(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7700851号
(P7700851)

(45)発行日　令和7年7月1日(2025.7.1)

(24)登録日　令和7年6月23日(2025.6.23)

(51)国際特許分類
*G09C 1/00 (2006.01)*

FI
G09C 1/00 620Z

請求項の数 20 （全38頁）

(21)出願番号　特願2023-521063(P2023-521063)
(86)(22)出願日　令和3年10月4日(2021.10.4)
(65)公表番号　特表2023-544198(P2023-544198A)
(43)公表日　令和5年10月20日(2023.10.20)
(86)国際出願番号　PCT/US2021/053415
(87)国際公開番号　WO2022/076327
(87)国際公開日　令和4年4月14日(2022.4.14)
審査請求日　令和6年8月6日(2024.8.6)
(31)優先権主張番号　63/087,866
(32)優先日　令和2年10月5日(2020.10.5)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　523112138
エヌティーティー リサーチ インコーポレイテッド
アメリカ合衆国 カリフォルニア州 ９４０８５ サニーベール スチュワート ドライブ ９４０
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100135079
弁理士　宮崎 修
(72)発明者　ダッタ プラティッシュ
アメリカ合衆国 カリフォルニア州 ９４０８５ サニーベール スチュワート ド
最終頁に続く

(54)【発明の名称】　分散型マルチ権限属性ベース暗号

(57)【特許請求の範囲】

【請求項１】

マルチ権限属性ベース暗号化スキームに従ってメッセージを暗号化するための、コンピュータで実装される方法であって、当該方法は：

暗号化のための$m_i$ビットを含む電子メッセージmを記憶媒体に記憶する段階と；

グローバル・セットアップ・アルゴリズムを実行してグローバル・パラメータを生成する段階であって：

LWEパラメータおよびノイズ分布を選択し；

ランダムな要素のデータyの第1列と、1に設定される対角線を除いてすべて0に設定される残りとをもつ行列Bを生成することによる、段階と；

権限セットアップ・アルゴリズムを実行して、権限の公開鍵および秘密鍵のペアを生成する段階であって：

第1のLWE行列Aを生成し；

第2のLWE行列Hを生成し；

前記権限の前記公開鍵を(A,H)に、前記秘密鍵を$T_A$に設定することによる、段階と；

鍵生成アルゴリズムを実行する段階であって：

一意的な識別子に暗号学的ハッシュ関数を適用することによって、ユーザーのためのランダム識別子ベクトルtを計算し；

k*A＝(1,t)*Hとなるようベクトルkを計算し；

ベクトルkを前記ユーザーについての秘密鍵として出力することによる、段階と；

前記メッセージmについて暗号化アルゴリズムを実行する段階であって：
メッセージmの各ビット$m_i$について：
行列Xおよびベクトルsならびに第1列がsである行列Vを生成し；
LWE行列Aおよび秘密Xを用いてLWEサンプル$c_i$を生成し；
LWE行列Hおよび秘密Xを用いてLWEサンプル$c_i'$を生成し、M*V*Bを加算し；
$m_i'$をs*yの最上位ビットとして計算し；
（$c_i$,$c_i'$）および$m_i$ XOR $m_i'$を計算することによる、段階と；
暗号化されたメッセージを記憶媒体に記憶する段階であって、前記暗号化されたメッセージは、各ビット$m_i$について、（$c_i$,$c_i'$）および$m_i^* = m_i$ XOR $m_i'$を含む、段階とを含む、
方法。

【請求項２】
前記秘密鍵を、1つの権限のみによって通信ネットワークを通じて配送することをさらに含む、請求項１に記載の方法。

【請求項３】
各ユーザーが属性のセットによって識別され、各暗号化されたメッセージについての復号能力が前記属性の関数に基づいている、請求項１に記載の方法。

【請求項４】
前記秘密鍵kを、任意の多項式数の独立権限によって通信ネットワークを通じて配送することをさらに含む、請求項３に記載の方法。

【請求項５】
各独立権限について、所定の数と属性のセットを選択することを含み、それにより、ユーザーが各権限からの少なくとも前記所定の数の属性を有する場合にのみ、ユーザーはメッセージmを復号することができる、請求項４に記載の方法。

【請求項６】
マルチ権限属性ベース暗号化スキームに従ってメッセージを復号するための、コンピュータで実装される方法であって、当該方法は：
$c_1 \cdots c_n$および$c_1' \cdots c_n'$および$m_1^* \cdots m_n^*$を表すビットを含むメッセージを、記憶媒体から読み出す段階であって、前記メッセージは属性ベース暗号化スキームに従って暗号化されている、段階と；
一意的な識別子に対して暗号学的ハッシュ関数を適用することによって、ユーザーについてのランダムな識別子ベクトルtを計算する段階と；
前記記憶媒体から秘密鍵kを取得する段階と；
復号アルゴリズムを実行する段階であって：
前記メッセージのi番目のビットを復号するために：
$c_i$*k＋$c_i'$(1,t)の線形結合を計算し；
その結果XOR $m_i$*の最上位ビットを計算する、段階と；
復号されたメッセージを前記記憶媒体に記憶する段階とを含む、
方法。

【請求項７】
前記秘密鍵kを、1つの権限のみによって通信ネットワークを通じて配送することをさらに含む、請求項６に記載の方法。

【請求項８】
各ユーザーが属性のセットによって識別され、各暗号化されたメッセージについての復号能力が前記属性の関数に基づく、請求項7に記載の方法。

【請求項９】
前記秘密鍵kを、任意の多項式数の独立権限によって通信ネットワークを通じて配送することをさらに含む、請求項8に記載の方法。

【請求項１０】
各独立権限について、所定の数および属性のセットを選択することをさらに含み、それ

により、ユーザーが各権限からの少なくとも前記所定の数の属性を有する場合にのみ、ユーザーは前記メッセージmを復号することができる、請求項９に記載の方法。
【請求項１１】
マルチ権限属性ベース暗号化スキームに従ってメッセージを暗号化するためのコンピュータ・システムであって、当該システムは：
暗号化のための$m_i$ビットを含む電子メッセージmを記憶するための記憶媒体と；
プロセッサとを有しており、該プロセッサは：
グローバル・セットアップ・アルゴリズムを実行してグローバル・パラメータを生成する段階であって：
LWEパラメータおよびノイズ分布を選択し；
ランダムな要素のデータyの第1列と、1に設定される対角線を除いてすべて0に設定される残りとをもつ行列Bを生成することによる、段階と；
権限セットアップ・アルゴリズムを実行して、権限の公開鍵および秘密鍵のペアを生成する段階であって：
第1のLWE行列Aを生成し；
第2のLWE行列Hを生成し；
前記権限の前記公開鍵を(A,H)に、前記秘密鍵を$T_A$に設定することによる、段階と；
鍵生成アルゴリズムを実行する段階であって：
一意的な識別子に暗号学的ハッシュ関数を適用することによって、ユーザーのためのランダム識別子ベクトルtを計算し；
k*A＝(1,t)*Hとなるようベクトルkを計算し；
ベクトルkを前記ユーザーについての秘密鍵として出力することによる、段階と；
前記メッセージmについて暗号化アルゴリズムを実行する段階であって：
メッセージmの各ビット$m_i$について：
行列Xおよびベクトルsならびに第1列がsである行列Vを生成し；
LWE行列Aおよび秘密Xを用いてLWEサンプル$c_i$を生成し；
LWE行列Hおよび秘密Xを用いてLWEサンプルci'を生成し、M*V*Bを加算し；
$m_i$'をs*yの最上位ビットとして計算し；
（$c_i$,$c_i$'）および$m_i$ XOR $m_i$'を計算することによる、段階とを実行するように構成されており；
前記記憶媒体はさらに、暗号化されたメッセージを記憶媒体に記憶するように構成されおり、前記暗号化されたメッセージは、各ビット$m_i$について、（$c_i$,$c_i$'）およびmi*＝$m_i$ XOR $m_i$'を含む、
システム。
【請求項１２】
前記プロセッサが、前記秘密鍵を、1つの権限のみによって通信ネットワークを通じて配送するようにさらに構成されている、請求項１１に記載のシステム。
【請求項１３】
各ユーザーが属性のセットによって識別され、各暗号化されたメッセージについての復号能力が前記属性の関数に基づいている、請求項１１に記載のシステム。
【請求項１４】
前記プロセッサが、前記秘密鍵を、任意の多項式数の独立権限によって通信ネットワークを通じて配送するようにさらに構成されている、請求項１３に記載のシステム。
【請求項１５】
前記プロセッサが、各独立権限について、所定の数と属性のセットを選択するようにさらに構成されており、それにより、ユーザーが各権限からの少なくとも前記所定の数の属性を有する場合にのみ、ユーザーはメッセージmを復号することができる、請求項１４に記載のシステム。
【請求項１６】
マルチ権限属性ベース暗号化スキームに従ってメッセージを復号するためのコンピュー

タ・システムであって、当該システムは：
$c_1 \cdots c_n$および$c_1' \cdots c_n'$および$m_1^* \cdots m_n^*$を表すビットを含むメッセージを記憶するように構成された記憶媒体であって、前記メッセージは属性ベース暗号化スキームに従って暗号化されている、記憶媒体と；
プロセッサとを有しており、該プロセッサは：
一意的な識別子に対して暗号学的ハッシュ関数を適用することによって、ユーザーについてのランダムな識別子ベクトルtを計算する段階と；
コンピュータ読み取り可能な媒体から秘密鍵kを取得する段階と；
復号アルゴリズムを実行する段階であって：
前記メッセージのi番目のビットを復号するために：
$c_i^* k + c_i'(1,t)$の線形結合を計算し；
その結果XOR $m_i^*$の最上位ビットを計算する、段階とを実行するように構成されており；
前記記憶媒体が、復号されたメッセージを記憶するようにさらに構成されている、
システム。
【請求項１７】
前記プロセッサが、前記秘密鍵kを、1つの権限のみによって通信ネットワークを通じて配送するようにさらに構成されている、請求項１６に記載のシステム。
【請求項１８】
各ユーザーが属性のセットによって識別され、各暗号化されたメッセージについての復号能力が前記属性の関数に基づく、請求項17に記載のシステム。
【請求項１９】
前記プロセッサが、前記秘密鍵を、任意の多項式数の独立権限によって通信ネットワークを通じて配送するようにさらに構成されている、請求項18に記載のシステム。
【請求項２０】
前記プロセッサが、各独立権限について、所定の数および属性のセットを選択するようにさらに構成されており、それにより、ユーザーが各権限からの少なくとも前記所定の数の属性を有する場合にのみ、ユーザーは前記メッセージmを復号することができる、請求項１９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連する出願への相互参照
【０００２】
本願は、2020年10月5日に出願された米国仮出願第63/087,866号の利益を主張するものであり、その全内容は参照により本願に組み込まれる。
【０００３】
発明の分野
【０００４】
本開示は、安全性が（ランダム・オラクル・モデルにおいて）誤差条件下での学習（Learning With Errors、LWE）の仮定のみに基づく、非自明なクラスのアクセス・ポリシーのための分散型のマルチ権限属性ベース暗号（multi-authority attribute-based encryption、MA-ABE）スキームに関する。
【背景技術】
【０００５】
本発明の背景
【０００６】
属性ベース暗号（ABE）は、従来の公開鍵暗号の一般化であり、受信者の資格情報（または属性）に基づいて、暗号化されたデータに対するきめ細かいアクセス制御を提供する。ABEには、暗号文規定型（ciphertext-policy）と鍵規定型（key-policy）の2つの化

身がある。暗号文規定型ABE（CP-ABE）では、名前が示すように、暗号文がアクセス・ポリシーに関連付けられ、鍵が属性に関連付けられる。鍵規定型ABE（KP-ABE）では、属性集合とアクセス・ポリシーの役割が入れ替わる。つまり、暗号文が属性に関連付けられ、鍵がアクセス・ポリシーに関連付けられる。KP-ABEどちらの場合も、属性がアクセス・ポリシーを満たす場合にのみ、復号が可能である。

【０００７】

Sahai and WatersおよびGoyalらによる着想以来、ABEは潜在的な応用の長いリストをもつ基本的な暗号プリミティブとなった。したがって、自然にABEスキームを設計することは、暗号コミュニティからの多大な注目を集めており、その結果、表現力、効率性、安全性、および基礎になる仮定の間のさまざまなトレードオフを達成する長い一連の研究がなされている。

【０００８】

ほとんどの研究は、双線形マップに関連する暗号学的仮定を安全性のベースとしている。他の仮定に基づく構築を求めるのは非常に自然なことである。第一に、これは概念的な観点から重要である。より多くの構築がスキームの存在に対する自信を高めるだけでなく、異なる仮定を使用した構築はしばしば新しい技術を必要とし、その結果、プリミティブの理解が向上するからである。第二に、これは、量子コンピュータによるグループ・ベースの構築に対する既知の攻撃に照らして重要である。この一般的な目標の中で、現在、基礎となる構成要素として双線形マップを回避する一握りのABEスキーム（IDベース暗号を超えるもの）がある。

【０００９】

これらの研究はすべて、現在量子コンピュータに対しても困難であると考えられている誤差条件下での学習（LWE）問題の困難さから安全性を導いている。しかしながら、1つの顕著な事実は、既存のLWEベースのABEスキームが鍵規定型の設定で設計されていることである。今日まで、LWE仮定に基づいてCP-ABEスキームを構築するという自然な双対問題は、本質的には完全に手つかずである。

【００１０】

LWEベースのCP-ABEスキームを実現する唯一の既知の方法は、アクセス・ポリシーを属性として表し、属性集合を回路として表すユニバーサル回路を使用することによって、回路ベースのKP-ABEスキームをCP-ABEスキームに変換することである。しかしながら、この変換は本来的に、制約されたクラスのアクセス・ポリシーのための、理想的とは程遠いパラメータをもつCP-ABEをもたらす。具体的には、任意の多項式、セキュリティ・パラメータにおけるs,dについて、それは、サイズsと深さdの回路をもって諸アクセス・ポリシーについてCP-ABEを構築することを許容する。さらに、何らかのアクセス・ポリシーfに関して生成される暗号文のサイズは（どんなKP-ABEから始めても）$|f| \cdot \mathrm{poly}(\lambda, s, d)$になる。つまり、たとえ暗号化されるfが非常に小さな回路を有していても、CP-ABE暗号文は最悪ケースの限界s,dとともにスケールする。

【発明の概要】

【発明が解決しようとする課題】

【００１１】

このように、LWEのみを仮定しながら、上記のユニバーサル回路ベースのCP-ABE構築を改善して、（ランダム・オラクル・モデルにおいて）LWEの困難さを仮定するいくつかの非自明なクラスのアクセス・ポリシーについて、真に分散化されたMA-ABEを作り出す必要がある。

【課題を解決するための手段】

【００１２】

発明の簡単な概要

【００１３】

本発明のいくつかの実施形態は、マルチ権限属性ベースの暗号化方式に従ってメッセージを暗号化するためのシステム、方法、ネットワーク・デバイス、および機械可読媒体を

含み、以下を含む：暗号化のための$m_i$ビットを含む電子メッセージmをコンピュータ化された記憶媒体に記憶する段階と；グローバル・セットアップ・アルゴリズムを実行してグローバル・パラメータを生成する段階であって：LWEパラメータおよびノイズ分布の選択し；ランダムな要素のデータyの第1列と、1に設定される対角線を除いてすべて0に設定される残りとをもつ行列Bを生成することによる、段階と；権限セットアップ・アルゴリズムを実行して、公開鍵および秘密鍵のペアを生成する段階であって：第1のLWE行列Aを生成し；第2のLWE行列Hを生成し；前記権限の前記公開鍵を(A,H)に、前記秘密鍵を$T_A$に設定することによる、段階と；鍵生成アルゴリズムを実行する段階であって：一意的な識別子に暗号学的ハッシュ関数を適用することによって、ユーザーのためのランダム識別子ベクトルtを計算し；k*A＝(1,t)*Hとなるようベクトルkを計算し；ベクトルkを前記秘密鍵として出力することによる、段階と；前記メッセージmについて暗号化アルゴリズムを実行する段階であって：メッセージmの各ビット$m_i$について：行列Xおよびベクトルsならびに第1列がsである行列Vを生成し；LWE行列Aおよび秘密Xを用いてLWEサンプル$c_i$を生成し；LWE行列Hおよび秘密Xを用いてLWEサンプルci'を生成し、M*V*Bを加算し；$m_i'$をs*yの最上位ビットとして計算し；（$c_i$,$c_i'$）および$m_i$ XOR $m_i'$を計算することによる、段階と；暗号化されたメッセージをコンピュータ化された記憶媒体に記憶する段階であって、前記暗号化されたメッセージは、各ビット$m_i$について、（$c_i$,$c_i'$）およびmi*＝$m_i$ XOR $m_i'$を含む、段階。

【００１４】

本発明の他の実施形態は、マルチ権限属性ベース暗号化スキームに従ってメッセージを復号するためのシステム、方法、ネットワーク・デバイスおよび機械読み取り可能な媒体を含み、下記を含む：$c_1$…$c_n$および$c_1'$…$c_n'$および$m_1*$…$m_n*$を表すビットを含むメッセージを、コンピュータ化された記憶媒体に記憶する段階であって、前記メッセージは属性ベース暗号化スキームに従って暗号化されている、段階と；一意的な識別子に対して暗号学的ハッシュ関数を適用することによって、ユーザーについてのランダムな識別子ベクトルtを計算する段階と；前記コンピュータ化された記憶媒体から秘密鍵kを取得する段階と；復号アルゴリズムを実行する段階であって：前記メッセージのi番目のビットを復号するために：$c_i$*k＋$c_i'$(1,t)の線形結合を計算し；その結果XOR $m_i*$の最上位ビットを計算する、段階と；復号されたメッセージを前記コンピュータ化された記憶媒体に記憶する段階。

【００１５】

さらなる実施形態は、前記秘密鍵を、1つの権限のみによって通信ネットワークを通じて配送することを含む。さらなる実施形態では、各ユーザーが属性の集合によって識別され、各暗号化されたメッセージについての復号能力が前記属性の関数に基づく。さらなる実施形態は、前記秘密鍵kを、任意の多項式数の独立権限によって通信ネットワークを通じて配送することを含む。さらなる実施形態は、各独立権限について、所定の数および属性の集合を選択することを含み、それにより、ユーザーが各権限からの少なくとも前記所定の数の属性を有する場合にのみ、ユーザーは前記メッセージmを復号することができる。

【図面の簡単な説明】

【００１６】

図面の簡単な説明

【００１７】

さらなる理解を提供するために含まれ、本明細書に組み込まれ、その一部を構成する添付の図面は、開示される実施形態を例解し、説明とともに、開示される実施形態の原理を説明するのに役立つ。

【００１８】

【図１】分散化されたマルチ権限属性ベース暗号化スキームについての例示的なシステム・アーキテクチャーを示している。

【００１９】

【図２】分散化されたマルチ権限属性ベース暗号化スキームについての例示的なシーケンス図を示している。

【００２０】
【図３】請求されるシステムおよび方法を実装するための例示的なコンピュータ・システム・アーキテクチャーを示している。
【００２１】
【図４】請求されるシステムおよび方法を実装するための例示的なコンピュータ・システム・アーキテクチャーのさらなる詳細を示している。
【発明を実施するための形態】
【００２２】
詳細な説明
【００２３】
標準的なABEスキームでは、鍵は中央機関によってのみ生成および発行されることができる。この概念の自然な拡張は、マルチ権限ABE（multi-authority AVE、MA-ABE）と呼ばれ、複数の当事者が機関の役割を果たすことを許容する〔本稿では権限主体を機関ということがあり、「権限」と「機関」を交換可能に使うことがある〕。MA-ABEスキームでは、異なる属性を制御する複数の機関があり、そのそれぞれが、システム内の他の機関との対話なしに、その制御下にある属性を所有するユーザーに秘密鍵を発行できる。具体的には、何らかのアクセス・ポリシーに関して生成された暗号文が与えられた場合、そのアクセス・ポリシーを満たす属性の集合を所有するユーザーは、それらの属性を制御するさまざまな機関から取得した個々の秘密鍵をプルすることによって、暗号文を復号できる。安全性は、権限のないユーザーに対する通例の結託耐性を必要とするが、重要な違いとして、今や属性機関の一部が堕落してもよく、よって、敵対ユーザーと結託してもよい。
【００２４】
ここに開示されているのは、安全性が（ランダム・オラクル・モデルにおいて）誤差条件下での学習（Learning With Errors、LWE）の仮定のみに基づく、非自明なクラスのアクセス・ポリシーのための分散型のマルチ権限属性ベース暗号（MA-ABE）スキームである。サポートされているアクセス・ポリシーは、選言標準形（Disjunctive Normal Form、DNF）公式によって記述されるものである。任意の非自明なクラスのアクセス・ポリシーをサポートするMA-ABEスキームのすべての以前の構築は、双線形マップ上のさまざまな仮定を前提として、（ランダム・オラクル・モデルにおいて）安全であることが証明されている。
【００２５】
開示されるシステムでは、任意の当事者が機関になることができ、共通の参照パラメータの初期集合の作成以外には、グローバルな調整の必要性はない。当事者は、単に、公開鍵を作成し、自分の属性を反映する秘密鍵を異なるユーザーに発行することによって、標準的なABE機関として行動することができる。ユーザーは、権限の選択された集合から発行された属性に対して、任意DNF公式を用いてデータを暗号化できる。最後に、システムは中央機関を必要としない。効率の面では、アクセス・ポリシーのサイズに対するグローバルな限界sを用いてスキームをインスタンス化する場合、公開鍵、秘密鍵、および暗号文のサイズはすべてsとともに増大する。
【００２６】
LWEを使用して暗号文規定型ABE（CP-ABE）スキームを構築するための新しいツールが開示される。これは、一般的なユニバーサル回路ベースの鍵規定型から暗号文規定型への変換を回避する、NCにおけるアクセス・ポリシーをサポートする証明可能に安全な〔つまり、安全性が証明できる〕CP-ABEスキームを含む。
【００２７】
また、DNF公式によって捕捉されたアクセス・ポリシーについて、無制限の数の属性権限をサポートする新しいMA-ABEスキームもここで開示される。このスキームは、ランダム・オラクル・モデルにおいて安全であることが証明されており、LWE問題の困難さに依拠している。
【００２８】

実施形態は、LWE仮定の下でDNF公式によって捕捉されたアクセス・ポリシーのための分散化されたMA-ABEスキームを含む。このスキームは、ランダム・オラクル・モデルにおいて、LWE仮定を、指数関数より小さい法対雑音比〔モジュラス対ノイズ比〕（modulus-to-noise ratio）とともに前提として、当事者たちの任意の結託に対して（静的に）安全である。

【００２９】

開示されたMA-ABEスキームでは、任意の当事者が任意の時点で機関になることができ、システムに参加できる属性機関の数に制限はなく、あるいは信頼されるセットアップ中に作成された共通参照パラメータの初期集合の作成以外に、グローバルな調整を必要としない。

【００３０】

ここで、証明可能に安全な直接CP-ABE構築であって、一般的なユニバーサル回路ベースの鍵規定型から暗号文規定型への変換を回避するものが開示される。特に、開示されるアプローチは、完全準同型暗号に触発された技法に基づいている以前のLWEベースの表現力のある（expressive）ABE構築から逸脱している。対照的に、開示されるCP-ABEは、線形秘密共有スキームの有用な特性に基づいており、判定型双線形ディフィー・ヘルマン仮定（decisional bilinear Diffie-Hellman assumption）に頼るウォーターズ（Waters）のCP-ABEスキームの、LWE版と見ることができる。

【００３１】

実施形態はまた、$NC^1$内のすべてのアクセス・ポリシーをサポートするCP-ABEスキームも含む。このスキームは、指数関数より小さい法対雑音比とともにLWE仮定を前提として、選択的に安全である。CP-ABEスキームは、敵がその暗号文クエリーをマスター公開鍵が公開される前に開示しなければならないが、安全性実験を通じて秘密鍵クエリーを適応的に行うことが許容される、標準的な選択的安全性を達成する。CP-ABE構築の実施形態はさらに、LWE仮定を前提とするすべての$NC^1$のためのCP-ABEスキームを含むCP-ABEの、LWEベースの直接構築を含む。CP-ABEスキームは、マルチ権限場面への拡張になじみやすい。

【００３２】

CP-ABEスキーム

【００３３】

セットアップ

【００３４】

システム内の各属性uについて、サンプル

【数１】

$$A_u \in \mathbb{Z}_q^{n\times m}$$

と、落とし戸$T_{Au}$と、別の一様にランダムな行列

【数２】

$$H_u \leftarrow \mathbb{Z}_q^{n\times m}.$$

さらに、サンプル

【数３】

$$y \leftarrow \mathbb{Z}_q^{n}.$$

出力は
【数４】

$$\mathrm{PK} = (y, \{A_u\}, \{H_u\}), \qquad \mathrm{SK} = \{T_{A_u}\}$$

【００３５】
属性集合Uのための鍵生成
【００３６】
【数５】

$$\hat{t} \leftarrow \mathrm{noise}^{m-1} \text{ および } t = (1, \hat{t}) \in \mathbb{Z}^m$$

とする。このベクトルtは、直観的には、特定のユーザーのすべての秘密鍵成分を一緒に結びつける要のはたらきをする。各属性u∈Uについて、$T_{Au}$を使用して、短ベクトル
【数６】

$$\tilde{k}_u \text{ ここで、} A_u \tilde{k}_u^{\top} = H_u t^{\top}$$

をサンプリングして
【数７】

$$\mathrm{SK} = (\{\tilde{k}_u\}, t)$$

を出力する。
【００３７】
行列Mが与えられたときのmsg∈{0,1}の暗号化
【００３８】
ρがMの行インデックスと属性の間をマッピングする関数であるとする。つまり、ρ(i)はMにおけるi番目の行に関連付けられた属性である。この手順は
【数８】

$$s \leftarrow \mathbb{Z}_q^n \text{ および } v_2, \ldots, v_{s_{\max}} \leftarrow \mathbb{Z}_q^m$$

をサンプリングし、
【数９】

$$c_i = sA_{\rho(i)} + \mathrm{noise}$$

$$\hat{c}_i = M_{i,1}(sy^{\top}, \overbrace{0, \ldots, 0}^{m-1}) + \left[\sum_{j \in \{2,\ldots,s_{\max}\}} M_{i,j} v_j\right] - sH_{\rho(i)} + \mathrm{noise}$$

を計算し、暗号文

【数１０】

$$\mathrm{CT} = \left(\{c_i\}_{i\in[\ell]}, \{\hat{c}_i\}_{i\in[\ell]}, C = \mathrm{MSB}(sy^{\top}) \oplus \mathrm{msg}\right).$$

を出力する。
【００３９】
復号
【００４０】
利用可能な属性が復号する資格があるとする。Iが、利用可能な属性に対応する行インデックスの集合であるとし、
【数１１】

$$\{w_i\}_{i\in I} \in \{0,1\} \subset \mathbb{Z}_q$$

が再構成係数であるとする。それぞれのi∈Iについて、ρ(i)がi番目の行に関連付けられた属性であるとする。手順は
【数１２】

$$K' = \sum_{i\in I} w_i\left(c_i\tilde{k}_{\rho(i)}^{\top} + \hat{c}_i t^{\top}\right)$$

を計算し、
【数１３】

$$\mathrm{msg}' = C \oplus \mathrm{MSB}(K').$$

を出力する。
【００４１】
MA-ABEスキーム
【００４２】
MA-ABEスキームは上記のスキームの一般化である。
【００４３】
記法
【００４４】
基礎となる安全性パラメータをλで表す。関数negl: N→Rは、任意の逆多項式関数よりも漸近的に小さい場合、つまり、あらゆるc＞0の定数について、すべてのλ＞$N_c$についてnegl(λ)≦$\lambda^{-c}$となるような整数$N_c$が存在する場合、無視できる。[n]＝{1,…,n}とする。
【００４５】
PPTは確率多項式時間（probabilistic polynomial-time）を表すとする。ある分布
（外１）

$$\mathcal{X}$$

について、xが分布

（外２）

$\mathcal{X}$

に従ってランダムにサンプリングされることを表すために、
（外３）

$x \leftarrow \mathcal{X}$

と書く。集合Xについて、xがXの要素上の一様分布に従ってサンプリングされることを表すために、x←Xと書く。ベクトルを表すにはvのような小文字を使い、行列にはMのような大文字を使う。デフォルトでは、すべてのベクトルは行ベクトルであるとする。行列のj番目の行は$M_j$と記され、行インデックスの集合Jについても同様に、すべてのj∈Jについての行$M_j$からなるMの部分行列を$M_J$と表す。ベクトルvについて、$\|v\|$がそのルムを表し、$\|v\|_\infty$がそのl∞ノルムを表すとする。

【００４６】

整数q≧2について、$Z_q$は、qを法とする整数の環を表すとする。$Z_q$を、範囲(－q/2,q/2]内の整数として表す。〔本稿では簡単のため黒板太字体などをローマン体で記すことがある。〕

【００４７】

区別不能性

【００４８】

ランダム変数の2つのシーケンスX＝{Xλ}λ∈NおよびY＝{Yλ}λ∈Nは、任意の非一様なPPTアルゴリズムAについて、すべてのλ∈Nについて

【数１４】

$$|\Pr[\mathcal{A}(1^\lambda, \mathcal{X}_\lambda) = 1] - \Pr[\mathcal{A}(1^\lambda, \mathcal{Y}_\lambda) = 1]| \leq \mathrm{negl}(\lambda)$$

のような無視できる関数negl(・)が存在する場合、計算上区別不能である。

【００４９】

離散領域Ω上の2つの分布DおよびD'について、DとD'の間の統計的距離は

【数１５】

$$\mathrm{SD}(\mathcal{D}, \mathcal{D}') = (1/2) \cdot \sum_{\omega \in \Omega} |\mathcal{D}(\omega) - \mathcal{D}'(\omega)|$$

として定義される。安全性パラメータλによってパラメータ指定されている分布の族D＝{Dλ}λ∈NおよびD'＝{D'λ}λ∈Nは、すべてのλ∈NについてSD(Dλ,D'λ)≦negl(λ)となるような無視できる関数が存在する場合、統計的に区別不能であると言われる。

【００５０】

格子

【００５１】

m次元格子Lは$R^m$の離散的な加法部分群である。正の整数n,m,qと行列$A \in Z_q^{n \times m}$が与えられたとき、

【数１６】

$\lambda_q^{\perp}(A)$ は格子$\{x \in \mathbb{Z}^m | Ax^{\mathsf{T}} = 0^{\mathsf{T}} \bmod q\}$を表す

とする。u∈$Z_q^n$について、
【数１７】

$\lambda_q^{u}(A)$ は剰余系$\left\{x \in \mathbb{Z}^m \middle| Ax^{\top} = u^{\top} \bmod q\right\}$を表す

とする。
【００５２】
離散ガウシアン
【００５３】
σを任意の正の実数をとする。パラメータσをもつガウス分布$D_\sigma$は確率分布関数$\rho_\sigma(x)=\exp(-\pi ¦ ¦ x^2 ¦ / \phi^2)$によって定義される。任意の離散集合L⊆$R^m$について、$\rho_\sigma(L)=\Sigma_{x\in L}\rho_\sigma(x)$を定義する。パラメータσをもつL上の離散ガウス分布$D_{L,\sigma}$は確率分布関数$\rho_{L,\sigma}=\rho_\sigma(x)/\rho_\sigma(L)$によって定義される。
【００５４】
打ち切りされた離散ガウシアン
【００５５】
パラメータσをもつ$Z^m$上の打ち切りされた離散ガウス分布は、
【数１８】

$\widetilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma}$

によって表され、$l_\infty$ノルムが
【数１９】

$\sqrt{m}\sigma$

を超えるときはいつも0を出力するという点を除いて、離散ガウス分布
【数２０】

$\mathcal{D}_{\mathbb{Z}^m,\sigma}$

と同じである。定義により、
【数２１】

$\widetilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma}$ は $\sqrt{m}\sigma$により有界である

ことに注意されたい。
【００５６】
格子の落とし戸
【００５７】

落とし戸のある格子は、ランダムに選ばれた格子と区別不能な格子であるが、困難な格子問題に対する効率的な解法を許容するある種の「落とし戸」をもつ。落とし戸格子サンプラーは、LT＝(TrapGen,SamplePre)と記され、次の構文および特性をもつ2つのアルゴリズムからなる。

【００５８】

【数２２】

$$\mathrm{TrapGen}(1^n, 1^m, q) \mapsto (A, T_A):$$

格子生成アルゴリズムは、入力として行列寸法n,m、法qを受け、落とし戸$T_A$とともに行列$A \in Z_q^{n \times m}$を出力するランダム化されたアルゴリズムである。

【００５９】

【数２３】

$$\mathrm{SamplePre}(A, T_A, \sigma, u) \mapsto s:$$

プリサンプリング・アルゴリズムは、入力として行列A、落とし戸$T_A$、ベクトル$u \in Z_q^n$、およびパラメータ$\sigma \in R$（これは出力ベクトルの長さを決定する）を受ける。これはベクトル

【数２４】

$$s \in \mathbb{Z}_q^m \text{ ここで、 } A \cdot s^{\mathsf{T}} = u^{\mathsf{T}} \text{ および } \| s \| \leq \sqrt{m} \cdot \sigma$$

を出力する。

【００６０】

<u>性質よくサンプリングされていること〔良好サンプリング性〕（Well-Sampledness）</u>

【００６１】

さらに、前述のサンプリング手順が、性質よくサンプリングされた要素を出力することを要求する。つまり、TrapGenによって出力される行列は一様ランダム行列のように見え、一様ランダム・ベクトル／行列を用いてSamplePreによって出力された原像は、適切なガウス分布から抽出されたエントリーをもつベクトル／行列と区別できない。

【００６２】

<u>向上された落とし戸サンプリング（Enhanced Trapdoor Sampling）</u>

【００６３】

$q:N \to N$、$\sigma:N \to R^+$を関数とし、LT＝(TrapGen,SamplePre)を、行列のq良好サンプリング性（q-well-sampledness）および原像の$(q,\sigma)$良好サンプリング性（$(q,\sigma)$-well-sampledness）の特性を満たす落とし戸格子サンプラーであるとする。我々は、向上された落とし戸格子サンプリング・アルゴリズムEnLT＝(EnTrapGen,EnSamplePre)を記述する。

【００６４】

【数２５】

$$\mathrm{EnTrapGen}(1^n, 1^m, q) \mapsto (A, T_A):$$

落とし戸生成アルゴリズムは
【数２６】

$2$つの行列$A_1 \in \mathbb{Z}_q^{n\times\lceil m/2\rceil}$ および $A_2 \in \mathbb{Z}_q^{n\times\lceil m/2\rceil}$ を

$(A_1, T_{\mathbf{A}_1}) \leftarrow \mathrm{TrapGen}(1^n, 1^{\lceil m/2\rceil}, q)$, $(A_2, T_{\mathbf{A}_2}) \leftarrow \mathrm{TrapGen}(1^n, 1^{\lceil m/2\rceil}, q)$として

生成する。それは両方の行列を列ごとにアペンドして、より大きな行列Aを$(A_1 \mid A_2)$として取得し、関連付けられた落とし戸$T_A$を、組み合わされた落とし戸情報$T_A=(T_{A1},T_{A2})$に設定する。
【００６５】
【数２７】

$\mathrm{EnSamplePre}(A, T_A, \sigma, Z) \mapsto S$:

原像サンプリング・アルゴリズムは、入力として、行列$A=(A_1 \mid A_2)$を、落とし戸$T_A=(T_{A1},T_{A2})$、パラメータ$\sigma=\sigma(\lambda)$、および行列$Z\in Z_q{}^{n\times k}$とともに受ける。それは、一様ランダム行列$W\leftarrow Z_q{}^{n\times k}$を選択し、$Y=Z-W$と設定する。次に、
【数２８】

行列$S_1, S_2 \in \mathbb{Z}^{\lceil m/2\rceil\times k}$ を $S_1 \leftarrow \mathrm{SamplePre}(A_1, T_{A_1}, \sigma, W)$ および $S_2 \leftarrow$

$\mathrm{SamplePre}(A_2, T_{A_2}, \sigma, Y)$として

計算する。列ごとに行列$S_1$と$S_2$を$S=(S_1 \mid S_2)$としてアペンドすることによって、最終的な出力行列$S\in Z^{m\times k}$を計算する。
【００６６】
誤差条件下での学習（Learning With Errors）
【００６７】
安全性パラメータ$\lambda\in N$について、$n:N\rightarrow N$、$q:N\rightarrow N$、$\sigma:N\rightarrow R^+$を$\lambda$の関数とする。$n=n(\lambda)$、$q=q(\lambda)$、$\sigma=\sigma(\lambda)$によってパラメータ指定された誤差条件下での学習（LWE）の仮定$LWE_{n,q,\sigma}$は、任意のPPTの敵Aについて、
【数２９】

任意の$\lambda\in\mathbb{N}$ について

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{LWE}_{n,q,\sigma}}(\lambda) \triangleq \left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathcal{O}_1^{s}(\cdot)}(1^\lambda) \mid s \leftarrow \mathbb{Z}_q^n\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\mathcal{O}_2(\cdot)}(1^\lambda)\right]\right| \leq \mathrm{negl}(\lambda),$$

となるような無視できる関数$negl(\cdot)$が存在することを述べる。ここで、オラクル$O_1{}^s(\cdot)$および$O_2(\cdot)$は次のように定義される：
【数３０】

$\mathcal{O}_1^s(\cdot)$ は固定構成された $s \in \mathbb{Z}_q^n$ を有しており、クエリーのたびに $a \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}$

を選び、$(a, sa^\top + e \bmod q)$を出力し、

$\mathcal{O}_2(\cdot)$ はクエリーのたびに $a \leftarrow \mathbb{Z}_q^n$, $u \leftarrow \mathbb{Z}_q$ を選び、 $(a, u)$を出力する。

【００６８】
格子問題の現在の現状技術を与えられれば、LWE仮定は任意の多項式n(・)および任意の関数q(・)、σ(・)について正しいと考えられ、それにより、すべてのλ∈Nについて、n＝n(λ)、q＝q(λ)、σ＝σ(λ)は次の制約条件を満たす：
【数３１】

$$2\sqrt{n} < \sigma < q < 2^n, \quad n \cdot \frac{q}{\sigma} < 2^{n^\epsilon}, \quad \text{および} \; 0 < \epsilon < 1/2$$

【００６９】
<u>線形秘密共有スキームについてのCP-ABEの概念</u>
【００７０】
q＝q(λ)として何らかの有限体$Z_q$上の線形秘密共有スキーム（linear secret sharing scheme、LSSS）によって捕捉されるアクセス構造のための暗号文規定型の属性ベース暗号化（CP-ABE）スキームは、次の構文をもつ4つの手順を含む。
【００７１】
【数３２】

$\mathrm{Setup}(1^\lambda, \mathbb{U}) \mapsto (\mathrm{PK}, \mathrm{MSK})$:

セットアップ・アルゴリズムは、単項での安全性パラメータλと、属性ユニバース（attribute universe）記述
【数３３】

$\mathbb{U}$

とを受け入れ、公開パラメータPKとマスター秘密鍵MSKとを出力する。PKは属性ユニバース
【数３４】

$\mathbb{U}$

の記述を含むとする。
【００７２】
【数３５】

$$\mathrm{KeyGen}(\mathrm{MSK}, U) \mapsto \mathrm{SK}:$$

鍵生成アルゴリズムは、入力としてマスター秘密鍵（master secret key）MSKと属性の集合
【数３６】

$$U \subseteq \mathbb{U}$$

を受け取り、秘密鍵（private key）SKを出力する。前記秘密鍵は暗黙的に属性集合Uを含むとする。
【００７３】
【数３７】

$$\mathrm{Enc}(\mathrm{PK}, \mathrm{msg}, (M, \rho)) \mapsto \mathrm{CT}:$$

暗号化アルゴリズムは、公開パラメータPK、メッセージmgs、およびLSSSアクセスポリシー(M,ρ)を受け入れる。ここで、Mは$Z_q$上の行列であり、ρはMの各行に
【数３８】

$$\mathbb{U}$$

における属性を割り当てる行ラベリング関数である。アルゴリズムは暗号文CTを出力する。暗号文は暗黙的に(M,ρ)を含んでいると想定する。
【００７４】
【数３９】

$$\mathrm{Dec}(\mathrm{PK}, \mathrm{CT}, \mathrm{SK}) \mapsto \mathrm{msg}':$$

復号アルゴリズムは、公開パラメータPK、何らかのLSSSアクセス・ポリシー(M,ρ)に関して生成された暗号文CT、および属性の何らかの集合
【数４０】

$$U \subset \mathbb{U}$$

についてのシークレット鍵を受け入れる。それは、Uにおける属性がLSSSアクセスポリシー(M,ρ)を満たす場合、つまりベクトル(1,0,…,0)が、ρによってU内の何らかの属性にマッピングされる、アクセス行列Mの行の線形スパン内にある場合に、メッセージmsg'を出力する。それ以外の場合、復号は失敗する。
【００７５】
線形秘密共有スキームのためのMA-ABEの概念
【００７６】
q＝q(λ)として、何らかの有限体$Z_q$上の線形秘密共有スキームLSSSによって捕捉されたアクセス構造のためのマルチ権限属性ベース暗号化（MA-ABE）システムMA-ABE＝(Gl

obalSetup,AuthSetup,KeyGen,Enc,Dec)は、次の構文をもつ5つの手順からなる。
（外４）

$\mathcal{AU}$

〔AUと記すこともある；他も同様〕によって権限ユニバースを表し、
（外５）

$\mathcal{GID}$

によってユーザーのグローバル識別子のユニバースを表す。さらに、各権限は1つの属性のみを制御すると想定し、よって、「権限」（authority）と「属性」（attribute）という語を交換可能に使用する。この定義は、各権限が潜在的に任意の数の属性を制御できる状況に自然に一般化される。
【００７７】
【数４１】

$$\mathrm{GlobalSetup}(1^{\lambda}) \mapsto \mathrm{GP}:$$

グローバル・セットアップ・アルゴリズムは、単項での安全性パラメータλを受け入れ、システムのためのグローバル公開パラメータGPを出力する。GPは、属性権限（attribute authorities）のユニバースAUとユーザーのグローバル識別子のユニバース
（外６）

$\mathcal{GID}$

の記述を含むとする。
【００７８】
【数４２】

$$\mathrm{AuthSetup}(\mathrm{GP}, u) \mapsto (\mathrm{PK}_u, \mathrm{SK}_u):$$

権限
【数４３】

$$u \in \mathcal{AU}$$

は、権限セットアップ・アルゴリズムを、その初期化中に、グローバル・パラメータGPを入力として呼び出し、その公開鍵と秘密鍵のペア$PK_u$、$SK_u$を受け取る。
【００７９】
【数４４】

$$\mathrm{KeyGen}(\mathrm{GP}, \mathrm{GID}, \mathrm{SK}_u) \mapsto \mathrm{SK}_{\mathrm{GID},u}:$$

鍵生成アルゴリズムは、入力としてグローバル・パラメータGP、ユーザーのグローバル識別子
【数４５】

$$\mathrm{GID} \in \mathcal{GID}$$

および権限
【数４６】

$$u \in \mathcal{AU}$$

の秘密鍵$SK_u$を受け、ユーザーについての秘密鍵$SK_{GID,u}$を出力する。
【００８０】
【数４７】

$$\mathrm{Enc}(\mathrm{GP}, \mathrm{msg}, (M, \rho), \{\mathrm{PK}_u\}) \mapsto \mathrm{CT}:$$

暗号化アルゴリズムは、グローバル・パラメータGP、メッセージmsg、LSSSアクセス・ポリシー(M,ρ)（ここで、Mは$Z_q$上の行列であり、ρはMの各行に
【数４８】

$$\mathcal{AU}$$

における属性／権限を割り当てる行ラベリング関数である）、およびρの範囲におけるすべての権限についての公開鍵の集合$\{PK_u\}$を受け入れる。アルゴリズムは暗号文CTを出力する。暗号文は暗黙的に(M,ρ)を含んでいると想定する。
【００８１】
【数４９】

$$\mathrm{Dec}(\mathrm{GP}, \mathrm{CT}, \{\mathrm{SK}_{\mathrm{GID},u}\}) \mapsto \mathrm{msg}':$$

復号アルゴリズムは、グローバル・パラメータGP、何らかのLSSSアクセスポリシー(M,ρ)に関して生成された暗号文CT、およびグローバル識別子GIDをもつユーザーが所有するユーザーID‐属性のペア（GID,U）に対応する鍵のコレクション$\{SK_{GID,u}\}$を受け入れる。アルゴリズムは、秘密鍵$\{SK_{GID,u}\}$に関連付けられた属性のコレクションがLSSSアクセスポリシー(M,ρ)を満たす場合、つまりベクトル(1,0,…,0)が、ρによって何らかの属性
【数５０】

$$u \in \mathcal{AU}$$

にマッピングされる、Mの行の線形スパン内にある含まれ、よって秘密鍵$SK_{GID,u}$がグローバル識別子GIDをもつユーザーによって所有されている場合に、メッセージmsg'を出力する。それ以外の場合、復号は失敗する。
【００８２】

線形独立性をもつ線形秘密共有スキーム

【００８３】

秘密共有スキームは、秘密を保持するディーラーとn当事者〔参加者〕の集合からなる。非公式には、ディーラーは秘密を「シェア」に「分割」し、それらを当事者間で分配する。「許諾された」当事者の部分集合が合同して秘密を回復できるべきであり、一方、他の当事者は回復できるべきではない。許諾された集合の集合の記述は、アクセス構造と呼ばれる。

【００８４】

アクセス構造：[n]内の数に関連付けられたn当事者のアクセス構造は、当事者の空でない諸部分集合の集合

【数５１】

$$\mathbb{A} \subseteq 2^{[n]} \setminus \emptyset$$

である。

（外７）

$\mathbb{A}$

内の集合は許諾された集合と呼ばれ、

（外８）

$\mathbb{A}$

内にない集合は許諾されていない集合と呼ばれる。アクセス構造は、

【数５２】

$$\forall B, C \in 2^{[n]} \quad B \in \mathbb{A} \text{ かつ } B \subseteq C \text{であれば } C \in \mathbb{A}$$

であれば単調（monotone）と呼ばれる。

【００８５】

単調なアクセス構造

（外９）

$\mathbb{A}$

についての秘密共有スキームは、秘密zを入力するとn個のシェア$sh_1,\cdots,sh_n$を出力するランダム化されたアルゴリズムであり、任意の

【数５３】

$$A \in \mathbb{A}$$

について、シェア$\{sh_i\}_{i \in A}$がzを決定し、他の集合は（ランダム変数のように）zとは独立である。

【００８６】

非単調秘密共有

【００８７】

（単調なものだけではなく）すべてのアクセス構造を捉える上記の概念の自然な一般化

は、非単調秘密共有と呼ばれる。具体的には、アクセス構造
（外１０）

$\mathbb{A}$

についての非単調秘密共有スキームは、秘密zを入力するとn個のペア$(sh_{1,0},sh_{1,1}),\cdots,(sh_{n,0},sh_{n,1})$と見なされる2n個のシェアを出力し、
【数５４】

任意の$A \in \mathbb{A}$ について、シェア$\{sh_{i,1}\}_{i\in A} \cup \{sh_{i,0}\}_{i\notin A}$ が $z$ を決定し、他の集合は$z$とは独立である

となるようなランダム化されたアルゴリズムである。
【００８８】
再構成手順がシェアの線形関数であるすべての（非単調）秘密共有スキームの部分集合は、線形（非単調）秘密共有スキームとして知られている。
【００８９】
線形（非単調）秘密共有スキーム
【００９０】
$q \in N$を素数位数とし、[n]を当事者の集合とする。当事者[n]に関するアクセス構造
（外１１）

$\mathbb{A}$

を実現する秘密のドメイン$Z_q$をもつ、非単調秘密共有スキームΠは、次の場合に線形である。
【００９１】
１．秘密$z \in Z_q$の、$i \in [n]$および$b \in \{0,1\}$についての各シェア$sh_{i,b}$は、$Z_q$内のエントリーをもつベクトルを形成する。
【００９２】
２．シェア生成行列と呼ばれる行列
【数５５】

$M \in \mathbb{Z}_q^{\ell\times d}$

と、Mの行に、[n]からの当事者インデックスまたは{n＋1,…,2n}からの別の当事者インデックスとして表されるその対応する否定でラベリングする関数
【数５６】

$\rho: [\ell] \to [2n]$

が存在し、下記を満たす：シェアの生成中に、ベクトル$v=(z,r_2,\cdots,r_d) \in Z_q^{\,d}$を考える。Πに従う秘密zのl個のシェアのベクトルは
【数５７】

$$\mathrm{sh} = M \cdot v^{\top} \in \mathbb{Z}_q^{\ell \times 1}$$

に等しい。i∈[n]かつb∈{0,1}の場合、シェア$sh_{i,b}$は、ρ(j)＝n・(1－b)＋iであるすべての$sh_j$値からなる（よって、前半のn個のシェアは「1のシェア」に対応し、後半のn個のシェアは「0のシェア」に対応する）。ペア(M,ρ)は、アクセス構造

（外１２）

$$\mathbb{A}$$

のLSSSポリシーと呼ばれる。

【００９３】

秘密を共有する上記の方法は、上で定義したような非単調秘密共有スキームの望ましい正しさと安全性を満たすことはよく知られている。

【数５８】

$$M \in \mathbb{Z}_q^{\ell \times d} \text{ および } \rho: [\ell] \to [2n]$$

であるLSSSポリシーおよび当事者の集合S⊆[n]について、

【数５９】

$$\hat{S} = S \cup \{i \in \{n+1, \ldots, 2n\} \mid i - n \notin S\} \subset [2n]$$

とする。

【数６０】

$$M_{\hat{S}}$$

を、

ρに従って

【数６１】

$$\hat{S}$$

に「属する」、Mのすべての行（すなわち、

【数６２】

$$\rho(j) \in \hat{S}$$

となる行j）からなるの部分行列を表すとする。

【００９４】

正しさ（correctness）は、S⊆[n]が許諾されている場合、ベクトル

【数６３】

$$(1, \overbrace{0, \ldots, 0}^{d-1}) \in \mathbb{Z}_q^d$$

が

【数６４】

$$M_{\hat{S}}$$

の行のスパンにあることを意味する。安全性（security）は、S⊆[n]が許諾されていない場合、ベクトル(1,0,…,0)が

【数６５】

$$M_{\hat{S}}$$

の行のスパンにないことを意味する。また、許諾されていない場合、ベクトル$d \in Z_q^d$であって、その最初の成分$d_1 = 1$であり、

【数６６】

$$M_{\hat{S}} d^{\top} = 0$$

であるようなベクトルが存在する。ここで、0は、すべて0のベクトルである。

【００９５】

すべての線形秘密共有スキームの特別な部分集合は、再構成係数が常にバイナリであるものである。そのようなLSSSを{0,1}-LSSSと呼ぶ。

【００９６】

上記の共有と再構成の方法は、単にスカラーではなく次元m∈Nのベクトル

【数６７】

$$\mathbf{z} \in \mathbb{Z}_q^m$$

を共有することに直接拡張される。

【００９７】

暗号文規定型のABEスキーム

【００９８】

$NC^1$回路によって表されるアクセス構造をサポートする暗号文規定型のABE（CP-ABE）スキームが以下に説明される。スキームの説明では、呈示の簡単のため、暗号化アルゴリズムと復号アルゴリズムの両方がアクセス・ポリシーを直接、そのLSSS表現で受け取ることを想定している。しかしながら、実際の実装では、暗号化アルゴリズムと復号アルゴリズムは代わりにアクセス・ポリシーの回路表現を受け入れ、そのLSSS表現を決定論的に計算することができる。これは、アクセス・ポリシーの回路記述がないと、復号アルゴリズムが復号の成功に必要とされる{0,1}再構成係数を効率的に決定できないことがありうるためである。

【００９９】

まず、我々の正しさと安全性の証明によって必要とされるパラメータ制約条件を与える

。任意の0＜ε＜1/2を固定する。任意のB∈Nについて、
【数６８】

$$\mathcal{U}_B$$

を、Z∩[－B,B]、すなわちの±Bの間の整数上の一様分布を表すとする。セットアップ・アルゴリズムは、以下の条件を満たす、パラメータn,m,σ,qおよびノイズ分布Χlwe,Χ1,Χ2,Χbigを選択する：
【数６９】

$$n = \mathrm{poly}(\lambda), \sigma < q,\ n \cdot q/\sigma < 2^{n^{\epsilon}},\ \chi_{\mathrm{lwe}} = \widetilde{\mathcal{D}}_{\mathbb{Z},\sigma} \qquad \text{(LWE安全性のため)}$$

$$m > 2s_{\max} n \log q + \omega \log n + 2\lambda \quad \text{(向上した落とし戸サンプリングおよびLHLのため)}$$

$$\sigma > \sqrt{s_{\max} n \log q \log m} + \lambda \qquad \text{(向上した落とし戸サンプリングのため)}$$

$$\chi_1 = \widetilde{\mathcal{D}}_{\mathbb{Z}^{m-1},\sigma},\ \chi_2 = \widetilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma} \qquad \text{(向上した落とし戸サンプリングのため)}$$

$$\chi_{\mathrm{big}} = \mathcal{U}_{\hat{B}}, \text{ where } \hat{B} > (m^{3/2}\sigma + 1)2^{\lambda} \qquad \text{(スマッジング／安全性のため)}$$

$$|\mathbb{U}| \cdot 3m^{3/2}\sigma\hat{B} < q/4 \qquad \text{(正しさのため)}$$

【０１００】
CP-ABE構築
【０１０１】
【数７０】

$$\mathrm{Setup}(1^{\lambda}, s_{\max}, \mathbb{U})$$

【０１０２】
セットアップ・アルゴリズムは、単項でエンコードされた安全性パラメータλ、スキームによってサポートされるLSSS行列の最大幅$s_{max}=s_{max}(\lambda)$、およびシステムに関連付けられた属性ユニバース
（外１３）

$$\mathbb{U}$$

を取り入れる。アルゴリズムはまず、前述のようにLWEの法q、次元n,m、そしてまた分布Χlwe,Χ1,Χ2,Χbigを選択する。次に、ベクトル
【数７１】

$$\mathbf{y} \leftarrow \mathbb{Z}_q^n$$

と行列のシーケンス

【数７２】

$$\{\mathbf{H}_u\}_{u\in\mathbb{U}} \leftarrow \mathbb{Z}_q^{n\times m}$$

を選択する。次いで、落とし戸をもつ行列のペア
【数７３】

$$\{(A_u, T_{A_u})\}_{u\in\mathbb{U}} \leftarrow \mathrm{EnTrapGen}(1^n, 1^m, q)$$

をサンプリングする。最後に、
【数７４】

$$\mathrm{PK} = \left(n, m, q, \chi_{\mathrm{lwe}}, \chi_1, \chi_2, \chi_{\mathrm{big}}, \mathrm{y}, \{A_u\}_{u\in\mathbb{U}}, \{H_u\}_{u\in\mathbb{U}}\right), \qquad \mathrm{MSK} = \left\{T_{A_u}\right\}_{u\in\mathbb{U}}$$

を出力する。
【０１０３】
KeyGen(MSK,U)
【０１０４】
鍵生成アルゴリズムは、入力としてマスター秘密鍵MSKと属性の集合
【数７５】

$$U \subseteq \mathbb{U}$$

を受け入れる。ベクトル
【数７６】

$$\hat{t} \leftarrow \chi_1$$

をサンプリングし、ベクトル
【数７７】

$$t = (1, \hat{t}) \in \mathbb{Z}^m$$

を設定する。それぞれのu∈Uについて、ベクトル
【数７８】

$$\hat{k}_u \leftarrow \chi_{\mathrm{big}}^m \text{ および } \tilde{k}_u \leftarrow \mathrm{EnSamplePre}(A_u, T_{\mathbf{A}_u}, \sigma, tH_u^\top - \hat{k}_u A_u^\top)$$

をサンプリングし、
【数７９】

$$k_u = \hat{k}_u + \tilde{k}_u$$

と設定する。最後に、
【数８０】

$$\mathrm{SK} = (\{k_u\}_{u \in U}, t)$$

を出力する。
【０１０５】
Enc(PK,msg,(M,ρ))
【０１０６】
暗号化アルゴリズムは、入力として、公開パラメータPK、暗号化すべきメッセージmsg∈{0,1}、およびLSSSアクセスポリシー(M,ρ)を受ける。ここで、
【数８１】

$$M = (M_{i,j})_{\ell \times s_{\max}} \in \{-1,0,1\}^{\ell \times s_{\max}} \subset \mathbb{Z}_q^{\ell \times s_{\max}} \text{ および } \rho: [\ell] \to \mathbb{U}$$

関数ρは、Mの行を
（外１４）

$\mathbb{U}$

における属性に関連付ける。ρは単射関数であるとする。手順はベクトル
【数８２】

$$s \leftarrow \mathbb{Z}_q^n \text{ および } \{v_j\}_{j \in \{2,\ldots,s_{\max}\}} \leftarrow \mathbb{Z}_q^m$$

をサンプリングする。さらに、ベクトル
【数８３】

$$\{e_i\}_{i \in [\ell]} \leftarrow \chi_{\mathrm{lwe}}^m \text{ および } \{\hat{e}_i\}_{i \in [\ell]} \leftarrow \chi_{\mathrm{big}}^m$$

をサンプリングする。それぞれの
【数８４】

$$i \in [\ell]$$

について、ベクトル
【数８５】

$$c_i, \hat{c}_i \in \mathbb{Z}_q^m$$

を
【数８６】

$$c_i = sA_{\rho(i)} + e_i$$

$$\hat{c}_i = M_{i,1}(sy^\top, \overbrace{0, \ldots, 0}^{m-1}) + \left[\sum_{j\in\{2,\ldots,s_{\max}\}} M_{i,j}v_j\right] - sH_{\rho(i)} + \hat{e}_i$$

のように計算し、

【数８７】

$$\mathrm{CT} = \left((M,\rho), \{c_i\}_{i\in[\ell]}, \{\hat{c}_i\}_{i\in[\ell]}, C = \mathrm{MSB}(sy^\top) \oplus \mathrm{msg}\right)$$

を出力する。

【０１０７】

Dec(PK,CT,MSK)

【０１０８】

復号は、入力として、公開パラメータPK、何らかのLSSSアクセスポリシー(M,ρ)の下で何らかのメッセージを暗号化する暗号文CT、および属性の何らかの部分集合

【数８８】

$$U \subseteq \mathbb{U}$$

に対応する秘密鍵SKを受ける。(1,0,…,0)がUに関連付けられたMの行のスパンにない場合、復号は失敗する。それ以外の場合は、Iを、∀i∈I: ρ(i)∈Uとなるような行列Mの行インデックスの集合であるとし、

【数８９】

$\{w_i\}_{i\in I} \in \{0,1\} \subset \mathbb{Z}_q$ を、$\sum_{i\in I} w_i M_i = (1,0,\ldots,0)$ となるようなスカラーである

とする。ここで、$M_i$はMのi番目の行である。手順は、

【数９０】

$$K' = \sum_{i\in I} w_i\left(c_i k_{\rho(i)}^\top + \hat{c}_i t^\top\right)$$

を計算し、

【数９１】

$$\mathrm{msg}' = C \oplus \mathrm{MSB}(K').$$

を出力する。

【０１０９】

<u>マルチ権限ABEスキーム</u>

【０１１０】

DNF公式によって表されるアクセス構造についてのMA-ABEスキームが以下に示される。このスキームは、

【数９２】

$$\text{グローバル識別子のユニバース}\mathcal{GID} \subset \{0,1\}^*, \text{ 権限識別子のユニバース}\mathcal{AU}$$

に関連付けられており、DNFアクセス・ポリシーを単調LSSSとして表すためにルーコ・ウォーターズ（Lewko-Waters）変換を使用する。我々のスキームでは、各権限は1つの属性のみを制御するとする。ただし、標準的な技法を使用して、各権限が先験的に有界数の属性を制御するスキームに簡単に一般化できる。さらに、我々のスキームで使用されるすべてのアクセスポリシー$(M,\rho)$は、高々$s_{max}$個の列をもつ行列Mと単射行ラベリング関数ρに対応するとする。つまり、権限／属性はMの高々1つの行に関連付けられる。Lewko-Waters変換は、基礎になる公式において各ANDゲートについての結果として得られるLSSS行列についての新しい列を導入するため、LSSS行列の列数の限界は、実装では、サポートされるDNF公式のANDゲート数に自然に変換される。我々のCP-ABEスキームと同様に、以下の我々のスキームの説明では、呈示の簡単のために、暗号化アルゴリズムと復号アルゴリズムの両方がアクセス・ポリシーを直接、そのLSSS表現で受け取ることを想定している。しかしながら、実際の実装では、暗号化アルゴリズムと復号アルゴリズムは代わりにアクセス・ポリシーのDNF表現を受け、Lewko-Waters変換アルゴリズムを使用してそのLSSS表現を決定論的に計算するべきであることに注意されたい。

【０１１１】

まず、我々の正しさおよび安全性の証明によって必要とされるパラメータ制約条件を与える。任意の$0<\varepsilon<1/2$を固定する。任意$B\in N$について、

【数９３】

$$\mathcal{U}_B$$

は、$Z\cap[-B,B]$、すなわち$\pm B$の間の整数での一様分布を表すとする。セットアップ・アルゴリズムは、次の制約を満たすパラメータn,m,σ,qおよびノイズ分布$\chi_{lwe},\chi_1,\chi_2,\chi_{big}$を選択する。

【数９４】

$$n = \text{poly}(\lambda),\ \sigma < q,\ n\cdot q/\sigma < 2^{n^{\epsilon}},\ \chi_{\text{lwe}} = \widetilde{\mathcal{D}}_{\mathbb{Z},\sigma} \quad \text{(LWE安全性のため)}$$

$$m > 2s_{\max} n\log q + \omega\log n + 2\lambda \quad \text{(向上した落とし戸サンプリングおよびLHLのため)}$$

$$\sigma > \sqrt{s_{\max} n\log q\log m} + \lambda \quad \text{(向上した落とし戸サンプリングのため)}$$

$$\chi_1 = \widetilde{\mathcal{D}}_{\mathbb{Z}^{m-1},\sigma},\ \chi_2 = \widetilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma} \quad \text{(向上した落とし戸サンプリングのため)}$$

$$\chi_{\text{big}} = \mathcal{U}_{\hat{B}}, \text{ where } \hat{B} > m^{3/2}\sigma 2^{\lambda} \quad \text{(スマッジング／安全性のため)}$$

$$|\mathcal{AU}|(m^{3/2}\sigma^2 + 2m\hat{B}^2) < q/4 \quad \text{(正しさのため)}$$

【０１１２】

MA-ABE構築

【０１１３】

GlobalSetup($1^{\lambda}$,$s_{max}$)

【０１１４】

グローバル・セットアップ・アルゴリズムは、単項でエンコードされた安全性パラメータλと、スキームによってサポートされるLSSS行列の最大幅$s_{max}$＝$s_{max}$(λ)を受け入れる。まず、前述のようにLWEの法q、次元n,m、そしてまた分布$X_{lwe}$,$X_1$,$X_2$,$X_{big}$を選択する。次に、ベクトル

【数９５】

$$\mathbf{y} \leftarrow \mathbb{Z}_q^n$$

をサンプリングし、行列

【数９６】

$$\mathbf{B}_1 \in \mathbb{Z}_q^{n\times m} \text{ を } B_1 = \left[ y^{\top} \parallel \overbrace{0^{\top} \parallel \cdots \parallel 0^{\top}}^{m-1} \right]$$

として設定する。ここで、各0∈$Z_q^n$である。さらに、ストリング

【数９７】

$$[-\hat{B},\hat{B}]$$

を区間

【数９８】

$$\mathrm{GID} \in \mathcal{GID}$$

内の整数のランダムな(m－1)次元ベクトルにマッピングするハッシュ関数

【数９９】

$$\mathrm{H}:\mathcal{GID} \rightarrow (\mathbb{Z} \cap [-\hat{B},\hat{B}])^{m-1}$$

を想定する。Hは安全性証明においてランダム・オラクルとしてモデル化される。最後に、ハッシュ関数Hとグローバル・パラメータ

GP＝(n,m,q,$s_{max}$,$X_{lwe}$,$X_1$,$X_2$,$X_{big}$,$B_1$)

を出力する。

【０１１５】

AuthSetup(GP,H,u)

【０１１６】

グローバル・パラメータGP、ハッシュ関数H、および権限識別子

【数１００】

$$u \in \mathcal{AU}$$

が与えられて、アルゴリズムは、行列‐落とし戸ペア
【数１０１】

$$(A_u, T_{\mathbf{A}_u}) \leftarrow \mathrm{EnTrapGen}(1^n, 1^m, q) \text{ 、ここで} A_u \in \mathbb{Z}_q^{n \times m}$$

を生成し、別の行列$H_u \leftarrow Z_q^{n \times m}$をサンプリングし、権限uについての公開鍵と秘密鍵のペア
$PK_u = (A_u, H_u)$、$MSK_u = T_{Au}$
を出力する。
【０１１７】
KeyGen(GP,H,GID,$MSK_u$)
【０１１８】
鍵生成アルゴリズムは、グローバル・パラメータGP、ハッシュ関数H、ユーザーのグローバル識別子GID、および権限の秘密鍵$MSK_u$を入力として受ける。まず、ベクトル$t_{GID} = (1, H(GID)) \in Z^m$を計算する。次に、ベクトル
【数１０２】

$$\hat{k}_{\mathrm{GID},u} \leftarrow \chi_{\mathrm{big}}^m$$

を選択し、ベクトル
【数１０３】

$$\tilde{k}_{\mathrm{GID},u} \leftarrow \mathrm{EnSamplePre}(A_u, T_{\mathbf{A}_u}, \sigma, t_{\mathrm{GID}} H_u^\top - \hat{k}_{\mathrm{GID},u} A_u^\top)$$

をサンプリングして、ユーザーGIDについての秘密鍵を
【数１０４】

$$\mathrm{SK}_{\mathrm{GID},u} = \hat{k}_{\mathrm{GID},u} + \tilde{k}_{\mathrm{GID},u}$$

として出力する。
【０１１９】
Enc(GP,H,msg,(M,ρ),{$PK_u$})
【０１２０】
暗号化アルゴリズムは、グローバル・パラメータGP、ハッシュ関数H、暗号化すべきメッセージ・ビット{0,1}、Lewko-Waters変換によって生成されたLSSSアクセス・ポリシー(M,ρ)
【数１０５】

$$\text{（ここで、} M = (M_{i,j})_{\ell \times s_{\max}} \in \{-1, 0, 1\}^{\ell \times s_{\max}} \subset \mathbb{Z}_q^{\ell \times s_{\max}} \text{ および} \rho : [\ell] \to \mathcal{AU}\text{）}$$

および関連する権限の公開鍵{$PK_u$}を受ける。関数ρは、Mの行を権限に関連付ける（各権限が単一の属性を制御すると想定していることを想起されたい）。ρは単射関数であるとする。手順は、ベクトル
【数１０６】

$$s \leftarrow \mathbb{Z}_q^n,\ \{v_j\}_{j\in\{2,\ldots,s_{\max}\}} \leftarrow \mathbb{Z}_q^m \text{ および } \{x_i\}_{i\in[\ell]} \leftarrow \mathbb{Z}_q^n$$

をサンプリングする。さらに、ベクトル
【数１０７】

$$\{\mathrm{e}_i\}_{i\in[\ell]} \leftarrow \chi_{\mathrm{lwe}}^m \text{ および } \{\hat{e}_i\}_{i\in[\ell]} \leftarrow \chi_{\mathrm{big}}^m$$

をサンプリングする。それぞれの
【数１０８】

$$i \in [\ell]$$

について、ベクトル
【数１０９】

$$c_i, \hat{c}_i \in \mathbb{Z}_q^m$$

を
【数１１０】

$$c_i = x_i A_{\rho(i)} + e_i$$

$$\hat{c}_i = M_{i,1} s B_1 + \left[\sum_{j\in\{2,\ldots,s_{\max}\}} M_{i,j} v_j\right] - x_i H_{\rho(i)} + \hat{e}_i$$

のように計算し、
【０１２１】
【数１１１】

$$\mathrm{CT} = \left((M,\rho), \{c_i\}_{i\in[\ell]}, \{\hat{c}_i\}_{i\in[\ell]}, C = \mathrm{MSB}(sy^{\top}) \oplus \mathrm{msg}\right)$$

を出力する。
【０１２２】
$\mathrm{Dec}(\mathrm{GP},H,\mathrm{CT},\mathrm{GID},\mathrm{SK}_{\mathrm{GID},u})$
【０１２３】
復号は、グローバル・パラメータGP、ハッシュ関数H、Lewko-Waters変換によって生成されたLSSSアクセス・ポリシーに関して生成された暗号文CT、ユーザー識別情報GID、およびそのユーザーが所有するアクセス行列の行インデックスの部分集合Iに対応する秘密鍵$\{\mathrm{SK}_{\mathrm{GID},\rho(i)}\}_{i\in I}$を入力として受ける。(1,0,…,0)が集合I内にインデックスをもつMの行のスパン内にない場合、復号は失敗する。それ以外の場合は、
【数１１２】

$$\{w_i\}_{i\in I} \in \{0,1\} \subset \mathbb{Z}_q$$

が

【数１１３】

$$\sum_{i\in I} w_i M_i = (1,0,\ldots,0)$$

となるようなスカラーであるとする。ここで、$M_i$はMのi番目の行である。そのようなスカラー$\{w_i\}_{i\in I}$の存在とその効率的な決定が保証される。アルゴリズムは、

【数１１４】

$$t_{\mathrm{GID}} = (1, \mathrm{H}(\mathrm{GID})) \in \mathbb{Z}^m \text{ 、続いて } K' = \sum_{i\in I} w_i \cdot \left(c_i \mathrm{SK}^{\top}_{\mathrm{GID},\rho(i)} + \hat{c}_i t^{\top}_{\mathrm{GID}}\right)$$

を計算し、

【０１２４】

【数１１５】

$$\mathrm{msg}' = C \oplus \mathrm{MSB}(K').$$

を出力する。

【０１２５】

<u>システム実装</u>

【０１２６】

図1を参照して、分散化されたマルチ権限属性ベース暗号化スキームについての例示的なシステム・アーキテクチャーが示されている。任意の随意データなどのメッセージの所有者〔オーナー〕105は、ここで説明するようにメッセージを暗号化し、生成された暗号文をクラウドストレージ110に記憶することができる。アクセス者115として示される別のユーザーは、この暗号文をクラウドストレージ110から取得しうる。公開鍵と秘密鍵を管理するために、複数の権限〔権限主体、オーソリティー〕120がインスタンス化されうる。権限120は、プライベート鍵をデータ所有者105に、シークレット鍵をアクセス者115に配布しうる。本稿で説明されるように、ユーザーが必要な権限からの少なくとも所定の数の属性を有している場合にのみ、ユーザーは暗号文を復号できる。

【０１２７】

図2を参照して、分散化されたマルチ権限属性ベース暗号化スキームのための例示的なシーケンス図が示されている。任意のデータがクラウド201に記憶されていてもよい。該データは、データ所有者202がクラウドにアップロードさせたものであってもよい。その後、ユーザー203はクラウド201から該データを取得することを望むことがありうる。ユーザー203は、最初にファイルの詳細を閲覧し、権限204に鍵を要求してもよい。ここでは単一の権限204のみが示されているが、複数の権限がインスタンス化されることができ、ユーザーはそれらの権限のうちの複数と通信してもよい。

【０１２８】

図3および図4は、本開示に記載されたさまざまな実施形態を実装するために有用な例示的なコンピュータ・システムを示す。さまざまな実施形態は、たとえば、図3に示されるコンピュータ・システム500のような一つまたは複数のコンピュータ・システムを使用し

て実装されうる。一つまたは複数のコンピュータ・システム500は、たとえば、ここで議論されている実施形態のいずれか、ならびにそれらの組み合わせおよびサブコンビネーションを実装するために使用されうる。

【０１２９】

コンピュータ・システム500は、プロセッサ504のような一つまたは複数のプロセッサ（中央処理装置、処理装置、CPUとも呼ばれる）を含んでいてもよい。プロセッサ504は、通信インフラ506（たとえばバスなど）に接続されてもよい。

【０１３０】

コンピュータ・システム500はまた、モニター、キーボード、ポインティングデバイスなどのユーザー入出力デバイス503をも含んでいてもよく、これらはユーザー入出力インターフェース502を通じて通信インフラ506と通信してもよい。プロセッサ504の一つまたは複数は、グラフィックス処理装置（GPU）であってもよい。ある実施形態では、GPUは、数学集約的なアプリケーションを処理するように設計された特化した電子回路であるプロセッサであってもよい。GPUは、コンピュータグラフィックスアプリケーション、画像、ビデオなどに共通の数学集約的なデータなど、大きなデータ・ブロックの並列処理のために効率的な並列構造を有していてもよい。

【０１３１】

コンピュータ・システム500は、ランダムアクセスメモリ（RAM）などのメインメモリ508をも含んでいてもよい。メインメモリ508は、一つまたは複数のレベルのキャッシュを含んでいてもよい。メインメモリ508は、制御ロジック（すなわち、コンピュータソフトウェア、命令など）および／またはデータを記憶していてもよい。コンピュータ・システム500は、一つまたは複数の二次記憶装置または二次メモリ510をも含んでいてもよい。二次メモリ510は、たとえば、ハードディスクドライブ512および／またはリムーバブルストレージデバイスまたはリムーバブルストレージドライブ514を含んでいてもよい。リムーバブルストレージドライブ514は、リムーバブルストレージユニット518と相互作用してもよい。リムーバブルストレージユニット518は、コンピュータソフトウェア（制御ロジック）および／またはデータを記憶した、コンピュータで使用可能または読み取り可能なストレージデバイスを含みうる。リムーバブルストレージドライブ514は、リムーバブルストレージユニット518から読むおよび／またはそれに書き込みすることができる。

【０１３２】

二次メモリ510は、コンピュータ・システム500によってコンピュータ・プログラムおよび／または他の命令および／またはデータがアクセスされることを許容するための他の手段、装置、コンポーネント、道具、または他のアプローチを含みうる。そのような手段、装置、コンポーネント、道具、または他のアプローチは、たとえば、リムーバブルストレージユニット522とインターフェース520を含みうる。リムーバブルストレージユニット522とインターフェース520の例は、プログラムカートリッジとカートリッジインターフェース、リムーバブルメモリチップ（EPROMまたはPROMなど）と付随するソケット、メモリスティックとUSBポート、メモリカードと付随するメモリカードスロット、および／または他のリムーバブルストレージユニットと付随するインターフェースを含みうる。

【０１３３】

コンピュータ・システム500はさらに、通信インターフェース524（たとえばネットワークインターフェース）をさらに含みうる。通信インターフェース524は、コンピュータ・システム500が外部デバイス、外部ネットワーク、外部エンティティなど（個別に、またまとめてリモートデバイス、ネットワーク、エンティティ528と称される）の任意の組み合わせと通信し、対話することを可能にしうる。たとえば、通信インターフェース524は、コンピュータ・システム500が外部またはリモートデバイス、ネットワーク、エンティティ528と通信経路526を通じて通信することを許容しうる。通信経路526は、有線および／または無線（またはその組み合わせ）であってもよく、LAN、WAN、インターネットなどの任意の組み合わせを含んでいてもよい。制御ロジックおよび／またはデータが、

通信経路526を介してコンピュータ・システム500との間で送受信されうる。

【０１３４】

コンピュータ・システム500は、いくつかの非限定的な例を挙げると、携帯情報端末（PDA）、デスクトップワークステーション、ラップトップまたはノートブックコンピュータ、ネットブック、タブレット、スマートフォン、スマートウォッチまたはその他のウェアラブルデバイス、アプライアンス、モノのインターネットの一部、および／または組み込みシステムのいずれかであってもよく、またはそれらの任意の組み合わせであってもよい。

【０１３５】

コンピュータ・システム500は、任意の配信パラダイムを通じて任意のアプリケーションおよび／またはデータにアクセスするまたはそれをホストする、クライアントまたはサーバーコンピューティングデバイスであってもよく、それは、リモートまたは分散クラウドコンピューティングソリューション；ローカルまたはオンプレミスソフトウェア（「オンプレミス」のクラウドベースソリューション）；「サービスとしての」モデル（たとえば、サービスとしてのコンテンツ（CaaS）、サービスとしてのデジタルコンテンツ（DCaaS）、サービスとしてのソフトウェア（SaaS）、サービスとしてのマネージドソフトウェア（MSaaS）、サービスとしてのプラットフォーム（PaaS）、サービスとしてのデスクトップ（DaaS）、サービスとしてのフレームワーク（FaaS）、サービスとしてのバックエンド（BaaS）、サービスとしてのモバイルバックエンド（MBaaS）、サービスとしてのインフラストラクチャー（IaaS）など）；および／または前述の例または他のサービスまたは配信パラダイムの任意の組み合わせを含むハイブリッドモデルを含むがこれらに限定されない。

【０１３６】

図4は、コンピュータ・システム900の例示的なマシンを示しており、その中で、ここで論じられる動作のいずれか一つまたは複数をマシンに実行させるための命令のセットが実行されうる。代替的な実装では、マシンはLAN、イントラネット、エクストラネット、および／またはインターネット内の他のマシンに接続されてもよい（たとえばネットワーク接続されてもよい）。マシンは、クライアントサーバーネットワーク環境におけるサーバーまたはクライアントマシンとして、ピアツーピア（または分散）ネットワーク環境におけるピアマシンとして、またはクラウドコンピューティングインフラストラクチャーまたは環境におけるサーバーまたはクライアントマシンとして動作しうる。

【０１３７】

マシンは、パーソナルコンピュータ（PC）、タブレットPC、セットトップボックス（STB）、パーソナルデジタルアシスタント（PDA）、携帯電話、ウェブアプライアンス、サーバー、ネットワークルーター、スイッチまたはブリッジ、専用のアプリケーションまたはネットワークセキュリティアプライアンスまたはデバイス、またはそのマシンによって行われるアクションを指定する一組の命令（シーケンシャルまたはその他）を実行できる任意のマシンでありうる。さらに、単一のマシンが例示されているが、「マシン」という用語は、ここで論じられている方法論のいずれか一つまたは複数を実行するための命令のセット（または複数のセット）を個別にまたは合同して実行するマシンの任意のコレクションを含むと解釈されるものとする。

【０１３８】

例示的なコンピュータ・システム900は、処理装置902、メインメモリ904（たとえば、リードオンリーメモリ（ROM）、フラッシュメモリ、同期DRAM（SDRAM）などのダイナミックランダムアクセスメモリ（DRAM）など）、静的メモリ906（たとえば、フラッシュメモリ、静的ランダムアクセスメモリ（SRAM）など）、およびデータ記憶装置918を含み、これらはバス930を介して相互に通信する。

【０１３９】

処理装置902は、マイクロプロセッサ、中央処理装置などの一つまたは複数の処理装置を表す。より具体的には、処理装置は、複雑命令セットコンピューティング（CISC）マイ

クロプロセッサ、縮小命令セットコンピューティング（RISC）マイクロプロセッサ、超長命令語（VLIW）マイクロプロセッサ、または他の命令セットを実装するプロセッサ、または命令セットの組み合わせを実装するプロセッサでありうる。処理装置902は、特定用途向け集積回路（ASIC）、フィールドプログラマブルゲートアレイ（FPGA）、デジタル信号プロセッサ（DSP）、ネットワークプロセッサなどのような、一つまたは複数の特殊用途の処理装置であってもよい。処理装置902は、ここで論じられる動作およびステップを実行するための命令926を実行するように構成される。

【０１４０】

コンピュータ・システム900は、ネットワーク920を通じて通信するためのネットワークインターフェースデバイス908をさらに含んでいてもよい。コンピュータ・システム900は、ビデオ表示装置910、英数字入力装置912（たとえばキーボード）、カーソル制御装置914（たとえばマウス）、グラフィックス処理装置922、信号生成装置916（たとえばスピーカー）、グラフィックス処理装置922、ビデオ処理装置928、およびオーディオ処理装置932を含みうる。

【０１４１】

データ記憶装置918は、機械可読媒体924（コンピュータ可読記憶媒体としても知られる）を含んでいてもよく、その上に、ここに記述された動作のいずれか一つまたは複数を具現する命令926（たとえばソフトウェア命令）の一つまたは複数のセットが記憶される。命令926はまた、コンピュータ・システム900によるその実行中に、完全にまたは少なくとも部分的にメインメモリ904内および／または処理装置902内に存在してもよく、メインメモリ904および処理装置902も機械可読記憶媒体を構成する。

【０１４２】

一例では、命令926は、開示された主題に対応する動作および機能を実装するための命令を含む。機械可読記憶媒体924は、ある例示的な実装では単一の媒体であると示されているが、「機械可読記憶媒体」という用語は、命令926の一つまたは複数のセットを記憶する単一の媒体または複数の媒体（たとえば、集中型または分散型データベース、および／または付随するキャッシュおよびサーバー）を含むものと解釈されるべきである。「機械可読記憶媒体」という用語は、機械による実行のために命令926のセットを記憶またはエンコードすることができ、かつ、機械に本開示の動作のいずれか一つまたは複数を実行させる任意の媒体をも含むと解釈される。よって、「機械可読記憶媒体」という用語は、固体メモリ、光学式媒体および磁気媒体を含むが、それらに限定されないと解釈されるべきである。

【０１４３】

詳細な説明の一部は、コンピュータメモリ内のデータビットに対する操作のアルゴリズムおよび記号表現を用いて呈示されている。これらのアルゴリズム記述および表現は、データ処理技術の当業者が、他の当業者に自分の仕事の内容を最も効果的に伝えるために使用される方法である。アルゴリズムは、ここでは、また一般に、望ましい結果につながる自己整合的な一連の操作であると考えられている。操作は、物理量の物理的操作を必要とするものである。必ずではないが、通例、これらの量は、記憶され、転送され、組み合わされ、他の仕方で操作されることが可能な電気的もしくは磁気的な信号の形を取る。主に慣用の理由により、時に、これらの信号を、ビット、値、要素、シンボル、キャラクタ、項、数などと称することが便利であると判明している。

【０１４４】

しかしながら、これらおよび同様の用語のすべては、適切な物理量に関連しており、そうした物理量に適用される単に便宜上のラベルであることを留意すべきである。そうでないことが明確に述べられるのでない限り、上述の議論から明白なように、本稿を通じて、「識別」または「決定」または「実行」または「執行」または「収集」または「生成」または「送信」などの用語を利用する議論は、コンピュータ・システムのレジスタおよびメモリ内の物理的（たとえば電子的）量として表わされたデータを操作して、コンピュータ・システムのメモリもしくはレジスタまたは他のそのような情報記憶装置内の物理的量と

して同様に表わされる他のデータに変換する、コンピュータ・システムまたは類似の電子コンピューティング装置のアクションおよびプロセスを指すことが理解される。

【０１４５】

本開示はまた、ここでの動作を実行するための装置に関する。この装置は、意図された目的のために特別に構築されることもあれば、あるいはコンピュータに記憶されたコンピュータ・プログラムによって選択的にアクティブ化または再構成されるコンピュータを含んでいてもよい。そのようなコンピュータ・プログラムは、フロッピーディスク、光ディスク、CD-ROM、磁気光学ディスクを含む任意の種類のディスク、読み出し専用メモリ（ROM）、ランダムアクセスメモリ（RAM）、EPROM、EEPROM、磁気カードまたは光学カード、または電子命令を記憶するのに適した任意の種類のメディアなどだがそれらに限定されないコンピュータ読み取り可能な記憶媒体に記憶されうる。各記憶媒体はコンピュータシステムバスに結合される。

【０１４６】

本稿に呈示される動作および図は、いかなる特定のコンピュータまたはその他の装置にも本質的に関連するものではない。さまざまなタイプのシステムが、本稿の教示によるプログラムとともに使用されてもよく、あるいは動作を実行するためのより特化した装置を構築するのに便利であることが証明される場合もある。これらの多様なシステムの構造は、本稿で記載されるように見える。さらに、本開示は、いかなる特定のプログラミング言語を参照して記載されているのでもない。本稿に記載されている開示の教示を実装するために、多様なプログラミング言語が使用されうることは理解されるであろう。

【０１４７】

本開示は、コンピュータシステム（または他の電子デバイス）をプログラムして本開示に従ったプロセスを実行するために使用されうる、命令を記憶している機械可読媒体を含みうるコンピュータ・プログラム・プロダクトまたはソフトウェアとして提供されうる。機械可読媒体は、機械（たとえばコンピュータ）によって読み取り可能な形式で情報を記憶するための任意の機構を含む。たとえば、機械可読（たとえば、コンピュータ可読）媒体は、読み出し専用メモリ（「ROM」）、ランダムアクセスメモリ（「RAM」）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリデバイスなどの機械（たとえばコンピュータ）可読記憶媒体を含む。

【０１４８】

いくつかの実施形態では、制御ロジック（ソフトウェア）が記憶された、有体の、非一時的なコンピュータ使用可能または読み取り可能な媒体を含む有体の、非一時的な装置または製造物が、ここではコンピュータ・プログラム・プロダクトまたはプログラム記憶装置と呼ばれることもある。これは、コンピュータ・システム500、メインメモリ508、二次メモリ510、およびリムーバブルストレージユニット518と522、および上記の任意の組み合わせを具現する有体の製造物を含むが、これらに限定されない。そのような制御ロジックは、一つまたは複数のデータ処理デバイス（コンピュータシステム500など）によって実行されると、そのようなデータ処理デバイスに、本稿で説明されるように動作させうる。

【０１４９】

本開示に含まれる教示に基づいて、当業者には、図3および図4に示されているもの以外のデータ処理デバイス、コンピュータ・システム、および／またはコンピュータアーキテクチャーを使用して、本開示の実施形態をどのように作成し、使用するかは明白であろう。特に、実施形態は、ここに記載されているもの以外のソフトウェア、ハードウェア、および／またはオペレーティングシステムの実装を用いて動作することができる。

【０１５０】

他のどのセクションでもなく、詳細な説明のセクションが、クレームを解釈するために使用されることが意図されていることが認識されるべきである。他のセクションは、発明者によって考えられている、すべてではなく一つまたは複数の例示的な実施形態を記載することができ、よって、本開示または添付のクレームをいかなる仕方でも限定することは

意図されていない。

【０１５１】

本開示は、例示的な分野および用途のための例示的な実施形態を説明するが、本開示はそれに限定されないことを理解すべきである。他の実施形態およびそれに対する修正が可能であり、本開示の範囲および精神内にある。たとえば、本段落の一般性を制限することなく、実施形態は、本願に記載されている図に示されているソフトウェア、ハードウェア、ファームウェア、および／またはエンティティに限定されない。さらに、実施形態は（本稿に明示的に記載されているか否かにかかわらず）、本稿に記載されている例を超える分野および用途に対して重要な有用性を有する。

【０１５２】

実施形態は、具体的な機能およびその関係の実装を示す機能的構成要素の助けを借りて、ここに記載されてきた。これらの機能的構成要素の境界は、説明の便宜のためにここで任意に定義されている。指定された機能および関係（またはその等価物）が適切に実行される限り、代替的な境界が定義されることができる。また、代替的な実施形態が、ここで説明する順序とは異なる順序を使用して、機能ブロック、ステップ、動作、方法などを実行することができる。

【０１５３】

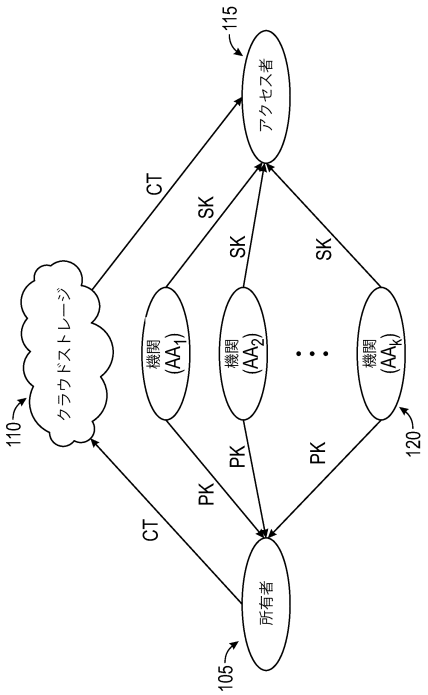
本稿での「一つの実施形態」、「ある実施形態」、「例示的実施形態」または同様の語句への言及は、記載された実施形態が特定の特徴、構造、または特性を含むことができるが、すべての実施形態が必ずしもその特定の特徴、構造、または特性を含むとは限らないことを示す。さらに、そのような語句は必ずしも同じ実施形態を指しているとは限らない。さらに、特定の特徴、構造、または特性がある実施形態に関連して記述されている場合、そのような特徴、構造、または特性を他の実施形態に組み込むことは、本稿で明示的に言及または記述されているか否かにかかわらず、当業者の知識の範囲内である。さらに、いくつかの実施形態は、「結合された」および「接続された」という表現やその派生形を使用して記述されることがある。これらの用語は、必ずしも相互の同義語として意図されているわけではない。たとえば、いくつかの実施形態は、2つ以上の要素が互いに物理的または電気的に直接接触していることを示すために、「接続された」および／または「結合された」という用語を使用して記述されることができる。しかしながら、「結合された」という用語は、2つ以上の要素が互いに直接接触していないが、それでも互いに協力または相互作用することを意味する場合もある。

【０１５４】

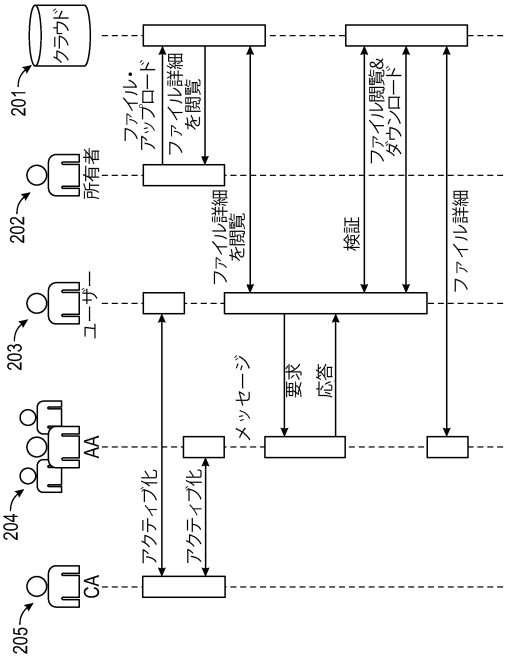
本開示の幅および範囲は、上記の例示的な実施形態のいずれによっても限定されるべきではなく、以下の請求項およびその等価物に従ってのみ定義されるべきである。前述の明細書では、本開示の実装は、その具体的な例示的な実装を参照して記載されてきた。以下の請求項に記載されているように、本開示の広義の精神および範囲から逸脱することなく、それにさまざまな修正が加えられうることは明らかであろう。よって、本明細書および図面は、制約する意味ではなく、例示する意味で考慮されるべきである。

【図面】

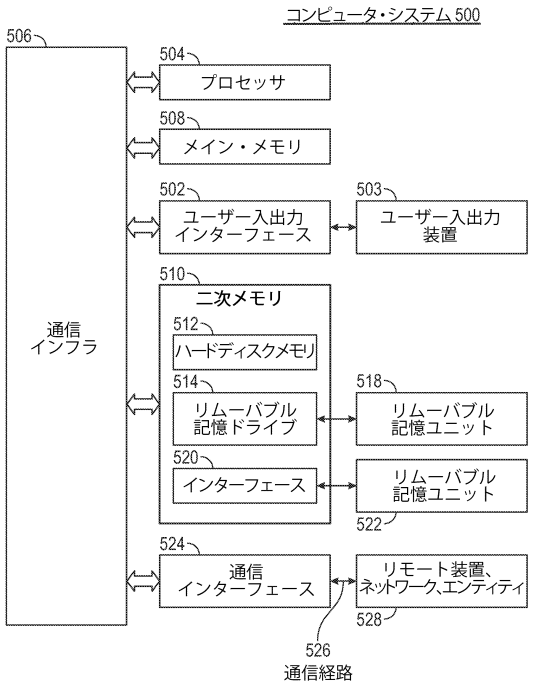
【図１】


115
アクセス者
CT
SK
SK
SK
クラウドストレージ
機関 ($AA_1$)
機関 ($AA_2$)
機関 ($AA_k$)
PK
PK
PK
CT
110
120
所有者
105

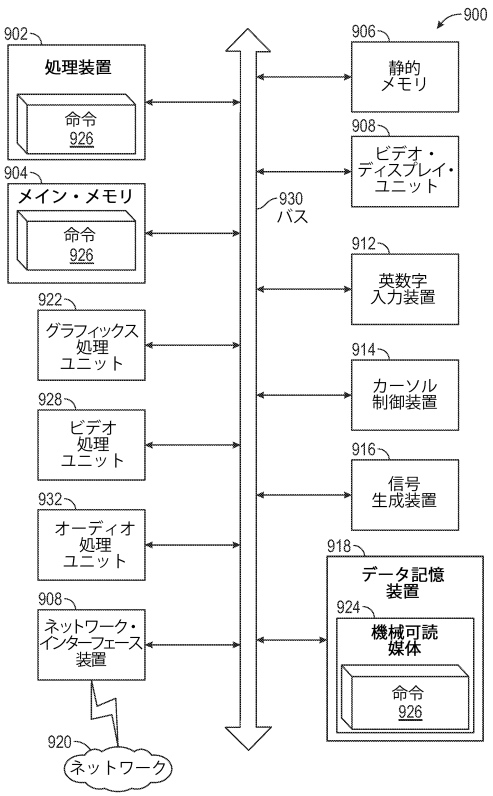
【図２】


クラウド
201
ファイル・アップロード
ファイル詳細を閲覧
ファイル閲覧&ダウンロード
所有者
202
ファイル詳細を閲覧
検証
ファイル詳細
ユーザー
203
メッセージ
要求
応答
AA
204
アクティブ化
アクティブ化
CA
205

【図３】


コンピュータ・システム 500
506
通信インフラ
504
プロセッサ
508
メイン・メモリ
502
ユーザー入出力インターフェース
503
ユーザー入出力装置
510
二次メモリ
512
ハードディスクメモリ
514
リムーバブル記憶ドライブ
518
リムーバブル記憶ユニット
520
インターフェース
リムーバブル記憶ユニット
522
524
通信インターフェース
リモート装置、ネットワーク、エンティティ
528
526
通信経路

【図４】


900
902
処理装置
命令 926
904
メイン・メモリ
命令 926
930
バス
922
グラフィックス処理ユニット
928
ビデオ処理ユニット
932
オーディオ処理ユニット
908
ネットワーク・インターフェース装置
920
ネットワーク
906
静的メモリ
908
ビデオ・ディスプレイ・ユニット
912
英数字入力装置
914
カーソル制御装置
916
信号生成装置
918
データ記憶装置
924
機械可読媒体
命令 926

フロントページの続き

ライブ ９４０
(72)発明者 コマルゴドスキー イラン
アメリカ合衆国 カリフォルニア州 ９４０８５ サニーベール スチュワート ドライブ ９４０
(72)発明者 ウォーターズ ブレント
アメリカ合衆国 カリフォルニア州 ９４０８５ サニーベール スチュワート ドライブ ９４０

審査官 行田 悦資

(56)参考文献 特開２０１７－１２６８５１（ＪＰ，Ａ）
国際公開第２０１６／１６２９４１（WO，Ａ１）
米国特許出願公開第２０１０／０１８５８６１（ＵＳ，Ａ１）
CHASE, M.，Multi-authority Attribute Based Encryption，Lecture Notes in Computer Science，vol. 4392，Springer，2007年02月21日，pp.515-534，4th Theory of Cryptography Conference, TCC 2007,〈DOI:10.1007/978-3-540-70936-7_28〉

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０９Ｃ １／００