【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9月28日(2006.9.28)

【公表番号】特表2006-500814(P2006-500814A)
【公表日】平成18年1月5日(2006.1.5)
【年通号数】公開・登録公報2006-001
【出願番号】特願2004-537385(P2004-537385)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成18年8月10日(2006.8.10)
【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】
各ユーザ設備により、少なくとも部分的に秘密であるそれぞれ固有の量に基づくそれぞれ相補的なデータで相互に対称的な演算を実行することを通じて、第１のユーザ設備iと第２のユーザ設備jとの間で共通の秘密データアイテムを生成する方法であって、
前記演算の結果は、前記共通の秘密データアイテムとして前記ユーザ設備の双方で使用され、
前記方法は、Abelian Varietyに定められるGAP Diffie-Hellmann問題に属する前記相補的なデータを定めることに基づくことを特徴とする方法。
【請求項２】
請求項１に記載の方法であって、
前記Abelian Varietyは、楕円曲線を通じた１次元を有する方法。
【請求項３】
請求項１に記載の方法であって、
双一次特性と非縮退特性と計算可能特性とを特徴とするペアFを、前記Abelian Varietyの２つの線形独立のポイントPとD(P)に適用することを有する方法。
【請求項４】
請求項１に記載の方法であって、
ユーザ設備iの前記演算は、$S_i=f_T(r_i)$及び$P_i=g(r_i)$に従った一方向関数fとgに基づき、パラメータTは、信頼できるマスター設備から取得したマスター秘密であり、結果Sは秘密に保持され、共通の秘密データは、

$$K_{ij}=F(S_i,P_j)=F(S_j,P_i)=K_{ji}$$

に従って計算される方法。
【請求項５】
請求項４に記載の方法であって、
前記演算は、データS_i及びP_iに基づき、

$$S_i:S_{i1}=T_{11}+r_iT_{12};\qquad (5')$$

$$S_{i2}=T_{21}+r_iT_{22};\qquad (6')$$

$$P_i:P_{i1}=r_iP;\qquad (7')$$

$P_{i2}=r_i^2P;$ (8')

である方法。

【請求項６】

請求項１に記載の方法であって、

ユーザ設備1は、データ$r_1D(P),r_1^2D(P)$をユーザ設備2に送信し、

ユーザ設備2は、データ$r_2D(P),r_2^2D(P)$をユーザ設備1に送信し、

それに続いて、トリプル$r_2D(P),r_2D(P),r_2^2D(P)$がDiffie-Hellmannトリプルであるか否かをユーザ設備1が検査し、トリプル$r_1D(P),r_1D(P),r_1^2D(P)$がDiffie-Hellmannトリプルであるか否かをユーザ設備2が検査し、

肯定的な場合に、

$\Pi_{k=1}^{2}e((t_{k1}+r_1t_{k2})P,v(r_2)_kD(P))=e(P,D(P))^{<v(r_1),Tv(r_2)>}$

に従ってユーザ設備1による共有鍵を計算し、ここで、$t_{12}=t_{21}$であり、$v(r_2)_k$はベクトル$v(r_2)$の第k成分を意味する方法。

【請求項７】

請求項１に記載の方法であって、

固有のパラメータを各ユーザ設備に割り当てることを通じて、１つ以上の選択されたユーザ設備を排除する標準的な機構の上に、取消機構を更に有する方法。

【請求項８】

請求項１に記載の方法であって、

前記共有の秘密の生成が、識別又は認証手順の初期ステップとして使用される方法。

【請求項９】

請求項１に記載の方法であって、

Weil Pairingは、真のプロトコルの実行の実質的に前にある時に求められる方法。

【請求項１０】

請求項１に記載の方法であって、

以前の秘密情報の漏洩に対して秘密情報を更新することを有する方法。

【請求項１１】

請求項１に記載の方法であって、

単一の統合した暗号化レベルのみを使用することを通じて実行される方法。

【請求項１２】

請求項１に記載の方法であって、

ランダム化機構が共通の秘密に適用される方法。

【請求項１３】

請求項１２に記載の方法であって、

前記ランダム化機構は、チャレンジ・レスポンス型機構に基づく方法。

【請求項１４】

第１のユーザ設備と第２のユーザ設備とを有し、請求項１に記載の方法に従って通信するように構成されたシステム。

【請求項１５】

請求項１４に記載のシステムの第１及び／又は第２のユーザ設備として動作するように構成された装置。

【請求項１６】

請求項１に記載の方法を実施するように１つ以上のデータ処理指向のハードウェアエンティティを制御する命令を有するコンピュータプログラム。