【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18年6月29日(2006.6.29)

【公表番号】特表2005-539441(P2005-539441A)
【公表日】平成17年12月22日(2005.12.22)
【年通号数】公開・登録公報2005-050
【出願番号】特願2004-536902(P2004-536902)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ

【手続補正書】
【提出日】平成18年5月11日(2006.5.11)
【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】
データ配信システムにおいてデジタルデータの層状の非対称暗号化を供給するための方法であって、
前記デジタルデータを第１の暗号化層において第１の鍵を使用して暗号化するステップと、
前記第１の鍵を前記第１の暗号化層において第２の鍵を使用して暗号化するステップと、
前記暗号化された第１の鍵を第２の暗号化層において第３の鍵を使用して暗号化するステップと、
前記暗号化されたデータ及び前記暗号化された第１の鍵を供給するステップと、
前記暗号化された第１の鍵を前記第２の暗号化層に従って復号化するステップと、
前記暗号化された第１の鍵を前記第１の暗号化層に従って復号化するステップと、
前記暗号化されたデジタルデータを前記第１の暗号化層に従って復号化するステップとを含む、方法。
【請求項２】
前記デジタルデータを暗号化するステップが前記システムの第１の当事者によって実行され、前記第１の鍵が対称鍵であり、
前記第１の鍵を前記第１の暗号化層において暗号化するステップが前記第１の当事者によって実行され、前記第２の鍵が第１の公開鍵対の公開鍵であり、
前記暗号化された第１の鍵を前記第２の暗号化層において暗号化するステップが前記システムの前記第１の当事者又は第２の当事者によって実行され、前記第３の鍵が第２の公開鍵対の公開鍵であり、
前記供給するステップが、前記暗号化されたデータ及び前記暗号化された第１の鍵をネットワークによって前記システムの第３の当事者へ供給し、
前記暗号化された第１の鍵を前記第２の暗号化層に従って復号化するステップが、前記第３の当事者により前記第２の公開鍵対の秘密鍵を使用して実行され、
前記暗号化された第１の鍵を前記第１の暗号化層に従って復号化するステップが、前記システムの前記第３の当事者又は第４の当事者により前記第１の公開鍵対の秘密鍵を使用して実行され、

前記暗号化されたデジタルデータを復号化するステップが、前記第３又は第４の当事者により前記復号化された第１の鍵を使用して実行される、請求項１に記載の方法。
【請求項３】
前記暗号化された第１の鍵を、前記第２の暗号化層における前記暗号化の後に第３の暗号化層において第４の鍵を使用して暗号化するステップと、
前記暗号化された第１の鍵を、前記第２の暗号化層による前記復号化ステップより前に前記第３の暗号化層に従って復号化するステップとをさらに含む、請求項１又は２に記載の方法。
【請求項４】
前記第１の鍵を前記第４の鍵を使用して暗号化するステップが、前記第１の当事者、前記第２の当事者又は第５の当事者のうち１つによって実行され、前記第４の鍵が、第３の公開鍵対の公開鍵であり、前記第３の暗号化層に従って復号化するステップが、前記システムの前記第３の当事者、前記第４の当事者又は第６の当事者のうち１つにより前記第３の公開鍵対の秘密鍵を使用して実行される、請求項３に記載の方法。
【請求項５】
前記第１の鍵を暗号化する１つ又は複数のステップが、前記デジタルデータを個々の暗号化層の暗号鍵を使用して暗号化することをさらに含む、請求項２～４のいずれか１項に記載の方法。
【請求項６】
前記暗号化された第１の鍵を暗号化する１つ又は複数のステップが、
前記第１の鍵をさらなる対称鍵を使用して暗号化することと、
前記さらなる対称鍵を前記１つ又は複数の暗号化ステップの暗号化層の個々の公開鍵対の公開鍵を使用して暗号化することと、
前記暗号化されたさらなる対称鍵を前記暗号化された第１の鍵に関連付けることであって、前記暗号化されたさらなる対称鍵が、任意の次の暗号化層によって前記第１の鍵と同様にして処理され、前記次の暗号化層が、暗号化された両方の鍵を１つの鍵情報部分として、又は２つの別個の暗号化された鍵と見なすこととを含み、
前記暗号化ステップの対応する復号化ステップが、
前記暗号化されたさらなる対称鍵を前記個々の暗号化層の公開鍵対の秘密鍵を使用して復号化することと、
前記暗号化された第１の鍵を前記復号化されたさらなる対称鍵を使用して復号化することとを含む、請求項２～５のいずれか１項に記載の方法。
【請求項７】
ネットワークを介する送信者から受信者までのデジタルデータの配信経路を制御するための方法であって、前記ネットワークが複数の接続されたネットワークノードを備え、
ａ）前記デジタルデータを第１の暗号化層において第１の鍵を使用して暗号化するステップと、
ｂ）前記第１の鍵を前記第１の暗号化層において第２の鍵を使用して暗号化するステップであって、前記第２の鍵が、前記デジタルデータの受信者に関連付けられる公開鍵である、ステップと、
ｃ）前記暗号化された第１の鍵を第２の暗号化層において第３の鍵を使用して暗号化するステップであって、前記第３の鍵が、第１のネットワークノードに関連付けられる公開鍵であり、前記デジタルデータが、配信経路沿いに前記ネットワークを介して前記受信者へ送られるように定義される、ステップと、
ｄ）前記暗号化されたデータ及び前記暗号化された第１の鍵を前記第１のネットワークノードへ供給するステップと、
ｅ）前記暗号化された第１の鍵を前記第１のネットワークノードにおいて前記第２の暗号化層に従って、前記第１のネットワークノードの前記公開鍵に対応する秘密鍵を使用して復号化するステップと、
ｆ）前記暗号化されたデータ及び前記暗号化された第１の鍵を前記受信者へ供給するス

テップと、
ｇ）前記暗号化された第１の鍵を前記第１の暗号化層に従って、前記受信者の前記公開鍵に対応する秘密鍵を使用して復号化するステップと、
ｈ）前記暗号化されたデジタルデータを前記第１の暗号化層に従って前記復号化された第１の鍵を使用して復号化するステップとを含む、方法。
【請求項８】
前記暗号化するステップｃ）が、前記送信者又は前記暗号化されたデータと前記暗号化された第１の鍵とからなるメッセージが先に通過した第３のネットワークノードによって実行される、請求項７に記載の方法。
【請求項９】
前記暗号化された第１の鍵を第３の暗号化層において第４の鍵を使用して暗号化するステップであって、前記第４の鍵が、第２のネットワークノードに関連付けられる公開鍵であり、前記デジタルデータが、配信経路沿いに前記ネットワークを介して前記受信者へ送られるように定義される、ステップと、
前記暗号化されたデータ及び前記暗号化された第１の鍵を前記第２のネットワークノードへ供給するステップと、
前記暗号化された第１の鍵を前記第２のネットワークノードにおいて前記第３の暗号化層に従って、前記第２のネットワークノードの前記公開鍵に対応する秘密鍵を使用して復号化するステップとをさらに含む、請求項７又は８に記載の方法。
【請求項１０】
前記暗号化するステップが、前記送信者、前記第１のネットワークノード又は前記暗号化されたデータと前記暗号化された第１の鍵とからなるメッセージが先に通過した第３のネットワークノードのうち１つによって実行される、請求項９に記載の方法。
【請求項１１】
各ネットワークノードにより前記暗号化されたデジタルデータ及び前記暗号化された第１の鍵を受信した後に実行される、
前記暗号化されて受信された第１の鍵が前記ネットワークノードにより特定の暗号化層に従って復号化されるかどうかを確立するステップと、
前記ネットワークノードが前記暗号化された第１の鍵を復号化しなければならない場合、前記暗号化された第１の鍵を前記特定の暗号化層に従って個々の秘密鍵を使用して復号化するステップと、
前記受信者を含む前記ネットワークの次のネットワークノードを確立するステップであって、前記暗号化されたデジタルデータ及び前記暗号化された第１の鍵が前記ネットワークノードによって供給されなければならない、ステップと、
前記暗号化された第１の鍵が少なくとも１つのさらなる暗号化層において前記次のネットワークノードに関連付けられる公開鍵及び／又はさらなるネットワークノードの公開鍵を使用して暗号化されなければならないかどうかを確立するステップと、
前記暗号化された第１の鍵が暗号化されなければならない場合、前記公開鍵を取得し、前記暗号化された第１の鍵を前記さらなる暗号化層に従って前記公開鍵を使用して暗号化するステップとをさらに含む、請求項７～１０のいずれか１項に記載の方法。
【請求項１２】
前記送信者及び／又は前記暗号化されたデータ及び前記暗号化された第１の鍵を送信するネットワークノードが、前記受信者を含む前記ネットワークの少なくとも１つのネットワークノードを特定し、前記暗号化されたデータ及び前記暗号化された第１の鍵が、前記受信者へ送信される際にこれを通過しなければならない、請求項７～１１のいずれか１項に記載の方法。
【請求項１３】
前記特定することが、少なくとも前記暗号化された第１の鍵を暗号化層に従って前記特定されたネットワークノードの公開鍵を使用して暗号化することよりなる、請求項１２に記載の方法。

【請求項１４】
公開鍵システムにおけるデジタルデータの配信を前記デジタルデータ上のデジタル署名を使用して制御するための方法であって、
前記デジタルデータのハッシュ値を送信者により算出するステップと、
第１のデジタル署名を前記送信者により、前記ハッシュ値を第１のデジタル署名スキームに従って第１の公開鍵対の第１の秘密鍵を使用して暗号化することによって算出するステップと、
第２のデジタル署名を、前記第１のデジタル署名を第２のデジタル署名スキームに従って第２の公開鍵対の第２の秘密鍵を使用して暗号化することによって算出するステップと、
前記第２のデジタル署名及び前記デジタルデータを前記デジタルデータの受信者へ供給するステップと、
前記第２のデジタル署名の第１の検証値を前記第２のデジタル署名スキームに従って前記第２の公開鍵対の公開鍵を使用して算出するステップと、
前記第１の検証値の第２の検証値を前記第１のデジタル署名スキームに従って前記第１の公開鍵対の公開鍵を使用して算出するステップと、
前記デジタルデータのハッシュ値を取得するステップと、
前記取得されたハッシュ値と前記第２の検証値とを比較するステップと、
前記比較するステップの結果、値が異なれば、前記受信者へのデータ配信プロセスは意図されたプロセスフローから外れていることを確立するステップとを含む、方法。
【請求項１５】
前記第１のデジタル署名を前記供給されたデジタルデータ及び前記供給された第２のデジタル署名と共に前記供給するステップ、又はさらなる供給するステップのいずれかにおいて取得するステップと、
前記取得された第１のデジタル署名と前記算出された第１の検証値とを比較するステップと、
前記比較するステップの結果、値が異なれば、前記受信者へのデータ配信プロセスは意図されたプロセスフローから外れていることを確立するステップとをさらに含む、請求項１４に記載の方法。
【請求項１６】
前記ハッシュ値を取得するステップが、
前記ハッシュ値を前記供給されたデジタルデータから、前記送信者によって実行された前記ハッシュ値を算出する第１のステップと同様にして算出するステップ、又は
前記ハッシュ値を、前記供給するステップにおいて前記供給されたデジタルデータ及び前記供給された第２のデジタル署名と共に取得するステップのうち少なくとも１つを含む、請求項１４又は１５に記載の方法。
【請求項１７】
前記第２のデジタル署名を算出するステップが、
前記第１のデジタル署名を交換するために、前記第２のデジタル署名の算出に先立って第３のデジタル署名を、前記第１のデジタル署名を第３のデジタル署名スキームに従って第３の公開鍵対の第３の秘密鍵を使用して暗号化することによって算出するステップをさらに含み、
前記第２の検証値を算出するステップが、
前記第１の検証値を交換するために、前記第２の検証値の算出に先立って前記第１の検証値の第３の検証値を、前記第３のデジタル署名スキームに従って前記第３の公開鍵対の公開鍵を使用して算出するステップをさらに含む、請求項１４～１６のいずれか１項に記載の方法。
【請求項１８】
前記第３のデジタル署名を前記供給されたデジタルデータ及び前記供給された第２のデジタル署名と共に前記供給するステップ、又はさらなる供給するステップの１つにおいて

取得するステップと、
前記取得された第３のデジタル署名と前記算出された第１の検証値とを前記第２の検証値を算出するステップに先立って比較するステップと、
前記比較するステップの結果、値が異なれば、前記受信者へのデータ配信プロセスは意図されたプロセスフローから外れていることを確立するステップとをさらに含む、請求項１７に記載の方法。
【請求項１９】
前記デジタル署名が、前記配信プロセスのために請求項１～６における少なくとも１つの請求項に定義されているように暗号化され、前記デジタル署名を算出するステップの各々及び前記検証値を算出する個々のステップ、比較し且つ確立する個々のステップが、前記暗号化層の１つに関連付けられ、且つこれに関連して実行される、請求項１４～１８のいずれか１項に記載の方法。
【請求項２０】
ネットワークを介する送信者から受信者までのデジタルデータの配信経路を制御するための方法であって、前記ネットワークが、複数の接続されたネットワークノードを備え、前記方法が、請求項１４～１８のいずれか１項のステップを含み、前記ネットワークノードの少なくとも１つが、前記デジタル署名を算出するステップの１つを実行する、方法。
【請求項２１】
前記ネットワークノードの少なくとも１つが、前記検証値を算出するステップと、ハッシュ値を取得するステップと、比較するステップと、確立するステップとを実行する、請求項２０に記載の方法。
【請求項２２】
前記ネットワークノードの少なくとも１つが、各ステップが前記公開鍵対の特定の１つに関連付けられる、
前記検証値を算出するステップ、
前記デジタル署名を取得するステップ、
前記取得されたデジタル署名と前記算出された検証値とを比較するステップ、
前記確立するステップのうち少なくとも１つのグループを実行する、請求項２０又は２１に記載の方法。
【請求項２３】
前記暗号化された第１の鍵を第３の暗号化層において第４の鍵を使用して暗号化するステップであって、前記第４の鍵が、第２のネットワークノードに関連付けられる公開鍵であり、前記デジタルデータが、配信経路沿いに前記ネットワークを介して前記受信者へ送られるように定義される、ステップと、
前記暗号化されたデータ及び前記暗号化された第１の鍵を前記第２のネットワークノードへ供給するステップと、
前記暗号化された第１の鍵を前記第２のネットワークノードにおいて前記第３の暗号化層に従って前記第２のネットワークノードの前記公開鍵に対応する秘密鍵を使用して復号化するステップとをさらに含む、請求項７又は８に記載の方法。
【請求項２４】
各々が前記公開鍵対の１つに関連付けられる署名スキームは互いに異なるものであることが可能であり、前記システム、前記デジタルデータの送信者又は前記デジタルデータを前記システム内の他の当事者へ供給する前記システム内の他の当事者により予め決められ、又は指定される、請求項１４～２３のいずれか１項に記載の方法。
【請求項２５】
各ネットワークノードにより前記デジタルデータ及び前記デジタル署名を受信した後に実行される、
前記受信されたデジタル署名が前記ネットワークによってデジタル式に署名されなければならないかどうかを確立するステップと、
前記ネットワークノードが前記受信されたデジタル署名をデジタル式に署名しなければ

ならない場合、前記受信されたデジタル署名を交換するために、前記デジタルデータ及び前記算出されたデジタル署名のさらなるネットワークノード又は前記受信者への供給に先立ってさらなるデジタル署名を、前記受信されたデジタル署名をさらなるデジタル署名スキームに従ってさらなる公開鍵対のさらなる秘密鍵を使用して暗号化することによって算出するステップと、

前記受信者を含む前記ネットワークの次のネットワークノードを確立するステップであって、前記デジタルデータ及び前記算出されたデジタル署名が、前記ネットワークノードによって供給されなければならない、ステップとをさらに含む、請求項２０～２４のいずれか１項に記載の方法。