えば「クラウド」内のセミ信頼機関のためにも秘密鍵を発行し得る。
【００２８】
ＡＢＥ暗号文との用語は、アクセスポリシーに従って暗号化されたメッセージに概して関連し得る。本明細書が開示する技術によれば、ＡＢＥ暗号文は、１つのステップがメッセージのホスト（データオーナー又はエンクリプタ、例えば患者）によって実行され、１つのステップがセミ信頼プロキシによって実行される２つのステップで作成され得る。
【００２９】
ホスト（データオーナー又はエンクリプタ）は、アクセスポリシーによって指定される属性間で共有される秘密鍵に複数の属性がバインドされる中間暗号文を作成し得る。中間暗号文はアクセスポリシーの記述と共に、計算能力の高いセミ信頼プロキシに伝送される。プロキシはこの中間暗号文の一部を解読して、暗号化された秘密鍵を得ることができる。プロキシはこの暗号化された秘密鍵を使用して、ポリシー内に現れる属性間でこの秘密鍵のシェアを分配することにより、アクセスポリシーに基づく暗号文を作成する。これは、それ自体が当該技術分野において良く知られている秘密分散法を用いて実行され得る。
【００３０】
図２は、属性ベース暗号システムを示す。エンクリプタ２０１は、例えばユーザ入力部（図示なし）を介して又はデータベース（図示なし）から、メッセージＭ及びアクセスポリシーＰを受信する。アクセスポリシーに関連付けられた暗号文（ＡＢＥ）の生成後、暗号文（ＡＢＥ）は、この場合、ストレージサーバ２０２に送信される。デクリプタ２０３は、サーバ２０２から（又は、エンクリプタ２０１から直接）暗号文（ＡＢＥ）を取り出し、ポリシーＰを満たす属性のセットに関連付けられた秘密鍵に基づき、暗号文ＡＢＥを解読してオリジナルメッセージＭのコピーを引き出し得る。
【００３１】
図３は、暗号化及び解読がセミ信頼プロキシシステムによって実行される属性ベース暗号システムを示す。図４は、図３に示される属性ベース暗号システムの動作方法を示す。ステップ４０１において、第１のエンクリプタ３０１がメッセージＭ及び属性のセットに関するポリシーＰを決定し、ここで、ポリシーは複数の構成要素を含む。要素は合わせて

ポリシーを形成する。メッセージM及びポリシーPは、例えば、ユーザ入力によって、外部ソースから受信することによって、又は自動的に生成することによって決定され得る。

【００３２】

ステップ４０２において、第１のエンクリプタ３０１はメッセージの暗号化された表現Cと、複数の要素の暗号化された表現Dとを生成し得る。これは、それ自体が当該技術分野において良く知られている暗号技術を用いて実行され得る。

【００３３】

暗号文Cはアクセスポリシーの複数の要素の暗号表現Dと共に第２のエンクリプタ３０２に伝送され得る。この第２のエンクリプタ３０２は、セミ信頼プロキシとも呼ばれ得る。この伝送は任意の方法で実行され、例えば、無線若しくは有線通信技術によって又はリムーバブル記憶媒体によって実行され得る。

【００３４】

ステップ４１０において、第２のエンクリプタはメッセージの暗号表現C及び複数の要素の暗号表現Dを受け取る。ステップ４１１において、第２のエンクリプタは、メッセージの暗号表現C及び複数の要素の暗号表現Dを、ポリシーに関連付けられた属性ベース暗号メッセージＡＢＥに変換する。この属性ベース暗号メッセージＡＢＥは、図２と同様に更に処理され、すなわち、サーバ２０２内に保存され、かつ／又はポリシーPを満たす属性のセットに関連付けられた秘密鍵を有するデクリプタ２０３に伝送され得る。デクリプタ２０３は属性ベース暗号化された暗号文ＡＢＥを解読して、メッセージMのコピーを得ることができる。

【００３５】

あるいは、図３に示されるように、第２のエンクリプタ３０２によって生成された属性ベース暗号文ＡＢＥはサーバ３０３内に保存され、かつ／又は、プロキシデクリプタ３０４に伝送され得る。プロキシデクリプタ３０４は、プロキシデクリプタ３０４が属性ベース暗号文ＡＢＥを属性ベースではない通常の暗号文C＊に変換することを可能にする、ポリシーPを満たす属性のセットに関連付けられた鍵を備える。例えば、プロキシデクリプタはＥｌＧａｍａｌ暗号文を生成する。プロキシデクリプタによって生成されたこの暗号文C＊は、最終デクリプタ３０５に送られる。最終デクリプタ３０５は低コストデバイス上に実装され、ＥｌＧａｍａｌ解読等の計算的に安価な通常の解読を実行して、通常の暗号文C＊をメッセージMのコピーに変換する。

【００３６】

図５は、プロキシエンクリプタを用いる暗号化方法の他の実施形態を示す。ステップ４０１において、図４の実施形態と同様にメッセージ及びポリシーが決定される。ステップ５０１において、第１のエンクリプタ３０１は秘密を生成する。このような秘密は、例えば、所定の範囲内の乱数であり得る。例えば、秘密分散法において容易に使用され得る秘密が生成される。ステップ５０２において、第１のエンクリプタ３０１は、秘密に基づいてメッセージMを暗号化して、メッセージの暗号化された表現（C）を得ることができる。また、ステップ５０３において、第１のエンクリプタはポリシーPの要素をそれぞれ秘密に基づいて変換して、対応するポリシー暗号文要素Dを得ることができる。例えば、第１のエンクリプタはポリシーの属性に応じた数字を秘密に応じて累乗してもよい。また、ステップ５０４において、第１のエンクリプタは秘密を暗号化して暗号化された秘密Sを得ることができる。例えば、第１のエンクリプタは所定の数字をｓ乗してもよい。その結果をｄ乗してもよく、ここで、

$$\gamma/d$$

が秘密鍵として第２のエンクリプタ３０２に与えられる。ここで、

$$\gamma$$

はランダムに選択される秘密の数字であり得る。

【００３７】

ステップ４１０において、情報が第２のエンクリプタに伝送されて受け取られた後、ス

テップ５１０において、第２のエンクリプタは第２のエンクリプタ秘密鍵に基づいて、暗号化秘密Ｓの複数の暗号化シェアを生成し得る。例えば、これは当該技術分野においてそれ自体が良く知られている秘密分散法によって実行され得る。例えば、閾値秘密分散法又は加法的（additive）秘密分散法が採用され得る。

【００３８】

ステップ５１１において、第２のエンクリプタは各ポリシー暗号文要素Ｄを暗号化秘密の各暗号化シェアと組み合わせて（結合して）、ポリシーの暗号表現を得ることができる。このようなポリシー暗号文要素と暗号化シェアとの組み合わせオペレーションは、例えば、暗号化シェアとポリシー暗号文要素との乗算を含み得る。他の組み合わせ演算も可能であり、例えば、乗算の前に、ポリシー暗号文要素及び／又は暗号化シェアから中間数値が導出されてもよい。

【００３９】

図１は、属性ベース暗号のためのシステムを示す。システムは第１のエンクリプタ１１と第２のエンクリプタ１２とを含み得る。第２のエンクリプタ１２はセミ信頼プロキシとも呼ばれ得る。第１のエンクリプタは、メッセージと属性のセットに関するポリシーとを決定するための入力ユニット１を含み、ここでポリシーは複数の要素を含む。例えば、入力ユニット１は、ユーザがデバイスにデータを入力することを可能にするユーザインターフェイスに動作的に結合され得る。また、このようなユーザインターフェイスは、ユーザがデータのアクセスポリシーを設定することを可能にするよう構成されてもよい。あるいは、アクセスポリシーは、例えば入力されるデータの種類に基づいて自動的に決定されてもよい。あるいは、入力ユニット１は、メッセージ及びポリシーを他のデバイス又は同じデバイスの他のユニットから受信するよう構成されてもよい。また、メッセージ及び／又はアクセスポリシーは自動的に決定されてもよい。

【００４０】

第１のエンクリプタ１１は、入力ユニット１に動作的に結合される第１の暗号ユニット２を含み得る。第１の暗号ユニット２は、メッセージの暗号表現及び複数の要素の暗号表現を生成するよう構成され得る。

【００４１】

第２のエンクリプタ１２は第１のエンクリプタ１１とは異なるデバイス上に実装され得るが、これは限定ではない。第２のエンクリプタ１２は第１のエンクリプタ１１より大きな処理能力を利用可能でもよく、第２のエンクリプタ１２は、属性ベース暗号化を用いてデータを暗号化することに関連する計算タスクを第１のエンクリプタ１１よりも容易に実行し得る。また、第１のエンクリプタ１１及び第２のエンクリプタ１２は、ネットワーク通信及び／又はリムーバブルメディア交換を含む任意の種類のデータ通信技術によって互いに通信するよう構成され得る。例えば、第１のエンクリプタ１１と第２のエンクリプタ１２との間で安全なデータ接続がセットアップされ得る。例えば、第１のエンクリプタは、暗号化メッセージ及び複数の要素の暗号表現を第２のエンクリプタ１２に伝送するための第１の伝送ユニット９を含む。

【００４２】

第２のエンクリプタ１２は、メッセージの暗号表現及び複数の要素の暗号表現を受信するための受信ユニット３を含み得る。これらのアイテムは第１のエンクリプタによって生成されたものである。

【００４３】

第２のエンクリプタは、更に、メッセージの暗号表現及び複数の要素の暗号表現を、ポリシーに関連付けられた属性ベース暗号メッセージ（ＡＢＥ暗号文）に変換するための第２の暗号ユニット４を含み得る。

【００４４】

第１のエンクリプタ１１はモバイル端末の一部として実装され、第２のエンクリプタ１２は、デスクトップコンピュータ又はサーバシステム等、モバイル端末とは異なるデバイスの一部として実装され得る。

【００４５】
第１の暗号ユニット２は、（疑似）乱数等の秘密を生成するよう構成された秘密生成器５を含み得る。第１の暗号ユニット２は、更に、秘密に基づいてメッセージを暗号化してメッセージの暗号表現を取得するよう構成されたメッセージ暗号化ユニット６を含み得る。第１の暗号ユニット２は、更に、秘密に基づいてポリシーの各要素を変換して対応するポリシー暗号文要素を取得するよう構成されたポリシー変換ユニット７を含み得る。第１の暗号ユニットは、更に、秘密を暗号化して暗号化秘密を取得するよう構成された秘密暗号化ユニット８を含み得る。
【００４６】
第２の暗号ユニット４は、暗号化秘密の解読を可能にしない鍵に基づいて暗号化秘密の複数の暗号化シェアを生成するよう構成されたシェア生成ユニット１３を含み得る。第２の暗号ユニットは、更に、各ポリシー暗号文要素を暗号化秘密の各暗号化シェアと組み合わせてポリシーの暗号表現を取得するよう構成された組み合わせユニット１４を含み得る。ＡＢＥ暗号文は、メッセージの暗号表現及びポリシーの暗号表現を含み得る。
【００４７】
システムは、要素が属性に対応するように構成され得る。例えば、各要素はアクセスポリシーに関連する異なる属性に対応し得る。ポリシー内の属性間の関係に関する情報も、第１の暗号ユニットから第２の暗号ユニットに伝達されてもよい。第２の暗号ユニットは、秘密分散法によってこれらの関係をＡＢＥ暗号文に併合する。
【００４８】
組み合わせユニット１４は、暗号化秘密の暗号化シェアによってポリシー内の属性間の関係を施行するよう構成され得る。例えば、メッセージを解読するために属性の少なくとも特定の組み合わせに関連付けられた鍵が必要であるように、暗号化シェアを用いて属性が組み合わせられてもよい。
【００４９】
第２の暗号ユニット４は、秘密を解読することなく暗号化秘密から直接暗号化シェアを生成するよう構成され、ここで、暗号化シェアを解読せずに暗号化シェアを組み合わせて秘密を得ることはできない。これは例えば、秘密及びそのシェアを、それぞれ、所定の数の秘密乗又は秘密のシェア乗として表現することによって実現され得る。例えば、第１の暗号ユニット２は、所定の数を秘密を表す値で累乗することによって秘密を暗号化するための秘密暗号化ユニット８を備え得る。
【００５０】
例えば、第１及び第２のエンクリプタは、モバイル端末上で動作するデータ入力アプリケーションが生成する医療情報を含むメッセージをやり取りするための通信システムの一部であり得る。
【００５１】
第２のエンクリプタ１２は、ＡＢＣ暗号文を例えばＡＢＥ暗号文を保存するためのストレージサーバ等の他のエンティティに、又はＡＢＥ暗号文を解読するための他のユーザデバイスに直接伝送するための第２の伝送ユニット１５を含み得る。
【００５２】
システムは、更に、第２のエンクリプタ１２のための鍵を生成するよう構成された鍵生成器１６を含み、ここで、この鍵は第２の暗号ユニット４が秘密の暗号化シェアを生成することを可能にするが、第２の暗号ユニット４が秘密を解読することは可能にしない。このような鍵生成器１６は、個別のユーザの属性に関連付けられた秘密鍵を含め、ユーザ秘密鍵及び／又は公開鍵を発行可能な中央鍵権限の一部であり得る。しかし、後者の鍵は別の鍵権限によって生成されてもよい。
【００５３】
プロキシは、ホストによって指定されたアクセス制御ポリシーによって指定される属性とは異なる属性を使用できなくてもよい。したがって、プロキシは、適切な属性を保持しないユーザが解読し得る暗号文を作成できなくてもよい。また、プロキシを使用すること

により、ホスト（限られた計算能力しか持たないモバイルデバイスであり得る）にかかる計算ワークロードを低減することができる。ポリシー内の属性間の関係の施行をカバーしない態様でスキームを実施することができる。

【００５４】

以下、スキームの一実施形態をより詳細に解明する。この実施形態はスキームの一例を表すに過ぎない。変形例及び代替的実施形態は、本開示に基づき、当業者の範囲内である。表１は、本明細書の残部で使用される記号の一部をまとめる。

【００５５】

［表１］：表記

λ	セキュリティパラメータ
G_1	巡回群G_1
G_T	ターゲット群G_T
$e(\cdot,\cdot)$	許容双線型写像$e: G_1 \times G_1 \rightarrow G_T$
g	巡回群G_1の生成元
a_j	ユーザが保持する属性
ω	ユーザが保持する属性のセット
τ	アクセス構造
r_u	確率的にユニークな各ユーザの乱数値$r_u \in Z_p$
s	暗号文に関連付けられたランダム秘密鍵$s \in Z_p$
M	暗号化されるべきメッセージ
SK_ω	属性セットωに関連付けられた秘密鍵
SK_{proxy}	プロキシ（クラウドプロバイダ）のための秘密鍵

【００５６】

本実施形態は、関与するパーティの制御下で実行され得る複数のアルゴリズムを含む。鍵の配給及びユーザ権限の割り当てを制御する１つ以上の権限が存在し得る。これは、異なるユーザへの属性の割り当て並びにユーザの適切な属性に関連付けられたユーザ鍵の生成及び配給を含む。セットアップアルゴリズム、データオリジネーターアルゴリズムのための鍵生成、及びプロキシアルゴリズムのための鍵生成は、このような権限の１つ以上によって実行され得る。ここで、データオリジネーター（又はデータオーナー）は、メッセージを属性ベース暗号化を用いて暗号化することを望むパーティである。データオリジネーターは、適切な権限からデータオリジネーター秘密鍵

SK_ω

を受け取り、利用可能な属性の宇宙に関するポリシーを選択又は定義し、暗号化されるべきデータを提供し得る。このようなデータはここではメッセージと呼ぶ。メッセージは、例えば、患者データベースへのデータベースエントリー、又は、ポリシー内に定められるクレデンシャルのセットを有する一人以上に送られるべきメモを含み得る。メッセージはプロキシに送られ得る。プロキシは、属性ベース暗号方式から知られる方法で、データオリジネーターから受け取った情報をポリシーに関連付けられた暗号文に変換し得る。データコンシューマは、暗号文を受け取り、適切な属性のセットに関連付けられた鍵に基づいて解読するパーティである。

【００５７】

本実施形態は以下のアルゴリズムの実施を含み得る。

【００５８】

セットアップ

入力：

λ

ランダム生成元

$g \in G_1$

を選択、ランダムに

$\alpha, \beta, \gamma, d \in Z_p$

を選択し、秘密に保つ；

暗号ハッシュ関数

$H_1: \{0,1\}^* \rightarrow G_1$

及び

$H_2: G_T \rightarrow \{0,1\}^n$

を選択；

$A = e(g,g)^{\alpha}$

を設定；

$\hat{A} = e(g,g)^{(\alpha+\gamma)\beta\gamma}$

を設定。

公開パラメータは

$PK = (G_1, G_T, e, H_1, H_2, g^{\beta d})$

からなり得る。

マスター秘密鍵は

$MK = (g^{\alpha}, g^{\gamma}, d)$

からなり得る。

【００５９】

以下から明らかになるように、

$\hat{A}$

は、エンクリプタが自身のためにプロキシ（例えば、クラウドプロバイダ）がＡＢＥ暗号文を作成することを必要とする場合に使用される。

【００６０】

第１のエンクリプタ又はデータオリジネーターのための鍵生成

入力：

PK, MK, ω

ランダムに

$r_u \in Z_p$

を選択し、秘密鍵

SK_{ω}

を以下のように設定する。

$$SK_{\omega} = (D^{(1)} = g^{\alpha} g^{\gamma} g^{\beta r_u},$$

$$D^{(2)} = g^{\beta r_u},$$

$$\forall a_j \in \omega: D_j^{(3)} = H_1(a_j)^{r_u})$$

【００６１】
第２のエンクリプタ又はプロキシのための鍵生成
入力：
PK, MK
プロキシのための鍵
SK_{proxy}
は次のように生成される。
$SK_{proxy} = \gamma/d$
プロキシの公開鍵として
$g^{\beta d}$
が使用されることに留意されたい。
【００６２】
（第１のエンクリプタ又はデータオリジネーターによって実行される）暗号化
入力：
PK, M, τ
「秘密」
$s \in Z_p$
をランダムに選択；
メッセージＭの中間暗号文を以下のように設定。
$CT_{intermediate} = (\tilde{C} = g^{\beta ds}, C = M \oplus H_2(\hat{A}^s), \forall a_j \in \tau: C_j' = H_1(a_j)^{-s})$
【００６３】
（第２のエンクリプタ又はプロキシによって実行される）ポリシー施行
入力：
$CT_{intermediate}, \tau, SK_{proxy}$
$\tilde{C}$
を次のように解読
$\hat{C} = \tilde{C}^{SK_{proxy}} = g^{s\gamma\beta} = g^{\hat{s}}, \text{ for } \hat{s} = s\gamma\beta ;$
ポリシー作成
$\forall a_j \in \tau: C_j = g^{\hat{s}_j} H_1(a_j)^{-s} ;$
ここで、

$\hat{s}_j$

は、例えば加法的秘密分散法又は閾値秘密分散法を使用して計算された

$\hat{s}$

のシェアである。

$\hat{s}$

を分散させるために、プロキシは

$\hat{s}$

を直接使用する必要はなく、

$\widehat{C}$

へのアクセスがあればよい。当業者は加法的秘密分散法及び閾値秘密分散法を知っている。ある閾値秘密分散法がShamir, Adi (1979), "How to share a secret", Communications of the ACM22 (11): 612-613に開示されている。
以下のように最終暗号文を作成。

$$CT = (C, \widehat{C}, \forall\, a_j \in \tau: C_j = g^{\hat{s}_j} H_1(a_j)^{-s})$$

【００６４】
解読
入力：

SK_ω, CT

仮定：

ω

がアクセス構造

τ

を満たすとする。そうでなければ、解読は失敗する。

$Z^{(1)} = \prod_{a_i \in \omega} e(C_j, D^{(2)}) \cdot e(\widehat{C}, D_j^{(3)}) = e(g,g)^{\hat{s}\beta r_u}$

を計算；

$Z^{(2)} = e(\widehat{C}, D^{(1)}) = e(g^{\hat{s}}, g^{\alpha} g^{\gamma} g^{\beta r_u}) = e(g,g)^{(\alpha+\gamma)\hat{s}} \cdot e(g,g)^{\hat{s}\beta r_u}$

を計算；

$$Z^{(3)} = \frac{Z^{(2)}}{Z^{(1)}} = e(g,g)^{(\alpha+\gamma)\hat{s}}$$

を計算；

$$M = C \oplus H_2(Z^{(3)})$$

を解読。
【００６５】
本発明は、本発明を実施するよう適合されたコンピュータプログラム、特にキャリア上の又はキャリア内のコンピュータプログラムにも応用されることが理解されよう。プログラムは、ソースコード形態、オブジェクトコード形態、部分的にコンパイルされた形態等の中間ソース及びオブジェクトコード形態、又は本発明に係る方法の実装における使用に

適した任意の他の形態を取り得る。また、このようなプログラムは多様なアーキテクチャ設計を有し得ることが理解されよう。例えば、本発明に係る方法又はシステムの機能を実装するプログラムコードは、１つ以上のサブルーチンに分割され得る。これらのサブルーチン間で機能を分配する多様な態様が当業者にとって明らかであろう。サブルーチンは共に１つの実行可能なファイル内に保存され、自己充足型プログラムを形成し得る。このような実行可能ファイルは、例えばプロセッサ命令及び／又はインタープリター命令（例えば、Ｊａｖａ（登録商標）インタープリター命令）等のコンピュータ実行可能命令を含み得る。あるいは、サブルーチンの１つ以上又は全てが少なくとも１つの外部ライブラリファイル内に保存され、静的に又は動的に、例えばランタイムにてメインプログラムとリンクされてもよい。メインプログラムは、少なくとも１つのサブルーチンへのコールを少なくとも１つ有する。また、サブルーチンも互いへのコールを有し得る。コンピュータプログラム製品に関連する一実施形態は、ここに述べられる方法のうちの少なくとも１つの方法の各処理ステップに対応するコンピュータ実行可能命令を含む。これらの命令はサブルーチンに分割され、かつ／又は静的に若しくは動的にリンクされ得る１つ以上のファイル内に保存され得る。コンピュータプログラム製品に関連する他の実施形態は、ここで述べられるシステム及び／又は生産物のうちの少なくとも１つの各手段に対応するコンピュータ実行可能命令を含む。これらの命令はサブルーチンに分割され、かつ／又は静的に若しくは動的にリンクされ得る１つ以上のファイル内に保存され得る。

【００６６】

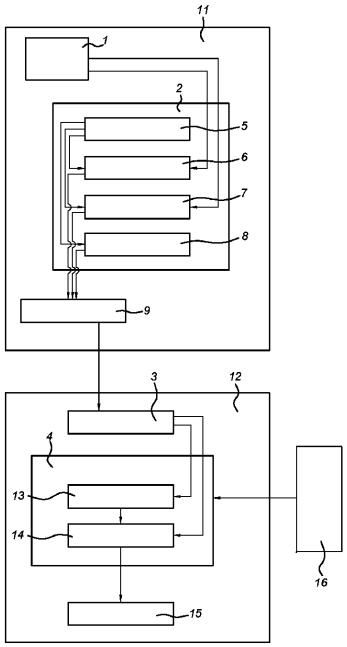
コンピュータプログラムのキャリアは、プログラムを保持し得る任意のエンティティ又はデバイスであり得る。例えば、キャリアは例えばＣＤ－ＲＯＭ若しくは半導体ＲＯＭなどのＲＯＭ、又は例えばフラッシュドライブ若しくはハードディスクなどの磁気記録媒体等の記憶媒体を含み得る。更に、キャリアは電気信号又は光信号等、電気若しくは光ケーブルを介して又は無線若しくは他の手段によって伝達され得る送信可能なキャリアであってもよい。プログラムがこのような信号で具現化されるとき、キャリアはこのようなケーブル又は他のデバイス若しくは手段によって構成され得る。あるいは、キャリアはプログラムが組み込まれる集積回路であり、集積回路は関連する方法を実行するように又はその実行において使用されるよう適合される。

【００６７】

上記実施形態は本発明を限定ではなく説明し、当業者は、特許請求の範囲から逸脱することなく多くの代替的実施形態を設計し得ることに留意されたい。請求項において、括弧内の如何なる参照符号も特許請求の範囲を限定するものと解されるべきではない。動詞「含む（又は備える若しくは有する等）」及びその活用形の使用は、請求項内に記載されるもの以外の要素又はステップの存在を除外しない。要素は複数を除外しない。本発明は複数の異なる要素を含むハードウェアによって、及び適切にプログラミングされたコンピュータによって実現され得る。複数の手段を列挙する装置クレームにおいて、これらのうちのいくつかが同一のハードウェアアイテムによって具現化されてもよい。いくつかの手段が互いに異なる従属請求項内に記載されているからといって、これらの手段の組み合わせを好適に使用することができないとは限らない。

【図１】

Fig. 1



【図２】

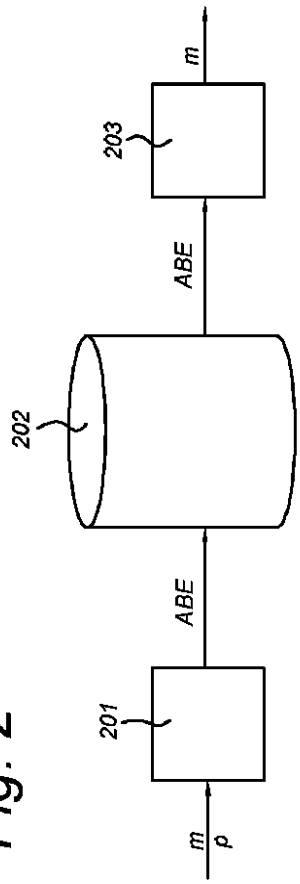


Fig. 2

【図３】

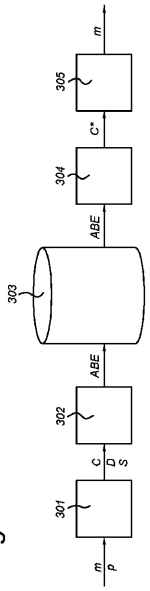
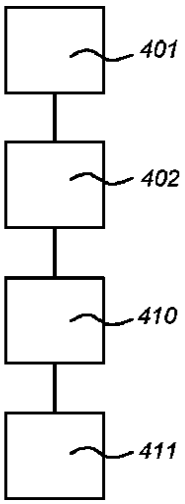


Fig. 3

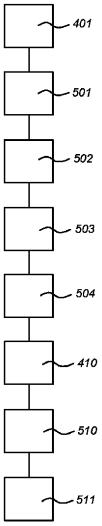
【図４】

Fig. 4



【図５】

Fig. 5



フロントページの続き

(72)発明者 イグナテンコ ターニャ
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５
(72)発明者 アシム モハメド
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５

審査官 金沢 史明

(56)参考文献 国際公開第２０１１／０４５７２３（WO，Ａ１）
米国特許出願公開第２０１２／０３００９３６（ＵＳ，Ａ１）
特開２０１１－１２４８５３（ＪＰ，Ａ）
国際公開第２０１２／０２５８６６（WO，Ａ１）
Xiaohui LIANG et al., Attribute Based Proxy Re-encryption with Delegating Capabilities, Proceedings of the 4th International Symposium on Information, Computer and Communications Security (ASIACCS'09), ACM, ２００９年 3月, pp. 276-286

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ 1／００
Ｈ０４Ｌ 9／００－ 9／３８
ＩＥＥＥ Ｘｐｌｏｒｅ
ＴＨＥ ＡＣＭ ＤＩＧＩＴＡＬ ＬＩＢＲＡＲＹ