【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27年9月24日(2015.9.24)

【公開番号】特開2015-144495(P2015-144495A)
【公開日】平成27年8月6日(2015.8.6)
【年通号数】公開・登録公報2015-050
【出願番号】特願2015-99791(P2015-99791)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０９Ｃ　1/00　６２０Ｚ

【手続補正書】
【提出日】平成27年8月10日(2015.8.10)
【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】
送信者のコンピュータと受信者のコンピュータとの間で通信を行う方法であって、
前記送信者のコンピュータ及び前記受信者のコンピュータはそれぞれ、プロセッサと、情報記憶手段とを有し、
前記方法は、
前記送信者のコンピュータのプロセッサに、受信者の識別情報を取得させる工程と、
前記送信者のコンピュータのプロセッサに、前記受信者が解読鍵を取得するために必要な、受信確認返信要求情報を指定させる工程であって、前記受信確認返信要求情報は、返信アドレスと、前記受信者に送信されるメッセージに対応するメッセージ識別子とを含む、該工程と、
前記送信者のコンピュータのプロセッサに、前記受信者の識別情報および前記受信確認返信要求情報から暗号鍵を導かせる工程と、
前記送信者のコンピュータのプロセッサに、前記受信者の識別情報および前記受信確認返信要求情報から導かれた前記暗号鍵および双線形写像を使用してメッセージを暗号化させる工程であって、前記メッセージを暗号化させる工程は、前記送信者のコンピュータが、代数群の要素Ｐを得て、秘密乱数ｒを選択し、かつｒＰの値を計算する工程を含む、該工程と、
前記送信者のコンピュータのプロセッサに、暗号化されたメッセージおよび計算された値ｒＰを前記送信者のコンピュータから前記受信者のコンピュータに送信させる工程と、
前記受信者のコンピュータに、前記暗号化されたメッセージ及び計算された前記値ｒＰを受信させる工程と、
個人鍵作成器に、前記暗号化されたメッセージの前記受信者からの解読鍵の要求を受信させる工程であって、前記解読鍵の要求は、前記受信確認返信要求情報及び前記受信者の識別情報を含む、該工程と、
前記解読鍵の要求を受け取った後、前記個人鍵作成器に、前記メッセージの受信確認返信を前記送信者のコンピュータに与えさせる工程と、
前記個人鍵作成器に、前記暗号鍵に前記代数群の持つ群作用を適用することによって解

読鍵を作成させ、作成された前記解読鍵を受信者に送信させる工程と、
前記受信者のコンピュータのプロセッサに、前記解読鍵を受け取った後、前記解読鍵および前記双線形写像を使用して前記暗号化されたメッセージを解読させる工程とを含むことを特徴とする方法。
【請求項２】
前記個人鍵作成器に、前記解読鍵の要求を受け取った後、受信結果をログの一部として記憶媒体上に格納させる工程を更に含むことを特徴とする請求項１に記載の方法。