[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/30

[12] 发明专利申请公开说明书

[21] 申请号 03822191.8

[43] 公开日 2005 年 10 月 12 日

[11] 公开号 CN 1682485A

[22] 申请日 2003.8.11 [21] 申请号 03822191.8
[30] 优先权
[32] 2002. 9.20 [33] EP [31] 02078952.5
[86] 国际申请 PCT/IB2003/003641 2003.8.11
[87] 国际公布 WO2004/028075 英 2004.4.1
[85] 进入国家阶段日期 2005.3.18
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 P·T·图伊斯 M·E·范迪克
B·肖恩马克斯

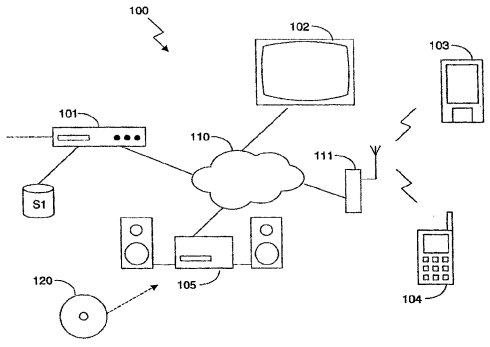
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 岳 刘 杰

权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称 产生公共密钥的方法和系统

[57] 摘要

一种在第一用户装置与第二用户装置之间通过其每一个产生公共密码数据项的方法，每个用户装置按各互补数据项执行互相对称的运算，这些运算基于各独特的运算量，其中至少部分是密码。 运算的结果用于所述两个装置上作为所述公共密码数据项。 特别是，本方法基于限定属于在阿贝尔簇中限定的一种 GAP Diffie – Hellmann 问题的互补数据。更具体地讲，该阿贝尔簇在椭圆曲线上的维数为 1。




ISSN1008-4274

知识产权出版社出版

1. 一种在第一用户装置 i 与第二用户装置 j 之间通过其每一个产生公共密码数据项的方法，该用户装置按各互补的数据项执行互相对称的运算，这些运算基于各独特的运算量，其中至少部分是密码，又其中，所述运算的一个结果被用于所述两个用户装置上作为所述公共密码数据项，

所述方法特征在于其基于限定属于在阿贝尔簇内限定的一种 GAP Diffie－Hellmann 问题的所述互补数据。

2. 权利要求 1 的方法，其中，所述阿贝尔簇在椭圆曲线上的维数为 1。

3. 权利要求 1 的方法，其中包含将具有特征为双线性特性、非退化特性和可计算性特性的一个对偶 F 用到所述阿贝尔簇中两个线性独立的点 P 和 D(P)上。

4. 权利要求 1 的方法，其中，用于用户装置 i 的所述运算是基于按照 $s_i=f_T(r_i)$和 $P_i=g(r_i)$的单向函数 f, g，其中，参数 T 是从可信的主装置上得到的主密码，运算结果 s 仍保持保密性，而公共密码数据按照下式计算:

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

5. 权利要求 4 的方法，其中，所述运算基于数据 $S_i$和 $P_i$:

$$S_i:s_{i1}=T_{11}+r_iT_{12};\quad (5')\qquad s_{i2}=T_{21}+r_iT_{22};\quad (6')$$

$$P_i:p_{i1}=r_iP;\quad (7')\qquad p_{i2}=r_i^2P;\quad (8')。$$

6. 权利要求 1 的方法，其中，用户装置 1 向用户装置 2 发送数据 $r_1D(P)$, $r_1^2D(P)$, 用户装置 2 向用户装置 1 发送数据 $r_2D(P)$, $r_2^2D(P)$, 随后由用户装置 1 检验三重数组 $r_2D(P)$, $r_2D(P)$, $r_2^2D(P)$是否为 Diffie－Hellmann 三重数组，并由用户装置 2 检验三重数组 $r_1D(P)$, $r_1D(P)$, $r_1^2D(P)$是否为 Diffie－Hellmann 三重数组，当检验为肯定时由用户装置 1 按照下式计算公共密码:

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

式中，$t_{12}=t_{21}$且 $v(r_2)_k$代表矢量 $v(r_2)$的第 k 个分量。

7. 权利要求 1 的方法，还包含在标准方案之上的无效方案，通过向每个用户装置指配其自身的独特参数以排除一个或多个所选择的用户装置。

8. 权利要求 1 的方法，其中，此种共享密码的产生在认证和证实方法中被应用作初始步骤。

9. 权利要求 1 的方法，其中，对 Weil 对偶性的估值实质上在执行正常的协议之前的瞬间进行。

10. 权利要求 1 的方法，并包含密码信息更新，以对抗早先的密码信息的泄漏。

11. 权利要求 1 的方法，其执行只是通过使用单个的综合加密层级。

12. 权利要求 1 的方法，对公共密码用随机化方案。

13. 权利要求 12 的方法，其随机化方案基于任务响应机制。

14. 一种包含第一用户装置和第二用户装置的系统，该系统被安排成按照权利要求 1 中的方法进行通信。

15. 一种装置，被安排成在权利要求 14 的系统中以第一和/或第二用户装置而工作。

16. 一种计算机程序产品，包含用于控制一种或多种数据处理的硬件实体，以实施权利要求 1 的方法。

# 产生公共密钥的方法和系统

## 发明背景

本发明涉及在第一用户装置与第二用户装置之间通过其每一个产生一种公共密码数据项的方法，该用户装置按各自的互补数据执行互相对称的运算，这些运算基于各独特的运算量，其中至少部分是密码，又其中，所述运算的一个结果被用在所述两个用户装置上作为所述公共密码的数据项，这在权利要求 1 的前序中有更多叙述。

在密码学中，共用密钥产生是一个重要问题．这个问题伸展到各种应用领域，诸如消费电子领域内的付费电视系统和各种认证方法中．密码数据项可以用作加密密钥或解密密钥，借以在用户装置或其他装置之间实现互相证实．先有技术中广泛地考虑 Diffie－Hellmann 方案，但这类方案的缺点是缺乏控制机理来校验所计算的密码数据项的真实性。另一方法，在美国专利 US Patent 5,218,637 中提出一种基于证书的系统，它可以设置共用密码数据项，该案卷号为 PHQ 90.021，并转让给本发明的受让人，他正是本发明的共同发明人之一。本技术可解决问题，但另一方面它需要复杂的构造，至少使用两个层级的公开密钥加密术。本发明的首要目的是只使用单个的综合加密术层级。这意味着，不需要第二密码数据项使验证运算生效。

本发明的再一个目的在于，系统应能用额外的用户装置扩展，给予它们的秘密等级与本发明可实现的现有系统的秘密等级相同，但并不需要为此额外修改此种现有系统。本发明的再另外一个目的在于，在得知与任意大的用户装置子集相关联的密码数据项上，不能为系统中存在的任何另加装置简明方便地计算出各的密码数据项．本发明的再进一步的目的是可以简洁地表示各种运算量和使用的数据项。

## 发明概要

因此，其中本发明的一个目的是提供一种改进的方法，用以在两个用户装置间产生一个公共密码数据项，同时能满足上面的要求。

所以，按照本发明的各个方面之一，本发明的特征在于权利要求 1 中的特征部分。具体讲，本发明的第一实施例基于所谓的 Weil 对偶性的

实用度，这在 CRYPTO 2001 期刊上登载的由 Dan Boneh 和 Matt Franklin 撰写的题目为“Identity Based Encryption from the Weil Pairing（基于 Weil 对偶性加密的认证）”的简明报告中有详细讨论。此外，本发明的第二个并且更宽泛的实施例基于所谓阿贝尔簇（Abelian Varieties）热点椭圆曲线的实用性，在椭圆曲线上 Weil 对偶性起作用，构成一个亚类。然而，对于本发明那样相同情况的运算和目的来说，上面的概念没有对此加以考虑。在 CRYPTO 2002 期刊上登载的由 K.Rubin 和 A.Silverberg 撰写的题目为“Supersingular Abelian Varieties in Cryptology（密码术中的超奇异点阿贝尔簇）”的简明报告中详细讨论了阿贝尔簇。本发明的再一个优点在于，由于有效地应用简明的数学方法，可以有简洁的表示式。

本发明还涉及一种包含第一用户装置和第二用户装置的系统，按照权利要求 1 中的方法它们安排成可以通信；一种装置，安排成在权利要求 3 中的系统内可工作为第一和/或第二用户装置；一个计算机程序产品，它包含计算机指令用以控制一种或多种数据处理的硬件实体，以实施权利要求 1 中的方法。本发明的再一个有利方面已在有关的从属权利要求中描述了。

## 附图简要说明

本发明的这些和更多的情况和优点将参照公开的优选实施例并具体地参考下面的附图在下面较详细地进行论述。

图 1 是按照本发明的一个系统，所包含的各种装置通过网络互连起来，按本发明的安排进行工作；

图 2 是图 1 中系统的总体表示。

## 所使用方法的数学表述

本发明的基本实施例基于 Weil 对偶性，这是从椭圆曲线到有限域的一种双线性映射。它通过对椭圆曲线的简洁表示来表达有限域上的离散对数问题。这种方法能应用共用的密码数据项以及长度小于 200 比特的其它参数，同时，仍用比码破碎实际较差的已有技术系统的计算复杂性大的计算来表示破碎码。此外，所提出的系统十分健壮，当有限数目的参加者知晓数据时不会暴露系统秘密，否则，有任意的依从用户时将考

虑产生新的共用密钥。

此外，每个用户或装置有其自身的独特参数，当情况需要时用户或装置可以在标准方案之上设置无效方案以排除所选择的装置。因此，系统在任何一对用户之间容许产生共用密码数据项，而比传统的系统所要求的存储容量要小。

现在，本实施例提出的协议基于 Diffie－Hellmann 问题的扩展版本。应当指出，在椭圆曲线 E 上，计算 Diffie－Hellmann（CDH）的问题是：对于给定的一个点 P∈E 和给定的 aP 与 bP，没有算法用以计算多项式时间算法中的 abP。现在，本发明采用扩展的 Diffie－Hellmann 问题或即 EDH，它在本发明中定义如下：

$$P, aP, bP, a^2P, b^2P \rightarrow abP$$

不可否认，在通用模型中仍然存在计算上的困难问题。不过，在椭圆曲线上的判定 Deffie－Hellmann 即 DDH 问题要简单得多。DDH 问题的定义如下：当给定三个点 aP、bP、cP（其中 P∈E）时，可判定是否 cP = (a*b)P。这种运算的相对简单性依据于已知的 Weil 对偶性方面高效可算的双线性映射，这将在下面进一步讨论。此外，所参考的出版物内已给出有另外的信息。具体讲，此类 CDH 运算困难而 DDH 相对简单的群称之为呈现一种 GAP Diffie－Hellmann 群。此类群可在阿贝尔簇中找到，其中，超奇异点椭圆曲线是维数为 1 的一个子类。于是，有着 CDH 问题计算困难而 DDH 容易得多的各种可行的此类椭圆曲线，可以应用下面示例的实施例曲线：

$$E^{+}: y^2 = x^3 + 2x + 1 \text{ over } F_3l$$

$$E^{-}: y^2 = x^3 + 2x - 1 \text{ over } F_3l$$

现在，令<P>为具有保密参数α的第一阶 q 的 $E/F_pl$ 子群。该参数α必须充分大，以使得计算 Diffie－Hellmann 问题 CDH 足够困难，但与此同时又不太大，以使判定 Diffie－Hellmann（DDH）的运算不是十分困难。应当注意，上述两个示例曲线的保密参数为α = 6(见 Boneh 的报告)。此外，我们假设在我们的建议中的失真映象（distortion map）D 或群同构的可用性，以使得点 D(P) ∈ $E/F_pl$ 对点 P 线性独立。失真映象原理在 EUROCRYPT 2001 期刊上由 E.Verheul 撰写的题目为“Evidence that XTR is more Secure than Supersingular Elliptic Curve Cryptosystems（XTR 比之超奇异点椭圆曲线加密系统更安全的论据）”

的论文中有明晰讨论。由此，该失真映象在群<P>与<D(P)>之间构成一个可高效计算的同构。应当注意，本例子中的椭圆曲线只是该方面大量曲线中的两个。

现在，就这两个线性独立的点 P 和 D(P)可应用 Weil 对偶性解决某些问题。为此，令 E[q]表示由 P 和 D(P)产生的 $E/F_p l\alpha$的子群。在此场合下，按照 e：E[q] x E[q]→F*pl，Weil 对偶性是一个映象，它满足下面的性质：

1. 对于 P∈E [q]，可得到 e (P, P)=1。

2. 对于所有 P1, P2 ∈E [q]和 r, s ∈Z，可得到双线性特性 $e(aP1, bP2) = e(P1,P2)^{ab}$。

3. 如果对 P∈E[q]而言对所有 P'∈E [q]得到 e(P, P')=1，则有非退化特性 P=O。

4. 对于所有 P1, P2 ∈E [q]，可以高效地计算 Weil 对偶性 e(P1, P2)，这是可计算性特性。

于是，可建立下面的方案。两个用户装置之每一个从可信的第三方获得下面的密码数据项，那些数据项在下面对用户 i 予以列出（应当指出，信用方可以是两个共同运算的用户装置之一）：

5. $(t_{11} + r_i t_{12})P$

6. $(t_{12} + r_i t_{22})P$

此外，又提供下面的两个数据项：

7. $r_i D(P)$

8. $r_i^2 D(P)$

然而，后两个数据项不必需保持秘密，因此，例如可以存储于公开的索引中以供此后的查询。此外，定义出下面的对称矩阵 $T(T_{12} = T_{21})$：

$$T=\begin{pmatrix} t_{11} & t_{12} \\ t_{12} & t_{22} \end{pmatrix} \in M_2(Z_q)$$

此外，引入矢量 v(r)，它们如下地与点 r ∈$Z_q$ 相关联：v(r)=(1, r)。于是，此后的协议进程为：

首先，用户 1 向用户 2 发送数据 $r_1 D(P)$, $r_1^2 D(P)$，此外，用户 2 向用户 1 发送数据 $r_2 D(P)$, $r_2^2 D(P)$，随后由用户 1 检验是否三重数组 $r_2 D(P)$,

$r_2D(P)$, $r_2^2D(P)$为 Diffie－Hellmann 三重数组，并由用户 2 检验是否三重数组 $r_1D(P)$, $r_1D(P)$, $r_1^2D(P)$为 Diffie－Hellmann 三重数组，在两个检验都为肯定的场合由用户 1 按照下式计算出共用密钥:

$$\Pi_{i=1}^{2} e((t_{11}+r_1 t_{12})P, v(r_2)_i D(P)) = e(P, D(P))^{\langle v(r_1), Tv(r_2)\rangle}$$

它是秘密的公共密钥。这里，$t_{12}=t_{21}$且 $v(r_2)$代表矢量 $v(r_2)$的第 i 个分量。可以证明，上面的协议安全性很高。安全性的有效主要原因在于探求 EDH 问题很困难。

进一步提高安全性等级的额外措施是伴随采用时间戳记使产生的共用密钥散列化。此外，用于产生共用密码而形成的协议的产生可以用作认证方法的初始步骤，它公开于欧洲专利申请 EP 02 075 983.3 中，其卷号为 PHNL 020192，并转让给本专利申请的同一受让人。

此外，通过预先已计算的对 Weil 对偶性 $e((t_{11}+r_1t_{12})P, D(P))$的估测，可以更高效地作出协议。虽然在提升存储设备上付出了代价，但在正常地实施协议上不再需要计算该 Weil 对偶性。

优选实施例详细说明

图 1 示明包含各种装置 101－105 的系统 100，各种装置通过网络互连起来，安排成按照本发明进行工作。本例子中该系统是一个家用系统，包含的装置诸如有收音机、电视机等。通常，有一个特别的装置是系统的主控，它控制其他装置。一般地，通过一个或多个装置接收内容，诸如从宽带网、互联网或卫星之类的外部信号源上经由居住区网关或机顶盒 101 进行接收。最终使内容在网络上传输过来，在装置之一中合适地呈现。

典型地，家用网络中的所有装置根据实施要求来实现安全性架构。应用这种架构，这些装置能互相证实，以保密方式分配内容。由安全性高的系统管理对内容的正常访问。这能防止未保护的内容泄漏到未被授权的装置上，又可防止来自不信任装置的数据进入系统中。依靠此种保护，事先已成功地证实的其他装置方能分配到由合格装置给出的内容。这样，可确保对手不会通过预谋的装置接收未被授权的拷贝。具体的装置如果它由授权的厂家制造，它只能成功地证实其自身，这是因为例如只有授权的厂家方知道成功地证实所必需的具体密码，原因是授权厂家的装置配置有由可信的第三方颁发的证明书。

图 2 示明图 1 之系统的一般化表示。图中，由试验器 P、校验器 V 和可信的第三方 TTP 配合运行。这里，校验器 V 通过使用从可信的第三方 TTP 上接收到的信息来证实试验器 P。最好，证实是互相的，以便试验器 P 也知道校验器 V 是证实了的。

对试验方 P 证实校验方 V 所需的信息假设在事先已由 TTP 分发给双方 P 和 V。做到这一点可以通过三方之间合适的通信装置。这样，可以生成动态协议，并容许更新信息，以应付对手企图达到未被授权地接入先前分发的密码。

试验器 P 和校验器 V 诸如可以是图 1 中的载体 120（它配置有提供所需功能度的芯片）以及音频重放装置 105。此种场合下，多半地没有从 TTP 到试验器 P 和校验器 V 的通信信道。因此，密码必须事先生效，例如在装置制造时。

这里，试验器 P 中包含组网模块 301、密码术处理器 302 和存储媒介 303。应用组网模块 301，试验器 P 能够针对校验器 V 发送和接收数据。组网模块 301 可以连接至图 1 中的网络 110 上，或是通过诸如无线方式与校验器 V 建立直接的连接。

用加密处理器 302 来执行按照本发明的方法。通常，该处理器 302 可以用硬件与软件的组合来实现，但另一种方法也可用单纯的硬件或软件来整个地实现。

现在，试验器 P 可以在存储媒介内存储所执行算法的各种参数，它又可进一步保存某些内容以分发给成功证实后的校验器 V。存储媒介 303 还能用来存储从 TTP 上接收到的信息。为了增强系统的安全性，不只是存储单个参数数据，可以取代地或额外地存储一个或多个中间计算结果。

类似地，校验器 V 中包含组网模块 311、加密处理器 312 以及所具功能度对应于试验器 P 之功能度的存储装置 313。如果校验器 V 以盘上芯片的载体来实现，则存储装置 313 可对应于能应用的光盘或其他盘体的存储器，不过，可取的方法是存储于盘上芯片的 ROM 内。

另外，试验器 P 和校验器 V 内可配置由硬件或软件实现的伪随机号码发生器 304、314，并给以加密方式提供强大的伪随机号码。这些号码能用于本发明的各种优选应用内。

补充的数学表示法

根据上述，公共密钥的产生可如下地实现：

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

同时，传输下面的数据；

$S_i=f_T(r_i)$ (5, 6)，以及

$P_i=g(r_i)$ (7, 8)

所传输数据项的另一种表示法为：

| | | |
|---|---|---|
| $S_i$ | $s_{i1}=T_{11}+r_iT_{12}$ | (5') |
| | $s_{i2}=T_{21}+r_iT_{22}$ | (6') |
| $P_i$ | $p_{i1}=r_iP$ | (7') |
| | $P_{i2}=r_i^2P$ | (8') |

这里，$T_{ij}=t_{ij}*P$，并且各数字值表示与早先的表达式相对应。

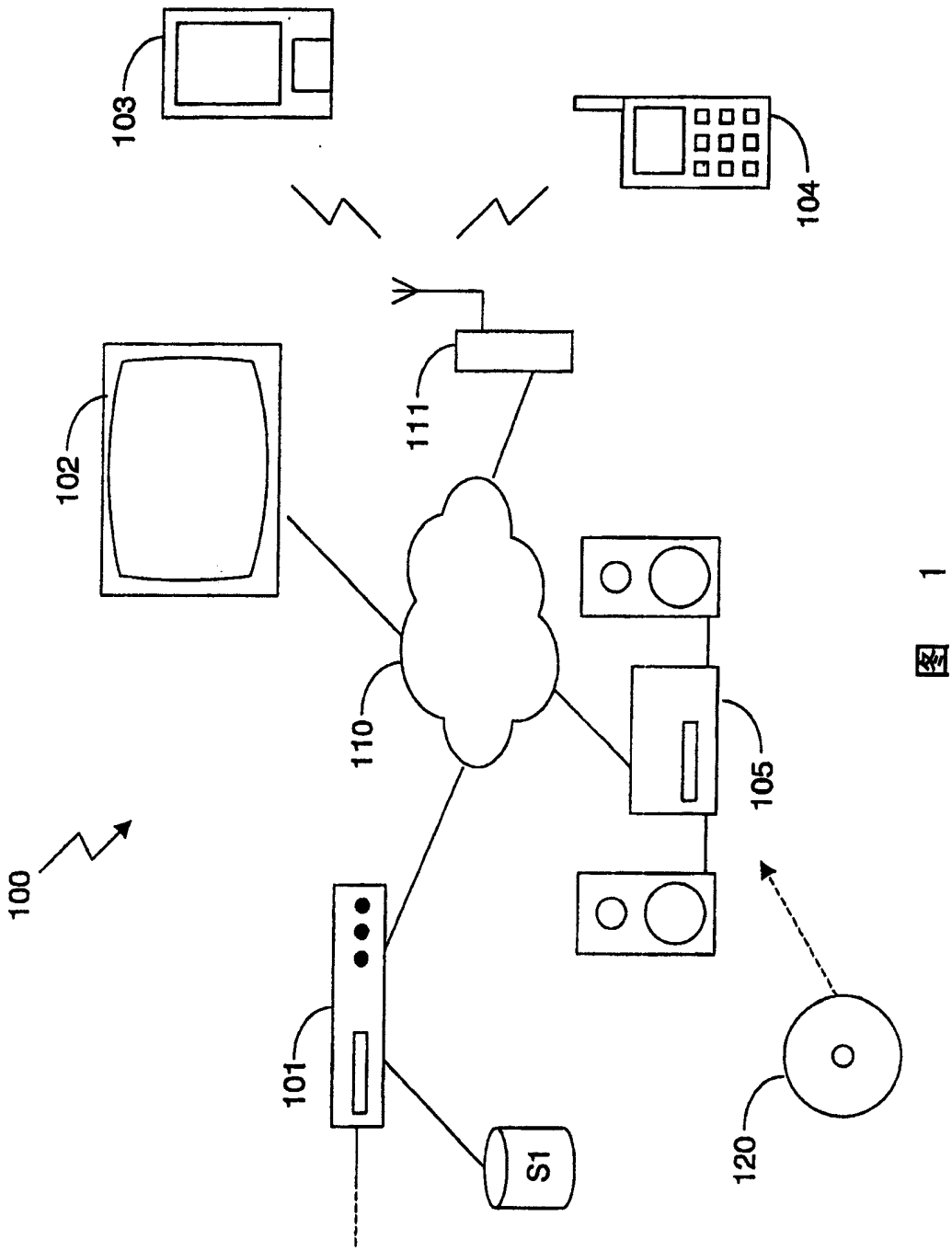



图 1

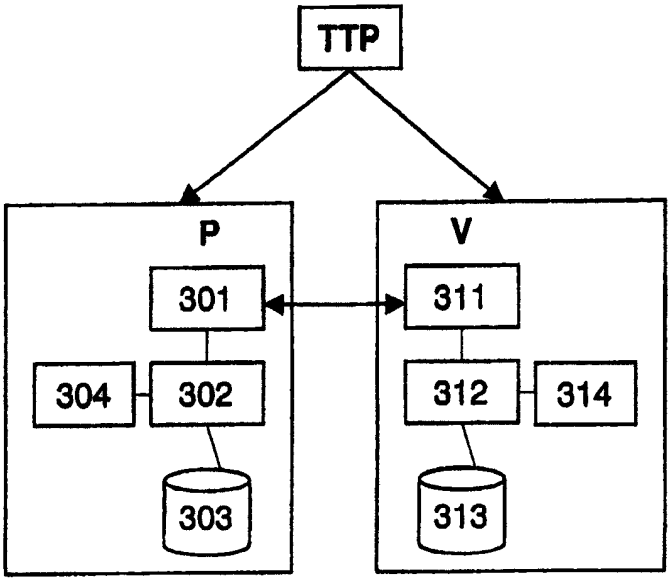



图 2