【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25年11月7日(2013.11.7)

【公開番号】特開2012-50053(P2012-50053A)
【公開日】平成24年3月8日(2012.3.8)
【年通号数】公開・登録公報2012-010
【出願番号】特願2010-224752(P2010-224752)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｃ

【手続補正書】
【提出日】平成25年9月20日(2013.9.20)
【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】
Ｌ個（Ｌ≧２）の秘密鍵s_i（ｉ＝１～Ｌ）、及びｎ次多変数多項式の組Ｆ（ｎ≧２）について$y_i = F(s_i)$を満たすＬ個の公開鍵y_iを保持する鍵保持部と、
（Ｌ－１）個の$y_i = F(s_i)$を満たす秘密鍵s_iを用いた認証プロトコルを検証者との間で実行する認証プロトコル実行部と、
を備え、
前記認証プロトコル実行部は、
前記検証者からＬ個のチャレンジCh_iを受信するチャレンジ受信部と、
前記チャレンジ受信部により受信されたＬ個のチャレンジCh_iの中から（Ｌ－１）個のチャレンジCh_iを任意に選択するチャレンジ選択部と、
前記秘密鍵s_iを用いて、前記チャレンジ選択部により選択された（Ｌ－１）個のチャレンジCh_iのそれぞれに対する（Ｌ－１）個の回答Rsp_iを生成する回答生成部と、
前記回答生成部により生成された（Ｌ－１）個の回答Rsp_iを前記検証者に送信する回答送信部と、
を含む、
認証装置。
【請求項２】
前記認証プロトコル実行部は、
前記検証者に対し、Ｌ個の前記秘密鍵s_iのそれぞれに対応するメッセージCmt_iを送信するメッセージ送信部をさらに含み、
前記チャレンジ受信部は、前記メッセージ送信部により送信された各メッセージCmt_iに応じて、前記検証者によりｋ通り（ｋ≧２）の検証パターンの中から選択された検証パターンを示すチャレンジCh_iを受信する、
請求項１に記載の認証装置。
【請求項３】
前記メッセージCmt_iが$Cmt_i = (c_{i,1}, \cdots, c_{i,N})$である場合、
前記メッセージ送信部は、一方向性関数Ｈを用いて新たなメッセージ$Cmt' = H(Cmt_1, \cdots, Cmt_L)$を算出して当該メッセージ$Cmt'$を前記検証者に送信し、
前記回答送信部は、前記回答Rsp_iと共に、当該回答Rsp_iを利用しても前記検証

者が復元できない前記メッセージCmt_iの要素を送信する、
請求項２に記載の認証装置。
【請求項４】
前記鍵保持部は、前記Ｌ個の秘密鍵s_iのうち、１つの秘密鍵s_{i_0}（$1 \leqq i_0 \leqq L$）を保持しないようにし、
前記認証プロトコル実行部は、前記認証プロトコルの中で実行される前記秘密鍵s_{i_0}に関する処理を偽証アルゴリズムに基づいて実行する、
請求項２に記載の認証装置。
【請求項５】
Ｌ個の秘密鍵s_i（$i=1 \sim L$）、ｎ次多変数多項式の組Ｆ（$n \geqq 2$）について$y_i = F(s_i)$を満たすＬ個の公開鍵y_iを保持する鍵保持部と、
検証者からＱ組（$Q \geqq 2$）のＬ個のチャレンジ$Ch_i^{(j)}$（$j=1 \sim Q$）を受信するチャレンジ受信部と、
前記チャレンジ受信部により受信されたＱ組のＬ個のチャレンジ$Ch_i^{(j)}$の中から１組のＬ個のチャレンジ$Ch_i^{(j)}$を任意に選択するチャレンジ選択部と、
前記秘密鍵s_iを用いて、前記チャレンジ選択部により選択されたＬ個のチャレンジ$Ch_i^{(j)}$のそれぞれに対するＬ個の回答Rsp_iを生成する回答生成部と、
前記回答生成部により生成されたＬ個の回答Rsp_iを前記検証者に送信する回答送信部と、
を備える、
認証装置。
【請求項６】
前記検証者に対し、Ｌ個の前記秘密鍵s_iのそれぞれに対応するメッセージCmt_iを送信するメッセージ送信部をさらに含み、
前記チャレンジ受信部は、前記メッセージ送信部により送信された各メッセージCmt_iに応じて、前記検証者によりｋ通り（$k \geqq 2$）の検証パターンの中から選択された検証パターンを示すチャレンジ$Ch_i^{(j)}$を受信する、
請求項５に記載の認証装置。
【請求項７】
前記メッセージCmt_iが$Cmt_i = (c_{i,1}, \cdots, c_{i,N})$である場合、
前記メッセージ送信部は、一方向性関数Ｈを用いて新たなメッセージ$Cmt' = H(Cmt_1, \cdots, Cmt_L)$を算出して当該メッセージ$Cmt'$を前記検証者に送信し、
前記回答送信部は、前記回答Rsp_iと共に、当該回答Rsp_iを利用しても前記検証者が復元できない前記メッセージCmt_iの要素を送信する、
請求項６に記載の認証装置。
【請求項８】
Ｌ個（$L \geqq 2$）の秘密鍵s_i（$i=1 \sim L$）、及びｎ次多変数多項式の組Ｆ（$n \geqq 2$）について$y_i = F(s_i)$を満たすＬ個の公開鍵y_iを生成する鍵生成ステップと、
（Ｌ－１）個の$y_i = F(s_i)$を満たす秘密鍵s_iを用いた認証プロトコルを検証者との間で実行する認証プロトコル実行ステップと、
を含み、
前記認証プロトコル実行ステップは、
前記検証者からＬ個のチャレンジCh_iを受信するチャレンジ受信ステップと、
前記チャレンジ受信ステップで受信されたＬ個のチャレンジCh_iの中から（Ｌ－１）個のチャレンジCh_iを任意に選択するチャレンジ選択ステップと、
前記秘密鍵s_iを用いて、前記チャレンジ選択ステップで選択された（Ｌ－１）個のチャレンジCh_iのそれぞれに対する（Ｌ－１）個の回答Rsp_iを生成する回答生成ステップと、
前記回答生成ステップで生成された（Ｌ－１）個の回答Rsp_iを前記検証者に送信する回答送信ステップと、

を含む、
認証方法。
【請求項９】
Ｌ個（Ｌ≧２）の秘密鍵s_i（ｉ＝１～Ｌ）、及びｎ次多変数多項式の組Ｆ（ｎ≧２）について$y_i = F(s_i)$を満たすＬ個の公開鍵y_iを保持する鍵保持機能と、
（Ｌ－１）個の$y_i = F(s_i)$を満たす秘密鍵s_iを用いた認証プロトコルを検証者との間で実行する認証プロトコル実行機能と、
をコンピュータに実現させるためのプログラムであり、
前記認証プロトコル実行機能は、
前記検証者からＬ個のチャレンジCh_iを受信するチャレンジ受信機能と、
前記チャレンジ受信機能により受信されたＬ個のチャレンジCh_iの中から（Ｌ－１）個のチャレンジCh_iを任意に選択するチャレンジ選択機能と、
前記秘密鍵s_iを用いて、前記チャレンジ選択機能により選択された（Ｌ－１）個のチャレンジCh_iのそれぞれに対する（Ｌ－１）個の回答Rsp_iを生成する回答生成機能と、
前記回答生成機能により生成された（Ｌ－１）個の回答Rsp_iを前記検証者に送信する回答送信機能と、
を含む、
プログラム。
【請求項１０】
Ｌ個の秘密鍵s_i（ｉ＝１～Ｌ）、ｎ次多変数多項式の組Ｆ（ｎ≧２）について$y_i = F(s_i)$を満たすＬ個の公開鍵y_iを生成する鍵生成ステップと、
検証者からＱ組（Ｑ≧２）のＬ個のチャレンジ$Ch_i^{(j)}$（ｊ＝１～Ｑ）を受信するチャレンジ受信ステップと、
前記チャレンジ受信ステップで受信されたＱ組のＬ個のチャレンジ$Ch_i^{(j)}$の中から１組のＬ個のチャレンジ$Ch_i^{(j)}$を任意に選択するチャレンジ選択ステップと、
前記秘密鍵s_iを用いて、前記チャレンジ選択ステップで選択されたＬ個のチャレンジ$Ch_i^{(j)}$のそれぞれに対するＬ個の回答Rsp_iを生成する回答生成ステップと、
前記回答生成ステップで生成されたＬ個の回答Rsp_iを前記検証者に送信する回答送信ステップと、
を含む、
認証方法。
【請求項１１】
Ｌ個の秘密鍵s_i（ｉ＝１～Ｌ）、ｎ次多変数多項式Ｆ（ｎ≧２）について$y_i = F(s_i)$を満たすＬ個の公開鍵y_iを保持する鍵保持機能と、
検証者からＱ組（Ｑ≧２）のＬ個のチャレンジ$Ch_i^{(j)}$（ｊ＝１～Ｑ）を受信するチャレンジ受信機能と、
前記チャレンジ受信機能により受信されたＱ組のＬ個のチャレンジ$Ch_i^{(j)}$の中から１組のＬ個のチャレンジ$Ch_i^{(j)}$を任意に選択するチャレンジ選択機能と、
前記秘密鍵s_iを用いて、前記チャレンジ選択機能により選択されたＬ個のチャレンジ$Ch_i^{(j)}$のそれぞれに対するＬ個の回答Rsp_iを生成する回答生成機能と、
前記回答生成機能により生成されたＬ個の回答Rsp_iを前記検証者に送信する回答送信機能と、
をコンピュータに実現させるためのプログラム。