【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19年4月26日(2007.4.26)

【公表番号】特表2002-539489(P2002-539489A)
【公表日】平成14年11月19日(2002.11.19)
【出願番号】特願2000-604568(P2000-604568)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｚ
Ｇ０９Ｃ　1/00　６２０Ｚ

【手続補正書】
【提出日】平成19年3月9日(2007.3.9)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】　１つ以上の関数と、１つ以上のデータと、該１つ以上の関数と該１つ以上のデータとのそれぞれのメモリ位置に対応する暗号化されたメモリアドレスのアレイとを備えるコンポーネントオブジェクトを有するシステムにおける、該１つ以上の関数と該１つ以上のデータとへのアクセスを制御する方法であって、
少なくとも１つの鍵スプリットを受信することと、
該少なくとも１つの鍵スプリットに基づいて、該１つ以上の関数と該１つ以上のデータとのうちアクセスが許可されている第１の組の関数及びデータと、アクセスが許可されていない第２の組の関数及びデータとを決定することと、
暗号化されたメモリアドレスの該アレイ内の、該第１の組の関数及びデータに対応する１つ以上のメモリアドレスを解読することと、
該第１の組の関数及びデータにアクセスするために、該解読された１つ以上のメモリアドレスを提供することと
を含むアクセス制御方法。
【請求項２】　暗号化されたメモリアドレスの前記アレイ内の前記第２の組の関数及びデータに対応するメモリアドレスを、エラーコードに対応するように変更することを更に含む請求項１記載の方法。
【請求項３】　１つ以上の関数と、１つ以上のデータと、該１つ以上の関数と該１つ以上のデータとのそれぞれのメモリ位置に対応する暗号化されたメモリアドレスのアレイとを備えるコンポーネントオブジェクトを有するシステムにおける、該１つ以上の関数と該１つ以上のデータとへのアクセスを制御する方法であって、
少なくとも１つの鍵スプリットを受信することと、
該少なくとも１つの鍵スプリットを用いて、該１つ以上の関数と該１つ以上のデータとのうち１つに対応する暗号化された１つのメモリアドレスを解読しようとすることと、
該１つのメモリアドレスの解読が成功した場合、該１つ以上の関数と該１つ以上のデータとのうちの前記対応する１つにアクセスするために、該解読された１つのメモリアドレスを提供することと
を含むアクセス制御方法。
【請求項４】　前記１つのメモリアドレスの解読が失敗した場合、エラーコードを提供することを更に含む請求項３記載の方法。

【請求項５】　保護された通信チャネルを確立する方法であって、
第１の者が、保護コール通知を第２の者に送信することと、
該第１の者と該第２の者とが、ベース、プライム、及びサブプライムパラメータをアクセスすることと、
該第２の者が、該ベース、プライム、及びサブプライムパラメータに基づいて第２の公開鍵と第２の秘密鍵とを有する第２の非対称鍵ペアを生成することと、
該第２の者が、該第２の公開鍵を該第１の者に送信することと、
該第１の者が、ネットラベルと、秘密ラベルと、乱数と、第１の公開鍵及び第１の秘密鍵を有する第１の非対称鍵ペアとを該ベース、プライム、及びサブプライムパラメータに基づいて生成し、共通鍵を該第２の公開鍵に基づいて生成することと、
該第１の者が、該ネットラベルと秘密ラベルと乱数とを該共通鍵を使用して暗号化することと、
該第１の者が、該暗号化されたネットラベルと暗号化された秘密ラベルと暗号化された乱数と該第１の公開鍵とを該第２の者に送信することと、
該第２の者が、該共通鍵を該第１の公開鍵に基づいて生成することと、
該第２の者が、該暗号化されたネットラベルと暗号化された秘密ラベルと暗号化された乱数とを該共通鍵を使用して解読することと、
該第１の者と該第２の者とが、それぞれの識別番号を互いに通知し、保護された通信チャネルを確立することと
を含む方法。
【請求項６】　請求項５記載の方法であって、前記保護コール通知は第１の保護コール通知であり、前記ネットラベルは第１ネットラベルであり、前記秘密ラベルは第１秘密ラベルであり、前記乱数は第１乱数であり、前記共通鍵は第１の共通鍵であり、前記暗号化されたネットラベルは第１の暗号化された第１ネットラベルであり、前記暗号化された秘密ラベルは第１の暗号化された第１秘密ラベルであり、前記暗号化された乱数は第１の暗号化された第１乱数であり、
前記第１の者と第２の者のうち一方が、該第１の者と第２の者のうちいずれかを送信者として指定し、他方を非送信者として指定することと、
該送信者が、該第１の者と第２の者の間の前記保護された通信チャネルを停止することと、
該送信者が、第３の者と通信チャネルを確立することと、
該送信者が、第２の保護コール通知を該第３の者に送信することと、
該第３の者が、前記ベース、プライム、及びサブプライムパラメータをアクセスすることと、
該第３の者が、該ベース、プライム、及びサブプライムパラメータに基づいて第３の公開鍵と第３の秘密鍵とを有する第３の非対称鍵ペアを生成することと、
該第３の者が、該第３の公開鍵を該送信者に送信することと、
該送信者が、第２秘密ラベルと、第２ネットラベルと、第２乱数と、該ベース、プライム、及びサブプライムパラメータに基づいて第４の公開鍵及び第４の秘密鍵を有する第４の非対称鍵ペアとを生成し、第２の共通鍵を該第３の公開鍵に基づいて生成することと、
該送信者が、該第２秘密ラベルと該第１ネットラベルと該第１乱数とを該第２の共通鍵を使用して暗号化し、暗号化された第２秘密ラベルと、第２の暗号化された第１ネットラベルと、第２の暗号化された第１乱数とを提供することと、
該送信者が、該暗号化された第２秘密ラベルと、該第２の暗号化された第１ネットラベルと、該第２の暗号化された第１乱数と、該第４の公開鍵とを該第３の者に送信することと、
該第３の者が、該第２の共通鍵を該第３の公開鍵に基づいて生成することと、
該第３の者が、該暗号化された第２秘密ラベルと該第２の暗号化された第１ネットラベルと該第２の暗号化された第１乱数とを該第２の共通鍵を使用して解読することと、
該送信者が、該送信者と該第３の者の間の前記保護された通信チャネルを停止すること

と、
該送信者が、該第３の者と該非送信者とに会議コール通知を送信することと、
該送信者が、該第２ネットラベルと第２乱数とを該第１又は第２の公開鍵を使用して暗号化し、第１の暗号化された第２ネットラベルと第１の暗号化された第２乱数とを提供することと、
該送信者が、該第１の暗号化された第２ネットラベルと該第１の暗号化された第２乱数とに対する第１のエラー検出値を生成することと、
該送信者が、該非送信者に該第１の暗号化された第２ネットラベルと、該第１の暗号化された第２乱数と、該第１のエラー検出値とを送信することと、
該非送信者が、該第１の暗号化された第２ネットラベルと該第１の暗号化された第２乱数とに対する第２のエラー検出値を生成することと、
該非送信者が、該第１と第２のエラー検出値を比較することで、該第１の暗号化された第２ネットラベルと該第１の暗号化された第２乱数との有効性をチェックすることと、
該非送信者が、該第１の暗号化された第２ネットラベルと該第１の暗号化された第２乱数とを該第１又は第２の秘密鍵を使用して解読することと、
該送信者が、該第２ネットラベルと該第２乱数とを該第３の公開鍵を使用して暗号化し、第２の暗号化された第２ネットラベルと第２の暗号化された第２乱数とを提供することと、
該送信者が、該第２の暗号化された第２ネットラベルと該第２の暗号化された第２乱数とに対する第３のエラー検出値を生成することと、
該送信者が、該第３の者に該第２の暗号化された第２ネットラベルと、該第２の暗号化された第２乱数と、該第３のエラー検出値とを送信することと、
該第３の者が、該第２の暗号化された第２ネットラベルと該第２の暗号化された第２乱数とに対する第４のエラー検出値を生成することと、
該第３の者が、該第３と第４のエラー検出値を比較することで、該第２の暗号化された第２ネットラベルと該第２の暗号化された第２乱数との有効性をチェックすることと、
該第３の者が、該第２の暗号化された第２ネットラベルと該第２の暗号化された第２乱数とを該第３の秘密鍵を使用して解読することと
を更に含む方法。
【請求項７】　保護された通信チャネルを確立する方法であって、
第１の者と他の者達とを含む三者以上の間で通信リンクを確立することと、
該第１の者が、同報会議コール通知を該他の者達に送信することと、
該第１の者と該他の者達とが、ベース、プライム、及びサブプライムパラメータをアクセスすることと、
該第１の者が、ネットラベルと、乱数と、該ベース、プライム、及びサブプライムパラメータに基づいて第１の公開鍵と第１の秘密鍵とを有する第１の非対称鍵ペアとを生成することと、
該第１の者が、該第１の公開鍵を該他の者達のそれぞれに送信することと、
該他の者達がそれぞれ、プライベートラベルと、該ベース、プライム、及びサブプライムパラメータに基づいて他の公開鍵及び他の秘密鍵を有する他の非対称鍵ペアとを生成し、該第１の公開鍵に基づいて他の共通鍵を生成することと、
該他の者達がそれぞれ、該プライベートラベルを該他の共通鍵を使用して暗号化することと、
該他の者達がそれぞれ、該暗号化されたプライベートラベルと該他の公開鍵とを該第１の者に送信することと、
該第１の者が、該他の者達が送信した該他の公開鍵のそれぞれからそれぞれの共通鍵を計算することと、
該第１の者が、該各暗号化されたプライベートラベルをそれぞれの該共通鍵を使用して解読することと、
該第１の者が、該ネットラベル及び乱数を、該各共通鍵を使用して暗号化することと、

該第１の者が、該各暗号化されたネットラベル及び暗号化された乱数をそれぞれ対応する該他の者に送信することと、
該他の者達がそれぞれ、該暗号化されたネットラベル及び暗号化された乱数を該他の共通鍵を使用して解読することと、
該第１の者と該他の者達とが、該ネットラベル及び乱数を使用して保護された通信チャネルを確立することと
を含む方法。
【請求項８】　前記第１の者が、前記各他の者に対するエラーチェックコードをそれぞれの前記暗号化されたネットラベル及び暗号化された乱数から導出することと、
該第１の者が、該各エラーチェックコードをそれぞれの該他の者に送信することと、
該他の者達がそれぞれ、前記暗号化されたネットラベル及び暗号化された乱数の有効性を、該エラーチェックコードを使用して確認することと
を更に含む請求項７記載の方法。
【請求項９】　１つ以上の関数と、１つ以上のデータと、該１つ以上の関数と該１つ以上のデータとのそれぞれのメモリ位置に対応する暗号化されたメモリアドレスのアレイとを備えるコンポーネントオブジェクトを有するコンピュータシステムにおける、該１つ以上の関数と該１つ以上のデータとへのアクセスを制御する方法であって、
少なくとも１つの鍵スプリットを受信することと、
該少なくとも１つの鍵スプリットに基づいて、該１つ以上の関数と該１つ以上のデータとのうちの１つへのアクセスが許可されているか否かを判断することと、
該１つ以上の関数と該１つ以上のデータとのうちの１つへのアクセスが許可されている場合は、
該暗号化されたメモリアドレスのアレイ内の、該１つ以上の関数と該１つ以上のデータとのうちの該１つに対応する１つ以上のメモリアドレスを解読することと、
該１つ以上の関数と該１つ以上のデータとのうちの該１つにアクセスするために、該解読された１つ以上のメモリアドレスを提供することと
を含むアクセス制御方法。
【請求項１０】　前記１つ以上の関数へのアクセスの許可が前記少なくとも１つの鍵スプリットに基づいて決定される請求項９記載の方法。
【請求項１１】　前記１つ以上のデータへのアクセスの許可が前記少なくとも１つの鍵スプリットに基づいて決定される請求項９記載の方法。
【請求項１２】　前記１つ以上の関数と前記１つ以上のデータとへのアクセスの許可は前記少なくとも１つの鍵スプリットに基づいて決定する請求項９記載の方法。
【請求項１３】　アクセスが許可されていない前記１つ以上の関数と前記１つ以上のデータとのそれぞれのメモリアドレスをエラーコードに対応するように変更することを更に含む請求項９記載の方法。