(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6276426号
(P6276426)
(45)発行日　平成30年2月7日(2018.2.7)　(24)登録日　平成30年1月19日(2018.1.19)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675B
G09C 1/00 (2006.01)　　G09C 1/00 640D

請求項の数 22　(全 25 頁)

(21)出願番号　特願2016-569940 (P2016-569940)
(86)(22)出願日　平成27年6月1日(2015.6.1)
(65)公表番号　特表2017-517770 (P2017-517770A)
(43)公表日　平成29年6月29日(2017.6.29)
(86)国際出願番号　PCT/US2015/033608
(87)国際公開番号　WO2015/187591
(87)国際公開日　平成27年12月10日(2015.12.10)
審査請求日　平成29年5月24日(2017.5.24)
(31)優先権主張番号　14/294,015
(32)優先日　平成26年6月2日(2014.6.2)
(33)優先権主張国　米国(US)

早期審査対象出願

(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　ビリー・ボブ・ブラムリー
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

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】半決定論的デジタル署名生成

(57)【特許請求の範囲】
【請求項１】
デジタル署名を得るための電子デジタル署名生成デバイスにおいて動作する方法であって、
処理回路によって、半決定論的ノンスを得るように前記電子デジタル署名生成デバイスの半決定論的ノンス生成コンポーネントを制御するステップであって、
前記半決定論的ノンスが、完全にランダムなノンスと完全に決定論的なノンスとの間の部分的な量の決定論性を有し、かつ、デジタル署名を得るために前記電子デジタル署名生成デバイスによって使用されるデジタル署名生成プロトコルに関連付けられた値の全範囲内から完全にランダムに得られるノンスよりも決定論的であり、
前記半決定論的ノンスが、鍵導出関数と、秘密鍵と、メッセージと、前記半決定論的ノンスを結果として生じるように選択されたメッセージごとの値とを使用して得られ、かつ、
前記メッセージごとの値が、前記結果として生じるノンスが完全にランダムではないように、前記デジタル署名を生成するために使用される前記デジタル署名生成プロトコルに関連付けられた値の前記全範囲と比較して値の制限された範囲内でランダムに得られる、ステップと、
前記処理回路によって、前記半決定論的ノンスに部分的に基づいてデジタル署名を得るように前記電子デジタル署名生成デバイスのデジタル署名生成コンポーネントを制御するステップと、

前記処理回路によって、前記半決定論的ノンスに部分的に基づいて生成された前記デジタル署名を使用してメッセージに署名するために、前記電子デジタル署名生成デバイスのメッセージ署名コンポーネントを制御するステップと
を備える方法。
【請求項２】
前記半決定論的ノンス生成コンポーネントによって使用される前記メッセージごとの値が、秘密ノンスと、公開ノンスと、カウンタと、文脈特定メッセージとのうちの1つまたは複数である、請求項1に記載の方法。
【請求項３】
前記ノンスから前記デジタル署名を生成するために前記デジタル署名生成コンポーネントによって使用される前記デジタル署名生成プロトコルが、デジタル署名アルゴリズム(DSA)、楕円曲線DSA(ECDSA)、エルガマル、シュノール、ナイバーグ-リュッペル、ロシア規格GOST　R34.10-2001デジタル署名アルゴリズム、および韓国証明書ベースDSA(KCDSA)プロトコルのうちの1つまたは複数を含む、請求項1に記載の方法。
【請求項４】
前記半決定論的ノンスが、前記メッセージごとの値と、前記鍵導出関数と、前記秘密鍵と、前記メッセージとに基づいて、
連結値を得るために、前記秘密鍵を前記電子デジタル署名生成デバイスのメモリ内の前記メッセージごとの値に連結するステップと、
ハッシュ化メッセージを得るために、前記メッセージにハッシュ関数を適用するステップと、
前記半決定論的ノンスを得るために、前記連結値および前記ハッシュ化メッセージに前記鍵導出関数を適用するステップと
によって得られる、請求項1に記載の方法。
【請求項５】
処理回路を備えるデバイスであって、前記処理回路が、
前記処理回路の半決定論的ノンス生成コンポーネントを使用して半決定論的ノンスを得ることであって、
前記半決定論的ノンスが、完全にランダムなノンスと完全に決定論的なノンスとの間の部分的な量の決定論性を有することによって特徴付けられ、
前記半決定論的ノンスが、デジタル署名を得るためにデジタル署名生成デバイスによって使用されるデジタル署名生成プロトコルに関連付けられた値の全範囲内から完全にランダムに得られるノンスよりも決定論的であり、
前記半決定論的ノンスが、鍵導出関数と、秘密鍵と、メッセージと、前記半決定論的ノンスを結果として生じるように選択されたメッセージごとの値とを使用して得られ、かつ、
前記メッセージごとの値が、前記結果として生じるノンスが完全にランダムではないように、前記デジタル署名を生成するために使用される前記デジタル署名生成プロトコルに関連付けられた値の前記全範囲と比較して値の制限された範囲内でランダムに得られる、半決定論的ノンスを得ることと、
前記処理回路のデジタル署名生成コンポーネントを使用して前記半決定論的ノンスに部分的に基づいてデジタル署名を得ることと、
前記半決定論的ノンスに部分的に基づいて生成された前記デジタル署名を使用してメッセージに署名するために、前記デジタル署名生成デバイスのメッセージ署名コンポーネントを制御することと
を行うように構成された、デバイス。
【請求項６】
前記半決定論的ノンス生成コンポーネントによって使用される前記メッセージごとの値が、秘密ノンスと、公開ノンスと、カウンタと、文脈特定メッセージとのうちの1つまたは複数である、請求項5に記載のデバイス。

【請求項７】
前記ノンスから前記デジタル署名を生成するために前記処理回路の前記デジタル署名生成コンポーネントによって使用される前記デジタル署名生成プロトコルが、デジタル署名アルゴリズム(DSA)、楕円曲線DSA(ECDSA)、エルガマル、シュノール、ナイバーグ-リュッペル、ロシア規格GOST R34.10-2001デジタル署名アルゴリズム、および韓国証明書ベースDSA(KCDSA)プロトコルのうちの1つまたは複数を含む、請求項5に記載のデバイス。
【請求項８】
前記処理回路が、前記メッセージごとの値と、前記鍵導出関数と、前記秘密鍵と、前記メッセージとに基づいて、
連結値を得るために、前記秘密鍵をデジタル署名生成デバイスのメモリ内の前記メッセージごとの値に連結することと、
ハッシュ化メッセージを得るために、前記メッセージにハッシュ関数を適用することと、
前記半決定論的ノンスを得るために、前記連結値および前記ハッシュ化メッセージに前記鍵導出関数を適用することと
によって、前記半決定論的ノンスを得るように構成された、請求項5に記載のデバイス。
【請求項９】
電子デジタル署名生成デバイスであって、
半決定論的ノンスを得るための半決定論的ノンス生成手段であって、
前記半決定論的ノンスが、完全にランダムなノンスと完全に決定論的なノンスとの間の部分的な量の決定論性を有することによって特徴付けられ、
前記半決定論的ノンスが、デジタル署名を得るために前記電子デジタル署名生成デバイスによって使用されるデジタル署名生成プロトコルに関連付けられた値の全範囲内から完全にランダムに得られるノンスよりも決定論的であり、
前記半決定論的ノンスが、鍵導出関数と、秘密鍵と、メッセージと、前記半決定論的ノンスを結果として生じるように選択されたメッセージごとの値とを使用して得られ、かつ、
前記メッセージごとの値が、前記結果として生じるノンスが完全にランダムではないように、前記デジタル署名を生成するために使用される前記デジタル署名生成プロトコルに関連付けられた値の前記全範囲と比較して値の制限された範囲内でランダムに得られる、手段と、
前記半決定論的ノンスに部分的に基づいてデジタル署名を得るためのデジタル署名生成手段と、
前記半決定論的ノンスに部分的に基づいて生成された前記デジタル署名を使用してメッセージに署名するためのメッセージ署名手段と
を備える電子デジタル署名生成デバイス。
【請求項１０】
デジタル署名を得るための電子デジタル署名生成デバイスの少なくとも1つの処理回路の動作を制御するための非一時的機械可読記憶媒体であって、前記非一時的機械可読記憶媒体が、前記少なくとも1つの処理回路によって実行されたとき、前記少なくとも1つの処理回路に、
半決定論的ノンスを得るように前記電子デジタル署名生成デバイスの半決定論的ノンス生成コンポーネントを制御することであって、
前記半決定論的ノンスが、完全にランダムなノンスと完全に決定論的なノンスとの間の部分的な量の決定論性を有することによって特徴付けられ、
前記半決定論的ノンスが、デジタル署名を得るために前記電子デジタル署名生成デバイスによって使用されるデジタル署名生成プロトコルに関連付けられた値の全範囲内から完全にランダムに得られるノンスよりも決定論的であり、
前記半決定論的ノンスが、鍵導出関数と、秘密鍵と、メッセージと、前記半決定論的ノンスを結果として生じるように選択されたメッセージごとの値とを使用して得られ、か

つ、
前記メッセージごとの値が、前記結果として生じるノンスが完全にランダムではないように、前記デジタル署名を生成するために使用される前記デジタル署名生成プロトコルに関連付けられた値の前記全範囲と比較して値の制限された範囲内でランダムに得られる、制御することと、
前記半決定論的ノンスに部分的に基づいてデジタル署名を得るように前記電子デジタル署名生成デバイスのデジタル署名生成コンポーネントを制御することと、
前記半決定論的ノンスに部分的に基づいて生成された前記デジタル署名を使用してメッセージに署名する前記電子デジタル署名生成デバイスのメッセージ署名コンポーネントを制御することと
を行わせる1つまたは複数の命令を有する、非一時的機械可読記憶媒体。
【請求項１１】
連結値を得るために、前記秘密鍵を前記電子デジタル署名生成デバイスのメモリ内の前記メッセージごとの値に連結し、
ハッシュ化メッセージを得るために、前記メッセージにハッシュ関数を適用し、
前記半決定論的ノンスを得るために、前記連結値および前記ハッシュ化メッセージに前記鍵導出関数を適用する
ように前記半決定論的ノンス生成コンポーネントを制御するための命令をさらに含む、請求項10に記載の非一時的機械可読記憶媒体。
【請求項１２】
前記半決定論的ノンスが、前記半決定論的ノンス生成コンポーネントによって、前記デジタル署名生成コンポーネントによって使用される乗算係数(q)に関連付けられた値の全範囲と比較して値の制限された範囲内でランダムまたは擬似ランダムに選択されたメッセージごとの値を使用して得られる、請求項1に記載の方法。
【請求項１３】
前記半決定論的ノンスが、前記半決定論的ノンス生成コンポーネントによって、前記デジタル署名生成コンポーネントによって使用される乗算係数(q)に関連付けられた値の全範囲と比較して値の制限された範囲内でランダムまたは擬似ランダムに選択されたメッセージごとの値を使用して得られる、請求項5に記載のデバイス。
【請求項１４】
前記半決定論的ノンスが、前記半決定論的ノンス生成手段によって、デジタル署名生成コンポーネントによって使用される乗算係数(q)に関連付けられた値の全範囲と比較して値の制限された範囲内でランダムまたは擬似ランダムに選択されたメッセージごとの値を使用して得られる、請求項9に記載の電子デジタル署名生成デバイス。
【請求項１５】
前記デジタル署名生成コンポーネントによって使用される乗算係数(q)に関連付けられた値の全範囲と比較して値の制限された範囲内でランダムまたは擬似ランダムに選択されたメッセージごとの値を使用して前記半決定論的ノンスを得るための命令をさらに含む、請求項10に記載の非一時的機械可読記憶媒体。
【請求項１６】
前記署名されたメッセージを別個のデバイスに送信するように送信機を制御するステップをさらに含む、請求項1に記載の方法。
【請求項１７】
半決定論的ノンスを使用して得られたデジタル署名に基づいて別のデバイスによって署名された署名されたメッセージを受信するステップと、
前記受信した署名されたメッセージを検証するステップと
をさらに含む、請求項1に記載の方法。
【請求項１８】
前記署名されたメッセージを別個のデバイスに送信するために装備された送信機をさらに含む、請求項5に記載のデバイス。

【請求項１９】
半決定論的ノンスを使用して得られたデジタル署名に基づいて別のデバイスによって署名された署名されたメッセージを受信するために装備された受信機をさらに含み、前記処理回路が、前記デジタル署名を検証するように前記デバイスの検証コンポーネントを制御するようにさらに構成された、請求項5に記載のデバイス。
【請求項２０】
前記秘密鍵に関連付けられた公開鍵に基づいて前記別個のデバイスが前記署名されたメッセージを検証したとの確認応答を受信するステップをさらに含む、請求項16に記載の方法。
【請求項２１】
前記秘密鍵に関連付けられた公開鍵に基づいて前記別個のデバイスが前記署名されたメッセージを検証したとの確認応答を受信するステップをさらに含む、請求項18に記載のデバイス。
【請求項２２】
前記署名されたメッセージを別個のデバイスに送信するための手段と、
前記秘密鍵に関連付けられた公開鍵に基づいて前記別個のデバイスが前記署名されたメッセージを検証したとの確認応答を受信するための手段と
をさらに含む、請求項9に記載のデバイス。
【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、内容全体が参照により本明細書に組み込まれる、2014年6月2日に米国特許商標庁に出願した、米国非仮特許出願第14/294,015号の優先権および利益を主張するものである。
【０００２】
様々な特徴は、デジタル署名生成に関し、具体的には、ノンス(nonce)ベースのデジタル署名生成に関する。
【背景技術】
【０００３】
デジタル署名アルゴリズム(DSA:Digital Signature Algorithm)および楕円曲線DSA(ECDSA:Elliptic Curve DSA)などのデジタル署名方式は、ノンス(すなわち、そのような手続きによって使用されるメッセージごとの秘密番号)が異なるメッセージのために再利用される場合、失敗する可能性がある。すなわち、ハッカーまたは悪意のあるエンティティは、デジタル署名で使用される長期秘密鍵を決定する可能性があり、それによって、悪意のあるエンティティが別な方法で有効であるように見える偽の署名を作成することを可能にする。この問題に対処するために、ノンスの決定論的生成が提案されており、この決定論的生成では、ノンスkは、k=HMAC(d,h(m))に従って大まかに生成され、ここで、dは、長期秘密鍵であり、hは、ハッシュ関数であり、mは、署名されるべきメッセージであり、HMACは、ハッシュベースのメッセージ認証コード関数である。各メッセージは、それによって、所与の鍵dのための単一のk値に決定論的につながる。決定論的な方式は、たとえば、T. Porninによる「Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)」、2013年8月に記載されている。決定論的方式の1つの問題は、攻撃者は、そうでなければ攻撃を妨げることになるノイズを減少させるために測定を繰り返すことができるので、特定のサイドチャネル攻撃、たとえば、電力差分解析(DPA(differential power analysis))に秘密鍵を潜在的にさらすことである。
【０００４】
前述の論文へのリクエストフォーコメンツ(RFC:Request for Comments)(すなわち、RFC 6979、ISSN:2070-1721)によれば、攻撃者が、署名動作を実行するのにかかる時間の長さ

、または署名動作の各点において消費される電力などの、実施態様の態様を正確に測定することができるときはいつも、サイドチャネル攻撃は、考慮事項である。したがって、そのようなアルゴリズムの決定論がサイドチャネル攻撃のいくつかの形態における攻撃者に有用である可能性があるので、実施態様は、サイドチャネルを介する秘密鍵の漏洩を避けるために、防御策を使用すべきである。ノンスは、署名オラクルへの呼び出しごとに異なるので、署名を生成するために使用される署名生成演算のべき乗または小数点乗算部分において、DSA(または同様の技術)は、電力、電磁放射、またはタイミングなどのサイドチャネルを利用するDPA型のサイドチャネル解析攻撃の標的にはめったにならないことに留意されたい。その代わり、攻撃者は、攻撃者の能力に関してはるかに制限された、たとえば、サイドチャネルにおけるノイズを減少させるために測定を繰り返すことができない、単純電力解析(SPA:simple power analysis)技法を用いる、ノンスの決定論的生成は、この自然なサイドチャネル耐性を排除または妨げるのを助ける可能性がある。言い換えれば、ノンスの決定論的生成は、デジタル署名技法にける特定の脆弱性を減少させることできるが、他の脆弱性が生じる可能性がある。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】T. Porninによる「Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)」、2013年8月

【発明の概要】

【発明が解決しようとする課題】

【０００６】

したがって、たとえば、デジタル署名を生成する際に使用するための改善されたノンスベースの手続きを提供することが有用であろう。

【課題を解決するための手段】

【０００７】

デジタル署名を得るためのデジタル署名生成デバイスにおいて動作する方法は、デジタル署名生成デバイスを使用して非ランダムかつ非決定論的ノンスを得るステップと、非ランダムかつ非決定論的ノンスに部分的に基づいて、デジタル署名生成デバイスを使用してデジタル署名を得るステップとを含む。

【０００８】

別の態様では、デバイスは、非ランダムかつ非決定論的ノンスを得、非ランダムかつ非決定論的ノンスに部分的に基づいてデジタル署名を得るように構成された処理回路を含む。

【０００９】

さらに別の態様では、デバイスは、非ランダムかつ非決定論的ノンスを得るための手段と、非ランダムかつ非決定論的ノンスに部分的に基づいてデジタル署名を得るための手段とを含む。

【００１０】

依然としてさらに別の態様では、デジタル署名を得るための機械可読記憶媒体が提供され、機械可読記憶媒体は、1つまたは複数の命令を含み、1つまたは複数の命令は、少なくとも1つの処理回路によって実行されたとき、少なくとも1つの処理回路に、非ランダムかつ非決定論的ノンスを得させ、非ランダムかつ非決定論的ノンスに部分的に基づいてデジタル署名を得させる。

【図面の簡単な説明】

【００１１】

【図１】サイドチャネル攻撃の対象となるDSA/ECDSAシステムを示す図である。

【図２】サイドチャネル攻撃の対象となる別の例示的なDSA/ECDSAシステムを示す図であり、システムは、スマートカードリーダを含む。

【図３】例示的な暗号署名デバイスと、署名検証デバイスと、それらの間で交換される情報とを示す図である。
【図４】モバイルデバイスの例示的なシステムオンチップ(SoC)を示す図であり、SoCは、暗号署名デバイスと署名検証デバイスとを有するデジタル署名プロセッサを含む。
【図５】メッセージごとの値(すなわちソルト(salt))を使用して導出されたノンスに基づくデジタル署名生成のための例示的な手続きの概要を提供する図である。
【図６】メッセージごとの値(すなわちソルト)を使用して導出されたノンスに基づいてデジタル署名を生成するための例示的な手続きを示す図である。
【図７】図1～図6のシステム、方法、および装置を利用し得る処理システムを用いる装置のためのハードウェア実施態様の一例を示すブロック図である。
【図８】図7の処理回路の例示的なコンポーネントを示すブロック図である。
【図９】図7の機械可読媒体の例示的な命令コンポーネントを示すブロック図である。
【図１０】ノンスがメッセージごとの値(すなわちソルト)から導出されるデジタル署名生成で使用するための例示的な手続きの別の概要を提供する図である。
【図１１】ノンスが半決定論的に生成されるデジタル署名生成で使用するための例示的な手続きの概要を提供する図である。
【図１２】デジタル署名生成で使用するためのさらなる例示的な手続きを提供する図である。
【発明を実施するための形態】
【００１２】
以下の説明では、本開示の様々な態様の完全な理解を提供するために、具体的な詳細が与えられる。しかしながら、これらの態様が、これらの具体的な詳細なしに実施されてもよいことが、当業者には理解されよう。たとえば、回路は、不必要な詳細で態様を不明瞭にすることを避けるために、ブロック図で示される場合がある。他の事例では、よく知られている回路、構造、および技法は、本開示の態様を不明瞭にしないために、詳細には示されない場合がある。
【００１３】
「例示的」という語は、本明細書では、「例、事例、または例示として役に立つ」ことを意味するために使用される。本明細書に「例示的」として記載された任意の実施態様または態様は、必ずしも本開示の他の態様よりも好ましいまたは有利であると解釈されるべきではない。同様に、「態様」という用語は、本開示のすべての態様が、開示された特徴、利点、または動作モードを含むことを必要としない。
【００１４】
概要
いくつかの新規な特徴は、ノンスベースのデジタル署名生成で使用するためのデバイスおよび方法に関係する。ノンスベースの署名方式の一例は、1991年8月にNational Institute of Standards and Technology(NIST)によって最初に提案された、デジタル署名のための米連符情報処理規格である、上述のDSAである。従来のDSAは、以下のように説明され得る。素数pおよびqを取り、ここで、
【００１５】
【数１】

$$g \in F_p^*$$

【００１６】
は、次数qのものである。dを、ランダムに選ばれ、1≦d<qを満たす長期秘密鍵とする。$y=g^d \bmod p$を公開鍵とする。hは、暗号ハッシュ関数を表す。メッセージmに署名するために、システムは、範囲1≦k≦qの範囲内でランダムに一様にノンスk(すなわち、メッセージごとの秘密番号)を、

$r=g^k \bmod p \bmod q$ (1)
$s=k^{-1}(h(m)+rd) \bmod q$ (2)
を使用して選択し署名(r,s)を計算し、ここで、h(m)は、(少なくともDSPの例では)セキュアハッシュアルゴリズム(SHA(Secure Hash Algorithm))-1またはSHA-2を使用することなどによるmのハッシュである。
【００１７】
ECDSAは、同様であるが、
【００１８】
【数２】

$$F_p^*$$

【００１９】
の楕円曲線上で動作する。ノンスを用いる他のそのような署名方式は、エルガマル(ElGamal)、シュノール(Schnorr)、ナイバーグ-リュッペル(Nyberg-Rueppel)、ロシア規格GOST R34.10-2001デジタル署名アルゴリズム(ここでGOSTは、実質的に「国の規格」を意味するロシアの頭文字である)、および韓国証明書ベースDSA(KCDSA(Korean Certificate-based DSA))を含む。これらの技法では、kが2つの異なるメッセージのために再利用される場合、方式は、すぐに破壊される。すなわち、ノンスkおよび秘密鍵dを決定するためにガウス消去法を用いて解かれ得る2つの未知数を有する2つの式、
$s_1=k\text{-}1(h(m_1)+rd) \bmod q$ (3)
$s_2=k\text{-}1(h(m_2)+rd) \bmod q$ (4)
を得る。
そのようなことは、たとえば、署名するとき、貧弱な暗号技術、またはエントロピーの不足によって実際に起こる可能性がある。この点について、DSAおよびECDSA(および他の同様のノンスベースの署名方式)は、ノンスの高品質なメッセージごとのランダム性の要件のため、実際に壊れる可能性がある。上述したように、解決策が提案されており、その解決策では、kは、以下のようにkを決定論的に本質的に計算して生成される。
$k=HMAC(d,h(m))$ (5)
すなわち、各メッセージは、秘密鍵dのための特定の値を仮定すれば、単一のk値につながる。ここで、HMACは、長期秘密鍵dに適用され、メッセージmのネスト化ハッシュ関数hでkを生じる。したがって、メッセージごとのランダム性は、必要とされない。しかしながら、上記で説明したように、サイドチャネルの脆弱性は、決定論的ノンスで発生する可能性がある。
【００２０】
用語に関する注記:値k(「メッセージごとの秘密番号」または「セッション署名鍵」である)は、本明細書では、利便性および簡潔さのため「ノンス」と呼ばれる。しかしながら、値kの特徴は、機密、一意性、および予測不可能性(すなわちエントロピー)を提供するが、より伝統的なノンスは、これらの属性の各々を提供しない、または必要としないので、値kは、より伝統的なノンスとは異なる。したがって、用語が本明細書で使用される場合、「ノンス」は、少なくとも若干のセキュリティ、一意性、および予測不可能性を提供するデジタル署名生成で使用するためのメッセージごとの秘密番号である。
【００２１】
図1は、サイドチャネル攻撃の対象となる例示的なデジタル署名システム100を示す。簡単に言うと、メッセージ102は、暗号署名デバイス106によって処理され、暗号署名デバイス106は、メッセージに署名するために秘密鍵104を使用してデジタル署名を生成するためにDSAまたはECDSA手続きを用い得る。署名されたメッセージ108は、次いで、一般にセキュリティ保護されていないチャネル109を介して転送され、イエス/ノー検証114をもたらすために公開鍵110を使用してDSAまたはECDSA署名検証デバイス112によって処理される。

署名デバイス106によって使用されるノンスが決定論的である場合、デジタル署名手続きは、電力シグネチャおよびタイミング情報を得るために、電源122によって提供される電力信号120を監視することなどによって、署名デバイス106に関連付けられた電力およびタイミング情報118を監視するサイドチャネル攻撃デバイスまたはシステム116に対して脆弱である可能性があり、秘密鍵を攻撃者または他の悪意のあるエンティティ(たとえば、ハッカー)に潜在的にさらす。逆に、署名デバイス106によって使用されるノンスがランダムに割り当てられる(すなわち、ノンスが完全に非決定論的である)場合、デジタル署名手続きは、ノンスが繰り返されるならば、前述のガウス消去法手続きに対して脆弱である。述べたように、同じノンスが異なるメッセージのために再利用される場合、手続きのセキュリティは、すぐに失敗し、ハッカーが秘密鍵を得ることを可能にする。

【００２２】

図2は、サイドチャネル攻撃の対象となる別の例示的なデジタル署名システム200を示し、攻撃対象のシステムは、1つまたは複数のスマートカード204を受け入れるスマートカードリーダ206である。再び、スマートカードによって用いられるデジタル署名を生成するために使用されるノンスが決定論的である場合、秘密鍵は、潜在的には、電源222によって提供される電力信号220から得られる電力およびタイミング情報218に基づいて(この例では、電力測定オシロスコープ216とサイドチャネルコンピュータ/アナライザ217とを含む)サイドチャネル攻撃システムによって導出される可能性がある。またさらに、この例では、電磁誘導(EMI)信号、音響信号など219が、コンピュータ/アナライザ217による分析のために、適切なセンサーまたは検出器221によって取得され得る。同様の攻撃は、決定論的ノンスが使用される場合、秘密鍵を導出するために、ユニバーサルシリアルバス(USB)デバイス、スマートフォンなどに対して開始され得る。

【００２３】

したがって、一態様では、メッセージごとの値(すなわち、ソルト)v、具体的には、半決定論的ノンス(すなわち、完全に決定論的でも完全にランダムでもないノンス)をもたらすために選択されたソルトに基づいてノンスkを生成するための技法が、本明細書で説明される。従来、「ソルト」は、典型的には、パスワードまたはパスフレーズをハッシュする一方向関数への追加の入力として使用されるランダムデータ値であると考えられることに留意されたい。本明細書では、しかしながら、ソルトという用語は、完全にランダムであるか、完全に決定論的であるか、または、完全にランダムでも完全に決定論的でもない値に設定され得るメッセージごとの値を指す。本明細書に記載の様々な例では、ソルト値(salt value)は、半決定論的ノンス(semi-deterministic nonce)を生成するように設定され、ここで、「半決定論的(semi-deterministic)」は、本明細書では、完全にランダム(fully random)と完全に決定論的(fully deterministic)との間の決定論の部分的な程度を有することによって特徴付けられるものとして定義される。他の例では、しかしながら、ソルトは、完全にランダムなノンスをもたらすように完全にランダムな値に設定され得る。ソルトはまた、完全に決定論的なノンスをもたらすように空の文字列に設定され得る。半決定論的は、半ランダムとも呼ばれ得る。

【００２４】

さらに、ソルトvは、制限されたまたは制約された値の範囲内でランダムに得られ得る。そのようなソルトは、完全にランダムではない。したがって、(ノンスからデジタル署名を生成するために使用されるデジタル署名生成プロトコルに関連付けられた値の完全な範囲と比較すると)値の制限された範囲内でランダムに得られたソルト値を使用して得られたノンスは、完全に決定論的でも完全にランダムでもなくなるので、本明細書では、半決定論的ノンスであると考えられる。本明細書に記載の例は、ソルトから導出されるノンスを含み、ソルトは、はるかにより大きい数の許容値からではなく、32ビットの値のみの中から「ランダムに」選択される。依然としてさらに、本明細書では、非ランダムノンスの「非ランダム性」は、少なくとも部分的に決定論的であり、完全にランダムではないことによって特徴付けられる。非決定論的ノンスの「非決定論性」は、少なくとも部分的にランダムであり、完全に決定論的ではないことによって特徴付けられる。

【００２５】
1つの特定の例では、ノンスkは、以下のように生成され(ここで、||は、連結を示す)、
k=HMAC(d||v,h(m)) (6)
ここでh(m)は、メッセージmのハッシュであり、dは、長期鍵であり、vは、ソルトである。ソルトは、たとえば、秘密ノンス、公開ノンス、カウンタ、文脈特定メッセージ、または空の文字列のうちの1つまたは複数であり得る(ここで、秘密ノンスおよび公開ノンスは、必ずしも前述のkについての考慮事項の対象ではない従来のノンスであり得る)。メッセージごとのソルト値vが空の文字列である場合、式は、式5の決定論的手法に戻ることに留意されたい。そのように、署名方式は、ノンスの再利用に対する機密を維持するが、サイドチャネルセキュリティを潜在的に失うことになる。vが許容値の全範囲からランダムかつ一様に選ばれる場合、方式は、完全に非決定論的であり、したがって、その他の点で(ノンスの再利用に対して脆弱な)DSAなどの従来の非決定論的デジタル署名技法の特性を維持する。ソルトがカウンタまたは文脈特定メッセージである場合などの、メッセージごとのソルト値vが非ランダムかつ非決定論的である場合には、式6は、半決定論的ノンスkを提供し、半決定論的ノンスkは、一般的に、導入された非決定論性により、(ノンスの再利用も回避しながら)サイドチャネル攻撃を非常に困難にする。この点について、(a)カウンタが用いられるとき、署名されるべき所与のメッセージmは、同じノンスkに決定論的につながらず、依然として(b)カウンタは、ランダムではなく、したがって完全には非決定論的ではないので、カウンタは、半決定論的である。同様に、(a)文脈特定メッセージは、文脈に基づいて変化するので、所与のメッセージmは、同じノンスkに決定論的につながらず、依然として(b)文脈特定メッセージは、ランダム値ではなく、したがって完全には非決定論的ではないので、文脈特定メッセージは、半決定論的である。(メッセージごとのソルト値vとして使用される)秘密ノンスまたは公開ノンスは、同様に、そのような値が完全にランダムでも完全に決定論的でもない限り、半決定論的である。公開ノンスは、プロトコルメッセージにおいて、たとえば、「client hello」トランスポート層セキュリティ(TLS(Transport Layer Security))メッセージにおいてすでに提供され得る。

【００２６】
また、(ノンスがランダムに得られる値の範囲が、ノンスの再利用が実際上の問題にならないほど大きい場合など)デジタル署名生成システムが、ノンスの再利用が問題にならない状況では、メッセージごとのソルト値vに基づいてノンスkを生成することは、デジタル署名生成システムがランダムなノンスを便利に用いることを可能にする。同様に、サイドチャネル攻撃が問題にならない状況では、メッセージごとのソルト値vに基づいてノンスkを生成することは、デジタル署名生成システムが完全に決定論的なノンスを便利に用いることを可能にする。すなわち、メッセージごとのソルト値vの使用は、単一のデジタル署名生成システムが、全体のセキュリティニーズに応じたvの選択に基づいて、決定論的、半決定論的、または完全に非決定論的な属性を便利に利用することを可能にする。本明細書では一般的に、関数v=s(x)は、半決定論的ノンスkを生成する際に使用するための半決定論的なメッセージごとのソルト値vを(いくらかの入力文字列、値、または他の関数xから)生成するか、または他の方法で得るための任意の関数、手続き、またはアルゴリズムを表すために使用され得る。当業者が理解できるように、多種多様な半決定論的関数s(x)が、本明細書における一般的な技法に従って提供され得る。また、「得る」という用語は、たとえば、計算する、演算する、生成する、取得する、受信する、回収する、入力する、または他の適切な対応するアクションを実行することを広くカバーする。

【００２７】
図3は、暗号署名デバイス302および署名検証デバイス304の例示的な動作を示すタイミング図300を提供する。処理は、305において、暗号署名デバイス302が(すでに確立されている公開/秘密鍵対y、dの)秘密鍵dを入力し、たとえば、秘密ノンス、公開ノンス、カウンタ、文脈特定メッセージ、またはからの文字列、すなわち、非ランダムかつ非決定論的なソルトとして、メッセージごとのソルト値vを得ることで開始する。秘密鍵dは、たとえば、暗号署名デバイス302の記憶デバイスから入力され得、記憶デバイスでは、秘密鍵dは

、署名検証デバイス304による(併せて、いくつかの例では、図示しない信頼機関デバイスまたは認証機関デバイスによる)初期公開鍵/秘密鍵生成および交換手続き(図示せず)の後、保存されている。DSAベースの例では、p、q、およびgを含む特定のグローバルパラメータが用いられ、ここで、pは、素数であり、gは、群生成器(group generator)であり、qは、群位数(および、gの乗法的位数(multiplicative order))である。例示的なDSAの例では、pは、素数であり、ここで、512≦L≦1024について$2^{L-1}<p<2^{L}$であり、Lは、64の倍数である(すなわち、512ビットと1024ビットとの間のビット長が、64ビット単位Nで使用される)。しかしながら、Lは、たとえば、256の単位(N)で3072以上までのように、より長くてもよい。Lが512≦L≦1024の範囲内である例示的なDSAの例では、qは、q-1の素因数であり、ここで、$2^{159}<q<2^{160}$である(すなわち、160ビットのビット長が使用される)。その例示的な例では、$g=h^{(p-1)/q} \bmod p$であり、ここで、hは、$h^{(p-1)/q} \bmod p>1$であるように$1<h<(p-1)$である任意の整数である。秘密鍵dは、0<d<qであるランダムまたは擬似ランダムな整数である。公開鍵yは、$g^{d} \bmod p$である。これは、いくらかの背景情報を提供するDSPパラメータの1つの例示的な例である。実際には、様々な値は、異なって選ばれ得る。当業者は、特定の用途のためのp、qのビット長およびハッシュ関数を選択することに精通している。依然としてさらに、ECDSAのためのパラメータの選択は、まったく異なることに留意されたい。

【００２８】

306では、暗号署名デバイス302は、メッセージごとのソルト値v、秘密鍵d、およびメッセージmから、たとえば、

$k=HMAC(d||v,h(m))$ (7)

または

$k=HMAC(v||d,h(m))$ (8)

を使用してノンスkを生成する。

HMAC以外の鍵導出関数が用いられ得るが、HMACが便利であることに留意されたい。ソルトvを秘密鍵と連結することは、HMAC関数が変更される必要がないように、連結結果が(メッセージmのハッシュとともに)HMACの2つの入力パラメータのうちの1つとして適用されることを可能にする。さらに、HMACは、任意の長さのパラメータを受け入れることができ、したがって、HMACは、それによって長さに関係なく結果を受け入れることができるので、連結は、ソルトと秘密鍵とをコーミングするために特に便利である。さらに、連結されたソルト/秘密鍵でのHMACの使用は、一般的に相互使用可能な方式を提供し、それによって、デジタル信号生成、署名、およびその後の検証の全体的な数学は、一般的に、そうではない従来のノンスベースの技法と同じである。選ばれた関数が、悪意のあるエンティティが利用し得る情報の漏洩をもたらさない限り、連結以外の関数がソルトおよび秘密鍵を結合するために代わりに使用され得ることにも留意されたい。例として、ソルトおよび秘密鍵の排他的論理和をとることは、サイドチャネル情報を漏洩する可能性があり、したがって、推奨されない。

【００２９】

308では、暗号署名デバイス302は、たとえば、

$r=g^{k} \bmod p \bmod q$ (9)

および

$s=k^{-1}(h(m)+rd) \bmod q$ (10)

を使用して、ノンスkに部分的に基づいてデジタル署名(r,s)を生成し、メッセージmに署名し、ここで、上記で論じたように、pは、素数であり、qは、群位数であり、gは、群生成器である。

【００３０】

310では、暗号署名デバイス302は、デジタル署名(r,s)で署名されたメッセージmを、署名検証デバイス304を有する遠隔または外部システムに送信する。多くの場合、メッセージmはまた、暗号化されることになるが、そのような暗号化は、本明細書で論じるデジタル署名生成手続きとは別であり、異なり得ることに留意されたい。312では、署名検証デ

バイス304は、公開鍵yを得、314では、公開鍵yを使用してメッセージmの署名(r,s)を検証する。公開鍵は、たとえば、暗号署名デバイス302による初期鍵交換手続き後にそこに記憶されている場合、署名検証デバイス304の記憶デバイスから得られ得る(または、たとえば、認証機関のサーバから得られ得る)。316では、署名検証デバイス304は、次いで、署名(r,s)が検証された場合、メッセージmを出力するか、または他の方法で処理する。DSAベースの例では、検証は、$w=(s')^{-1}\mathrm{mod}q$、u1=[h(m')w]mod q、u2=(r')w mod q、および$v=[(g^{u1}y^{u2})\mathrm{mod}\ p]\mathrm{mod}\ q$のように値w、u1、u2、およびvを計算することによって実行され得、ここで、s'、r'、およびm'は、r、s、およびmの受信されたバージョンを表す。署名検証デバイスは、次いで、v=r'を検証する。

【００３１】

例示的なシステムオンチップハードウェア環境

本明細書に記載のデジタル署名の署名および検証システムおよび手続きは、広範囲のデバイス内で、および広範囲の用途のために利用され得る。具体的な例を提供するために、署名コンポーネントと検証コンポーネントの両方を有するデジタル署名プロセッサがモバイル通信デバイスまたは他のアクセス端末内で使用するためのSoC処理回路上に設けられた例示的なハードウェア環境をここで説明する。この点について、モバイルデバイスは、非対称鍵暗号化(すなわち、公開鍵暗号化)のための十分な計算リソースを欠いているように従来見られているが、モバイルデバイスは、ますますより強力なプロセッサとより大量のメモリとを提供されている。十分なリソースにより、非対称鍵生成、署名、および検証は、そのようなデバイス内で提供され得る。デジタル署名の署名および検証システムおよび手続きが実装され得る他の例示的なハードウェア環境は、他の通信デバイスおよびコンポーネント、および、それらで使用するための周辺デバイスなど、ならびに、インターネットに接続された従来のデスクトップコンピュータおよび(商品またはサービスのオンライン購入を容易にするために、インターネットベースの商業ベンダーによって用いられ得るような)取引サーバを含む。全体的な手続きの態様はまた、たとえば、鍵交換を容易にするために、信頼機関サーバを利用し得る。

【００３２】

図4に、様々な新規の特徴を活用できる一例による、モバイル通信デバイスのSoC処理回路400を示す。このSoC処理回路は、Qualcomm Incorporated社のSnapdragon(商標)処理回路とすることができる。SoC処理回路400は、アプリケーション処理回路410を含み、アプリケーション処理回路410は、デジタル署名署名デバイス415とデジタル署名検証デバイス417とを有するデジタル署名プロセッサ413と協働して動作するように装備されたマルチコアCPU412を含む。デジタル署名署名デバイス415は、オンライン商取引サーバ(図示せず)などの遠隔システムに送られるべきデジタル署名メッセージのために使用され得る。署名検証デバイス417は、(モバイル通信デバイスが、受信したメッセージの署名を検証することを必要とするアプリケーション、すなわち、「アプリ」を実行する場合に必要とされ得るように)遠隔デバイスから受信したデジタル署名を検証するために使用され得る。他の例では、デジタル署名プロセッサ413は、デジタル署名署名デバイス415のみ、または、いくつかの場合には、デジタル署名検証デバイス417のみを含み得る。すなわち、両方のコンポーネントは、必要ではない。

【００３３】

アプリケーション処理回路410は、通常、モバイル通信デバイスのすべてのコンポーネントの動作を制御する。一態様では、アプリケーション処理回路410は、内部共有ハードウェア(HW)リソース430の一部を形成する内部共有記憶デバイス432の鍵記憶要素433における公開鍵および秘密鍵の記憶を含むデータの記憶を制御するためのホスト記憶コントローラ450に結合される。アプリケーション処理回路410は、SoC処理回路400の様々なコンポーネントのためのブートシーケンス命令を記憶するブートROM418をも含むことができる。SoC処理回路400は、アプリケーション処理回路410によって制御される1つまたは複数の周辺サブシステム420をさらに含む。周辺サブシステム420は、ストレージサブシステム(たとえば、読取専用メモリ(ROM)、ランダムアクセスメモリ(RAM))、ビデオ/グラフィックス

サブシステム(たとえば、デジタル信号処理回路(DSP)、グラフィックス処理回路ユニット(GPU))、オーディオサブシステム(たとえば、DSP、アナログ-デジタル変換器(ADC)、デジタル-アナログ変換器(DAC))、電力管理サブシステム、セキュリティサブシステム(たとえば、他の暗号化コンポーネントおよびデジタル著作権管理(DRM)コンポーネント)、入出力(I/O)サブシステム(たとえば、キーボード、タッチスクリーン)、ならびに有線およびワイヤレスの接続性サブシステム(たとえば、universal serial bus(USB)、全地球測位システム(GPS)、Wi-Fi、Global System Mobile(GSM(登録商標))、符号分割多元接続(CDMA)、4G Long Term Evolution(LTE)モデム)を含むことができるが、これに限定されない。モデムサブシステムである例示的な周辺サブシステム420は、DSP422、様々な他のハードウェア(HW)およびソフトウェア(SW)コンポーネント424、ならびに様々なラジオ周波数(RF)コンポーネント426を含む。一態様では、各周辺サブシステム420は、関連する周辺サブシステム420のプライマリブートイメージ(図示せず)を記憶するブートROM428をも含む。

【００３４】

前述のように、SoC処理回路400は、さらに、内部共有ストレージ432(たとえば、スタティックRAM(SRAM)、フラッシュメモリなど)などの様々な内部共有HWリソース430を含み、内部共有ストレージ432は、様々なランタイムデータまたは他のパラメータを記憶するため、およびホストメモリを提供するために、アプリケーション処理回路410および様々な周辺サブシステム420によって共有される。図4の例では、内部共有ストレージ432は、公開鍵と秘密鍵とを記憶するために使用され得る、前述の鍵記憶要素、部分、またはコンポーネント433を含む。他の例では、鍵は、モバイルデバイスの他の場所に記憶される。

【００３５】

一態様では、SoC400のコンポーネント410、418、420、428、および430は、シングルチップ基板上に集積される。SoC処理回路400は、異なるチップ基板上に配置され得、1つまたは複数のバスを介してSoC処理回路400と通信することができる、様々な外部共有HWリソース440をさらに含む。外部共有HWリソース440は、たとえば、外部共有ストレージ442(たとえば、ダブルデータレート(DDR)ダイナミックRAM)および/または永久的もしくは半永久的データストレージ444(たとえば、セキュアデジタル(SD)カード、ハードディスク(HDD)、埋込み型マルチメディアカード、ユニバーサルフラッシュデバイス(UFS:universal flash device)、など)を含み得、それらは、オペレーティングシステム(OS)情報、システムファイル、プログラム、アプリケーション、ユーザデータ、オーディオ/ビデオファイル、などの様々なタイプのデータを記憶するために、アプリケーション処理回路410および様々な周辺サブシステム420によって共有され得る。SoC処理回路400を組み込んだモバイル通信デバイスが活性化されると、SoC処理回路は、システムブートアッププロセスを開始し、システムブートアッププロセスでは、アプリケーション処理回路410は、様々な周辺サブシステム420のためのブートシーケンス命令を含むSoC処理回路400のためのブート命令を取得するために、ブートROM418にアクセスし得る。周辺サブシステム420は、追加の周辺ブートRAM428を有することもできる。

【００３６】

例示的なデジタル署名の署名および検証手続き

図5は、図4のアプリケーション処理回路のデジタル署名プロセッサ、または、他の適切な装備されたコンポーネント、デバイス、システム、もしくは処理回路によって用いられ得るデジタル署名の署名および検証動作500の概要を提供する。502では、デジタル署名プロセッサは、メッセージごとのソルト値vを得、ここで、vは、半決定論的ノンスをもたらすように選択または制約される。504では、デジタル署名プロセッサは、メッセージごとのソルト値vと、鍵導出関数Fと、秘密鍵dと、署名されるべきメッセージmとに基づいて、半決定論的ノンスkを生成する。506では、デジタル署名プロセッサは、半決定論的ノンスkと、署名されるべきメッセージmとに基づいて、デジタル署名(r,s)を生成する。508では、デジタル署名プロセッサは、デジタル署名(r,s)を付加することによって、メッセージmに署名する。510では、デジタル署名プロセッサは、オンライン商取引サーバなどの遠隔デバイスに、署名されたメッセージmを送信し、遠隔デバイスは、次いで、秘密鍵dに関連

付けられた公開鍵yに基づいて、署名されたメッセージの署名を検証することを試みる(ここで、公開鍵は、リモートデバイスと以前に交換されている)。すでに述べたように、多くの場合、メッセージmはまた、暗号化されることになり、そのような暗号化は、本明細書で論じるデジタル署名生成手続きとは別であり、異なり得る。512では、デジタル署名プロセッサは、遠隔デバイスが署名されたメッセージmを公開鍵yに基づいて検証しことの確認を受信し、または、署名が検証されなかった場合にエラーメッセージを受信する。図5の手続きは、一般的には、ソルトを使用して導出されたノンスを利用するように変更された、DSA/ECDSAまたは他のノンスベースのデジタル署名規格およびプロトコルに従って実行され得る。

【００３７】

図6は、さらなる例示的な詳細が提供されるソルトから導出されたノンスに基づいてデジタル署名を生成するための例示的な手続き600を示す。602では、デジタル署名プロセッサは、非ランダムかつ非決定論的なノンス(すなわち、半決定論的ノンス)をもたらすのに十分なメッセージごとのソルト値vを得、ここで、たとえば、ソルトvは、秘密ノンス、公開ノンス、カウンタ、文脈特定メッセージ、空のストリング、もしくは、任意の適切な半決定論的関数s(x)の結果であり、または、ソルトは、結果として生じるノンスが完全にランダムではないように、(ノンスからデジタル署名を生成するために使用されるデジタル署名生成プロトコルに関連付けられた値の全範囲と比較して)値の制限された範囲内でランダムに得られる。この点について、デジタル署名プロセッサは、たとえば、結果として生じるノンスkにより大量の非決定論性を与えるために、単なるカウンタよりも文脈特定メッセージを用い得る。さらにより大量の非決定論性を得るために、デジタル署名プロセッサは、たとえば、文脈特定メッセージよりも秘密ノンスを用い得、ここで、秘密ノンスは、文脈特定メッセージと比較してより大きい程度の非決定論性を提供する。前述のように、デジタル署名プロセッサは、値の制限された範囲内からランダムにソルトを得得る。この点について、DSAは、従来は、1からq-1までからkを均一かつランダムに取るように動作し、ここで、qは、(256ビット程度の)生成器からの乗法的位数である。したがって、602では、メッセージごとのソルト値vは、値のはるかにより小さいセット内からランダムに選択され得る(たとえば、32ビット値のみの中から均一かつランダムに選択され得る)。一般的に、半決定論的関数s(x)は、それによって結果として生じるノンスkの非決定論性の程度を設定、調整、または制御するために、結果として生じるメッセージごとのソルト値vの非決定論性の程度を設定、調整、または制御するように選ばれ、もしくは選択され得る。

【００３８】

604では、デジタル署名プロセッサは、メッセージごとのソルト値vと、HMAC鍵導出関数と、秘密鍵dと、署名されるべきメッセージmとに基づいて、たとえば、連結値をもたらすために秘密鍵dをメッセージごとのソルト値vに連結し、ハッシュ化メッセージh(m)をもたらすためにメッセージmにハッシュ関数hを適用し、ノンスkをもたらすために連結値およびハッシュ化メッセージにHMAC関数を適用することによって、ノンスkを生成し

$$k=HMAC(d||v,h(m)) \quad (11)$$

または

$$k=HMAC(v||d,h(m)) \quad (12)$$

となる。

【００３９】

606では、デジタル署名プロセッサは、ノンスkに部分的に基づいてデジタル署名(r,s)を生成し、たとえば、DSA手続きを使用してメッセージmに署名し、

$$r=g^k \bmod p \bmod q \quad (13)$$

および

$$s=k^{-1}(h(m)+rd) \bmod q \quad (14)$$

となり、ここで、(上記で論じたように)pは、素数であり、qは、群位数であり、gは、群生成器であり、または、ECDSA、エルガマル、シュノール、ナイバーグ-リュッペル、ロシ

ア規格GOST R34.10-2001デジタル署名アルゴリズム、および韓国証明書ベースDSA(KCDSA)などの他のノンスベースの手続きを使用してメッセージmに署名する。

【００４０】

例示的なシステムおよび方法

図7に、図1～図6のシステム、方法、および装置を実施することができる全体的なシステムまたは装置700を示す。本開示の様々な態様によれば、要素、要素の何らかの部分、または要素の何らかの組合せを、図4のSoC処理回路などの1つまたは複数の処理回路704を含む処理システム714を用いて実施することができる。たとえば、装置700を、モバイル通信システムのユーザ機器(UE)とすることができる。装置700を、無線ネットワークコントローラ(RNC)とともに使用することができる。SoCに加えて、処理回路704の例は、マイクロプロセッシング回路、マイクロコントローラ、デジタル信号処理回路(DSP)、フィールドプログラマブルゲートアレイ(FPGA)、プログラマブル論理デバイス(PLD)、状態機械、ゲートロジック(gated logic)、個別のハードウェア回路、および本開示全体にわたって記述される様々な機能性を実行するように構成された他の適切なハードウェアを含む。すなわち、処理回路704は、装置700内で利用されるように、デジタル署名の生成、署名、および検証を実行するプロセスなどの、上記で説明し、図3、図5、および図6に示すプロセス(および、図10～図12に示すもの)のうちの任意の1つまたは複数を実施するために使用され得る。

【００４１】

図7の例では、処理システム714を、全般的にバス702によって表されるバスアーキテクチャを用いて実施することができる。バス702は、処理システム714の特定の応用例および全体的な設計制約に依存して、任意の個数の相互接続するバスおよびブリッジを含むことができる。バス702は、1つまたは複数の処理回路を含む様々な回路(全般的に処理回路704によって表される)、記憶デバイス705、および機械可読、プロセッサ可読、処理回路可読、またはコンピュータ可読の媒体(全般的に、非一時的機械可読媒体706によって表される)をリンクする。バス702は、タイミングソース、周辺機器、電圧レギュレータ、および電力管理回路などの様々な他の回路をもリンクすることができ、これらの他の回路は、当技術分野で周知であり、したがって、これ以上は説明しない。バスインターフェース708は、バス702とトランシーバ710との間のインターフェースを提供する。トランシーバ710は、伝送媒体を介して様々な他の装置と通信するための手段を提供する。装置の性質に依存して、ユーザインターフェース712(たとえば、キーパッド、ディスプレイ、スピーカ、マイクロホン、ジョイスティック)を提供することもできる。

【００４２】

処理回路704は、バス702の管理と、機械可読媒体706上に記憶されたソフトウェアの実行を含む全般的な処理との責任を負う。ソフトウェアは、処理回路704によって実行されるときに、処理システム714に、任意の特定の装置について本明細書で説明される様々な機能を実行させる。機械可読媒体706は、ソフトウェアを実行するときに処理回路704によって操作されるデータを記憶するのにも使用され得る。

【００４３】

処理システム内の1つまたは複数の処理回路704は、ソフトウェアまたはソフトウェアコンポーネントを実行することができる。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、または他のいずれとして呼ばれる場合であっても、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアモジュール、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行可能ファイル、実行のスレッド、手続き、関数、その他を意味するものとして幅広く解釈されなければならない。処理回路は、タスクを実行し得る。コードセグメントは、手続き、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または、命令、データ構造、もしくはプログラム文の任意の組合せを表し得る。コードセグメントは、情報、データ、引数、パラメータを、ま

たはメモリもしくはストレージの内容を渡すおよび/または受け取ることによって、別のコードセグメントまたはハードウェア回路に結合され得る。情報、引数、パラメータ、データなどを、メモリ共有、メッセージパッシング、トークンパッシング、ネットワーク伝送などを含む任意の適切な手段を介して渡し、転送し、または伝送することができる。

【００４４】

ソフトウェアは、機械可読媒体706上に存在することができる。機械可読媒体706は、非一時的機械可読媒体とすることができる。非一時的な処理回路可読、機械可読、またはコンピュータ可読の媒体は、たとえば、磁気記憶デバイス(たとえば、ハードディスク、フロッピディスク、磁気ストリップ)、光ディスク(たとえば、コンパクトディスク(CD)またはデジタル多用途ディスク(DVD))、スマートカード、フラッシュメモリデバイス(たとえば、カード、スティック、またはキードライブ)、RAM、ROM、プログラマブルROM(PROM)、消去可能PROM(EPROM)、電気的消去可能PROM(EEPROM)、レジスタ、リムーバブルディスク、ハードディスク、CD-ROM、ならびに機械またはコンピュータによってアクセスされ読み取られ得るソフトウェアおよび/または命令を記憶する任意の他の適切な媒体を含む。「機械可読媒体」、「コンピュータ可読媒体」、「処理回路可読媒体」、および/または「プロセッサ可読媒体」という用語は、ポータブルまたは固定式の記憶デバイス、光学記憶デバイス、ならびに命令および/またはデータを記憶し、含み、または担持することのできる様々な他の媒体などの非一次的媒体を含むことができるが、これに限定されない。したがって、本明細書で説明される様々な方法を、「機械可読媒体」、「コンピュータ可読媒体」、「処理回路可読媒体」、および/または「プロセッサ可読媒体」内に記憶され、1つまたは複数の処理回路、機械、および/またはデバイスによって実行され得る命令および/またはデータによって完全にまたは部分的に実施することができる。機械可読媒体は、たとえば、搬送波、伝送線、およびコンピュータによってアクセスされ、読み取られ得るソフトウェアおよび/または命令を伝送するための任意の他の適切な媒体をも含むことができる。

【００４５】

機械可読媒体706は、処理システム714内に、処理システム714の外部に存在し、あるいは、処理システム714を含む複数のエンティティにまたがって分散され得る。機械可読媒体706を、コンピュータプログラム製品内で実施することができる。たとえば、コンピュータプログラム製品は、パッケージング材料内に機械可読媒体を含むことができる。当業者は、特定の応用例およびシステム全体に課せられる全体的な設計制約に依存して、本開示全体で提示される説明される機能性をどのようにして最もよく実施すべきかを認めるであろう。たとえば、機械可読媒体706は、処理回路704によって実行されたとき、処理回路に、非ランダムかつ非決定論的なノンスを得させ、非ランダムかつ非決定論的なノンスに部分的に基づいてデジタル署名を得させる1つまたは複数の命令を有し得る。

【００４６】

機能は図面に示す1つまたは複数のコンポーネント、ステップ、特徴、および/または機能は、単一のコンポーネント、ブロック、特徴もしくは機能に再配置および/または結合され、複数のコンポーネント、ステップもしくは機能に具現化され得る。追加の要素、コンポーネント、ステップ、および/または機能はまた、本開示から逸脱することなく、追加され得る。図に示す装置、デバイス、および/またはコンポーネントは、図に記載した方法、特徴、またはステップのうちの1つまたは複数を実行するように構成され得る。また、本明細書で説明したアルゴリズムは、効率的にソフトウェアに実装されてもよく、かつ/またはハードウェアに組み込まれてもよい。

【００４７】

本明細書に開示した例に関連して説明した様々な例示的な論理ブロック、モジュール、回路、要素、および/またはコンポーネントは、汎用処理回路、デジタル信号処理回路(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コンポーネント、個別ゲートもしくはトランジスタロジック、個別のハードウェアコンポーネント、または、本明細書に記載の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。汎用処理回路は、マイクロプロセッシング回路とすることができるが、代替案では、処理回路を、何らかの従来の処理回路、コントローラ、マイクロコントローラ、または状態機械とすることができる。処理回路はまた、コンピューティングコンポーネントの組合せとして、たとえば、DPSおよびマイクロプロセッシング回路の組合せ、いくつかのマイクロプロセッシング回路、DSPコアと併せた1つもしくは複数のマイクロプロセッシング回路、または任意の他のそのような構成として実装され得る。

【００４８】

したがって、本開示の一態様では、図4および図7に示す処理回路413および/または704は、図3、図5、および/もしくは図6(ならびに/または、以下で論じる図10、図11、および/もしくは図12)に記載のアルゴリズム、方法、および/またはブロックを実行するために特別に設計されたおよび/または結線された専用処理回路(たとえば、ASIC)であり得る。したがって、そのような専用処理回路(たとえば、ASIC)は、図3、図5、および/もしくは図6(ならびに/または、以下で論じる図10、図11、および/もしくは図12)に記載のアルゴリズム、方法、および/またはブロックを実行するための手段の一例であり得る。機械可読記憶媒体は、専用処理回路(たとえば、ASIC)によって実行されたとき、専用処理回路に、本明細書に記載のアルゴリズム、方法、および/またはブロックを実行させる命令を記憶し得る。

【００４９】

図8は、デジタル署名生成器804とデジタル署名検証器806とを有するデジタル署名プロセッサ802を有する処理回路704の選択された例示的なコンポーネントを示す。具体的には、図8のデジタル署名生成器804は、半決定論的ノンスを生成する際に使用するためのメッセージごとのソルト値vを得るまたは生成するように動作可能なソルト生成モジュール/回路808を含む。デジタル署名生成器804はまた、デジタル署名を生成する際に使用するための半決定論的ノンスkを得るもしくは生成するように、または、そのような動作を達成するために他のモジュール/回路を制御するように動作可能な非ランダムかつ非決定論的ノンス生成モジュール/回路810を含む。たとえば、連結モジュール/回路812は、連結値をもたらすために秘密鍵をソルトに連結するように動作可能であり、ここで、秘密鍵は、(擬似乱数生成器(PRNG)を含み得る)秘密鍵入力モジュール/回路814によって得られ得る。ハッシュ関数モジュール/回路816は、ハッシュ化メッセージをもたらすために、署名されるべきメッセージにハッシュ関数を適用するように動作可能である。鍵導出関数(HMAC)モジュール/回路816は、ノンス生成モジュール/回路810の制御下でノンスをもたらすために、連結値およびハッシュ化メッセージにHMACなどの鍵導出関数を適用するように動作可能である。デジタル署名生成モジュール/回路820は、ノンス生成モジュール/回路810によって(またはその制御下で)生成されたノンスに部分的に基づいてデジタル署名を生成するように動作可能である。メッセージ署名モジュール/回路822は、次いで、たとえば、図7のトランシーバ710に接続され得る署名/メッセージ送信/受信モジュール/回路828を使用して遠隔デバイスに送信するためのメッセージにデジタル署名で署名するように動作可能である。

【００５０】

デジタル署名を使用してメッセージに署名することは、単にメッセージに署名を付加する単純なことであり得、したがって、実際的な実施態様では、別個のメッセージ署名モジュール/回路は、設けられなくてもよい。さらに、実施的な実施提要では、デジタル署名生成器全体は、デジタル署名を使用してメッセージに署名するのに役立つので、メッセージ署名モジュールと呼ばれ得る。別々の署名生成コンポーネントおよびメッセージ署名コンポーネントは、必要とされないが、完全性および一般性のために別々に示されている。デジタル信号プロセッサ802が遠隔デバイスから受信した署名を検証することを必要とする場合、公開鍵入力モジュール/回路824は、(図7のトランシーバ710を介して)公開鍵を入力または別の方法で得る。署名検証モジュール/回路826は、次いで、公開鍵を使用して遠隔デバイスから受信した署名されたメッセージの署名を検証するために動作可能である。

【００５１】
図9は、デジタル署名を生成または検証する際に使用するための機械またはコンピュータ可読媒体706の選択された例示的な命令を示す。簡単に言えば、図9の機械可読媒体706は、様々な命令を含み、様々な命令は、図7の処理回路704によって実行されたとき、処理回路に、デジタル署名の生成および検証動作を制御または実行させる。具体的には、図9のデジタル署名生成命令904は、ノンスを生成する際に使用するためのメッセージごとのソルト値vを得るまたは生成するように動作可能なソルト生成命令908を含む。非ランダムかつ非決定論的ノンス生成命令910は、デジタル署名を生成する際に使用するための半決定論的ノンスkを得るまたは生成するように動作可能である。連結命令912は、連結値をもたらすために秘密鍵をソルトに連結するように動作可能であり、ここで、秘密鍵は、秘密鍵入力命令914によって得られ得る。ハッシュ関数命令916は、ハッシュ化メッセージをもたらすために、署名されるべきメッセージにハッシュ関数を適用するように動作可能である。鍵導出関数(HMAC)命令918は、ノンスをもたらすために連結値およびハッシュ化メッセージにHMACなどの鍵導出関数を適用するように動作可能である。デジタル署名生成命令920は、ノンス生成命令910によって(またはその制御の下で)生成されたノンスに部分的に基づいてデジタル署名を生成するように動作可能である。メッセージ署名命令922は、次いで、たとえば、署名/メッセージ送信/受信命令928を使用して遠隔デバイスに送信するためのメッセージにデジタル署名を署名するように動作可能である。図8のモジュール822を参照して上述したコメントは、ここでも適用可能である。デジタル信号プロセッサが遠隔デバイスから受信した署名を検証することを必要とする場合、公開鍵入力命令924は、(図7のトランシーバ710を介して)遠隔デバイスから公開鍵を入力するまたは別の方法で得る。署名検証命令926は、次いで、公開鍵を使用して、遠隔デバイスから受信した署名されたメッセージの署名を検証するように動作可能である。
【００５２】
図10は、図8のデジタル署名生成器804、または、図4のアプリケーション処理回路410などのデジタル署名を生成するか、または別の方法で得るための他の適切に装備されたデジタル署名生成デバイスによって実行され得る方法または手続き1000を概括的に示し、要約する。1002では、デジタル署名生成器は、非ランダムかつ非決定論的ノンスを得、1004では、デジタル署名生成器は、たとえば、上記で説明した技法を使用して、非ランダムかつ非決定論的ノンスに部分的に基づいてデジタル署名を得る。
【００５３】
図11は、図8のデジタル署名プロセッサ802または他の適切に装備されたデバイスによって実行され得る例示的な方法または手続き1100を示す。1102では、デジタル署名プロセッサ802は、半決定論的ノンスをもたらすのに十分なメッセージごとの値を生成するか、または別の方法で得、ここで、メッセージごとの値は、秘密ノンス、公開ノンス、カウンタ、および文脈特定メッセージのうちの1つまたは複数であり、または、メッセージごとの値は、結果として生じるノンスが完全にランダムではないように、(ノンスからデジタル署名を生成するために使用されるデジタル署名生成プロトコルに関連付けられた値の全範囲と比較して)値の制限された範囲内でランダムに得られる。1104では、デジタル署名プロセッサ802は、鍵導出関数と、秘密鍵と、メッセージと、完全にランダムなノンスと完全に決定論的なノンスとの間の部分的な量の決定論性(partial amount of determinism)を有することによって特徴付けられる半決定論的ノンスをもたらすように選択されたメッセージごとの値とを使用して、非ランダムかつ非決定論的ノンスを生成するか、または別の方法で得、ここで、ノンスの非ランダム性は、少なくとも部分的に決定論的であり、完全にはランダムではないものとして特徴付けられ、ノンスの非決定論性は、少なくとも部分的にランダムであり、完全には決定論的ではないものとして特徴付けられる。1106では、デジタル署名プロセッサ802は、非ランダムかつ非決定論的ノンスに部分的に基づいてデジタル署名を生成するか、または別の方法で得る。1108では、デジタル署名プロセッサ802は、非ランダムかつ非決定論的ノンスに部分的に基づいて得られたデジタル署名を使用してメッセージに署名する。すでに述べたように、メッセージに署名することは、単に

メッセージにデジタル署名を付加することを伴い得、したがって、別々の署名生成コンポーネントおよびメッセージ署名コンポーネントは、必要とされないが、完全性および一般性のために別々に示されている。

【００５４】

図12は、図8のデジタル署名プロセッサ802によって、または、鍵導出関数と、秘密鍵と、メッセージと、メッセージごとの値とを使用してノンスを得るか、もしくは別の方法で生成するための図11のブロック1104で使用するための他の適切に装備されたデジタル署名生成デバイスによって実行され得る例示的な方法または手続きを示す。1202では、デジタル署名プロセッサ802は、連結値を得るために、秘密鍵をメッセージごとの値に連結する。1204では、デジタル署名プロセッサ802は、ハッシュ化メッセージを得るために、メッセージにハッシュ関数を適用する。1206では、デジタル署名プロセッサ802は、半決定論的ノンスを得るために、連結値およびハッシュ化メッセージに鍵導出関数を適用し、ここで、鍵導出関数は、HMAC関数である。

【００５５】

本開示の諸態様が、本明細書で、フローチャート、流れ図、構造図、またはブロック図として描かれるプロセスとして説明される場合があることに留意されたい。流れ図が、動作を順次プロセスとして説明する場合があるが、動作の多くを、並列にまたは同時に実行することができる。加えて、動作の順序を再配置することができる。プロセスは、その動作が完了したときに終了される。プロセスは、メソッド、関数、手続き、サブルーチン、サブプログラムなどに対応することができる。プロセスが関数に対応するときには、その終了は、呼び出す側の関数またはメイン関数への関数のリターンに対応する。

【００５６】

当業者は、本明細書に開示された態様に関連して説明した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が、電子ハードウェアとして、コンピュータソフトウェアとして、または両方の組合せとして実施され得ることをさらに理解するであろう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的なコンポーネント、ブロック、モジュール、回路、およびステップが、上記では概してそれらの機能に関して説明した。そのような機能性が、ハードウェアまたはソフトウェアのどちらとして実施されるのかは、具体的な適用例と、システム全体に課せられる設計制約とによって決まる。

【００５７】

本明細書に開示された例に関連して説明した方法またはアルゴリズムは、処理ユニット、プログラミング命令、または他の命令の形態で、直接ハードウェアにおいて、プロセッサによって実行可能なソフトウェアモジュールにおいて、または両方の組合せにおいて具体化され得、単一のデバイス内に含まれ得、または複数のデバイスに分散され得る。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、または当技術分野において知られている任意の他の形態の記憶媒体に常駐し得る。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、記憶媒体はプロセッサに結合され得る。代替において、記憶媒体は、プロセッサと一体であり得る。

【００５８】

本明細書に開示された本発明の様々な特徴は、本発明から逸脱することなく、異なるシステムで実施され得る。上記の実施形態は、単なる例であり、本発明を限定するものとして解釈されるべきではないことに留意すべきである。実施形態の説明は例示的なものであり、特許請求の範囲を限定するものではない。そのように、本教示は、他のタイプの装置に容易に適用され得、多くの代替、修正、変形が、当業者には明らかであろう。

【符号の説明】

【００５９】

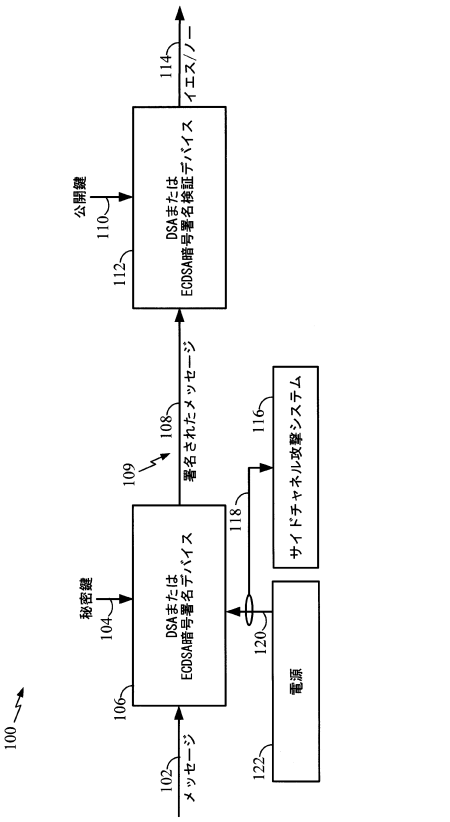
100　デジタル署名システム

102　メッセージ

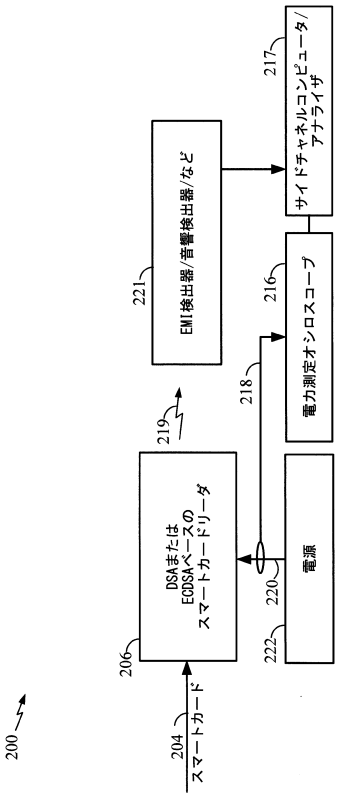
104 秘密鍵
106 暗号署名デバイス
108 署名されたメッセージ
109 チャネル
110 公開鍵
112 DSAまたはECDSA署名検証デバイス
114 イエス/ノー検証
116 サイドチャネル攻撃デバイスまたはシステム
118 電力およびタイミング情報
120 電気信号
122 電源
200 デジタル署名システム
204 スマートカード
206 スマートカードリーダ
216 電力測定オシロスコープ
217 サイドチャネルコンピュータ/アナライザ
218 電力およびタイミング情報
219 電磁誘導(EMI)信号、音響信号など
220 電力信号
221 センサーまたは検出器
222 電源
302 暗号署名デバイス
304 署名検証デバイス
400 SoC処理回路
410 アプリケーション処理回路
412 マルチコアCPU
413 デジタル署名プロセッサ
415 デジタル署名署名デバイス
417 署名検証デバイス
418 ブートROM
420 周辺サブシステム
422 DSP
424 ハードウェア(HW)およびソフトウェア(SW)コンポーネント
426 ラジオ周波数(RF)コンポーネント
428 ブートROM
430 内部共有ハードウェア(HW)リソース
432 内部共有記憶デバイス、内部共有ストレージ
433 鍵記憶要素
440 外部共有HWリソース
442 外部共有ストレージ
444 永久的もしくは半永久的データストレージ
450 ホスト記憶コントローラ
700 システムまたは装置
702 バス
704 処理回路
705 記憶デバイス
706 非一時的機械可読媒体
708 バスインターフェース
710 トランシーバ
712 ユーザインターフェース

714 処理システム
802 デジタル署名プロセッサ
804 デジタル署名生成器
806 デジタル署名検証器
808 ソルト生成モジュール/回路
810 非ランダムかつ非決定論的ノンス生成モジュール/回路
812 連結モジュール/回路
814 秘密鍵入力モジュール/回路
816 ハッシュ関数モジュール/回路
820 デジタル署名生成モジュール/回路
822 メッセージ署名モジュール/回路
824 公開鍵入力モジュール/回路
826 署名検証モジュール/回路
828 署名/メッセージ送信/受信モジュール/回路
904 デジタル署名生成命令
908 ソルト生成命令
910 非ランダムかつ非決定論的ノンス生成命令
912 連結命令
914 秘密鍵入力命令
916 ハッシュ関数命令
918 鍵導出関数(HMAC)命令
920 デジタル署名生成命令
922 メッセージ署名命令
924 公開鍵入力命令
926 署名検証命令
928 署名/メッセージ送信/受信命令

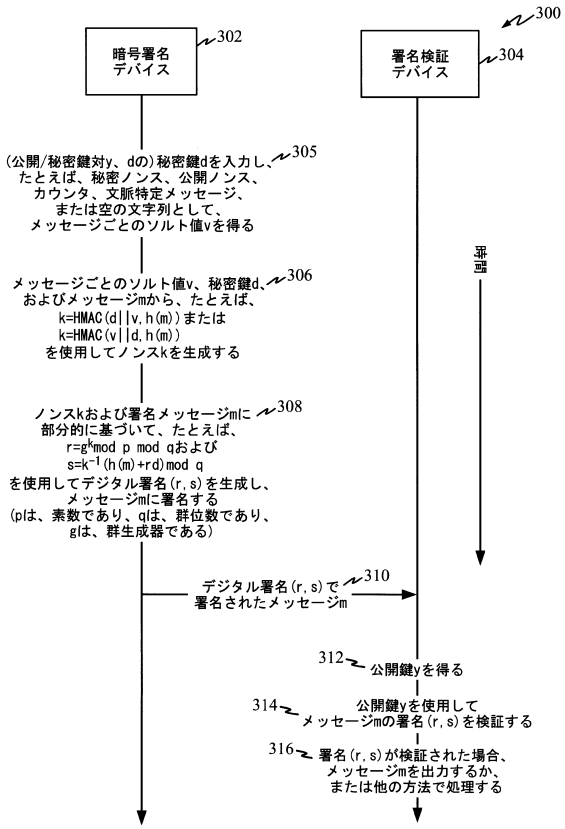
【図１】


100
102
メッセージ
104
秘密鍵
106
DSAまたは
ECDSA暗号署名デバイス
108
署名されたメッセージ
109
110
公開鍵
112
DSAまたは
ECDSA暗号署名検証デバイス
114
イエス/ノー
116
サイドチャネル攻撃システム
118
120
電源
122

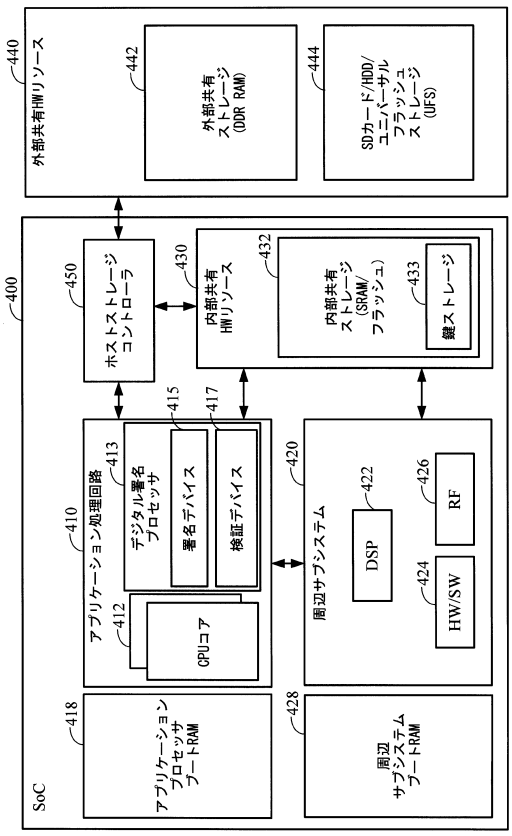
【図２】


200
204
スマートカード
206
DSAまたは
ECDSAベースの
スマートカードリーダ
217
サイドチャネルコンピュータ/
アナライザ
216
電力測定オシロスコープ
218
219
EMI検出器/音響検出器/など
220
電源
221
222

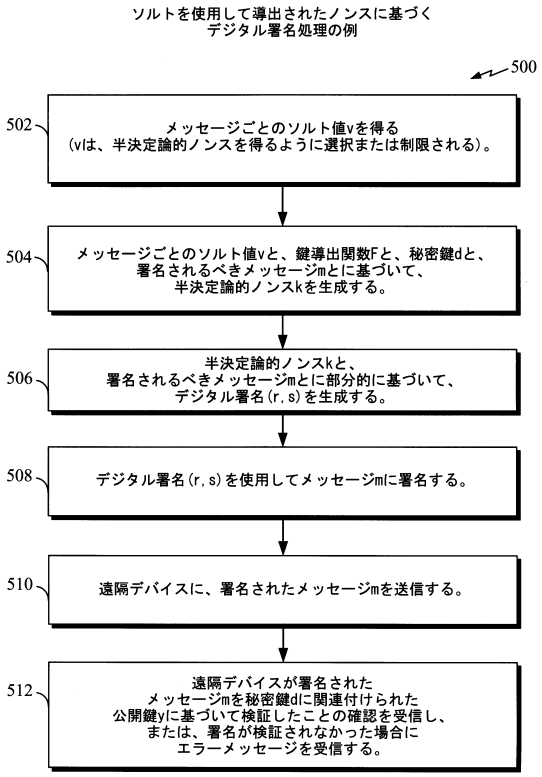
【図３】


300
暗号署名
デバイス
302
署名検証
デバイス
304
(公開/秘密鍵対y、dの)秘密鍵dを入力し、
たとえば、秘密ノンス、公開ノンス、
カウンタ、文脈特定メッセージ、
または空の文字列として、
メッセージごとのソルト値vを得る
305
メッセージごとのソルト値v、秘密鍵d、
およびメッセージmから、たとえば、
k=HMAC(d||v,h(m))または
k=HMAC(v||d,h(m))
を使用してノンスkを生成する
306
ノンスkおよび署名メッセージmに
部分的に基づいて、たとえば、
r=g^k mod p mod qおよび
s=k^-1(h(m)+rd)mod q
を使用してデジタル署名(r,s)を生成し、
メッセージmに署名する
(pは、素数であり、qは、群位数であり、
gは、群生成器である)
308
デジタル署名(r,s)で
署名されたメッセージm
310
再開
312
公開鍵yを得る
314
公開鍵yを使用して
メッセージmの署名(r,s)を検証する
316
署名(r,s)が検証された場合、
メッセージmを出力するか、
または他の方法で処理する

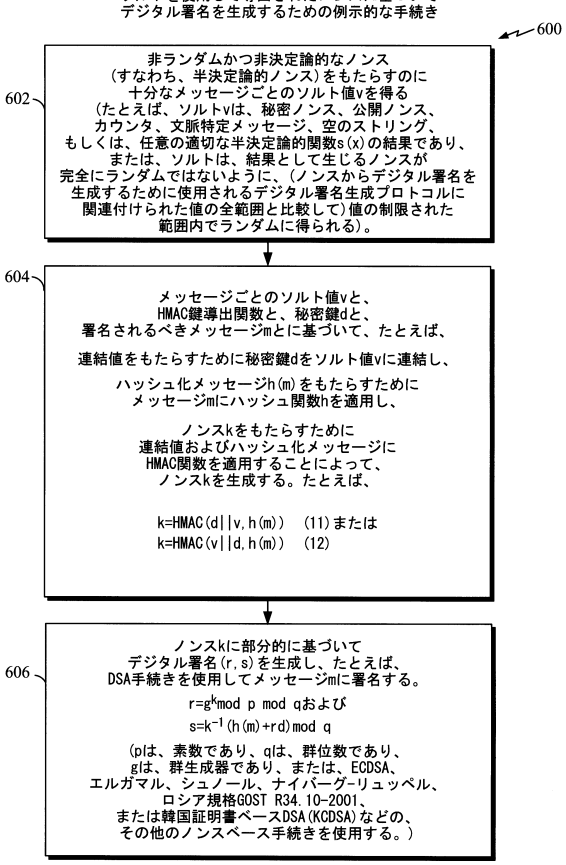
【図４】


400
SoC
440
外部共有HWリソース
442
外部共有
ストレージ
(DDR RAM)
444
SDカード/HDD/
ユニバーサル
フラッシュ
ストレージ
(UFS)
450
ホストストレージ
コントローラ
430
内部共有
HWリソース
432
内部共有
ストレージ
(SRAM/
フラッシュ)
433
鍵ストレージ
410
アプリケーション処理回路
412
GPUコア
413
デジタル署名
プロセッサ
415
署名デバイス
417
検証デバイス
420
周辺サブシステム
422
DSP
424
HW/SW
426
RF
418
アプリケーション
プロセッサ
ブートRAM
428
周辺
サブシステム
ブートRAM

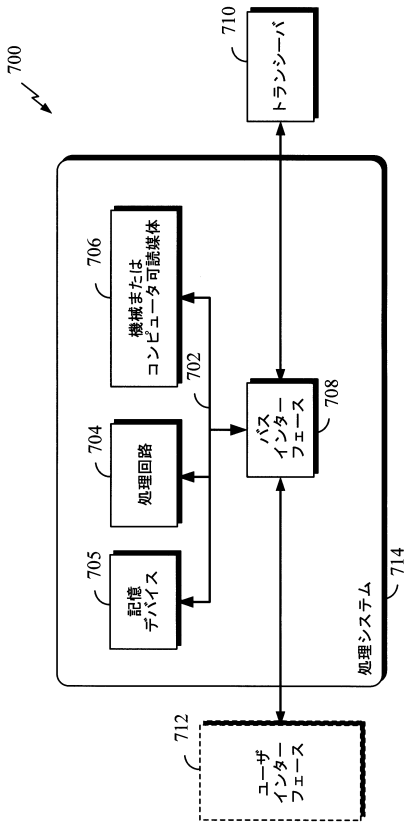
【図５】


ソルトを使用して導出されたノンスに基づく
デジタル署名処理の例
500
502
メッセージごとのソルト値vを得る
(vは、半決定論的ノンスを得るように選択または制限される)。
504
メッセージごとのソルト値vと、鍵導出関数Fと、秘密鍵dと、
署名されるべきメッセージmとに基づいて、
半決定論的ノンスkを生成する。
506
半決定論的ノンスkと、
署名されるべきメッセージmとに部分的に基づいて、
デジタル署名(r,s)を生成する。
508
デジタル署名(r,s)を使用してメッセージmに署名する。
510
遠隔デバイスに、署名されたメッセージmを送信する。
512
遠隔デバイスが署名された
メッセージmを秘密鍵dに関連付けられた
公開鍵yに基づいて検証したことの確認を受信し、
または、署名が検証されなかった場合に
エラーメッセージを受信する。

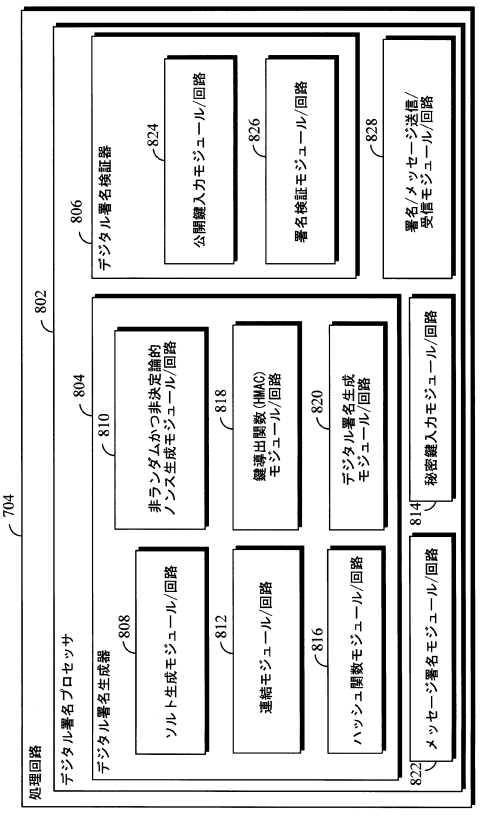
【図６】


ソルトを使用して導出されたノンスに基づいて
デジタル署名を生成するための例示的な手続き
600
602
非ランダムかつ非決定論的なノンス
(すなわち、半決定論的ノンス)をもたらすのに
十分なメッセージごとのソルト値vを得る
(たとえば、ソルトvは、秘密ノンス、公開ノンス、
カウンタ、文脈特定メッセージ、空のストリング、
もしくは、任意の適切な半決定論的関数s(x)の結果であり、
または、ソルトは、結果として生じるノンスが
完全にランダムではないように、(ノンスからデジタル署名を
生成するために使用されるデジタル署名生成プロトコルに
関連付けられた値の全範囲と比較して)値の制限された
範囲内でランダムに得られる)。
604
メッセージごとのソルト値vと、
HMAC鍵導出関数と、秘密鍵dと、
署名されるべきメッセージmとに基づいて、たとえば、
連結値をもたらすために秘密鍵dをソルト値vに連結し、
ハッシュ化メッセージh(m)をもたらすために
メッセージmにハッシュ関数hを適用し、
ノンスkをもたらすために
連結値およびハッシュ化メッセージに
HMAC関数を適用することによって、
ノンスkを生成する。たとえば、
k=HMAC(d||v,h(m)) (11)または
k=HMAC(v||d,h(m)) (12)
606
ノンスkに部分的に基づいて
デジタル署名(r,s)を生成し、たとえば、
DSA手続きを使用してメッセージmに署名する。
r=g^k mod p mod qおよび
s=k^-1(h(m)+rd)mod q
(pは、素数であり、qは、群位数であり、
gは、群生成器であり、または、ECDSA、
エルガマル、シュノール、ナイバーグ-リュッペル、
ロシア規格GOST R34.10-2001、
または韓国証明書ベースDSA(KCDSA)などの、
その他のノンスベース手続きを使用する。)

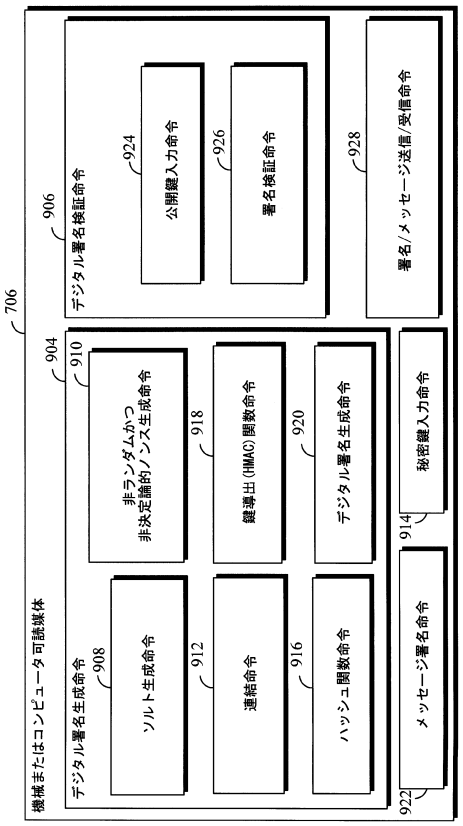
【図７】


700
710
トランシーバ
706
機械または
コンピュータ可読媒体
704
処理回路
705
記憶
デバイス
702
バス
インター
フェース
708
714
処理システム
712
ユーザ
インター
フェース

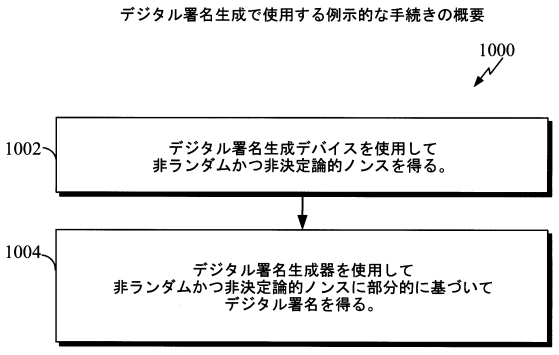
【図８】


704
処理回路
802
デジタル署名プロセッサ
804
デジタル署名生成器
808
ソルト生成モジュール/回路
812
連結モジュール/回路
816
ハッシュ関数モジュール/回路
810
非ランダムかつ非決定論的
ノンス生成モジュール/回路
818
鍵導出関数(HMAC)
モジュール/回路
820
デジタル署名生成
モジュール/回路
814
秘密鍵入力モジュール/回路
822
メッセージ署名モジュール/回路
806
デジタル署名検証器
824
公開鍵入力モジュール/回路
826
署名検証モジュール/回路
828
署名/メッセージ送信/
受信モジュール/回路

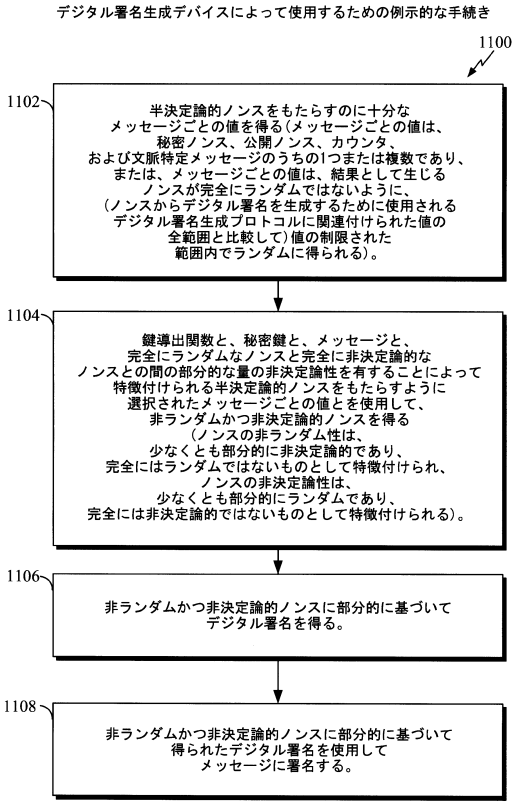
【図９】



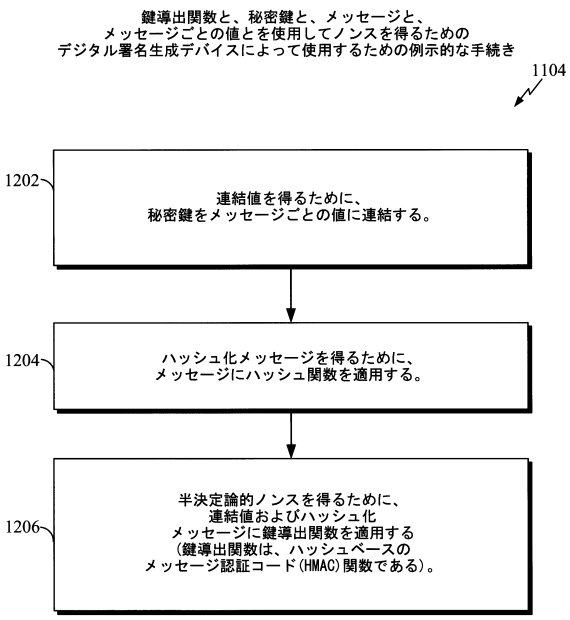
【図１０】



【図１１】



【図１２】



フロントページの続き

(56)参考文献 国際公開第２０１４／０７５０００（WO，Ａ１）
特表平０７－５０２３４６（ＪＰ，Ａ）
特開２００７－０８７１７１（ＪＰ，Ａ）
特表２００１－５０７４７９（ＪＰ，Ａ）
PORNIN, T., Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), RFC 6979, [online], ２０１３年 ８月, [2017年6月9日検索], ＵＲＬ, https://www.rfc-editor.org/info/rfc6979

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ