【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成26年6月5日(2014.6.5)

【公開番号】特開2014-75787(P2014-75787A)
【公開日】平成26年4月24日(2014.4.24)
【年通号数】公開・登録公報2014-021
【出願番号】特願2013-193278(P2013-193278)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/79　(2013.01)
Ｇ０６Ｆ　21/71　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　21/02　１７９Ｂ
Ｇ０６Ｆ　21/02　１７１Ｂ
Ｇ０６Ｆ　21/24　１６６Ａ

【手続補正書】
【提出日】平成25年9月19日(2013.9.19)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ＲＦＩＤタグを利用する方法であって、
リーダから呼び掛けを受信し、
$S = f(s, O_E)$，$U = f(u, O_O)$，$B = E(n, k_E)$，$G = f(A, k_O)$を計算し、
ここで、Ａは、前記呼び掛け及び前記ＲＦＩＤタグのプライベートキーの関数、
ｓ及びｕは、前記ＲＦＩＤタグによって生成された乱数、
ｎは、前記タグの識別子、
k_E及びk_Oは、それぞれ前記リーダの第１パブリックキー及び第２パブリックキーの関数、及び
O_E及びO_Oは、前記リーダによって提供されるオリジネータであり、
Ｓ、Ｕ、Ｂ、及びＧを前記リーダに返信し、
前記返信データは、呼び掛け応答及び前記タグの識別子を含み、同一の呼び掛けに対して応答するときであっても、それぞれの応答で特有であることを特徴とする方法。
【請求項２】
請求項１において、
前記オリジネータO_E及びO_Oは、楕円曲線上のポイントであることを特徴とする方法。
【請求項３】
請求項１において、
前記オリジネータO_E及びO_Oは、大きい素数のジェネレータであることを特徴とする方法。

【請求項４】
請求項１において、
前記ＲＦＩＤタグの初期化を含み、
前記初期化は、機密性のための第１キー対の第１パブリックキーと、難読化のための第２キー対の第２パブリックキーと、タグの識別子とを、前記リーダから受信することを含むことを特徴とする方法。
【請求項５】
請求項４において、
前記初期化は、認証のための第３のキー対を選択し、前記第３キー対のパブリックキーを前記リーダへ送信することを含むことを特徴とする方法。
【請求項６】
請求項４において、
前記初期化は、認証のための第３キー対のプライベートキーを前記リーダから受信し、前記第３キー対の前記プライベートキーが前記ＲＦＩＤタグによってのみ格納されることを特徴とする方法。
【請求項７】
データを送信及び受信するトランシーバと、
暗号計算を実行する暗号ロジックと、を有し
前記トランシーバは、リーダシステムから呼び掛けを受信し、
前記暗号ロジックは、$S = f(s, O_E)$，$U = f(u, O_O)$，$B = E(n, k_E)$，$G = f(A, k_O)$を計算し、
Ａは、前記呼び掛け及び前記低処理電力システムのプライベートキーの関数であり、
ｓ及びｕは、乱数であり、
ｎは、前記低処理電力システムの識別子であり、
k_E及びk_Oは、それぞれ前記リーダの第１パブリックキー及び第２パブリックキーの関数であり、
O_E及びO_Oは、前記リーダによって提供されるオリジネータであり、
前記トランシーバは、Ｓ，Ｕ，Ｂ，及びＧを前記リーダシステムに返信し、前記返信データは、呼び掛け応答及び前記タグの識別子を含み、同一の呼び掛けに対して応答するときであっても、それぞれの応答で特有であることを特徴とする低処理電力システム。
【請求項８】
請求項７において、
前記低処理電力システムのプライベートキーと、前記低処理電力システムの識別子とを格納する安全なメモリを有することを特徴とする低処理電力システム。
【請求項９】
請求項７において、
前記暗号ロジックは、乱数ｓ及びｕを生成することを特徴とする低処理電力システム。
【請求項１０】
請求項７において、
前記リーダの前記パブリックキーと、前記タグの識別子とを含む初期化データを格納するメモリを有することを特徴とする低処理電力システム。
【請求項１１】
請求項７において、
前記オリジネータO_E及びO_Oは、楕円曲線上のポイントであり、
前記オリジネータO_E及びO_Oは、同じ楕円曲線上の同じポイントであることを特徴とする低処理電力システム。
【請求項１２】
リーダシステムによって安全に質問されるように設計された低処理電力システムであって、
前記リーダシステムから呼び掛けを受信するトランシーバと、

前記呼び掛けに対する応答を計算する暗号ロジックと、を有し、
前記応答は、前記低処理電力システムのプライベートキーを含み、
前記暗号ロジックは、前記リーダシステムへ返信するための返信データを計算し、
前記返信データは、前記呼び掛けに対する応答と、暗号化キーと、認証キーと、難読化キーとの組み合わせであることを特徴とする低処理電力システム。

【請求項１３】
請求項１２において、
前記暗号化キーは、２つの乱数を生成するものであり、第１乱数を暗号化キーで暗号化し、第２乱数を難読化キーで暗号化し、認証キーを前記リーダシステムのパブリックキーで暗号化することを特徴とする低処理電力システム。