

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号

特表2023-521276

(P2023-521276A)

(43)公表日 令和5年5月24日(2023.5.24)

(51)国際特許分類	F I	テーマコード (参考)
H 0 4 L 9/08 (2006.01)	H 0 4 L 9/08 D	5 K 0 6 7
H 0 4 W 84/10 (2009.01)	H 0 4 W 84/10 1 1 0	
H 0 4 W 12/041 (2021.01)	H 0 4 W 12/041	
H 0 4 W 12/03 (2021.01)	H 0 4 W 12/03	
H 0 4 W 60/04 (2009.01)	H 0 4 W 60/04	
審査請求 未請求 予備審査請求 未請求 (全25頁) 最終頁に続く		

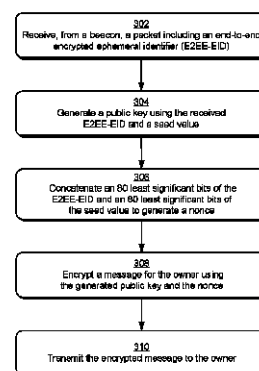
(21)出願番号	特願2022-547944(P2022-547944)	(71)出願人	502208397
(86)(22)出願日	令和3年4月5日(2021.4.5)		グーグル エルエルシー
(85)翻訳文提出日	令和4年10月13日(2022.10.13)		G o o g l e L L C
(86)国際出願番号	PCT/US2021/025743		アメリカ合衆国 カリフォルニア州 9 4
(87)国際公開番号	WO2021/211315		0 4 3 マウンテン ビュー アンフィシ
(87)国際公開日	令和3年10月21日(2021.10.21)		アター パークウェイ 1 6 0 0
(31)優先権主張番号	63/010,370		1 6 0 0 Amphitheatre P
(32)優先日	令和2年4月15日(2020.4.15)		arkway 9 4 0 4 3 Mounta
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	in View, CA U. S. A.
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA ,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,A T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR ,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く		110001195
		(72)発明者	弁理士法人深見特許事務所
			ユング, マーセル・エム・エム
			アメリカ合衆国、9 4 0 4 3 カリフォ
			ルニア州、マウンテン・ビュー、アンフ
			ィシアター・パークウェイ、1 6 0 0
			最終頁に続く

(54)【発明の名称】 エンドツーエンドの暗号化された位置検出

(57)【要約】

本文書には、サイティングしたデバイスからサイティングされたデバイスのオーナーに位置情報を転送する役割を果たす、信頼できない可能性があるクラウドサービスを通して転送される位置情報のエンドツーエンド暗号化を保証する方法、デバイス、システム、および手段が記載されている。位置情報のエンドツーエンド暗号化は、位置情報がサイターからオーナーまでネットワークノードを通過する際に、オーナーに関連付けられていないサイターデバイスによって提供される位置情報のプライバシーを守る。

300



10

Fig. 3

【特許請求の範囲】

【請求項 1】

サイターからオーナーにメッセージを安全に伝達する方法であって、前記方法は、前記サイターが、

エンドツーエンドの暗号化されたエフェメラル識別子（E 2 E E - E I D）を含むパケットをビーコンから受信することと、

受信した前記 E 2 E E - E I D とシード値とを用いて公開鍵を生成することと、

前記 E 2 E E - E I D の 8 0 個の最下位ビットと前記シード値の 8 0 個の最下位ビットとを連結してノンスを生成することと、

生成した前記公開鍵と前記ノンスとを用いて前記オーナーへのメッセージを暗号化することと、

暗号化した前記メッセージを前記オーナーに送信することとを備える、方法。

10

【請求項 2】

前記サイターが、前記オーナーへの前記メッセージを生成することをさらに備える、請求項 1 に記載の方法。

【請求項 3】

前記サイターが、前記サイターの位置を前記メッセージに含めることをさらに備え、前記位置は、前記サイターが前記ビーコンから前記パケットを受信したときの前記サイターの位置である、請求項 2 に記載の方法。

【請求項 4】

前記オーナーへのメッセージを暗号化することは、前記サイターが、A E S - E A X - 2 5 6 暗号化を用いて前記メッセージを暗号化することを備える、先行する請求項のいずれか 1 項に記載の方法。

20

【請求項 5】

受信した前記 E 2 E E - E I D とシード値とを用いて公開鍵を生成することは、前記サイターが、前記公開鍵を表す曲線上の点 R を算出することを備える、先行する請求項のいずれか 1 項に記載の方法。

【請求項 6】

前記パケットは B l u e t o o t h アドバタイズメントパケットであり、前記 B l u e t o o t h アドバタイズメントパケットは B l u e t o o t h アドバタイズチャンネルで受信される、先行する請求項のいずれか 1 項に記載の方法。

30

【請求項 7】

オーナーにメッセージを安全に伝達するためにビーコンがエフェメラル識別子を生成する方法であって、前記方法は、前記ビーコンが、

前記ビーコンと前記オーナーとの間で共有されるアイデンティティ鍵を決定することと、

前記アイデンティティ鍵と時間値とを用いて、エンドツーエンドの暗号化されたエフェメラル識別子（E 2 E E - E I D）を生成することと、

前記 E 2 E E - E I D を含むビーコンパケットを生成することと、

前記ビーコンパケットを送信することとを備え、前記ビーコンパケットは、前記オーナーに安全なメッセージを送信するためにサイターによって使用可能である、方法。

40

【請求項 8】

電子デバイスであって、

無線トランシーバと、

プロセッサと、

方法 1 から方法 7 のいずれか 1 つを実行するように前記電子デバイスを構成するように前記プロセッサによって実行可能な命令とを備える、電子デバイス。

【請求項 9】

前記電子デバイスはビーコンであり、前記ビーコンは、固定装着されたビーコン、可動物体に貼付可能なアセットタグ、人間が持ち運ぶ個人タグ、無線イヤホン、スマートウォ

50

ッチ、カメラ、携帯電話、またはモバイルコンピューティングデバイス、のうちの1つである、請求項8に記載の電子デバイス。

【請求項10】

前記電子デバイスはサイターであり、前記サイターは、スマートフォン、無線ローカルエリアネットワーク(WLAN)アクセスポイント、ホームオートメーションハブ、セキュリティハブ、HVACハブ、エネルギー管理ハブ、スマートスピーカ、サーモスタット、危険検知器、ネットワーク接続されたカメラ、照明ユニット、照明コントローラ、玄関インターフェイスデバイス、占有センサ、ホームオートメーション境界ルータ、手持ち式タグスキャナ、または固定装着されたタグスキャナ、のうちの1つである、請求項8に記載の電子デバイス。

10

【請求項11】

サイターからのメッセージをオーナーが安全に受信する方法であって、前記方法は、前記オーナーが、

リゾルバから前記メッセージを取出すことを備え、前記メッセージは、エンドツーエンドの暗号化されたエフェメラル識別子(E2E-EID)を含み、前記オーナーがさらに、

受信した前記E2E-EIDとシード値とを用いて公開鍵を生成することと、

前記E2E-EIDの80個の最下位ビットと前記シード値の80個の最下位ビットとを連結してノンスを生成することと、

生成した前記公開鍵と前記ノンスとを用いて、受信した前記メッセージを復号化することとを備える、方法。

20

【請求項12】

前記メッセージは前記サイターの位置を含み、前記位置は、前記E2E-EIDを生成したビーコンから前記サイターがパケットを受信したときの前記サイターの位置である、請求項11に記載の方法。

【請求項13】

受信した前記メッセージを復号化することは、前記オーナーが、AES-EAX-256復号化を用いて前記メッセージを復号化することを備える、請求項11または請求項12に記載の方法。

【請求項14】

電子デバイスであって、

プロセッサと、

方法11から方法13のいずれか1つを実行するように前記電子デバイスを構成するように前記プロセッサによって実行可能な命令とを備える、電子デバイス。

【請求項15】

プロセッサによる実行に応答して、請求項1から請求項7および請求項11から請求項13のいずれか1項に記載の方法を実行させる命令を備える、コンピュータ読取可能記憶媒体。

【発明の詳細な説明】

【背景技術】

40

【0001】

背景

エフェメラル識別子を用いるビーコンシステムは、どのクライアントがビーコンシステムのビーコン信号を利用できるかを開発者が制御できるように設計されている。ビーコンとビーコンのオーナーとの間で共有されるエフェメラル識別子および鍵により、サイター(sighter)がエフェメラル識別子をリゾルバサービスに送信すると、リゾルバサービスがビーコンのオーナーを決定することができる。ビーコンのサイターとリゾルバとの間の通信、およびリゾルバとオーナーとの間の通信は保護されているが、ビーコンおよび／またはサイターとオーナーとの間の通信はいずれも安全ではなく、リゾルバが見ることができる。

50

【発明の概要】

【0002】

概要

この概要は、エンドツーエンドの暗号化された位置検出の簡略化された概念を紹介するために提供されている。この簡略化された概念については、詳細な説明にさらに後述する。この概要は、クレームされている主題の不可欠な特徴を特定するよう意図されているわけではなく、クレームされている主題の範囲の決定に用いることを意図されているわけでもない。

【0003】

局面において、無線ネットワークにおけるエンドツーエンドの暗号化された位置検出のための方法、デバイス、システム、および手段が記載されており、サイターは、エンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）を含むパケットをビーコンから受信する。サイターは、受信したE2EE-EIDとシード値とを用いて公開鍵を生成する。サイターは、E2EE-EIDの80個の最下位ビットとシード値の80個の最下位ビットとを連結してノンスを生成する。サイターは、生成した公開鍵とノンスとを用いてオーナーへのメッセージを暗号化し、サイターは、暗号化したメッセージをオーナーに送信する。

【0004】

局面において、無線ネットワークにおけるエンドツーエンドの暗号化された位置検出のための方法、デバイス、システム、および手段が記載されており、ビーコンは、ビーコンとオーナーとの間で共有されるアイデンティティ鍵を決定する。ビーコンは、アイデンティティ鍵と時間値とを用いて、エンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）を生成する。ビーコンは、E2EE-EIDを含むビーコンパケットを生成してビーコンパケットを送信し、送信されるビーコンパケットは、オーナーに安全なメッセージを送信するために、ビーコンパケットを受信するサイターによって使用可能である。

【0005】

局面において、無線ネットワークにおけるエンドツーエンドの暗号化された位置検出のための方法、デバイス、システム、および手段が記載されており、オーナーは、リゾルバからメッセージを取出し、メッセージは、エンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）を含む。オーナーは、受信したE2EE-EIDとシード値とを用いて公開鍵を生成する。オーナーは、E2EE-EIDの80個の最下位ビットとシード値の80個の最下位ビットとを連結してノンスを生成し、オーナーは、生成した公開鍵とノンスとを用いて、受信したメッセージを復号化する。

【0006】

記載されているエンドツーエンドの暗号化された位置検出のためのシステムおよび方法の特徴および概念は、いくつものさまざまな環境、システム、デバイス、および／またはさまざまな構成で実現することができるが、以下の例示的なデバイス、システム、および構成の文脈の中でエンドツーエンドの暗号化された位置検出の実施形態について説明する。

【0007】

エンドツーエンドの暗号化された位置検出の実施形態について、以下の図面を参照して説明する。図面全体を通して、同一の番号を使用して同様の特征および構成要素を参照する。

【図面の簡単な説明】

【0008】

【図1】エンドツーエンドの暗号化された位置検出のさまざまな実施形態を実現することができる環境の一例を示す図である。

【図2】エンドツーエンドの暗号化された位置検出の局面に従う、デバイス間のデータおよび制御トランザクションの一例を示す図である。

10

20

30

40

50

【図 3】本明細書に記載されている技術の実施形態に従う、エンドツーエンドの暗号化された位置検出の方法の一例を示す図である。

【図 4】本明細書に記載されている技術の実施形態に従う、エンドツーエンドの暗号化された位置検出の方法の一例を示す図である。

【図 5】本明細書に記載されている技術の実施形態に従う、エンドツーエンドの暗号化された位置検出の方法の一例を示す図である。

【図 6】本明細書に記載されている技術の 1 つ以上の実施形態に従う、ネットワーク環境で実現することができるネットワークデバイスの一例を示す図である。

【図 7】本明細書に記載されている技術の 1 つ以上の実施形態に従う、ネットワーク環境で実現することができるビーコンデバイスの一例を示す図である。

10

【発明を実施するための形態】

【0009】

詳細な説明

本文書には、サイティング (sight) したデバイスからサイティングされたデバイスのオーナーに位置情報を転送する役割を果たす、信頼できない可能性があるクラウドサービスを通して転送される位置情報のエンドツーエンド暗号化を保証する方法、デバイス、システム、および手段が記載されている。位置情報のエンドツーエンド暗号化は、位置情報がサイターからオーナーまでのネットワークノードを通過する際に、オーナーに関連付けられていないサイターデバイスによって提供される位置情報のプライバシーを守る。

【0010】

20

多くの電子デバイスは、動作中に短距離無線信号をアドバタイズする、イヤホン、スマートウォッチ、スマートフォン、カメラ、追跡タグなどのデバイスである。アドバタイズされる無線信号は、適切な無線技術およびプロトコルを用いて、スマートフォン、ネットワーク接続されたスピーカ、ホームオートメーションハブ、セキュリティハブなどの受信機が、これらの電子デバイスを識別することを可能にする。受信機がその位置（たとえば地理的な位置）を認識している場合、受信機は、アドバタイズされた信号を電子デバイスから受信した位置を、電子デバイスのアイデンティティと共にアップロードすることができる。たとえば、受信機は、電子デバイスがサイティングされた位置をサービス（たとえばクラウドベースのサービス）にアップロードして、電子デバイスのオーナーが電子デバイスを置き忘れた場合に電子デバイスの位置を問い合わせることを可能にすることができる。

30

【0011】

しかしながら、報告された電子デバイスの位置情報およびデバイスのアイデンティティのプライバシーを、この情報を取得して悪用する可能性がある悪人から保護するために考慮する必要がある。電子デバイスに不変の識別子をアドバタイズメント送信でブロードキャストさせると、誰でも電子デバイスを追跡できるようになる可能性があり、その情報を用いて、電子デバイスを持ち運ぶ人物（電子デバイスを所有する人物など）または電子デバイスが取り付けられ得る物体を追跡できる可能性もある。

【0012】

E d d y s t o n e - E I D および F a s t P a i r などのプロトコルは、オーナー（オーナーのみ）が電子デバイスを識別できるように、所定のメカニズムに基づく回転識別子を含むメッセージを電子デバイスにアドバタイズさせることにより、電子デバイスのアイデンティティのプライバシーを保護する技術を導入している。しかしながら、これらのアプローチにさらなる保護を追加して、報告された電子デバイスの位置をオーナー以外には非公開にすることができる。

40

【0013】

たとえば、B l u e t o o t h（登録商標）L o w E n e r g y（B l u e t o o t h L E : B L E）ビーコンなどの低電力無線ビーコンは、ビーコンパケット（たとえば、アドバタイズチャネルのプロトコルデータユニット（P D U））で情報を送信する。ビーコンは、非暗号化データなどの直接識別可能なブロードキャスト情報を送信することも

50

あれば、エフェメラル識別子（エフェメラルID：EID）などの数分ごとに変わる識別子をブロードキャストすることもある。エフェメラル識別子は、個々のビーコンとアイデンティティ鍵（エフェメラルアイデンティティ鍵、すなわちEIK）を共有するオーナーによって、有用な情報に解明することができる。以下の記載では頻繁にBLEに言及しているが、BLEは簡単にするために記載されている無線技術の一例であり、本明細書に記載されているエフェメラル識別子は別の無線技術（たとえば、ウルトラワイドバンド（UWB）、無線ローカルエリアネットワーク（WLAN）、近距離無線通信（NFC）、パーソナルエリアネットワーク（PAN）、IEEE 802.15.4、ZigBee（登録商標）、Threadなど）にも同様に適用され得る。

【0014】

環境の例

図1は、エンドツーエンドの暗号化された位置検出のさまざまな実施形態を実現することができる環境の一例100を示す。環境100は、ビーコン110と、サイター120と、リゾルバ130と、オーナー140とを含む。ビーコン110は、102で示すように、ビーコンパケットを定期的にブロードキャスト（たとえば送信）する、BLEビーコン、ヘッドセットなどのデバイスである。サイター（またはオブザーバー）120は、104で示すように、ビーコンパケットを受信し、受信したパケットをリゾルバサービスに転送することができる、スマートフォンなどのデバイスである。たとえば、サイター120は、受信したパケットをインターネット150を介してリゾルバサービス130に転送する。この例では、インターネット150は、サイター120、リゾルバ130、および／またはオーナー140を相互に接続する有線および／または無線、ローカルおよび／またはワイドエリアネットワークの任意の組合せを表している。クラウドベースのリゾルバサービス（解明サービス）などのリゾルバ130は、106で示すように、受信したEIDを共有鍵および関連付けられたオーナーのハッシュ値と比較して正しいオーナーを決定し、受信したパケットを正しいオーナー140に転送する。これに代えてまたはこれに加えて、オーナー140は、オーナー140に関連付けられた任意のビーコン110について、サイター120から受信したパケットまたはメッセージをリゾルバ130に問い合わせることができる。オーナー140は、ビーコン110に関連付けられた、スマートフォン、コンピュータ、またはクラウドベースのサービスなどのデバイスまたはサービスである。オーナー140は1つ以上のビーコン110を所有し、それらのビーコン110の各々の共有鍵を格納してもよい。

【0015】

図1に示すような通信用に構成された任意の適切なデバイスとともに、エンドツーエンドの暗号化された位置検出を使用することができる。オーナー140は、任意のオーナーコンピューティングシステムであってもよい。ビーコン110は、オーナーコンピューティングシステムに関連付けられた任意のデバイスであってもよい。デバイスからオーナーコンピューティングシステムへの通信は、（デバイスおよびオーナーコンピューティングシステムの両方のアイデンティティを隠すことによって）匿名化され、ルーティングシステム（たとえばリゾルバ130）を伴って匿名性を解明してオーナーコンピューティングシステムおよびデバイスを識別し、デバイスをオーナーコンピューティングシステムに接続する。サイター120は、匿名性にもかかわらず、デバイスからビーコンパケットを受信し、デバイスのサイティングに関するサイティング情報をそのオーナーコンピューティングシステムに送信する仲介デバイスである、任意のサイターシステムであってもよい。サイティング情報は、オーナーコンピューティングシステム以外のリゾルバ（およびその他のネットワークノード）から安全に保たれる。

【0016】

ビーコン110は、ビーコン110とオーナー140との間で共有される共有鍵（EIK）から生成されるエフェメラル識別子（EID）と、ビーコン110によってEIDが生成される時間とを含むビーコンパケット（たとえば、BLEアドバタイズメントパケット）を定期的に送信（ブロードキャスト）するデバイスである。ビーコン110は、ビー

10

20

30

40

50

コン110およびそのオーナー140が知っている回転数で新しいEIDを計算する。ビーコン110は、限られた計算リソースおよび電力リソースを有してもよく、限られた範囲にわたってビーコンパケットをブロードキャストする。サイター120は、ビーコン110からビーコンパケットを受信することができ、より長距離のネットワーク（たとえばワイドエリアネットワーク：WAN）にアクセスできる。サイター120は、より長距離のネットワークを介して、リゾルバ130などのクラウドベースのサービスに接続することができる。これは、サイター120が、受信したビーコンパケットをクラウドベースのリゾルバ130に転送することを可能にする。リゾルバ130は、デバイス（サーバ）、またはクラウドベースのサービスを形成するデバイスの集合体であってもよい。リゾルバ130は、オーナー140のセットと、それらのオーナーについて関連付けられたEIDとを格納している。リゾルバ130は、ビーコンパケットから受信したEIDをその格納しているEIDのセットと比較して、受信したビーコンパケットについて関連付けられたオーナー140を決定する。受信したビーコンパケットについてのオーナー140が識別されると、リゾルバ130は、ビーコンパケットをそのパケットの正しいオーナー140に転送することができる。

10

20

30

40

50

【0017】

ビーコン110の初期化時に、ビーコン110およびオーナー140は、108で示すように、楕円曲線ディフィー・ヘルマン鍵合意プロトコルを用いて、ビーコン110とオーナー140との間で共有される鍵（EIK）を交換する。共有されるEIKは、リゾルバ130が、時間に基づいてEIDからビーコン110のアイデンティティを解明し、ビーコン110および／またはサイター120からのメッセージをオーナー140に送ることを可能にする。サイター120とリゾルバ130との間の通信、およびリゾルバ130とオーナー140との間の通信は、トランスポートレイヤーセキュリティ（TLS）を用いて保護されている。しかしながら、ビーコン110および／またはサイター120とオーナー140との間の通信はいずれも、リゾルバ130が見ることができる。サイター120からオーナー140への安全な（暗号化された）エンドツーエンド通信チャネルを追加することにより、サイター120とオーナー140との間のメッセージの暗号化ペイロードにアクセスできないルーティング要素としてリゾルバ130を用いて、ビーコン110および／またはサイター120からオーナー140へのメッセージに機密性が提供される。

【0018】

エンドツーエンドの暗号化された位置検出

局面において、ビーコン110をオーナー140とペアリングすると、ビーコン110およびオーナー140は（たとえばスマートフォン上のアプリケーションを用いることによって）共通の状態を開始し、上述のように共有される256ビットの対称アイデンティティ鍵（EIK）に同意する。また、ビーコン110およびオーナー140は、ビーコン110が送信するブロードキャストパケットに含まれるエンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）の値を回転させるための周波数（たとえば回転周期）を決定する。ビーコン110は内部クロックを含む。たとえば、ビーコン110は、1秒間隔で増加する内部クロックを維持することができる。これらのパラメータ（回転周期、アイデンティティ鍵、およびクロックからの現在の時間）から、ビーコン110およびオーナー140（またはこれら3つのパラメータを所有する任意のデバイス）は疑似乱数生成器を規定することができ、その出力はこれらのパラメータを所有している者であれば誰でも予測可能である。

【0019】

エンドツーエンドの暗号化された位置検出プロトコルは、この疑似乱数生成器メカニズムを用いる。256ビットの高度暗号化標準（AES）電子コードブック（ECB）（AES-ECB-256）を用いて乱数を生成して、表1に示すデータ構造を暗号化する。

【0020】

【表 1】

バイトオフセット	フィールド	記述
0 ～ 1 0	パディング	値 = 0 x F F
1 1	K	回転周期指数
1 2 ～ 1 5	T S [0] … T S [3]	3 2 ビットのビッグエンディアン形式のビーコンタイムカウンタ。K 個の最下位ビットをクリアする。
1 6 ～ 2 6	パディング	値 = 0 x 0 0
2 7	K	回転周期指数
2 8 ～ 3 1	T S [0] … T S [3]	3 2 ビットのビッグエンディアン形式のビーコンタイムカウンタ。K 個の最下位ビットをクリアする。

10

20

【 0 0 2 1 】

データ構造の AES-ECB-256 の結果は、 r で表される 256 ビットの数である。以下の計算では、SECP160R1 (SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 20, 2000 で定義) の楕円曲線ドメインパラメータ (F_p 、 n 、および G) を本明細書中の楕円曲線暗号 (ECC) 演算に使用している。

【 0 0 2 2 】

【数 1】

r' は、

$$r = r' \bmod n \quad (1)$$

30

を計算することによって有限体 F_p に射影される。

【 0 0 2 3 】

【数 2】

R は、

$$R = r * G \quad (2)$$

によって計算され、使用されている公開鍵を表す曲線上の点である。ビーコンは、 R の x 座標である R_x を、その E2EE エフェメラル識別子としてアドバタイズする。なお、 R_x は、標準的な BLE アドバタイズメントチャンネル PDU に収まるように 20 バイトの長さである。

40

【 0 0 2 4 】

E2EE-EID フレームは、Eddystone サービスの汎用一意識別子 (UUID) に関連付けられたサービスデータブロックとして、アドバタイズメントチャンネル PDU で符号化される。E2EE-EID フレームのレイアウトを表 2 に示す。

【 0 0 2 5 】

50

【表 2】

バイトオフセット	フィールド	記述
0	フレームタイプ	値 = 0 x 4 0
1	E 2 E E – E I D [0]	暗号鍵の導出に使用可能な 2 0 バイトのエフェメラル識別子。
2	E 2 E E – E I D [1]	
...	...	
2 0	E 2 E E – E I D [1 9]	

10

【 0 0 2 6 】

エンドツーエンドの暗号化された位置検出の暗号化

メッセージ m （たとえばこのメッセージは、サイター 1 2 0 がビーコン 1 1 0 からアドレスメントメントを受信した、報告された位置である）を暗号化するために、ビーコン 1 1 0 から R_x を受信したサイター 1 2 0 は、上述のように F_p で乱数 s を生成する。

20

【 0 0 2 7 】

【数 3】

サイター 1 2 0 は、乱数および ECC 基点 G からシード S を算出する。

$$S = s * G \quad (3)$$

【 0 0 2 8 】

【数 4】

サイター 1 2 0 は、曲線方程式への代入、および可能な結果の中から任意の R_y 値を選ぶことによって、受信した R_x から公開鍵を表す曲線上の点 R を算出する。

30

$$R = (R_x, R_y) \quad (4)$$

【 0 0 2 9 】

【数 5】

サイター 1 2 0 は、公開鍵 k を算出する。

$$k = HKDFSAH256((s * R)_x) \quad (5)$$

式中、 $(s * R)_x$ は曲線乗算結果の x 座標である。

40

【 0 0 3 0 】

UR_x および LR_x は、それぞれ R_x の上位（最上位）および下位（最下位）80ビット（ビッグエンディアン形式）である。同様に、 US_x および LS_x は、それぞれ S の上位および下位80ビット（ビッグエンディアン形式）である。

【 0 0 3 1 】

【数 6】

サイター 1 2 0 は、以下のようにノンスを算出する。

$$\text{ノンス} = LR_x \parallel LS_x \quad (6)$$

50

【 0 0 3 2 】

【数 7】

サイター 1 2 0 は、以下のように $(m', \text{タグ})$ を算出する。

$$(m', \text{タグ}) = \text{AESEAX256ENC} (k, \text{ノンス}, m) \quad (7)$$

【 0 0 3 3 】

サイター 1 2 0 は、 UR_x 、 S_x 、 m' 、およびタグを含むメッセージをオーナー 1 4 0 に送信する。このメッセージは、リゾルバ 1 3 0 のような信頼できないノードを介して転送されてもよい。

【 0 0 3 4 】

エンドツーエンドの暗号化された位置検出の復号化

アイデンティティ鍵および回転周期指数を所有しているオーナーデバイス 1 4 0 は、サイター 1 2 0 からメッセージを受信してメッセージを復号化する。 UR_x を受信したオーナー 1 4 0 は、 UR_x の基となるビーコンタイムカウンタ値を取得し、上記に定義したように r の予想値を算出する。

【 0 0 3 5 】

【数 8】

オーナー 1 4 0 は、

$$R = r * G \quad (8)$$

を算出し、サイター 1 2 0 から受信したメッセージに提供されている UR_x の値との一致を検証する。

【 0 0 3 6 】

【数 9】

オーナー 1 4 0 は、曲線方程式への代入、および可能な結果の中から任意の S_y 値を選ぶことによって、シード S を算出する。

$$S = (S_x, S_y) \quad (9)$$

【 0 0 3 7 】

【数 1 0】

オーナー 1 4 0 は、公開鍵 k を算出する。

$$k = \text{HKDFSHA256}((r * S)_x) \quad (10)$$

式中、 $(r * S)_x$ は曲線乗算結果の x 座標である。

【 0 0 3 8 】

【数 1 1】

オーナー 1 4 0 は、ノンスを算出する。

$$\text{ノンス} = LR_x \parallel LS_x \quad (11)$$

【 0 0 3 9 】

【数 1 2】

オーナー 1 4 0 は、メッセージ m の復号値を算出する。

$$m = \text{AESEAX256DEC} (k, \text{ノンス}, m', \text{タグ}) \quad (12)$$

10

20

30

40

50

【0040】

位置検出システム

ユーザは、エンドツーエンドの暗号化された位置検出をサポートするビーコンデバイス（たとえば、スタンドアロンのビーコンデバイス、ビーコンを含むデバイス、他の Bluetooth プロファイルをサポートすることに加えてビーコン送信をサポートする Bluetooth デバイスなど）を入手すると、エンドツーエンドの暗号化された位置検出を構成するようにビーコンデバイスをプロビジョニングする。たとえば、ユーザは、上述のようにアイデンティティ鍵および回転周期を設定することによって、ユーザ機器（たとえばスマートフォンまたはコンピューティングデバイス）上のアプリケーションを用いてプロビジョニングを開始する。アイデンティティ鍵はビーコンデバイス（ビーコン110）とユーザデバイス（オーナー140）との間で共有されるが、サイター120およびリゾルバ130などのシステム内の他のデバイスからは秘密にされる。リゾルバ130（たとえばクラウドベースのリゾルバサービス）はアイデンティティ鍵を知らないが、リゾルバ130にはビーコン110および関連付けられたオーナー140の存在を認識させる。たとえば、プロビジョニングアプリケーションは、ビーコン110およびオーナー140の関連付けられたアイデンティティをリゾルバ130に提供し、リゾルバ130は次にそれらのアイデンティティを、サイター120から受信したメッセージのオーナー140のアイデンティティを解明するために後で使用するために、任意の適切な方法で格納する。ビーコン110は、アイデンティティ鍵を格納し、クロック時間を維持し、E2EE-IDを生成し、E2EE-IDを含むビーコンパケットを送信することができる、任意のデバイスである。たとえば、ビーコン110は、固定装着されたビーコン、可動物体に貼付可能なアセットタグ、人間が持ち運ぶ個人タグ、無線イヤホン、スマートウォッチ、カメラ、携帯電話、モバイルコンピューティングデバイスなどであってもよい。

10

20

【0041】

オーナーデバイス140は、上述のように、ある期間（たとえば次の24時間）について予想されるエフェメラル識別子を定期的に（たとえば毎日）事前に計算する。次に、オーナーデバイス140は、事前に計算したエフェメラル識別子を切り捨てる。たとえば、オーナーデバイス140は、公開鍵の長さの半分に等しい最下位ビット数を維持するなど、事前に計算したエフェメラル識別子を任意の適切な長さに切り捨てる。別の例では、オーナーデバイス140は、事前に計算したエフェメラル識別子の80個の最下位ビットを維持するように、事前に計算したエフェメラル識別子を切り捨てる。次に、オーナーデバイス140は、事前に計算して切り捨てたエフェメラル識別子をリゾルバ130にアップロードする。リゾルバ130は、事前に計算して切り捨てたエフェメラル識別子を、1以上のサイター120から受信したメッセージの所有権を解明する際に後で使用するために、ビーコン110およびオーナー140の過去に格納された、関連付けられたアイデンティティに関連付ける。

30

【0042】

サイター120は、ビーコンパケットを受信して解読してビーコン110の識別子を回復し、（上述のように）メッセージを生成して暗号化し、リゾルバ130にメッセージを伝達することができる、任意のデバイスである。たとえば、サイターデバイス120は、スマートフォン、無線ローカルエリアネットワーク（WLAN）アクセスポイント、ホームオートメーションハブ、セキュリティハブ、HVACハブ、エネルギー管理ハブ、スマートスピーカ、サーモスタット、（たとえば煙および／もしくは一酸化炭素用の）危険検知器、ネットワーク接続されたカメラ、照明ユニット、照明コントローラ、玄関インターフェイスデバイス、占有センサ、ホームオートメーション境界ルータ、手持ち式（たとえばモバイル）タグスキャナ、固定装着されたタグスキャナ、または、冷蔵庫、コンロおよびオーブン、洗濯機、乾燥機、空調装置、プールヒータ、灌漑システム、セキュリティシステムといった、接続器具および／もしくは制御システムなどのその他のタイプの無線ネットワークデバイス、ならびに、テレビ、エンターテイメントシステム、コンピュータ、インターホンシステム、車庫ドア開閉装置、天井ファン、コントロールパネルといった、

40

50

他の電子およびコンピューティングデバイスを含む。

【0043】

リゾルバ130は、サイター120が送信したメッセージペイロードの一部として含まれている部分識別子UR_xを用いて、メッセージに報告されているサイティングが特定のビーコン110のサイティングであることを判断する。リゾルバ130は、報告されたサイティングをこの特定のビーコン110に関連付け、受信メッセージと、この特定のビーコン110へのメッセージの関連付けとを格納する。リゾルバ130は、受信メッセージに関連付けられたビーコン110を解明することはできるが、メッセージ内容を復号化してビーコンサイティングの位置を特定することはできない。リゾルバ130は、任意のデバイス（たとえばコンピュータサーバ）、またはクラウドベースのサービスを形成するデバイスの集合体であってもよい。

10

【0044】

リゾルバ130はアイデンティティ鍵に関する知識がないので、将来のEIDを予測することができず、オーナー140からの事前に計算して切り捨てたエフェメラル識別子の定期的な更新がなければ、リゾルバ130はビーコン110を追跡することができない。リゾルバ130は、公開鍵全体を利用できないので、偽の位置を偽装することができず、また、リゾルバ130は、アイデンティティ鍵にアクセスできないので、中間者攻撃に利用されることがない。

【0045】

次に、ビーコンデバイス110のオーナー140は、ビーコン110の最後の既知の位置についてリゾルバ130に問い合わせることができる。次に、リゾルバ130は、暗号化された位置をオーナー140に転送する。これに代えてまたはこれに加えて、リゾルバ130は、メッセージを受信すると、または定期的にバッチで、オーナー140にメッセージを転送することができる。メッセージ内のタイムスタンプが与えられると、オーナー140は、上述のように、その時のビーコン110の予想される秘密鍵を推論して復号化アルゴリズムを実行することができる。

20

【0046】

図2は、エンドツーエンドの暗号化された位置検出の局面に従う、デバイス間のデータおよび制御トランザクションを示す。図示を明確にするために示していないが、エンドツーエンドの暗号化された位置検出の信頼性の高い動作を保証するために、図2に示すメッセージに対するさまざまな確認応答が実行されてもよい。

30

【0047】

205において、上述のように、ビーコン110のプロビジョニング中にビーコン110をオーナー140とペアリングする。ペアリングは、エンドツーエンドの暗号化された位置検出のための鍵を共有することを含む。210において、ビーコンは現在の時間に基づいてE2EE-EIDを生成する。

【0048】

215において、ビーコン110はビーコンパケットを生成する。ビーコン110はE2EE-EIDをビーコンパケットに含める。なお、E2EE-EIDの所定の回転数に基づいて、ビーコン110は、連続する回転サイクルごとに210および215の動作を繰返す（図2には図示せず）。220において、ビーコン110はビーコンパケットを送信する。ビーコン110は、回転サイクルごとにビーコンパケットを1回または複数回送信してもよい。

40

【0049】

225において、サイター120は、ビーコン110からビーコンパケットを受信した後、オーナー140に送信するメッセージを生成する。任意で、サイター120は、ビーコンパケットを受信したときのサイターの位置などの追加データをメッセージに含めてもよい。230において、サイターはリゾルバ130にメッセージを送信する。

【0050】

235において、リゾルバ130は、時間に基づいてE2EE-EIDからビーコン1

50

10のアイデンティティを解明し、アイデンティティをオーナー140のセットおよびそれらのオーナーについて関連付けられたE2EE-EIDと比較する。リゾルバが受信メッセージのオーナー140を識別した場合、リゾルバは240においてオーナー140にメッセージを転送する。245において、オーナーは受信メッセージを復号化する。

【0051】

方法の例

エンドツーエンドの暗号化された位置検出の1つ以上の実施形態に従う方法の例300～500について、それぞれ図3～図5を参照して説明する。方法ブロックが記載されている順序は、限定として解釈されることを意図しておらず、記載されている方法ブロックをいくらかでも省略してまたは任意の順序で組合せて方法または代替方法を実現することができる。一般に、本明細書に記載されている構成要素、モジュール、方法、および動作はいずれも、ソフトウェア、ファームウェア、ハードウェア（たとえば固定論理回路）、手動処理、またはそれらの任意の組合せを用いて実現可能である。これらの方法の例のいくつかの動作は、コンピュータ処理システムにローカルおよび／またはリモートであるコンピュータ読取可能記憶メモリ（媒体）に格納された実行可能な命令の一般的文脈の中で説明されてもよく、実現例は、ソフトウェアアプリケーション、プログラム、機能などを含み得る。これに代えてまたはこれに加えて、本明細書に記載されている機能はいずれも、少なくとも一部が、1つ以上のハードウェアロジックコンポーネントによって実行可能であり、1つ以上のハードウェアロジックコンポーネントは、フィールドプログラマブルゲートアレイ（FPGA）、特定用途向け集積回路（ASIC）、特定用途向け標準品（ASSP）、システムオンチップシステム（SOC）、複合プログラマブルロジックデバイス（CPLD）などであるが、これらに限定されるものではない。

【0052】

図3は、サイターからオーナーにメッセージを安全に伝達することに一般に関連する、エンドツーエンドの暗号化された位置検出の方法の例300を示す。ブロック302において、サイター（たとえばサイター120）は、エンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）を含むパケットをビーコン（たとえばビーコン110）から受信する。

【0053】

ブロック304において、サイターは、受信したE2EE-EIDとシード値とを用いて公開鍵（たとえば公開鍵k）を生成する。ブロック306において、サイターは、E2EE-EIDの80個の最下位ビットとシード値の80個の最下位ビットとを連結してノンスを生成する。

【0054】

ブロック308において、サイターは、生成した公開鍵とノンスとを用いてオーナーへのメッセージを暗号化する。ブロック310において、サイターは暗号化したメッセージをオーナーに送信する。たとえば、サイターはリゾルバ130を介してオーナー140にメッセージを転送する。

【0055】

図4は、オーナーにメッセージを安全に伝達するためにビーコンがエフェメラル識別子を生成することに一般に関連する、エンドツーエンドの暗号化された位置検出の方法の例400を示す。ブロック402において、ビーコン（たとえばビーコン110）は、ビーコンとオーナーとの間で共有されるアイデンティティ鍵を決定する。ブロック404において、ビーコンは、アイデンティティ鍵と時間値とを用いて、エンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）を生成する。

【0056】

ブロック406において、ビーコンは、E2EE-EIDを含むビーコンパケットを生成する。ブロック408において、ビーコンはビーコンパケットを送信し、ビーコンパケットは、オーナーに安全なメッセージを送信するためにサイター（たとえばサイター120）によって使用可能である。

10

20

30

40

50

【0057】

図5は、サイターからのメッセージをオーナーが安全に受信することに一般に関連する、エンドツーエンドの暗号化された位置検出の方法の例500を示す。ブロック502において、オーナー（たとえばオーナー140）は、リゾルバ（たとえばリゾルバ130）からメッセージを取出し、このメッセージは、エンドツーエンドの暗号化されたエフェメラル識別子（E2EE-EID）を含む。ブロック504において、オーナーは、受信したE2EE-EIDとシード値とを用いて公開鍵を生成する。

【0058】

ブロック506において、オーナーは、E2EE-EIDの80個の最下位ビットとシード値の80個の最下位ビットとを連結してノンスを生成する。ブロック508において、オーナーは、生成した公開鍵とノンスとを用いて受信メッセージを復号化する。

【0059】

デバイスの例

図6は、ビーコン110、サイター120、リゾルバ130、またはオーナー140など、本明細書に記載されているエンドツーエンドの暗号化された位置検出の1つ以上の実施形態に従うネットワーク内のネットワークデバイスのいずれか1つとして実現することができるネットワークデバイスの一例600を示す。ネットワークデバイス600は、電子回路、マイクロプロセッサ、メモリ、入出力（I/O）論理制御、通信インターフェイスおよびコンポーネント、ならびにネットワーク内のデバイスを実現する他のハードウェア、ファームウェアおよび／またはソフトウェアと統合することができる。

【0060】

この例では、ネットワークデバイス600は、実行可能な命令を処理する低電力マイクロプロセッサ602および／または高電力マイクロプロセッサ604（たとえばマイクロコントローラもしくはデジタル信号プロセッサ）を含む。また、このデバイスは、（たとえば電子回路を含むための）入出力（I/O）論理制御606を含む。マイクロプロセッサは、集積回路、プログラマブルロジックデバイス、1つ以上の半導体を用いて形成されたロジックデバイス、ならびにシステムオンチップ（SoC）として実現されたプロセッサおよびメモリシステムなどのシリコンおよび／またはハードウェアの他の実現例のコンポーネントを含み得る。これに代えてまたはこれに加えて、このデバイスは、ソフトウェア、ハードウェア、ファームウェア、または処理回路および制御回路で実現され得る固定論理回路のいずれか1つまたは組合せで実現することができる。また、低電力マイクロプロセッサ602および高電力マイクロプロセッサ604は、デバイスの1つ以上の異なるデバイス機能をサポートすることができる。たとえば、高電力マイクロプロセッサ604は計算集約的な動作を実行してもよく、低電力マイクロプロセッサ602は、1つ以上のセンサ608からの危険または温度を検出するなど、より単純な処理を管理してもよい。また、低電力プロセッサ602は、計算集約的な処理を行うために高電力プロセッサ604を起動または初期化してもよい。

【0061】

1つ以上のセンサ608は、加速度、温度、湿度、水分、供給電力、近接度、外部の動き、デバイスの動き、音声信号、超音波信号、光信号、火、煙、一酸化炭素、全地球測位衛星（GPS）信号、無線周波数（RF）、他の電磁信号または電磁場など、さまざまな特性を検出するように含まれて実現されてもよい。したがって、センサ608は、温度センサ、湿度センサ、危険関連センサ、他の環境センサ、加速度計、マイクロフォン、カメラを含むそれ以下の光センサ（たとえば電荷結合素子もしくはビデオカメラ）、能動または受動放射センサ、GPS受信機、および無線周波数識別検出器、のいずれか1つまたは組合せを含み得る。実現例において、ネットワークデバイス600は、1つ以上の一次センサと、1つ以上の二次センサとを含み得る。一次センサは、デバイスのコア動作（たとえば、サーモスタットにおける温度の検知、または煙検知器における煙の検知）の中心となるデータを検知し、二次センサは、エネルギー効率の目的またはスマート操作の目的で使用可能な他のタイプのデータ（たとえば、動き、光または音）を検知してもよい。

【0062】

ネットワークデバイス600は、メモリデバイスコントローラ610と、任意のタイプの不揮発性メモリおよび／または他の適切な電子データ記憶装置などのメモリデバイス612を含む。また、ネットワークデバイス600は、コンピュータ実行可能な命令としてメモリによって保持されてマイクロプロセッサによって実行されるオペレーティングシステム614など、さまざまなファームウェアおよび／またはソフトウェアを含み得る。また、このデバイスソフトウェアは、エンドツーエンドの暗号化された位置検出の実施形態を実現するメッセージングアプリケーション616を含み得る。また、ネットワークデバイス600は、別のデバイスまたは周辺コンポーネントとインターフェイスするためのデバイスインターフェイス618を含み、コンポーネント間のデータ通信を行うために無線ネットワークデバイスのさまざまなコンポーネントを結合する統合データバス620を含む。また、無線ネットワークデバイス内のデータバスは、異なるバス構造および／またはバスアーキテクチャのいずれか1つまたは組合せとして実現されてもよい。

10

【0063】

デバイスインターフェイス618は、（たとえばユーザインターフェイスとして）ユーザから入力を受信してもよく、および／またはユーザに情報を提供してもよく、受信した入力を用いて設定を決定することができる。また、デバイスインターフェイス618は、ユーザ入力に応答する機械コンポーネントまたは仮想コンポーネントを含み得る。たとえば、ユーザは摺動コンポーネントもしくは回転可能なコンポーネントを機械的に動かすことができ、またはタッチパッドに沿った動きが検出されてもよく、このような動きはデバイスの設定調整に対応してもよい。物理的および仮想的な可動ユーザインターフェイスコンポーネントは、ユーザが見かけの連続体の一部に沿って設定を入力することを可能にすることができる。また、デバイスインターフェイス618は、ボタン、キーパッド、スイッチ、マイクロフォン、撮像装置（たとえばカメラデバイス）など、任意の数の周辺機器から入力を受信してもよい。

20

【0064】

ネットワークデバイス600は、無線ネットワーク内の他の無線ネットワークデバイスと通信を行うための無線ネットワークインターフェイス、およびインターネットを介するなどしてネットワーク通信を行うための外部ネットワークインターフェイスなどの、ネットワークインターフェイス622を含み得る。また、ネットワークデバイス600は、無線ネットワークインターフェイスを介して他の無線ネットワークデバイスと無線通信を行うための、かつ複数の異なる無線通信システムのための、ワイヤレス無線システム624を含む。ワイヤレス無線システム624は、Wi-Fi（登録商標）、Bluetooth（登録商標）、BLE、モバイルブロードバンド、および／またはポイントツーポイントIEEE802.15.4を含み得る。異なる無線システムの各々は、特定の無線通信技術のために実現された無線デバイス、アンテナ、およびチップセットを含み得る。また、ネットワークデバイス600は、バッテリーなどの電源626、および／またはデバイスをライン電圧に接続するための電源626を含む。AC電源を用いてデバイスのバッテリーを充電してもよい。

30

【0065】

図7は、本明細書に記載されているエンドツーエンドの暗号化された位置検出の1つ以上の実施形態に従う、ネットワーク内のビーコンデバイス110として実現することができるビーコンデバイスの一例700を示す。ビーコンデバイス700は、電子回路、マイクロプロセッサ、メモリ、入出力（I/O）論理制御、通信インターフェイスおよびコンポーネント、ならびにネットワーク内のデバイスを実現する他のハードウェア、ファームウェアおよび／またはソフトウェアと統合することができる。

40

【0066】

この例では、ビーコンデバイス700は、実行可能な命令を処理する1つ以上のプロセッサ702（たとえばマイクロコントローラまたはデジタル信号プロセッサ）を含む。また、このデバイスは、（たとえば電子回路を含むための）入出力（I/O）論理制御70

50

4を含む。プロセッサは、集積回路、プログラマブルロジックデバイス、1つ以上の半導体を用いて形成されたロジックデバイス、ならびにシステムオンチップ（SoC）として実現されたプロセッサおよびメモリシステムなどのシリコンおよび／またはハードウェアの他の実現例のコンポーネントを含み得る。これに代えてまたはこれに加えて、このデバイスは、ソフトウェア、ハードウェア、ファームウェア、または処理回路および制御回路で実現され得る固定論理回路のいずれか1つまたは組合せで実現することができる。

【0067】

任意に、またはこれに加えて、1つ以上のセンサ706は、加速度、温度、湿度、水分、供給電力、近接度、外部の動き、デバイスの動き、音声信号、超音波信号、光信号、火、煙、一酸化炭素、全地球測位衛星（GPS）信号、無線周波数（RF）、他の電磁信号または電磁場など、さまざまな特性を検出するように含まれて実現されてもよい。したがって、センサ706は、温度センサ、湿度センサ、危険関連センサ、他の環境センサ、加速度計、マイクロフォン、カメラを含むそれ以下の光センサ（たとえば電荷結合素子もしくはビデオカメラ）、能動または受動放射センサ、GPS受信機、および無線周波数識別検出器、のいずれか1つまたは組合せを含み得る。実現例において、ビーコンデバイス700は、1つ以上の一次センサと、1つ以上の二次センサとを含み得る。一次センサは、デバイスのコア動作（たとえば、サーモスタットにおける温度の検知、または煙検知器における煙の検知）の中心となるデータを検知し、二次センサは、エネルギー効率の目的またはスマート操作の目的で使用可能な他のタイプのデータ（たとえば、動き、光または音）を検知してもよい。

【0068】

ビーコンデバイス700は、任意のタイプの不揮発性メモリおよび／または他の適切な電子データ記憶装置などのメモリ708を含む。また、ビーコンデバイス700は、コンピュータ実行可能な命令としてメモリによって保持されてプロセッサによって実行されるオペレーティングシステム710など、さまざまなファームウェアおよび／またはソフトウェアを含み得る。また、このデバイスソフトウェアは、エンドツーエンドの暗号化された位置検出プロトコルの実施形態を実現するビーコンアプリケーション712を含み得る。任意に、またはこれに加えて、ビーコンデバイス700は、別のデバイスまたは周辺コンポーネントとインターフェイスするためのデバイスインターフェイス714を含む。ビーコンデバイス700は、コンポーネント間のデータ通信を行うためにビーコンデバイスのさまざまなコンポーネントを結合する統合データバス716を含む。また、ビーコンデバイス内のデータバスは、異なるバス構造および／またはバスアーキテクチャのいずれか1つまたは組合せとして実現されてもよい。

【0069】

デバイスインターフェイス714は、（たとえばユーザインターフェイスとして）ユーザから入力を受信してもよく、および／またはユーザに情報を提供してもよく、受信した入力を用いて設定を決定することができる。また、デバイスインターフェイス714は、ユーザ入力に応答する機械コンポーネントまたは仮想コンポーネントを含み得る。たとえば、ユーザは摺動コンポーネントもしくは回転可能なコンポーネントを機械的に動かすことができ、またはタッチパッドに沿った動きが検出されてもよく、このような動きはデバイスの設定調整に対応してもよい。物理的および仮想的な可動ユーザインターフェイスコンポーネントは、ユーザが見かけの連続体の一部に沿って設定を入力することを可能にすることができる。また、デバイスインターフェイス714は、ボタン、キーパッド、スイッチ、マイクロフォン、撮像装置（たとえばカメラデバイス）など、任意の数の周辺機器から入力を受信してもよい。

【0070】

ビーコンデバイス700は、無線通信を行うためのワイヤレス無線システム718を含み得る。ワイヤレス無線システム718は、Wi-Fi、Bluetooth（登録商標）、BLE、モバイルブロードバンド、および／またはポイントツーポイントIEEE 802.15.4を含み得る。ワイヤレス無線システム718は、特定の無線通信技術のた

10

20

30

40

50

めの実現された無線デバイス、アンテナ、およびチップセットを含み得る。また、ビーコンデバイス 700 は、バッテリーなどの電源 720、および／またはデバイスをライン電圧に接続するための電源 720 を含む。AC 電源を用いてデバイスのバッテリーを充電してもよい。

【0071】

以下にいくつかの例を記載する。

例 1：

サイターからオーナーにメッセージを安全に伝達する方法であって、上記方法は、上記サイターが、

エンドツーエンドの暗号化されたエフェメラル識別子 (E2EE-ID) を含むパケットをビーコンから受信することと、 10

受信した上記 E2EE-ID とシード値とを用いて公開鍵を生成することと、

上記 E2EE-ID の 80 個の最下位ビットと上記シード値の 80 個の最下位ビットとを連結してノンスを生成することと、

生成した上記公開鍵と上記ノンスとを用いて上記オーナーへのメッセージを暗号化することと、

暗号化した上記メッセージを上記オーナーに送信することを含む、方法。

【0072】

例 2：

上記サイターが、上記オーナーへの上記メッセージを生成することをさらに含む、例 1 に記載の方法。 20

【0073】

例 3：

上記サイターが、上記サイターの位置を上記メッセージに含めることをさらに含み、上記位置は、上記サイターが上記ビーコンから上記パケットを受信した時の上記サイターの位置である、例 2 に記載の方法。

【0074】

例 4：

上記オーナーへのメッセージを暗号化することは、上記サイターが、AES-256 暗号化を用いて上記メッセージを暗号化することを含む、先行する例のいずれか 1 つに記載の方法。 30

【0075】

例 5：

受信した上記 E2EE-ID とシード値とを用いて公開鍵を生成することは、上記サイターが、上記公開鍵を表す曲線上の点 R を算出することを含む、先行する例のいずれか 1 つに記載の方法。

【0076】

例 6：

上記パケットは Bluetooth アドバタイズメントパケットであり、上記 Bluetooth アドバタイズメントパケットは Bluetooth アドバタイズチャンネルで受信される、先行する例のいずれか 1 つに記載の方法。 40

【0077】

例 7：

オーナーにメッセージを安全に伝達するためにビーコンがエフェメラル識別子を生成する方法であって、上記方法は、上記ビーコンが、

上記ビーコンと上記オーナーとの間で共有されるアイデンティティ鍵を決定することと、

上記アイデンティティ鍵と時間値とを用いて、エンドツーエンドの暗号化されたエフェメラル識別子 (E2EE-ID) を生成することと、

上記 E2EE-ID を含むビーコンパケットを生成することと、 50

上記ビーコンパケットを送信することを含み、上記ビーコンパケットは、上記オーナーに安全なメッセージを送信するためにサイターによって使用可能である、方法。

【0078】

例8：

電子デバイスであって、
無線トランシーバと、
プロセッサと、

例1から例7の方法のいずれか1つを実行するように上記電子デバイスを構成するように上記プロセッサによって実行可能な命令とを含む、電子デバイス。

【0079】

例9：

上記電子デバイスはビーコンであり、上記ビーコンは、固定装着されたビーコン、可動物体に貼付可能なアセットタグ、人間が持ち運ぶ個人タグ、無線イヤホン、スマートウォッチ、カメラ、携帯電話、またはモバイルコンピューティングデバイス、のうちの1つである、例8に記載の電子デバイス。

【0080】

例10：

上記電子デバイスはサイターであり、上記サイターは、スマートフォン、無線ローカルエリアネットワーク(WLAN)アクセスポイント、ホームオートメーションハブ、セキュリティハブ、HVACハブ、エネルギー管理ハブ、スマートスピーカ、サーモスタット、危険検知器、ネットワーク接続されたカメラ、照明ユニット、照明コントローラ、玄関インターフェイスデバイス、占有センサ、ホームオートメーション境界ルータ、手持ち式タグスキャナ、または固定装着されたタグスキャナ、のうちの1つである、例8に記載の電子デバイス。

【0081】

例11：

サイターからのメッセージをオーナーが安全に受信する方法であって、上記方法は、上記オーナーが、

リゾルバから上記メッセージを取出すことを含み、上記メッセージは、エンドツーエンドの暗号化されたエフェメラル識別子(E2EE-ID)を含み、上記オーナーがさらに、

受信した上記E2EE-IDとシード値とを用いて公開鍵を生成することと、

上記E2EE-IDの80個の最下位ビットと上記シード値の80個の最下位ビットとを連結してノンスを生成することと、

生成した上記公開鍵と上記ノンスとを用いて、受信した上記メッセージを復号化することを含む、方法。

【0082】

例12：

上記メッセージは上記サイターの位置を含み、上記位置は、上記E2EE-IDを生成したビーコンから上記サイターがパケットを受信した時の上記サイターの位置である、例11に記載の方法。

【0083】

例13：

受信した上記メッセージを復号化することは、上記オーナーが、AES-EAX-256復号化を用いて上記メッセージを復号化することを含む、例11または例12に記載の方法。

【0084】

例14：

電子デバイスであって、
プロセッサと、

10

20

30

40

50

例 1 1 から例 1 3 の方法のいずれか 1 つを実行するように上記電子デバイスを構成するように上記プロセッサによって実行可能な命令とを含む、電子デバイス。

【 0 0 8 5 】

例 1 5 : プロセッサによる実行に応答して、請求項 1 から請求項 7 および請求項 1 1 から請求項 1 3 のいずれか 1 項に記載の方法を実行させる命令を含む、コンピュータ読取可能記憶媒体。

【 0 0 8 6 】

エンドツーエンドの暗号化された位置検出の実施形態について、特徴および／または方法に特有の言い回しで説明してきたが、添付の特許請求の範囲の主題は、必ずしも記載されている特定の特征または方法に限定されるものではない。むしろ、これらの特定の特征および方法は、エンドツーエンドの暗号化された位置検出の例示的な実現例として開示されており、他の等価の特征および方法も添付の特許請求の範囲の範囲内であるように意図されている。さらに、さまざまな異なる実施形態が記載されており、各々の記載されている実施形態は独立してまたは 1 つ以上の他の記載されている実施形態に関連して実現可能であることが理解されねばならない。

【 図 面 】

【 図 1 】

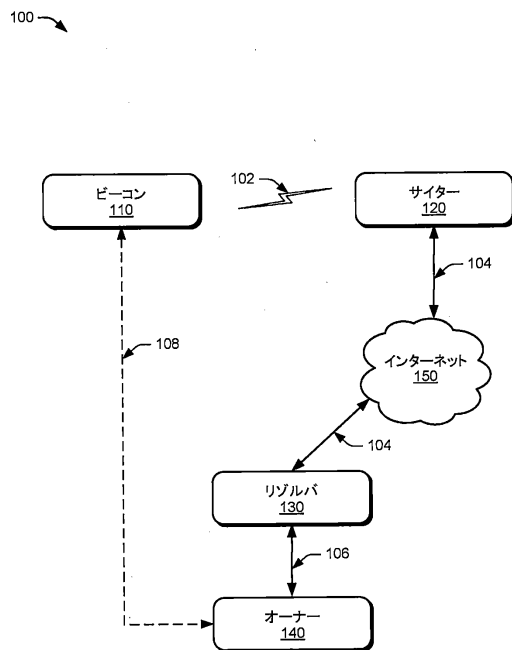


Fig. 1

【 図 2 】

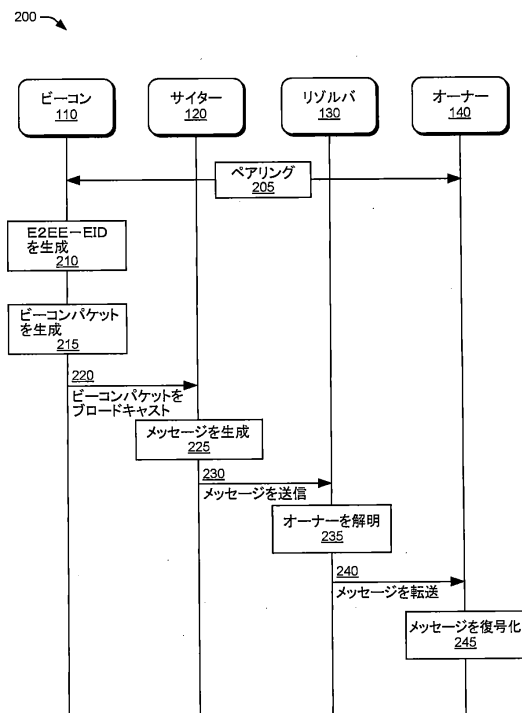


Fig. 2

【図 3】

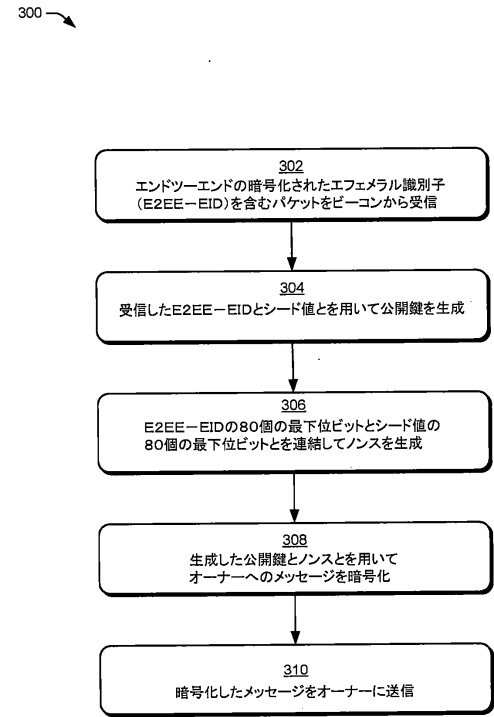


Fig. 3

【図 4】

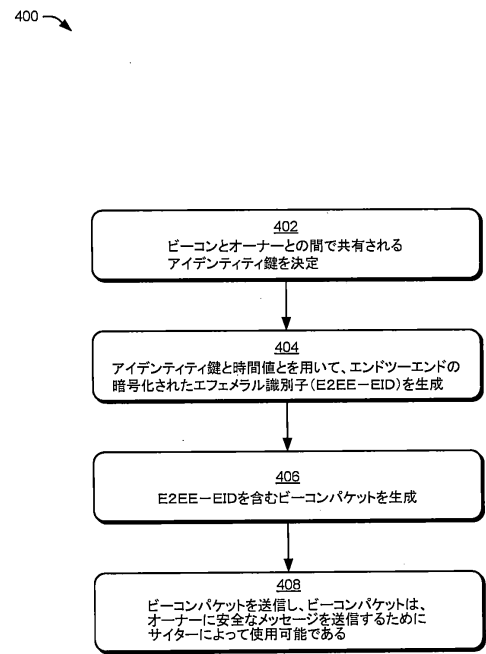


Fig. 4

【図 5】

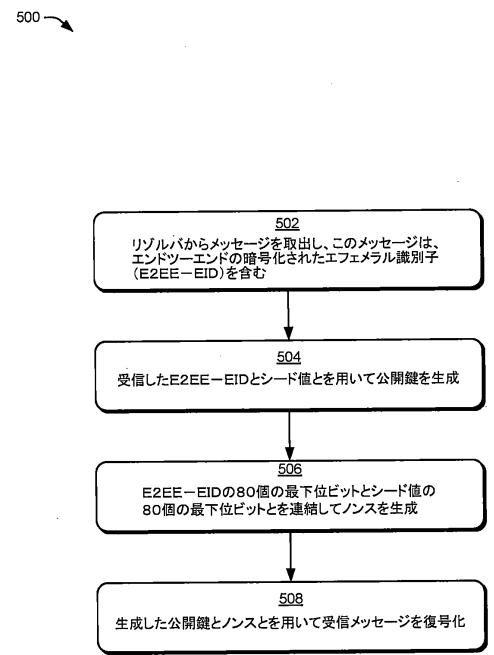


Fig. 5

【図 6】

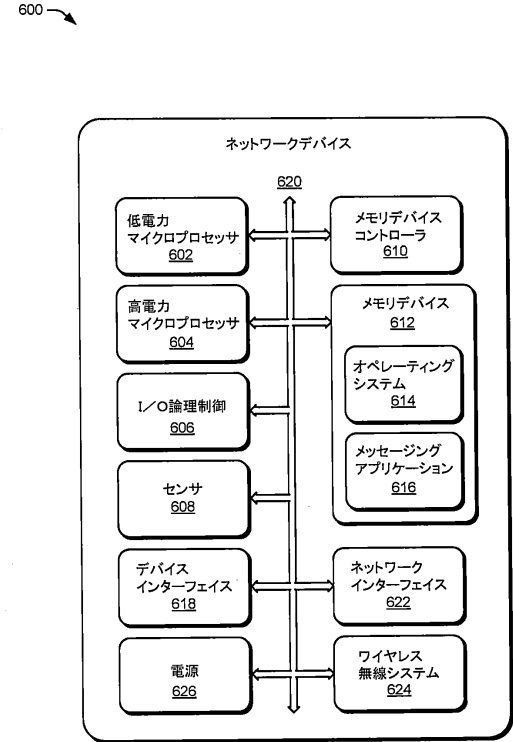


Fig. 6

10

20

30

40

50

【図 7】

700

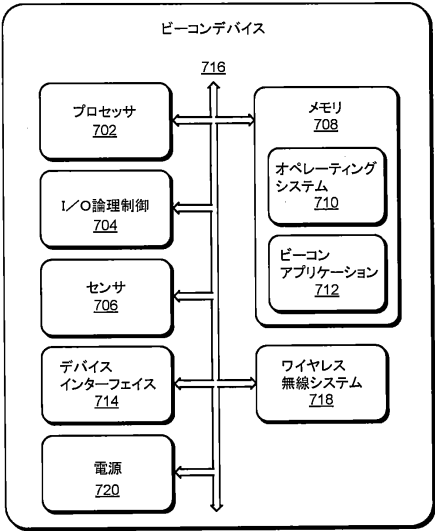


Fig. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2021/025743

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/08 H04W12/02 H04W12/03 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L H04W		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data, COMPENDEX, IBM-TDB		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DAN HARKINS (HPE): "privacy-for-password-identifiers", IEEE DRAFT; 11-20-0543-01-000M-PRIVACY-FOR-PASSWORD-ID ENTIFIERS, IEEE-SA MENTOR, PISCATAWAY, NJ USA , vol. 802.11m, no. 1 1 April 2020 (2020-04-01), pages 1-7, XP068167305, Retrieved from the Internet: URL:https://mentor.ieee.org/802.11/dcn/20/ 11-20-0543-01-000m-privacy-for-password-id entifiers.docx [retrieved on 2020-04-01] paragraph [12.4.3]	1-15
	----- -/-	
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
6 July 2021		14/07/2021
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Bec, Thierry

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/025743

Q(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2017/013450 A1 (ZIV ALON [IL] ET AL) 12 January 2017 (2017-01-12) figures 1-8 paragraph [0024] - paragraph [0079] -----	1-15
T	JOPPE W BOS ET AL: "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography", IACR, INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, vol. 20090901:153928, 1 September 2009 (2009-09-01), pages 1-19, XP061003560, [retrieved on 2009-09-01] paragraph [0003] -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2021/025743

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017013450 A1	12-01-2017	US 2017013450 A1	12-01-2017
		US 2018007555 A1	04-01-2018

Form PCT/ISA/210 (patent family annex) (April 2005)

10

20

30

40

50

フロントページの続き

(51)国際特許分類		F I	テーマコード (参考)	
H O 4 L	9/14 (2006.01)	H O 4 L	9/14	
H O 4 L	9/32 (2006.01)	H O 4 L	9/32	1 0 0 D
MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU, CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JO,JP,K E,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,N G,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM, TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW				
(72)発明者	ラザロブ, デイビッド			
	アメリカ合衆国、9 4 0 4 3 カリフォルニア州、マウンテン・ビュー、アンフィシアター・パー クウェイ、1 6 0 0			
F ターム (参考)	5K067 AA21 BB37 DD17 DD20 EE02 EE10 EE16 JJ61			