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

特許第6374490号
(P6374490)

(45)発行日　平成30年8月15日(2018.8.15)　(24)登録日　平成30年7月27日(2018.7.27)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 21/57	(2013.01)	G06F	21/57	

請求項の数 15　(全 14 頁)

(21)出願番号	特願2016-518322(P2016-518322)
(86)(22)出願日	平成26年5月5日(2014.5.5)
(65)公表番号	特表2016-521937(P2016-521937A)
(43)公表日	平成28年7月25日(2016.7.25)
(86)国際出願番号	PCT/US2014/036844
(87)国際公開番号	WO2014/197153
(87)国際公開日	平成26年12月11日(2014.12.11)
審査請求日	平成29年4月21日(2017.4.21)
(31)優先権主張番号	61/832,678
(32)優先日	平成25年6月7日(2013.6.7)
(33)優先権主張国	米国(US)
(31)優先権主張番号	14/037,050
(32)優先日	平成25年9月25日(2013.9.25)
(33)優先権主張国	米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ボラプラガタ・ヴェンカタ・ジャナキ・マノハー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】ファームウェアトラステッドプラットフォームモジュールのためのエンドースメント鍵証明書をプロビジョニングするための装置および方法

(57)【特許請求の範囲】

【請求項１】

ファームウェアトラステッドプラットフォームモジュール(fTPM)のためのエンドースメント鍵(EK)証明書をプロビジョニングするための方法であって、前記方法は、

ハードウェアトラステッドプラットフォーム(HWTP)から導出鍵(DK)を受信するステップであって、前記fTPMは前記HWTPに実装され、前記DKは前記HWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、前記HWKは前記HWTPに固有のものであり、前記HWKは前記fTPMが利用可能ではない、ステップと、

前記DKに基づいてエンドースメントプライマリシード(EPS)を生成するステップと、

前記EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するステップと、

前記HEPSをプロビジョニング局に転送するステップと、

前記HEPSに対応する前記EK証明書を前記プロビジョニング局から受信するステップとを含む方法。

【請求項２】

EKを備える公開鍵および秘密鍵を生成するステップであって、前記EK証明書が前記公開鍵を有する、ステップ、および、

前記fTPMのみが利用可能である前記HWTPのセキュアな不揮発性メモリに前記EK証明書を記憶するステップ

のうちの1つ又は複数をさらに含む、請求項1に記載の方法。

【請求項３】
前記プロビジョニング局がHEPSおよび対応するEK証明書のデータベースを有し、各HEPSおよび対応するEK証明書が1つのみの特定のfTPMに関連付けられる、請求項1に記載の方法。
【請求項４】
セキュアな施設においてエンドースメント鍵(EK)証明書およびハッシュ化エンドースメントプライマリシード(HEPS)を生成するための方法であって、前記EK証明書が、ハードウェアトラステッドプラットフォーム(HWTP)に固有のものであるハードウェア鍵(HWK)を有する特定のHWTPに関連付けられたファームウェアトラステッドプラットフォームモジュール(fTPM)のためのものであり、前記方法は、
前記HWTPのための暗号化導出鍵E[DK]を受信するステップであって、前記導出鍵(DK)は前記HWTPに固有のものである前記HWKから導出される、ステップと、
前記DKを生成するために前記セキュアな施設のための秘密鍵を使用して前記E[DK]を解読するステップと、
前記DKに基づいてエンドースメントプライマリシード(EPS)を生成するステップと、
前記EPSのハッシュに基づいて前記ハッシュ化エンドースメントプライマリシード(HEPS)を生成するステップと、
前記EPSに基づいてEKを生成するステップと、
前記EK証明書を生成するために前記EKの公開部分に署名するステップと、
データベース内で前記HEPSおよび前記EK証明書を関連付けるステップと
を含む方法。
【請求項５】
前記EPSのサイズが固定であり、前記EPSに基づいて前記EKを生成するために使用されるアルゴリズムに依存する、請求項4に記載の方法。
【請求項６】
前記データベースを、前記fTPMに前記EK証明書をプロビジョニングするための少なくとも1つの相手先商標製造業者(OEM)に送信するステップ
をさらに含む、請求項4に記載の方法。
【請求項７】
前記EKが公開鍵と秘密鍵とを備え、
前記EK証明書が前記公開鍵を含む、
請求項4に記載の方法。
【請求項８】
ハードウェアトラステッドプラットフォーム(HWTP)から導出鍵(DK)を受信するための手段であって、前記DKを前記受信するための手段は前記HWTPに実装され、前記DKは前記HWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、前記HWKは前記HWTPに固有のものであり、前記HWKは前記DKを前記受信するための手段が利用可能ではない、手段と、
前記DKに基づいてエンドースメントプライマリシード(EPS)を生成するための手段と、
前記EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するための手段と、
前記HEPSをプロビジョニング局に転送するための手段と、
前記HEPSに対応するエンドースメント鍵(EK)証明書を前記プロビジョニング局から受信するための手段と
を備えるリモート局。
【請求項９】
EKを備える公開鍵および秘密鍵を生成するための手段であって、前記EK証明書が前記公開鍵を有し、確定関数がハッシュ関数を含む、手段
をさらに備える、請求項8に記載のリモート局。
【請求項１０】
前記HWTPのセキュアな不揮発性メモリに前記EK証明書を記憶するための手段

をさらに備える、請求項8に記載のリモート局。
【請求項１１】
特定のハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信するための手段であって、前記導出鍵(DK)は前記HWTPに固有のものであるハードウェア鍵HWKから導出される、手段と、
前記DKを生成するためにセキュアな施設のための秘密鍵を使用して前記E[DK]を解読するための手段と、
前記DKに基づいてエンドースメントプライマリシード(EPS)を生成するための手段と、
前記EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するための手段と、
前記EPSに基づいてエンドースメント鍵(EK)を生成するための手段と、
EK証明書を生成するために前記EKの公開部分に署名するための手段であって、前記EK証明書が、前記固有のHWKを有する前記HWTPに関連付けられたファームウェアトラステッドプラットフォームモジュール(fTPM)のためのものである、手段と、
データベース内で前記HEPSおよび前記EK証明書を関連付けるための手段と
を備えるリモート局。
【請求項１２】
前記EPSのサイズが固定であり、前記EPSに基づいて前記EKを生成するために使用されるアルゴリズムに依存する、請求項11に記載のリモート局。
【請求項１３】
前記データベースを、前記fTPMに前記EK証明書をプロビジョニングするための少なくとも1つの相手先商標製造業者(OEM)に送信するための手段
をさらに備える、請求項11に記載のリモート局。
【請求項１４】
前記EKが公開鍵と秘密鍵とを備え、
前記EK証明書が前記公開鍵を含む、
請求項11に記載のリモート局。
【請求項１５】
コンピュータに請求項1乃至7のいずれか１項に記載の方法を実行させるためのコードを備える非一時的コンピュータ可読記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、参照により本明細書に組み込まれる、2013年6月7日に出願した米国仮出願第61/832,678号の利益を主張するものである。
【０００２】
本発明は一般に、ファームウェアトラステッドプラットフォームモジュール(fTPM:firmware trusted platform module)のためのエンドースメントプライマリシード(EPS:endorsement primary seed)およびエンドースメント鍵証明書(endorsement key certificate)をプロビジョニングすることに関する。
【背景技術】
【０００３】
EPSは、特定のトラステッドプラットフォームモジュール(TPM:trusted platform module)に固定/束縛された固定サイズのランダム値である。EPS値は機密である。エンドースメント鍵(EK:endorsement key)は、EPSを使用して生成された非対称鍵ペア(たとえば、RSA/ECCkey)である。この非対称鍵の秘密構成要素は機密である。対応するEK証明書(EKCert)は、対応するEKを保証する認証機関によって生成され、署名される。各TPM(ハードウェアモジュール)の製造業者は、固有のEPSおよび対応するEKCertを各TPMにプロビジョニングする。

【０００４】
ファームウェアTPM(fTPM)の場合、相手先商標製造業者(OEM:original equipment manufacturer)がTPMを使用してデバイスをブートアップするまで、不揮発性(NV:nonvolatile)ストレージは利用可能ではない。したがって、TPM製造業者には、工場内でEPSおよび対応するEKCertをプロビジョニングする方法がない。ヒューズ内にfTPMの固有のEPSおよびEKCert(署名)を記憶することは、ハードウェアの変更を必要とする。
【０００５】
デバイス初期化の間(または必要なときに)、TPMはEKを生成するためにEPSを使用する。TPMは対応する記憶されたEKCertを別のエンティティに提示することができ、そのエンティティはそれらが特定のTPMと通信していることを確実に判断することができる。EPSおよび秘密EKはセキュリティに敏感であり、TPMへのプロビジョニング中およびその後に漏らされてはならない。
【０００６】
そのようなハードウェアベースのTPMの場合、ハードウェアが作成されるとき、EKおよび証明書のペアが工場の現場で生成され、TPMのみがアクセス可能であるTPMのemmc/ヒューズ/ROM内部で融合される。TPMは、設計上、秘密情報を漏らしてはならないことになっている。
【０００７】
fTPMに関する問題は、fTPMがセキュアなカーネル(TrustZoneまたは他のそのような環境)で動作するソフトウェアであり、標準CPU上でロードおよび動作するということである。fTPMはすべてがソフトウェアであるので、デバイス固有の鍵をソフトウェアにプロビジョニングすることができない。また、最終的なデバイス(たとえば、モバイルフォン、タブレット、または他のそのようなデバイス)が工場内で作製されるときにEPS、EK、およびEKCertをプロビジョニングすることは、EPS、EK、およびEKCertのセキュアな生成に時間がかかるために特に困難である。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
したがって、fTPMのためのEKCertをプロビジョニングするための技法が必要とされている。
【課題を解決するための手段】
【０００９】
本発明の一態様は、ファームウェアトラステッドプラットフォームモジュール(fTPM)のためのエンドースメント鍵(EK)証明書をプロビジョニングするための方法に存在し得る。本方法では、導出鍵(DK:derived key)はハードウェアトラステッドプラットフォーム(HWTP)から受信される。fTPMはHWTPに実装され、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK:hardware key)から導出され、HWKはHWTPに固有のものであり、HWKはfTPMが利用可能ではない。エンドースメントプライマリシード(EPS)はDKに基づいて生成され、ハッシュ化エンドースメントプライマリシード(HEPS:hashed endorsement primary seed)はEPSのハッシュに基づいて生成される。HEPSはプロビジョニング局に転送され、HEPSに対応するEK証明書をプロビジョニング局から受信する。
【００１０】
本発明のより詳細な態様では、EKを備える公開鍵および秘密鍵が生成され得、EK証明書は公開鍵を有し得る。また、EK証明書は、fTPMのみが利用可能であるHWTPのセキュアな不揮発性メモリに記憶され得る。さらに、プロビジョニング局は、HEPSおよび対応するEK証明書のデータベースを有し得る。各HEPSおよび対応するEK証明書は、1つのみの特定のfTPMに関連付けられる。
【００１１】
本発明の別の態様は、ハードウェアトラステッドプラットフォーム(HWTP)から導出鍵(DK)を受信するための手段であって、DKを受信するための手段はHWTPに実装され、DKはHWTP

にセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはDKを受信するための手段が利用可能ではない、手段と、DKに基づいてエンドースメントプライマリシード(EPS)を生成するための手段と、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するための手段と、HEPSをプロビジョニング局に転送するための手段と、HEPSに対応するEK証明書をプロビジョニング局から受信するための手段とを備える局に存在し得る。

【００１２】

本発明の別の態様は、プロセッサを備える局であって、プロセッサが、ハードウェアトラステッドプラットフォーム(HWTP)から導出鍵(DK)を受信することであって、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはファームウェアトラステッドプラットフォームモジュール(fTPM)が利用可能ではない、受信することと、DKに基づいてエンドースメントプライマリシード(EPS)を生成することと、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成することと、HEPSをプロビジョニング局に転送することと、HEPSに対応するEK証明書をプロビジョニング局から受信することとを行うように構成される、局に存在し得る。

【００１３】

本発明の別の態様は、コンピュータ可読媒体を備えるコンピュータプログラム製品であって、コンピュータ可読媒体が、コンピュータに、ハードウェアトラステッドプラットフォーム(HWTP)から導出鍵(DK)を受信させるためのコードであって、ファームウェアトラステッドプラットフォームモジュール(fTPM)はHWTPに実装され、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはfTPMが利用可能ではない、コードと、コンピュータに、DKに基づいてエンドースメントプライマリシード(EPS)を生成させるためのコードと、コンピュータに、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成させるためのコードと、コンピュータに、HEPSをプロビジョニング局に転送させるためのコードと、コンピュータに、HEPSに対応するEK証明書をプロビジョニング局から受信させるためのコードとを備える、コンピュータプログラム製品に存在し得る。

【００１４】

本発明の別の態様は、セキュアな施設においてエンドースメント鍵(EK)証明書およびハッシュ化エンドースメントプライマリシード(HEPS)を生成するための方法に存在し得る。本方法では、特定のハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]が受信される。導出鍵(DK)は、HWTPに固有のものであるハードウェア鍵HWKから導出される。E[DK]は、DKを生成するためにセキュアな施設のための秘密鍵を使用して解読される。エンドースメントプライマリシード(EPS)は、DKに基づいて生成される。ハッシュ化エンドースメントプライマリシード(HEPS)は、EPSのハッシュに基づいて生成される。エンドースメント鍵(EK)は、EPSに基づいて生成される。EKの公開部分は、EK証明書を生成するために署名される。HEPSおよびEK証明書はデータベース内で関連付けられる。

【００１５】

本発明のより詳細な態様では、EPSのサイズは固定であってもよく、EPSに基づいてEKを生成するために使用されるアルゴリズムに依存し得る。EK証明書は、固有のHWKを有するHWTPに関連付けられたファームウェアトラステッドプラットフォームモジュール(fTPM)のためのものであり得る。データベースは、fTPMにEK証明書をプロビジョニングするための少なくとも1つの相手先商標製造業者(OEM)に送信され得る。EKは公開鍵と秘密鍵とを備え得、EK証明書は公開鍵を含み得る。

【００１６】

本発明の別の態様は、特定のハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信するための手段であって、導出鍵(DK)はHWTPに固有のものであるハードウェア鍵HWKから導出される、手段と、DKを生成するためにセキュアな施設のための秘密鍵を使用してE[DK]を解読するための手段と、DKに基づいてエンドースメント

プライマリシード(EPS)を生成するための手段と、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するための手段と、EPSに基づいてエンドースメント鍵(EK)を生成するための手段と、EK証明書を生成するためにEKの公開部分に署名するための手段と、データベース内でHEPSおよびEK証明書を関連付けるための手段とを備える局に存在し得る。

【００１７】

本発明の別の態様は、プロセッサを備える局であって、プロセッサが、ハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信することであって、導出鍵(DK)はHWTPに固有のものであるハードウェア鍵HWKから導出される、受信することと、DKを生成するためにセキュアな施設のための秘密鍵を使用してE[DK]を解読することと、DKに基づいてエンドースメントプライマリシード(EPS)を生成することと、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成することと、EPSに基づいてエンドースメント鍵(EK)を生成することと、EK証明書を生成するためにEKの公開部分に署名することと、データベース内でHEPSおよびEK証明書を関連付けることとを行うように構成される、局に存在し得る。

【００１８】

本発明の別の態様は、コンピュータ可読媒体を備えるコンピュータプログラム製品であって、コンピュータ可読媒体が、コンピュータに、ハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信させるためのコードであって、導出鍵(DK)はHWTPに固有のものであるハードウェア鍵HWKから導出される、コードと、コンピュータに、DKを生成するためにセキュアな施設のための秘密鍵を使用してE[DK]を解読させるためのコードと、コンピュータに、DKに基づいてエンドースメントプライマリシード(EPS)を生成させるためのコードと、コンピュータに、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成させるためのコードと、コンピュータに、EK証明書を生成するためにEKの公開部分に署名させるためのコードと、コンピュータに、データベース内でHEPSおよびEK証明書を関連付けさせるためのコードとを備える、コンピュータプログラム製品に存在し得る。

【図面の簡単な説明】

【００１９】

【図１】ワイヤレス通信システムの一例のブロック図である。

【図２】本発明による、ファームウェアトラステッドプラットフォームモジュールのためのエンドースメント鍵証明書をプロビジョニングするための方法の流れ図である。

【図３】ハードウェア鍵から導出鍵を生成し、導出鍵を暗号化するための方法の流れ図である。

【図４】セキュアな施設において、データベースに記憶するためのハッシュ化エンドースメントプライマリシードおよび対応するエンドースメント鍵証明書を生成するための方法の流れ図である。

【図５】受信されたハッシュ化エンドースメントプライマリシードに対応するエンドースメント鍵証明書をフェッチし、転送するための方法の流れ図である。

【図６】ハッシュ化エンドースメントプライマリシードおよび対応するエンドースメント鍵証明書のデータベースを生成するための方法の鍵およびシードの階層の概略図である。

【図７】ファームウェアトラステッドプラットフォームモジュールのためのエンドースメントプライマリシードおよび対応するエンドースメント鍵証明書をプロビジョニングするための方法の鍵およびシードの階層の概略図である。

【図８】トラステッドプラットフォームを備えた、メモリとプロセッサとを含むコンピュータのブロック図である。

【図９】プロセッサとメモリとを含むセキュアな施設コンピュータのブロック図である。

【発明を実施するための形態】

【００２０】

「例示的な」という言葉は、「例、事例、または例示としての役割を果たすこと」を意

味するように本明細書で使用される。「例示的な」として本明細書で説明する任意の実施形態は、必ずしも他の実施形態よりも好ましいか、または有利であると解釈されるべきではない。

【００２１】

図2および図3を参照すると、本発明の一態様は、ファームウェアトラステッドプラットフォームモジュール(fTPM)のためのエンドースメント鍵(EK)証明書をプロビジョニングするための方法200に存在し得る。本方法では、fTPMはハードウェアトラステッドプラットフォーム(HWTP)820から導出鍵(DK)を受信する(ステップ210)。fTPMはHWTPに実装され、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはfTPMが利用可能ではない。fTPMは、DKに基づいてエンドースメントプライマリシード(EPS)を生成し(ステップ220)、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成する(ステップ230)。fTPMは、HEPSをプロビジョニング局に転送し(ステップ240)、HEPSに対応するEK証明書をプロビジョニング局から受信する(ステップ250)。

【００２２】

本発明のより詳細な態様では、fTPMはEKを備える公開鍵および秘密鍵を生成し得、EK証明書は公開鍵を有し得る。また、fTPMは、fTPMのみが利用可能であるHWTPのセキュアな不揮発性(NV)メモリにEK証明書を記憶し得る。さらに、プロビジョニング局は、HEPSおよび対応するEK証明書のデータベース(DB)を有し得る。各HEPSおよび対応するEK証明書は、1つのみの特定のfTPMに関連付けられる。

【００２３】

図8をさらに参照すると、本発明の別の態様は、ハードウェアトラステッドプラットフォーム(HWTP)820から導出鍵(DK)を受信するための手段810であって、DKを受信するための手段810はHWTPに実装され、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはDKを受信するための手段が利用可能ではない、手段810と、DKに基づいてエンドースメントプライマリシード(EPS)を生成するための手段810と、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するための手段810と、HEPSをプロビジョニング局に転送するための手段810と、HEPSに対応するEK証明書をプロビジョニング局から受信するための手段810とを備える局(たとえば、コンピュータ800)に存在し得る。

【００２４】

本発明の別の態様は、ファームウェアトラステッドプラットフォームモジュール(fTPM)を実装するように構成されたハードウェアトラステッドプラットフォーム(HWTP)820を有するプロセッサ810であって、fTPMはハードウェアトラステッドプラットフォーム(HWTP)から導出鍵(DK)を受信し、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはfTPMが利用可能ではなく、fTPMはDKに基づいてエンドースメントプライマリシード(EPS)を生成し、fTPMはEPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成し、fTPMはHEPSをプロビジョニング局に転送し、fTPMはHEPSに対応するEK証明書をプロビジョニング局から受信する、プロセッサ810を備える局に存在し得る。

【００２５】

本発明の別の態様は、コンピュータ可読媒体830を備えるコンピュータプログラム製品であって、コンピュータ可読媒体830が、コンピュータ800に、ハードウェアトラステッドプラットフォーム(HWTP)820から導出鍵(DK)を受信させるためのコードであって、ファームウェアトラステッドプラットフォームモジュール(fTPM)はHWTPに実装され、DKはHWTPにセキュアに記憶されたハードウェア鍵(HWK)から導出され、HWKはHWTPに固有のものであり、HWKはfTPMが利用可能ではない、コードと、コンピュータに、DKに基づいてエンドースメントプライマリシード(EPS)を生成させるためのコードと、コンピュータに、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成させるためのコードと、コンピュータに、HEPSをプロビジョニング局に転送させるためのコードと、コ

ンピュータに、HEPSに対応するEK証明書をプロビジョニング局から受信させるためのコードとを備える、コンピュータプログラム製品に存在し得る。

【００２６】

fTPMは、ARMアーキテクチャのTrustZoneなどのセキュアな環境で動作する。デバイスが動作中であるとき、fTPMはセキュアな/暗号化NVメモリ(たとえば、そのコンテンツを暗号化したTrustZone NVメモリ)にアクセスすることができる。固有のハードウェア鍵(HWK)は、チップ製造中に、ハードウェアブロックのみがアクセス可能である各チップに融合される。

【００２７】

図3を参照すると、TPM(チップ)製造業者はランダム値からHWKを生成する(ステップ310)。DKは、TPMのハードウェア鍵導出関数(KDF)のエミュレーションを使用して、HWKに基づいて生成される(ステップ320)。DKは、暗号化DK(E[DK])を生成するためにセキュアな施設の公開鍵を使用して暗号化される(ステップ330)。E[DK]は、後でアクセスするためにセキュアな施設に送信される(ステップ340)。HWKは、HWKをチップに融合することによってチップに記憶され得る(ステップ350)。TPM(チップ)製造業者は次いで、HWKおよびDKを破壊する(ステップ360)。

【００２８】

図4を参照すると、セキュアな施設は製造された各TPM(すなわち、HWTP)のためのE[DK]を受信する。セキュアな施設は、セキュアな施設の秘密鍵を使用してDKを解読する(ステップ410)。セキュアな施設は、DKからEPS(典型的には32バイト)を生成するためにソフトウェアKDFを使用する(ステップ420)。EPSのサイズは固定であり、実際の非対称EK鍵生成を実行するために使用されるアルゴリズムに依存する。セキュアな施設は、EPSに基づいてEKを生成し(ステップ430)、EKCertを作成するためにEKの公開部分に署名する(ステップ440)。セキュアな施設は、ハッシュ化EPS(HEPS)を生成するためにEPSをハッシュする(ステップ450)。セキュアな施設は、HEPSおよび対応するEKCertをデータベースに記憶する(ステップ460)。このプロセスは、HEPSおよびEKCertの固有のペアを生成するために各TPMについて繰り返される。セキュアな施設のデータベースは顧客/OEMに送信される。

【００２９】

図5を参照すると、OEMは、その製造ライン上で、内部にTPMを備えたチップを内蔵するデバイスを作製する。各OEMは、記憶されたHEPSおよび対応するEKCertのデータベースをチップ製造業者から受け取る(ステップ510)。第1のブート/プロビジョニングステップの間、fTPMは固有のEPSを導出するためにDK上でKDFを使用する。fTPMはEPSをハッシュし、HEPSをOEMによって操作されるコンピュータ局におけるプロビジョニングソフトウェアに与える(ステップ520)。プロビジョニングソフトウェア/アプリケーションはHEPSに一致するEKCertを探索し(ステップ530)、EKCertをfTPMに転送する(ステップ540)。fTPMは、fTPMのみが利用可能であるTPMのNVメモリの公開部分において証明書をプロビジョニングし得る。

【００３０】

図6を参照すると、TPM製造業者は各TPMのための暗号化DKを生成する。セキュアな施設(典型的には、工場の現場から離れたTPM製造業者によって運営される)は、HEPSおよびEKCertのデータベースを生成する。OEMは、機密要素、すなわち、HWK、DK、EPS、および秘密EKを含まないデータベースを受け取る。データベースは、数十万個または数百万個のチップをカバーし得る。HEPSがなければ、EKCertを特定のチップに一致させることはランダムな推測を伴うことになる。

【００３１】

図7を参照すると、特定のHWTPのHWKおよびDKに対するHEPSの関係が示されている。HEPSは記憶された機密を明らかにせず、データベース内の対応するEKCertの識別を可能にするインデックスの一種として働く。

【００３２】

したがって、EK生成の時間がかかる部分はフィールドで必要とされるときはいつでも行

われ得るが、デバイスの製造プロセスの部分はそうではない。これにより、OEMの工場の現場においてEK(非対称鍵ペア、たとえば、RSA鍵ペア)生成の時間がかかるステップを実行する必要がなくなる。また、OEMは、EK証明書に署名するためのサービスを維持する/運営する必要がない。さらに、OEMは、そのデバイスのためのプロビジョニングを行うためのセキュアな施設を有する必要がない。

【００３３】

リモート局102は、TPM820を有するプロセッサ810と、メモリおよび/またはディスクドライブなどの記憶媒体830と、ディスプレイ840と、キーパッドなどの入力850と、ワイヤレス接続860とを含むコンピュータ800を備え得る。

【００３４】

図9を参照すると、セキュアな施設は、プロセッサ910と、メモリおよび/またはディスクドライブなどの記憶媒体920と、ディスプレイ930と、キーパッドなどの入力940と、ネットワーク/インターネット接続950とを含むコンピュータ900を含み得る。

【００３５】

本発明の別の態様は、特定のハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信するための手段910であって、導出鍵(DK)はHWTPに固有のものであるハードウェア鍵HWKから導出される、手段910と、DKを生成するためにセキュアな施設のための秘密鍵を使用してE[DK]を解読するための手段910と、DKに基づいてエンドースメントプライマリシード(EPS)を生成するための手段910と、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成するための手段910と、EPSに基づいてエンドースメント鍵(EK)を生成するための手段910と、EK証明書を生成するためにEKの公開部分に署名するための手段910と、データベース内でHEPSおよびEK証明書を関連付けるための手段910とを備える局(たとえば、コンピュータ900)に存在し得る。

【００３６】

本発明の別の態様は、プロセッサ910を備える局(たとえば、コンピュータ900)であって、プロセッサ910が、ハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信することであって、導出鍵(DK)はHWTPに固有のものであるハードウェア鍵HWKから導出される、受信することと、DKを生成するためにセキュアな施設のための秘密鍵を使用してE[DK]を解読することと、DKに基づいてエンドースメントプライマリシード(EPS)を生成することと、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成することと、EPSに基づいてエンドースメント鍵(EK)を生成することと、EK証明書を生成するためにEKの公開部分に署名することと、データベース内でHEPSおよびEK証明書を関連付けることとを行うように構成される、局に存在し得る。

【００３７】

本発明の別の態様は、コンピュータ可読媒体920を備えるコンピュータプログラム製品であって、コンピュータ可読媒体920が、コンピュータ900に、ハードウェアトラステッドプラットフォーム(HWTP)のための暗号化導出鍵E[DK]を受信させるためのコードであって、導出鍵(DK)はHWTPに固有のものであるハードウェア鍵HWKから導出される、コードと、コンピュータ900に、DKを生成するためにセキュアな施設のための秘密鍵を使用してE[DK]を解読させるためのコードと、コンピュータ900に、DKに基づいてエンドースメントプライマリシード(EPS)を生成させるためのコードと、コンピュータ900に、EPSのハッシュに基づいてハッシュ化エンドースメントプライマリシード(HEPS)を生成させるためのコードと、コンピュータ900に、EK証明書を生成するためにEKの公開部分に署名させるためのコードと、コンピュータ900に、データベース内でHEPSおよびEK証明書を関連付けさせるためのコードとを備える、コンピュータプログラム製品に存在し得る。

【００３８】

図1を参照すると、ワイヤレスリモート局(RS)102(たとえば、移動局MS)は、ワイヤレス通信システム100の1つまたは複数の基地局(BS)104と通信し得る。ワイヤレス通信システム100は、1つまたは複数の基地局コントローラ(BSC)106と、コアネットワーク108とをさらに含み得る。コアネットワークは、適切なバックホールを介して、インターネット110

および公衆交換電話網(PSTN)112に接続されてもよい。典型的なワイヤレス移動局は、ハンドヘルド電話またはラップトップコンピュータを含み得る。ワイヤレス通信システム100は、符号分割多元接続(CDMA)、時分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技法などのいくつかの多元接続技法のうちのいずれか1つを採用することができる。

【００３９】

情報および信号が様々な異なる技術および技法のいずれかを使用して表され得ることを当業者は理解されよう。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。

【００４０】

本明細書で開示する実施形態に関して説明する様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることを当業者はさらに諒解されよう。ハードウェアおよびソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップは、概してそれらの機能に関して上記で説明されてきた。そのような機能がハードウェアとして実装されるか、またはソフトウェアとして実装されるかは、特定の適用例および全体的なシステムに課された設計制約に依存する。当業者は、説明した機能を特定の適用例ごとに様々な方法で実装することができるが、そのような実装の決定は、本発明の範囲からの逸脱を引き起こすものと解釈されるべきではない。

【００４１】

本明細書で開示する実施形態に関して説明する様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、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)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明する機能を実行するように設計されたそれらの任意の組合せを用いて実装または実行され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装され得る。

【００４２】

本明細書で開示する実施形態に関して説明する方法またはアルゴリズムのステップは、直接ハードウェアで具現化されるか、プロセッサによって実行されるソフトウェアモジュールで具現化されるか、またはその2つの組合せで具現化され得る。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるようにプロセッサに結合される。代替として、記憶媒体は、プロセッサと一体であり得る。プロセッサおよび記憶媒体は、ASIC内に存在し得る。ASICはユーザ端末内に存在し得る。代替として、プロセッサおよび記憶媒体は、ユーザ端末内に個別構成要素として存在し得る。

【００４３】

1つまたは複数の例示的な実施形態では、説明した機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装され得る。コンピュータプログラム製品としてソフトウェアで実装された場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶されるか、またはコンピュータ可読媒体を介

して送信され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、非一時的コンピュータ可読記憶媒体と通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気記憶デバイス、または、命令もしくはデータ構造の形態の所望のプログラムコードを搬送もしくは記憶するために使用され得、コンピュータによってアクセスされ得る、任意の他の媒体を備え得る。また、任意の接続が適切にコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザーディスク(登録商標)(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピー(登録商標)ディスク(disk)およびブルーレイディスク(disc)を含み、ディスク(disk)は通常、データを磁気的に再生し、ディスク(disc)は、データをレーザーで光学的に再生する。上記の組合せもコンピュータ可読媒体の範囲内に含まれるべきである。

【００４４】

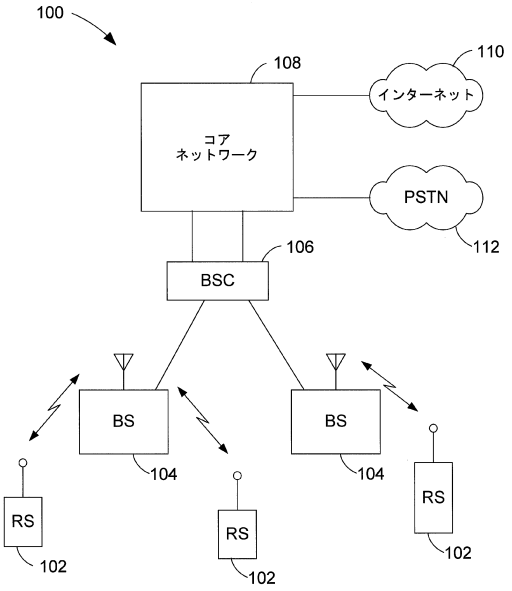
開示した実施形態の上記の説明は、いかなる当業者も本発明を作製または使用することを可能にするために提供される。これらの実施形態への様々な修正が当業者には容易に明らかになり、本明細書で定義する一般原理は、本発明の趣旨または範囲を逸脱することなしに他の実施形態に適用され得る。したがって、本発明は、本明細書に示す実施形態に限定されるものではなく、本明細書で開示する原理および新規の特徴に一致する最も広い範囲を与えられるべきである。

【符号の説明】

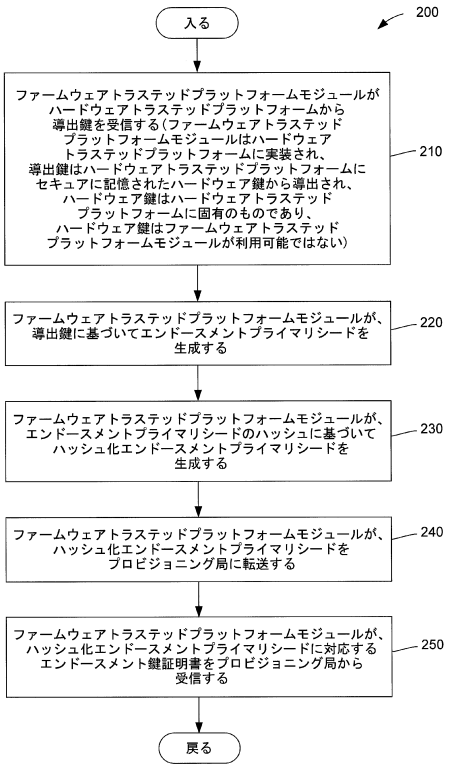
【００４５】

100 ワイヤレス通信システム
102 ワイヤレスリモート局(RS)
104 基地局(BS)
106 基地局コントローラ(BSC)
108 コアネットワーク
110 インターネット
112 公衆交換電話網(PSTN)
200 方法
800 コンピュータ
810 プロセッサ、手段
820 ハードウェアトラステッドプラットフォーム(HWTP)
830 コンピュータ可読媒体
840 ディスプレイ
850 入力
860 ワイヤレス接続
900 コンピュータ
910 プロセッサ、手段
920 記憶媒体
930 ディスプレイ
940 入力
950 ネットワーク/インターネット接続

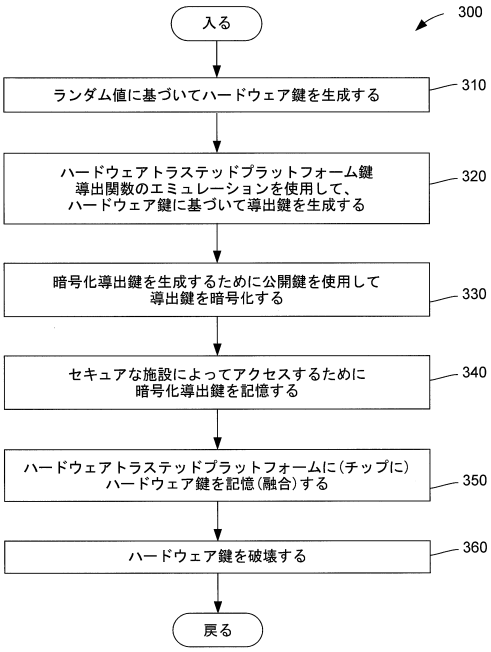
【図１】


100
108
110
コア
ネットワーク
インターネット
PSTN
112
106
BSC
BS
BS
104
104
RS
RS
RS
102
102
102

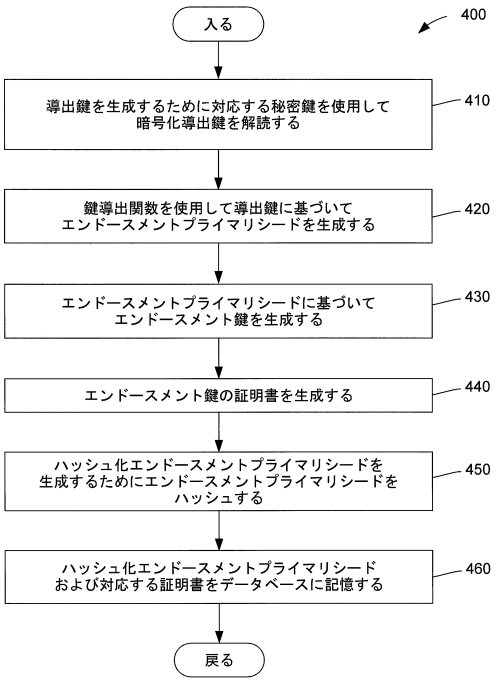
【図２】


入る
200
ファームウェアトラステッドプラットフォームモジュールが
ハードウェアトラステッドプラットフォームから
導出鍵を受信する（ファームウェアトラステッド
プラットフォームモジュールはハードウェア
トラステッドプラットフォームに実装され、
導出鍵はハードウェアトラステッドプラットフォームに
セキュアに記憶されたハードウェア鍵から導出され、
ハードウェア鍵はハードウェアトラステッド
プラットフォームに固有のものであり、
ハードウェア鍵はファームウェアトラステッド
プラットフォームモジュールが利用可能ではない）
210
ファームウェアトラステッドプラットフォームモジュールが、
導出鍵に基づいてエンドースメントプライマリシードを
生成する
220
ファームウェアトラステッドプラットフォームモジュールが、
エンドースメントプライマリシードのハッシュに基づいて
ハッシュ化エンドースメントプライマリシードを
生成する
230
ファームウェアトラステッドプラットフォームモジュールが、
ハッシュ化エンドースメントプライマリシードを
プロビジョニング局に転送する
240
ファームウェアトラステッドプラットフォームモジュールが、
ハッシュ化エンドースメントプライマリシードに対応する
エンドースメント鍵証明書をプロビジョニング局から
受信する
250
戻る

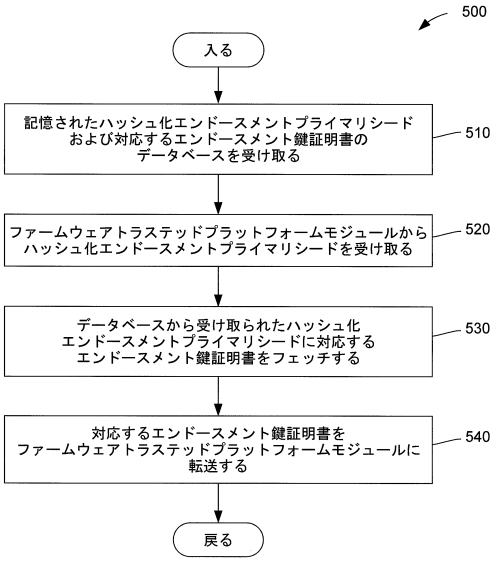
【図３】


入る
300
ランダム値に基づいてハードウェア鍵を生成する
310
ハードウェアトラステッドプラットフォーム鍵
導出関数のエミュレーションを使用して、
ハードウェア鍵に基づいて導出鍵を生成する
320
暗号化導出鍵を生成するために公開鍵を使用して
導出鍵を暗号化する
330
セキュアな施設によってアクセスするために
暗号化導出鍵を記憶する
340
ハードウェアトラステッドプラットフォームに（チップに）
ハードウェア鍵を記憶（融合）する
350
ハードウェア鍵を破壊する
360
戻る

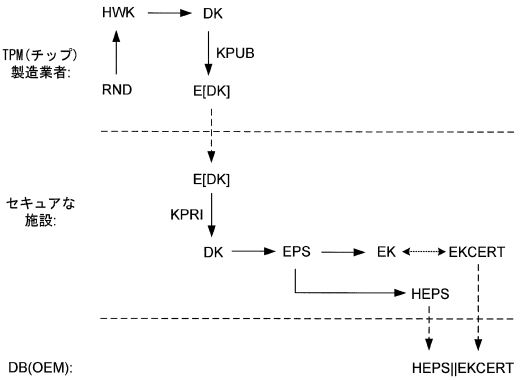
【図４】


入る
400
導出鍵を生成するために対応する秘密鍵を使用して
暗号化導出鍵を解読する
410
鍵導出関数を使用して導出鍵に基づいて
エンドースメントプライマリシードを生成する
420
エンドースメントプライマリシードに基づいて
エンドースメント鍵を生成する
430
エンドースメント鍵の証明書を生成する
440
ハッシュ化エンドースメントプライマリシードを
生成するためにエンドースメントプライマリシードを
ハッシュする
450
ハッシュ化エンドースメントプライマリシード
および対応する証明書をデータベースに記憶する
460
戻る

【図５】



【図６】



【図７】

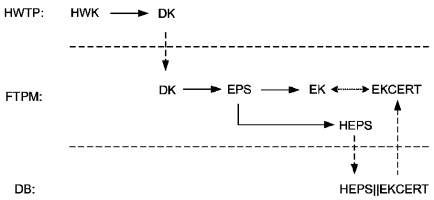
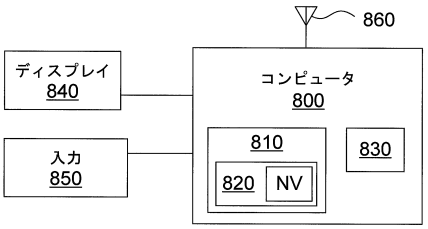
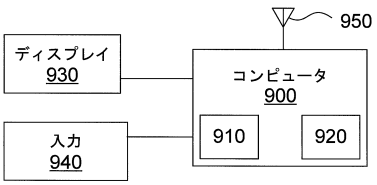


FIG. 7

【図８】



【図９】



フロントページの続き

(72)発明者　アシシュ・グローヴァー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　エイモン・コールマン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　青木　重徳

(56)参考文献　特開２００７－０２６４４２（ＪＰ，Ａ）
特表２００８－５００６５１（ＪＰ，Ａ）
国際公開第２０１３／０１９３６９（WO，Ａ１）
米国特許出願公開第２０１２／０１３７１３７（ＵＳ，Ａ１）
米国特許出願公開第２００５／０１４４４４０（ＵＳ，Ａ１）
米国特許出願公開第２００５／０２８３８２６（ＵＳ，Ａ１）
Trusted Platform Module Library Part 1: Architecture, TCG ［オンライン］, ２０１３年３月, Family "2.0" Level 00 Revision 00.96, pp.72-75, 171-172, ＵＲＬ, <https://trustedcomputinggroup.org/wp-content/uploads/TPM-Rev-1-Architecture-00.96-130315.pdf>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／５７
Ｈ０４Ｌ　　９／０８