【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６部門第２区分
【発行日】平成22年3月25日(2010.3.25)

【公開番号】特開2009-42787(P2009-42787A)
【公開日】平成21年2月26日(2009.2.26)
【年通号数】公開・登録公報2009-008
【出願番号】特願2008-284464(P2008-284464)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６２０Ａ

【手続補正書】
【提出日】平成22年2月4日(2010.2.4)
【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】
楕円曲線暗号データ通信システムにおいて、通話者によって受信されるメッセージｍのデジタル署名（ｒ，ｓ）を確認する方法であって、該システムは、楕円曲線上のベース・ポイントＰおよびオーダーｎを含む基礎となるパラメータを有し、該デジタル署名は、署名者の短期的な公開鍵のｘ座標から生成される第１の成分ｒと、該第１の成分ｒ、該署名者の短期的な秘密鍵ｋ、該署名者の長期的な秘密鍵ｄおよび該メッセージｍから生成される第２の成分ｓとを含み、該方法は、算術ロジック・ユニットと、計算において用いられる該基礎となるパラメータおよび値を記憶するレジスタとを有する暗号化／復号化ユニット（１６）において実行され、該方法は、
（ａ）該算術ロジック・ユニットが、該メッセージｍおよび該第２の成分ｓを用いて第１の値u_1を計算するステップと、
（ｂ）該算術ロジック・ユニットが、該第１の成分ｒおよび該第２の成分ｓを用いて第２の値u_2を計算するステップと、
（ｃ）該算術ロジック・ユニットが、第１の点Ｒ’＝$u_1 u_2^{-1}$Ｐ＋ＱのＸ座標（$X_{R'}$）を計算するステップであって、Ｑは、該署名者の該長期的な秘密鍵ｄに対応する長期的な公開鍵である、ステップと、
（ｄ）該算術ロジック・ユニットが、第２の点Ｒ＝u_2Ｒ’のＸ座標（X_R）を計算するステップと、
（ｅ）該算術ロジック・ユニットが、該第２の点ＲのＸ座標（X_R）を該第１の成分ｒと比較し、該第２の点ＲのＸ座標（X_R）が該第１の成分ｒに等しい場合には、該デジタル署名を確認するステップと
を含む、方法。
【請求項２】
前記点ＲのＸ座標（X_R）が、
（ｉ）前記算術ロジック・ユニットが、前記第２の値u_2のバイナリ表現を得ることと、
（ｉｉ）該算術ロジック・ユニットが、該第２の値u_2のそれぞれの連続的なデジットを検査し、前記第１の点Ｒ’だけ異なる一対の点を表現するバイナリ・デジットのベクトルに対して連続的な２倍及び加算演算を実行することにより、該一対の点のＸ座標のうち

の該点Ｒのｘ座標（X_R）に等しいｘ座標の値を得ることと
を含むステップを実行することによって計算される、請求項１に記載の方法。
【請求項３】
前記連続的な２倍及び加算演算の実行において、前記一対の点のＸ座標を表現するために射影座標が用いられる、請求項２に記載の方法。
【請求項４】
予め計算されている前記ベース・ポイントＰの整数倍は、前記レジスタに記憶されており、前記第１の点Ｒ’のＸ座標（$X_{R'}$）を計算するために前記算術ロジック・ユニットによって用いられる、請求項１～３のいずれか１項に記載の方法。
【請求項５】
請求項１～４のいずれか１項に記載の方法を実行する装置。
【請求項６】
請求項１～４のいずれか１項に記載の方法を実行するためのコンピュータ読み取り可能な命令を記憶したコンピュータ読み取り可能な媒体。