(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1694402 B
(45)授权公告日 2011.09.14

(21)申请号 200510066892.6

(22)申请日 2005.04.30

(30)优先权数据
04101879.7 2004.04.30 EP

(73)专利权人 捷讯研究有限公司
地址 加拿大安大略省

(72)发明人 迈克尔·K·布朗
赫伯特·A·利特尔
黛娜·L·M·戴维斯

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
H04W 12/06(2009.01)

(56)对比文件
US 2003/0233546 A1,2003.12.18, 全文.
US 5491750 A,1996.02.13, 全文.
WO 01/76134 A1,2001.10.11, 全文.
CN 1419356 A,2003.05.21, 全文.

审查员 白雪慧

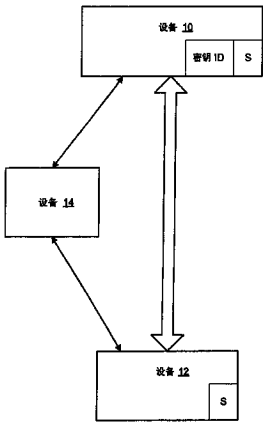
权利要求书 3 页 说明书 10 页 附图 1 页

(54)发明名称

设备认证

(57)摘要

在第一和第二设备每一个均具有共享密值的情况下,实现与第三设备通信的两个设备的认证。所述认证包括利用第三设备,将认证值从第一设备通信到第二设备。类似地,存在利用第三设备从第二设备到第一设备的数值通信。第三设备保留所通信的值。计算所述值以允许第三设备认证第一和第二设备,而无需第三设备接收共享密值。可以使用认证来建立第一和第二设备之间的通信信道。



CN 1694402 B

1. 一种由第三设备执行的方法，用于确定是否第一和第二设备均具有密钥值 h，第一和第二设备均具有公用密钥 P，所述公用密钥 P 的取值使得从乘积 hP 中获得密钥值 h 的运算是计算困难的运算，其中 F_q 是素数阶 q 的有限域，将公钥 P 定义为椭圆曲线 $E(F_q)$ 中的点，该点产生椭圆曲线 $E(F_q)$ 的阶 p 的素数子组，所述方法包括以下步骤：

第三设备从第一设备接收随机值 r_D 和公用密钥 P 的乘积 R_D，第三设备保留乘积 R_D 的拷贝；

第三设备从第二设备接收随机值 r_B 和公用密钥 P 的乘积 R_B 和质询值 e_D，第三设备保留乘积 R_B 和质询值 e_D 的拷贝；

第三设备将质询值 e_D 传送到第一设备；

第三设备从第一设备接收值 y_D 和质询值 e_B，第三设备保留值 y_D 和质询值 e_B 的拷贝，其中 $y_D = h-e_Dr_D \mod p$；

第三设备将质询值 e_B 传送到第二设备；

第三设备从第二设备接收值 y_B，其中 $y_B = h-e_Br_B \mod p$；以及

第三设备在满足条件 $y_BP+e_B R_B = y_DP+e_DR_D$ 时确定第一和第二设备均具有密钥值 h，其中

$1 < r_D < p-1$，$1 < r_B < p-1$，$1 < e_D < p-1$，并且 $1 < e_B < p-1$。

2. 根据权利要求 1 所述的方法，还包括：

第三设备在确定第一和第二设备均具有密钥值 h 之后，在第一和第二设备之间建立通信信道。

3. 根据权利要求 2 所述的方法，其中所述通信信道是第一和第二设备之间的直接通信信道。

4. 根据权利要求 2 所述的方法，其中所述通信信道上的所有通信都通过上述第三设备路由。

5. 根据权利要求 1 所述的方法，还包括：

第三设备从第二设备接收乘积 $R_C = r_CP$，r_C 是随机值，乘积 R_C 具有与乘积 R_B 和乘积 R_D 均不同的值；

第三设备获取不同于 e_B 和 e_D 的随机质询值 e_C，并且第三设备将质询值 e_C 传送到第二设备；

第三设备从第二设备接收值 y_C，其中 $y_C = h-e_Cr_C \mod p$；以及

当满足条件 $y_CP+e_CR_C = y_DP+e_DR_D$ 时，第三设备认证通信信道的闭合，

其中 $1 < r_C < p-1$，并且 $1 < e_C < p-1$。

6. 根据权利要求 1 所述的方法，还包括：

第三设备将乘积 R_B 送到第一设备，并且第三设备将值 y_B 送到第一设备，从而第一设备能够通过检查是否满足条件 $y_BP+e_BR_B = hP$ 来确定第二设备是否具有密钥值 h。

7. 根据权利要求 1 所述的方法，还包括：

第三设备将乘积 R_D 传送到第二设备，并且第三设备将值 y_D 传送到第二设备，从而第二设备能够通过检查是否满足条件 $y_DP+e_DR_D = hP$ 来确定第一设备是否具有密钥值 h。

8. 根据权利要求 1 所述的方法，其中密钥值 h 是从密值 s 中获得的，该方法还包括：

第三设备在满足条件 $y_BP+e_BR_B = y_DP+e_DR_D$ 时确定第一和第二设备均具有密值 s。

9. 根据权利要求 8 所述的方法，其中通过对密值 s 执行单向散列函数来从密值 s 获得值 h。

10. 根据权利要求 1 所述的方法，还包括：第三设备检查乘积 R_B 不等于无限点，和 / 或乘积 R_D 不等于无限点，和 / 或乘积 R_B 不等于乘积 R_D。

11. 根据权利要求 2 所述的方法，其特征在于通过将因特网协议地址分配给第一设备定义通信信道。

12. 一种第三设备，用于确定是否第一和第二设备均具有密钥值 h，第一和第二设备均具有公用密钥 P，所述公用密钥 P 的取值使得从乘积 hP 中获得密钥值 h 的运算是计算困难的运算，其中 F_q 是素数阶 q 的有限域，将公钥 P 定义为椭圆曲线 $E(F_q)$ 中的点，该点产生椭圆曲线 $E(F_q)$ 的阶 p 的素数子组，该第三设备包括：

用于从第一设备接收随机值 r_D 和公用密钥 P 的乘积 R_D，并且保留乘 积 R_D 的拷贝的装置；

用于从第二设备接收随机值 r_B 和公用密钥 P 的乘积 R_B 和质询值 e_D，并且保留乘积 R_B 和质询值 e_D 的拷贝的装置；

用于将质询值 e_D 传送到第一设备的装置；

用于从第一设备接收值 y_D 和质询值 e_B，并且保留值 y_D 和质询值 e_B 的拷贝的装置，其中 $y_D = h-e_Dr_D \mod p$；

用于将质询值 e_B 传送到第二设备的装置；

用于从第二设备接收值 y_B 的装置，其中 $y_B = h-e_Br_B \mod p$；以及

用于在满足条件 $y_BP+e_BR_B = y_DP+e_DR_D$ 时确定第一和第二设备均具有密钥值 h 的装置，其中

$1 < r_D < p-1$，$1 < r_B < p-1$，$1 < e_D < p-1$，并且 $1 < e_B < p-1$。

13. 根据权利要求 12 所述的第三设备，还包括：

用于在确定第一和第二设备均具有密钥值 h 之后，在第一和第二设备之间建立通信信道的装置。

14. 根据权利要求 13 所述的第三设备，其中所述通信信道是第一和第二设备之间的直接通信信道。

15. 根据权利要求 13 所述的第三设备，其中所述通信信道上的所有通信都通过上述第三设备路由。

16. 根据权利要求 12 所述的第三设备，还包括：

用于从第二设备接收乘积 $R_C = r_CP$ 的装置，r_C 是随机值，乘积 R_C 具有与乘积 R_B 和乘积 R_D 均不同的值；

用于获取不同于 e_B 和 e_D 的随机质询值 e_C 的装置，并且第三设备将质询值 e_C 传送到第二设备；

用于从第二设备接收值 y_C 的装置，其中 $y_C = h-e_Cr_C \mod p$；以及

用于当满足条件 $y_CP+e_CR_C = y_DP+e_DR_D$ 时，认证通信信道的闭合的装置，

其中 $1 < r_C < p-1$，并且 $1 < e_C < p-1$。

17. 根据权利要求 12 所述的第三设备，还包括：

用于将乘积 R_B 传送到第一设备，并且将值 y_B 传送到第一设备的装置，从而第一设备能

够通过检查是否满足条件 $y_BP+e_BR_B = hP$ 来确定 第二设备是否具有密钥值 h。

18. 根据权利要求 12 所述的第三设备，还包括：

用于将乘积 R_D 传送到第二设备，并且将值 y_D 传送到第二设备的装置，从而第二设备能够通过检查是否满足条件 $y_DP+e_DR_D = hP$ 来确定第一设备是否具有密钥值 h。

19. 根据权利要求 12 所述的第三设备，其中密钥值 h 是从共享密值 s 中获得的，该第三设备还包括：

用于在满足条件 $y_BP+e_BR_B = y_DP+e_DR_D$ 时确定第一和第二设备均具有密值 s 的装置。

20. 根据权利要求 12 所述的第三设备，其中通过对密值 s 执行单向散列函数来从密值 s 获得值 h。

21. 根据权利要求 12 所述的第三设备，还包括：

用于检查乘积 R_B 不等于无限点，和 / 或乘积 R_D 等于无限点，和 / 或乘积 R_B 不等于乘积 R_D 的装置。

22. 根据权利要求 13 所述的第三设备，其特征在于通过将因特网协议地址分配给第一设备定义通信信道。

设备认证

技术领域

[0001] 本发明通常涉及电子设备之间的通信，更具体地，涉及包括由第三设备的认证的两个电子设备的认证。

背景技术

[0002] 在电子设备之间的通信中，有时，需要两个设备使用第三设备来彼此通信。典型地，一个设备将对第三设备进行请求，寻求建立与第二设备的通信。在这样的情况下，第三设备可以充当网守，并且根据为两个设备所定义的许可，阻止或允许这样的通信。

[0003] 在设备之间的通信安全性成问题的情况下，可以向两个通信设备提供密值或密钥，可以用于确定是否可以在两个设备之间建立通信信道。第三设备可以根据由各个通信设备所保持的共享值，执行指令以允许或拒绝两个设备之间的通信。

[0004] 在更一般的方式中，可能存在针对第三设备认证两个设备的其他理由。在要认证的两个设备的每一个均具有相同的密值时，通过每一个设备向第三设备提供其密值的拷贝以进行比较，所述第三设备可以对所述两个设备进行认证。

[0005] 然而，如果第一或第二和第三设备之间的通信可能不安全，或者如果第三设备自身可能不安全，则由于使所述共享值的保密处于危险中，因此，典型地，对第三设备的密值或密钥的直接通信并不理想。

[0006] 以 Blom 的名义的美国专利申请 No. 2003/233546 提出了一种挑战响应认证过程，包括通过掩蔽函数来掩蔽由认证中心所产生的期望响应，并且将掩蔽的期望响应而非期望响应自身传送到在其上发生实际用户认证的中间方。所述中间方还从用户接收用户响应，并且利用与认证中心所进行的相同的掩蔽函数来产生掩蔽的用户响应。为了认证 用户，中间方然后认证所掩蔽的用户响应与从认证中心接收到的掩蔽后的期望响应相对应。

[0007] 因此，需要具有一种由其中降低了共享值的暴露危险的第三设备来认证两个设备的机制。

发明内容

[0008] 根据本发明的一个方面，提出了一种改进的设备认证方法。

[0009] 根据本发明的另一方面，提出了一种认证过程，用于认证每一个均具有共享密值的两个设备，其中，第三设备能够确定每一个通信设备是否均具有相同的共享密钥值，而无需直接具有该值。

[0010] 根据本发明的另一方面，提出了一种使用第三设备在两个设备之间建立通信信道的方法。正在寻求通信的两个设备具有共享密钥值。所述通信设备能够向第三设备证明其每一个均具有相同的密钥值（因此，得到认证）。在该认证过程中，第三设备能够确定每一个通信设备是否具有相同的共享密值，而无需第三设备具有该值。

[0011] 根据本发明的另一方面，提出了一种安全地闭合使用以上所述的认证建立的通信信道的方法。

[0012] 根据本发明的另一方面，提出了一种由第三设备来认证第一和第二设备的方法，所述第一和第二设备每一个均具有共享密钥值 h。每一个所述设备具有可用于其的公用密钥 P，对公用密钥 P 进行选择，从而使从乘积 hP 中获得密钥值 h 的运算是计算困难的运算，所述方法包括以下步骤：第一和第二设备使用第三设备，彼此传送第一组值和不同的第二组值，从而使第一设备能够利用等价于乘积 hP 的值来计算第一表达式，并且第二设备能够利用等于乘积 hP 的值来计算第二表达式，第三设备保留在第一和第二设备之间进行通信的数值拷贝，所述方法还包括步骤：第三设备计算并比较第一表达式和第二表达式的值以认证第一和第二设备。

[0013] 根据本发明的另一方面，提出了上述方法，其中第一设备是无线手持设备，第二设备是公司服务器，并且第三设备是路由器，其中，第三设备认证第一和第二设备的步骤包括：在第一和第二设备之间建 立通信信道的步骤。

[0014] 根据本发明的另一方面，提出了上述方法，其中，所建立的通信信道包括第三设备，作为信道的一部分，并且第三设备已经保留了在第一设备和第二设备之间进行传送的值，所述方法还包括以下步骤：闭合第二设备和第三设备之间的通信信道，闭合所述信道的步骤包括以下步骤：第二设备和第三设备交换闭合认证值组，以允许第三设备根据所保留的值和闭合认证值来执行对表达式的计算，以认证通信信道的闭合。

[0015] 根据本发明的另一方面，提出了一种利用第三设备认证第一和第二设备的方法，所述第一和第二设备每一个均具有共享密钥值 h，每一个设备用于对所定义的组 $E(F_q)$ 和 Z_p 执行数学运算，其中 F_q 是素数阶 q 的有限域，包括相对于所述组定义的标量相乘，所述方法包括以下步骤：

[0016] a) 获得公用密钥 P，从而使 P 产生阶数为 p 的组 $E(F_q)$ 的素数子组，并且使公用密钥 P 可用于每一个设备，

[0017] b) 第一设备获得随机值 r_D，从而使 $1 < r_D < p-1$ 并且计算值 $R_D = r_D P$，

[0018] c) 第一设备将值 R_D 传送到第三设备，

[0019] d) 第三设备保留值 R_D 的拷贝，并且将值 R_D 转发到第二设备，

[0020] e) 第二设备获得随机值 r_B，从而使 $1 < r_B < p-1$ 并且计算值 $R_B = r_B P$，其中确定 R_B 从而使其不等于 R_D，第二设备获得随机值 e_D 从而使 $1 < e_D < p-1$，第二设备将值 e_D 和 R_B 传送到第三设备，

[0021] f) 第三设备保留 R_B 和 e_D 的拷贝，并且将所述值转发到第一设备，

[0022] g) 第一设备计算值 $y_D = h - e_D r_D \mod p$，第一设备获得随机值 e_B，从而使 $1 < e_B < p-1$，第一设备将值 y_D 和 e_B 传送到第三设备，

[0023] h) 第三设备保留值 y_D 和 e_B 的拷贝，将所述值转发到第二设备，

[0024] i) 第二设备计算值 $y_B = h - e_B r_B \mod p$，并且第二设备将值 y_B 传送到第三设备，以及

[0025] j) 当满足条件 $y_B P + e_B R_B = y_D P + e_D R_D$ 时，第三设备认证第一和第二设备。

[0026] 根据本发明的另一方面，提出了上述方法，还包括步骤：当满足条件 $y_B P + e_B R_B = hP$ 时，第一设备认证第二设备。

[0027] 根据本发明的另一方面，提出了上述方法，还包括步骤：当满足条件 $y_D P + e_D R_D = hP$ 时，第二设备认证第一设备。

[0028] 根据本发明的另一方面，提出了上述方法，其中由未认证标识符来识别第一设备，

并且第二设备保留密钥值组，所述组包括与第一设备的密钥值共享的密钥值，所述方法包括步骤：第一设备将未认证标识符传送到第二设备中，由此，第二设备可以从所述密钥值组选择与第一设备的密钥值共享的密钥值。

[0029] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：从共享密钥值 s 中获得值 h。

[0030] 根据本发明的另一方面，提出了上述方法，其中获得值 h 的步骤包括步骤：对共享密钥值 s 执行单向散列函数。

[0031] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：第一、第二和第三设备的一个或多个检查值 e_D 不为零和 / 或值 e_B 不为零。

[0032] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：第一、第二和第三设备的一个或多个检查值 R_B 不等于无限点，和 / 或 R_D 不等于无限点。

[0033] 根据本发明的另一方面，提出了上述方法，其中第一、第二和第三设备的一个或多个检查值 R_B 不等于值 R_D。

[0034] 根据本发明的另一方面，提出了上述方法，其中第一设备是无线手持设备，第二设备是公司服务器，并且第三设备是路由器，其中，第三设备认证第一和第二设备的步骤包括：在第一和第二设备之间建立通信信道的步骤。

[0035] 根据本发明的另一方面，提出了上述方法，其中通过将因特网协议地址分配给第一设备来第一通信信道。

[0036] 根据本发明的另一方面，提出了上述方法，其中所建立的通信信道包括第三设备，作为信道的一部分，并且所述第三设备已经保留了 y_D、P、e_D 和 R_D，并且所述方法还闭合第二设备和第三设备之间的通信信道，闭合所述信道的步骤包括以下步骤：

[0037] k) 第二设备获得随机值 r_C 从而使 $1 < r_C < p-1$，并且计算值 $R_C = r_C P$，由此，将 R_C 限制为具有与 R_B 和 R_D 均不同的值，

[0038] 1) 第二设备将值 R_C 传送到第三设备；

[0039] m) 第三设备获得随机值 e_C，从而使 $1 < e_C < p-1$，第三设备将值 e_C 传送到第二设备，

[0040] n) 当满足条件 $y_C P + e_C R_C = y_D P + e_D R_D$ 时，第二设备认证所述闭合操作。

[0041] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：第二设备检查值 e_C 不为零。

[0042] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：第二设备检查值 R_C 不等于无限点。

[0043] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：第二和第三设备之一或全部检查值 R_C 不等于值 R_B 且不等于值 R_D。

[0044] 根据本发明的另一方面，提出了上述方法，其中还包括步骤：第二和第三设备之一或全部检查值 e_C 不等于值 e_D 且不等于值 e_B。

[0045] 根据本发明的另一方面，提出了一种包括具有在介质上具体实现的可执行程序代码的所述介质的程序产品，所述可执行程序代码可在第一设备、第二设备和第三设备上分别执行，所述可执行程序代码用于执行上述方法。

[0046] 根据本发明的另一方面，提出了一种包括第一设备、第二设备和第三设备的系统，

所述第一和第二设备每一个均具有共享密钥值 h，每一个所述设备具有可用于其的公用密钥 P，对公用密钥 P 进行选择，从而使从乘积 hP 中获得密钥值 h 的运算是计算困难的运算，所述第一设备、第二设备和第三设备每一个均具有用于存储并执行程序代码的存储单元和处理器，

[0047] 所述程序代码用于利用第三设备，在第一设备和第二设备之间对第一组和不同的第二组值进行传送；

[0048] 所述程序代码用于使第一设备利用等价于乘积 hP 的值来计算第一表达式，并且使第二设备利用等于乘积 hP 的值来计算第二表达式；

[0049] 所述程序产品用于使第三设备保留在第一和第二设备之间进行 传送的数值拷贝，并且所述程序代码用于使第三设备计算并比较第一表达式和第二表达式的值以认证第一和第二设备。

[0050] 根据本发明的另一方面，提出了上述系统，其中第一设备是无线手持设备，第二设备是公司服务器，并且第三设备是路由器，其中，用于使第三设备认证第一和第二设备的程序代码包括：用于在第一和第二设备之间建立通信信道的程序代码。

[0051] 根据本发明的另一方面，提出了上述系统，其中所建立的通信信道包括第三设备，作为信道的一部分，并且第三设备包括用于保留在第一设备和第二设备之间进行传送的值的存储器，所述程序代码还包括：用于闭合第二设备和第三设备之间的通信信道的程序代码，所述代码包括用于在第二设备和第三设备之间交换闭合认证值组，以允许第三设备根据所保留的值和闭合认证值来执行对表达式的计算，以认证通信信道的闭合的程序代码。

[0052] 根据本发明的另一方面，提出了一种包括第一设备、第二设备和第三设备的系统，第一和第二设备每一个均具有共享密钥值 h，每一个设备用于对所定义的组 $E(F_q)$ 和 Z_p 执行数学运算，其中 F_q 是素数阶 q 的有限域，包括相对于所述组定义的标量相乘，所述第一设备、第二设备和第三设备每一个均包括用于存储和执行程序代码的存储单元和处理器，

[0053] o) 所述程序代码用于获得公用密钥 P，从而使 P 产生阶数为 p 的组 $E(F_q)$ 的素数子组，并且使公用密钥 P 可用于每一个设备，

[0054] p) 所述程序代码用于使第一设备获得随机值 r_D，从而使 $1 < r_D < p-1$ 并且计算值 $R_D = r_D P$，

[0055] q) 所述程序代码用于使第一设备将值 R_D 传送到第三设备，

[0056] r) 所述程序代码用于使第三设备保留值 R_D 的拷贝，并且将值 R_D 转发到第二设备，

[0057] s) 所述程序代码用于使第二设备获得随机值 r_B，从而使 $1 < r_B < p-1$ 并且计算值 $R_B = r_B P$，其中确定 R_B 从而使其不等于 R_D，使第二设备获得随机值 e_D 从而使 $1 < e_D < p-1$，并且将值 e_D 和 R_B 传送到第三设备，

[0058] t) 所述程序代码用于使第三设备保留 R_B 和 r_D 的拷贝，并且将所述 值转发到第一设备，

[0059] u) 所述程序代码用于使第一设备计算值 $y_D = h - e_D r_D \bmod p$，以使第一设备获得随机值 e_B，从而使 $1 < e_B < p-1$，并且使第一设备将值 y_D 和 e_B 传送到第三设备，

[0060] v) 所述程序代码用于使第三设备保留值 y_D 和 e_B 的拷贝，将所述值转发到第二设备，

[0061] w) 所述程序代码用于使第二设备计算值 $y_B = h - e_B r_B \bmod p$，并且使第二设备将值

y_B 传送到第三设备，以及

[0062] x) 当满足条件 $y_BP+e_BR_B = y_DP+e_DR_D$ 时，所述程序代码用于使第三设备认证第一和第二设备。

[0063] 根据本发明的另一方面，提出了上述系统，其中第一设备是无线手持设备，第二设备是公司服务器，并且第三设备是路由器，其中用于使第三设备认证第一和第二设备的程序代码包括：用于在第一和第二设备之间建立通信信道的程序代码。

[0064] 本发明的优点包括相对于第三设备对两个设备进行认证，而无需第三设备已经与其通信，或者具有与两个认证设备所具有的共享密值有关的直接信息。

附图说明

[0065] 在仅作为示例示出了本发明的优选实施例的附图中，其中：

[0066] 图 1 是示出了两个设备和在前两个设备的认证中所使用的第三设备。

具体实施方式

[0067] 存在许多不同情况，其中寻求在两个不同的电子设备之间建立通信，并且第三设备用于控制这样的通信是否将发生。图 1 是示出了设备 10 和设备 12 的方框图，其中要建立通信信道。在图 1 所示的示例中，设备 14 确定这样的通信是否可以发生。通过确定每一个设备具有共享密值，根据对设备 10、12 的认证来进行确定。在图 1 所示的示例中，在设备 10、12 之间示出了直接通信信道。其他配置也是可能的，其中设备 10、12 使用设备 14 来建立通信，例如，通过设备 14 来路由所有通信。

[0068] 尽管优选实施例的描述涉及通信设备，但是本领域的技术人员将会理解，可以针对由第三设备来实现两个设备的认证的其他环境来实现优选实施例。每一个设备 10、12 必须能够与设备 14 进行通信，但是对设备 10、12 进行认证的最终目的不必一定是其彼此间的通信。

[0069] 本领域的技术人员将会理解，如该描述中所涉及的，电子设备包括能够与其他设备建立通信且能够执行如下所述的计算的所有方式的设备。特别地，所述设备包括通信服务器，例如电子邮件和其他消息服务器，与诸如因特网等网络、无线手持通信设备和其他服务器、桌面、便携或手持设备（包括典型地在计算环境或电话中所使用的设备）结合在一起使用。

[0070] 描述了优选实施例，作为针对这样的电子设备所实现的方法。能够以计算机程序产品来具体化该实现，包括可传递到该描述中所涉及的设备的介质上的程序代码。这样的程序代码可以在所涉及的设备上执行，从而实现所述方法。

[0071] 优选实施例的一个实现示例包括以下配置：其中图 1 所示的设备 14 是路由器，用于向作为无线手持设备的设备 10 分配 IP（因特网协议）地址。设备 14 的路由器建立无线手持设备 10 和公司服务器（在图 1 所述的示例中，表示为设备 12）之间的连接。在该示例中，设备 14 路由器从设备 12 公司服务器向手持设备 10 转发业务。为了没有其他设备能够从设备 14 路由器中不适当地获得 IP 地址，在优选实施例中，手持设备 10 和设备 12 公司服务器均具有密值 s。如以下所述，设备 14 路由器能够确定设备 10（手持）是可信设备，并且应该由设备 14（路由器）来建立与设备 12（公司服务器）的通信信道。在该示例中，一旦

已经由设备 14 路由器进行了认证，则通过使用所分配的 IP 地址，向手持设备 10 转发通信，并且利用因特网，转发来自设备 12 公司服务器的通信。

[0072] 以下所阐明的优选实施例的描述包括多个步骤，其中检查在设备之间所发送的值。为了确保在该方法中仅存在一个故障点，当这样的检查确定存在错误条件时，优选实施例的方案将要按照以下方式对数值之一进行重新定义，所述方式为：将使该方法不能在其最后的步骤 中认证这些设备。如本领域的技术人员所意识到的，可能存在用于实现这样的检查的其他方法，这将导致该方法在较早的位置处终止，或以另一方式来指定错误条件。

[0073] 参考设备 10、12、14 来描述优选实施例，每一个设备均能够实现密码函数，并且在实施例中，会共享以下密码系统参数。在组 $E(F_q)$ 和 Z_p 中实现所述数学运算。在优选实施例中，将 $E(F_q)$ 定义为相对于 F_q 的国家标准和技术协会 (NIST) 所批准的 521 比特的随机椭圆曲线。该曲线具有等于 1 的辅助因子。将域 F_q 定义为素数阶 q 的有限域。Z_p 是以 p 为模的整数组。在以下描述中，将公钥 P 定义为点 $E(F_q)$，产生阶 p 的 $E(F_q)$ 的素数子组。符号 xR 表示椭圆曲线标量相乘，其中 x 是标量且 R 是在 $E(F_q)$ 上的点。该椭圆曲线点 R 有时需要表示为整数，用于一些计算。该表达为 $\overline{R}=(\bar{x} \bmod 2^{\frac{f}{2}})+2^{\frac{f}{2}}$，其中 $\bar{x}$ 为椭圆曲线点 R 的 x 坐标的整数表示，并且 $f = \log_2 p+1$ 是 p 的比特长度。

[0074] 如将会意识到的，对于优选实施例的不同实现，对在其上要实现优选实施例的操作的组的选择可以改变。椭圆曲线是在密码术中用于这样的操作的通用组。任何数学定义组可以用于实现优选实施例。例如，由以素数为模的整数所定义的组可以用于实现。

[0075] 在表 1 中，如以下所阐明的，描述了优选实施例的计算和通信。在优选实施例中，s 是对设备 10 和设备 12 已知而对设备 14 未知的共享值。在优选实施例中，设备 12 可以与一个或多个设备进行通信，因此，设备 10 具有标识符密钥 ID，用于指定哪一设备或哪类设备正在寻求与设备 12 进行通信。类似地，在其他实施例中，设备 12 可以具有标识符以允许设备 10 指定哪一设备正在请求进行认证。将会理解，所述密钥 ID 自身不足以认证该设备。还将会理解，如果设备 10 的身份从该环境中显而易见，则密钥 ID 可能是不必须的。例如，如果设备 12 与单一设备 10 而不与其他这样的设备进行通信，则密钥 ID 可能是不必要的。

[0076] 表 1

[0077]

设备 10	设备 14	设备 12
计算：h = SHA-512(s)		计算：h = SHA-512(s)
产生随机 r_D，$1 < r_D < p-1$ 计算 $R_D = r_D P$		
将 R_D 发送到设备 14；将密钥 ID 发送到设备 14。		
	在 R_D == 无限点时，则 R_D = rand()。将 R_D 发送到设备 12；将密钥 ID 发送到设备 12	
		在 R_D == 无限点时，则 R_D = rand()。产生随机数 r_B，$1 < r_B < p-1$ 计算 $R_B = r_B P$ 在 $R_D == R_B$ 时，则选择另一 R_B。产生随机 e_D，$1 < e_D < p-1$ 将密钥 ID、e_D 和 R_B 发送到设备 14。

[0078]

设备 10	设备 14	设备 12
	在 R_B == 无限点时或 R_D == R_B 时，则 R_B = rand()。在 e_D == 0 时，则 e_D = rand()。将密钥 ID、e_D 和 R_B 发送到设备 10。	
在 R_B == 无限点时或 R_D == R_B 时，则 R_B = rand()。在 e_D == 0 时，则 e_D = rand()。计算 $y_D = h-e_D\ r_D \bmod p$ 产生随机 e_B，$1 < e_B < p-1$ 将 y_D 和 e_B 发送到设备 14.		
	在 e_B == 0 或 e_B == e_D 时，则 e_B = rand()。将 y_D 和 e_B 发送到设备 12。	
		在 e_B == 0 或 e_B == e_D 时，则 e_B = rand()。计算 $y_B = h-e_B\ r_B \bmod p$. 将 y_B 发送到设备 14。
	将 y_B 发送到设备 10.	

[0079]

设备 10	设备 14	设备 12
如果 $y_BP+e_B\ R_B$ ！= hP，则拒绝	如果 $y_BP+e_B\ R_B$ ！= $y_DP+e_D\ R_D$，则拒绝	如果 $y_DP+e_D\ R_D$ ！= hP，则拒绝

[0080] 上述表格指定了在优选实施例的处理中所采用的步骤，用于实现对两个通信设备（设备 10、12）的认证，包括第三方认证（设备 14）。本领域的技术人员将会理解，某些步骤可以采用不同的次序，并且如下所示，可以省略某些步骤。

[0081] 在优选实施例中所实现的第一步骤用于每一设备 10、12，以便根据共享密值 s 来计算散列函数。在该优选实施例中，该散列函数是 SHA-512 散列函数，如在联邦信息处理标准公布 180-2 中所定义的那样。可以使用其他类似函数。由两个设备 10、12 使用通过应用散列函数所达到的值 h。使用散列函数值 h 而不直接使用数值 s 使该过程更为安全，这是由于在以下所阐明的不同计算中并未直接使用共享密值 s。在优选实施例中，为了在初始阶段将共享值 s 提供给两个设备，可以由设备 10、12 之一随机地产生值 s，然后利用安全通信信道，将其通信到另一个。例如，在设备 10 是无线手持设备且设备 12 是公司服务器的情况下，可以由公司服务器产生共享密值的值，然后，当该设备处于通过安全网络连接与公司服务器相连的底座中时，将其通信到无线手持设备。

[0082] 在确定值 h 之后，优选实施例的认证过程中的下一步骤用于由设备 10 产生随机 r_D 值，以便与公用密钥值 P 进行组合。将该随机值定义为大于 1 且小于 p-1。在该示例中，将 p 定义为由椭圆曲线 $E(F_q)$ 中的点 P 所产生的 $E(F_q)$ 的素数组的阶数。一旦获得了随机 r_D 值，采用标量相乘 r_DP 的结果来计算值 R_D。然后，将该随机化公用密钥值 (R_D) 与密钥 ID 值一起发送到设备 14。在设备 14 处，实现对 R_D 值的错误检查。如果 R_D 等于无限点，则在公共密钥值存在错误（如果 P 是有效公用密钥，则标量乘积将不等于该无限点）。根据优选实施例，通过设置等于随机值的 R_D 值（由表 1 中的 R_D = rand() 的伪码来指定）来实现错误处理。然后，由设备 14 将该 R_D 值和密钥 ID 值转发到设备 12。将会注意，在优选实施例中，设备 14 将在存储器中保留其接收并转发的特定数值。这些保留的值用于最终的授权步骤，如以下所描述的那样。

[0083] 在设备 12 中，存在对 R_D 值的进一步错误检查（与无限点进行比较），并且如果需要，执行类似的错误处理步骤。设备 12 还产生其自己的随机值，以便与公用密钥 P 进行组合。随机值 r_B 定义在范围 1 到 p-1 内，并且标量乘积 r_BP 定义了值 R_B。执行设备 12 处的错误检查，以确保 R_B 不等于 R_D。如果这些值是等效的，则定义新随机值 r_B，并且计算新 R_B 值。

由于在 R_B 等价于 R_D 的情况下，攻击者能够确定值 h，因此采用该步骤。

[0084] 此外，在该步骤中，在设备 12 处，获得了随机定义的质询值 (challenge value) e_D。产生该 e_D 值，以使其大于 1 而小于 p-1。由设备 12 将由设备 12 所确定的 e_D 和 R_B 值发送到设备 14。设备 14 可以与包括设备 10 的设备组同时地执行多个类似事务。为了允许设备 14 确定哪一包括设备 10 的设备组以向其发送数值，还由设备 12 将密钥 ID 值、以及 e_D 和 R_B 值返回到设备 14。

[0085] 在设备 14 处，存在对 R_B 值执行的错误检查。将 R_B 值与无限点进行比较，并且可能采用错误处理步骤。按照对 R_D 进行比较且在以上所述的较早步骤中所采用的错误处理步骤的相同方式对 R_B 值执行比较和错误处理。类似地，将 R_D 和 R_B 的值彼此进行比较，并且如果确定其是等价的，则作为错误处理步骤，将 R_B 定义为随机值。将 R_D 和 R_B 的等价识别为错误条件，这是由于设备 12 按照确保其具有与 R_D 不同的值的方式来产生 R_B。如果在由设备 14 进行接收时，两个值是相同的，则必然在传输中存在错误，或者攻击者已经重新定义了这些值。

[0086] 此时，在设备 14 处执行进一步的检查以确保 e_D 没有值 0。如果该值为 0，则将 e_D 值设置为随机值。如果 e_D 已经被设置为值 0（可能由寻求获得信息以实现虚假认证的攻击者所进行），则值 h 可以变得已知。为了避免这种情况，将 e_D 赋予随机值。将会意识到，尽管可以将确保 R_D 不等于 R_B 的检查和确保 e_D 不等于 0 的检查称为错误检查，但是执行这些检查以确保攻击者不能够获得与值 h 有关的信息。

[0087] 一旦完成了以上所涉及的检查，则设备 14 向设备 10 发送密钥 ID、R_B 和 e_D 值。

[0088] 在优选实施例中，在接收到密钥 ID、R_B 和 e_D 值时，设备 10 将执行与在设备 10 处所执行的相同的检查，并且采用相同的错误处理步骤（根 据需要，将 R_B 或 e_D 设置为 0）。如同在设备 12 和设备 14 之间通信这些数值的情况，设备 14 和设备 10 之间的通信是攻击者可能寻求改变数值以通过不适当的设备认证对通信信道进行访问的可能点。

[0089] 如表 1 所示，一旦在设备 10 处已经发生了对值 R_B 和 e_D 的检查，则存在 y_D 值的计算。该值的定义如下：

[0090] $y_D = h - e_D \ r_D \mod p$

[0091] 如以下更详细地描述的，在比较中使用该 y_D 值，将对设备 10、12 彼此进行认证且相对于设备 14 进行认证。

[0092] 由设备 10 所执行的另一步骤是产生质询值。该质询值是从大于 1 且小于 p-1 的范围内随机地选取的 e_B 值。然后，将 y_D 和 e_B 值均发送到设备 14。

[0093] 在设备 14 处，将 e_B 值与 0 和与 e_D 进行比较。如果 e_B 具有等于以上值中的任一个，则将 e_B 设置为随机值。

[0094] 然后，由设备 14 将 e_B 值与 y_D 值一起发送到设备 12。在设备 12 处，再次检查 e_B 值（相对于 0 和 e_D），如果该检查不成功，则将 e_B 设置为随机值。然后，计算 y_B 值：

[0095] $y_B = h - e_B \ r_B \mod p$

[0096] 如将会看到的，按照与 y_D 的定义对称的方式来定义值 y_B。将对其进行计算的设备 12 将 y_B 值发送到设备 14，并且从设备 14 发送到设备 10。

[0097] 在该过程的这一点上，已经由设备 10 将 y_D 和 R_D 值发送到设备 12，并且已经由设备 12 将 y_B 和 R_B 值发送到设备 10。另外，还已经将转发到设备 14 和发送自设备 14 的数值

的拷贝保留在设备 14 中。结果，如将在表 1 中的最后步骤中将会看到的，执行认证步骤以认证设备 10 和设备 12 均具有相同的共享密值 s。

[0098] 特别地，在设备 14 中，当且仅当：

[0099] $y_B P+e_B R_B = y_D P+e_D R_D$

[0100] 时，存在两个设备的认证。

[0101] 在设备 10 处，当且仅当

[0102] $y_B P+e_B R_B = hP$

[0103] 时，存在对设备 12 的认证。

[0104] 在设备 12 处，当且仅当

[0105] $y_D P+e_D R_D = hP$

[0106] 时，存在对设备 10 的认证。

[0107] 如本领域的技术人员将会显而易见，以上所述的认证过程利用了在 Schnorr 标识策略（例如，参见 A.Menezes，P. van Oorschot and S.Vanstone.Handbook of Applied Cryptography，CRC 出版社，纽约，1997）中所描述和使用的特定数学运算和等价物。然而，优选实施例允许两个设备彼此相互认证，并且允许第三设备对两个设备进行认证。由第三设备（在该示例中的设备 14）所执行的认证示出了以下事实：第三设备并不知道在设备 10、12 之间共享的密值 s。将会注意到，作为已经采用的一系列重叠步骤的结果，同时执行设备 10、12 之间的相互认证。

[0108] 该优选实施例的认证过程适合于用于以下情况：正在定义两个设备之间的通信信道，并且第三设备将提供允许对信道进行建立的信息。在无线手持设备使用路由设备来对公司服务器进行访问时，这可能会发生。所述路由设备充当第三设备，需要服务器和无线手持设备的认证。上述过程允许执行这样的认证，并且使第三设备（例如，路由器）进行认证，而无需知道密值，并且具有减小的状态信息组。

[0109] 上述优选此时里的描述包括应用于 R 值的错误检查。执行该检查以确定 R 是否为有效的公用密钥值。如将会意识到，如果可以确保 R_D 并不等于 R_B，则可以从优选实施例的方法中省略该错误检查，尽管通常最好执行该检查以确保正在正确地执行该过程。此外，优选实施例描述了在设备 10 和设备 12 处的密值的散列值的计算。尽管优选的步骤是使对密值的直接使用最少，但是，并不需要使用散列值将该密值 s 编码为值 h。如果在这种方式下未使用散列值，则直接使用密值来计算不同的认证值。

[0110] 如以上所涉及的，可以在通过第三设备建立从一个设备到第二设备的通信信道时使用该认证过程。在这种情况下，有利地，使用认证协议来闭合 (close) 第三设备和另两个设备之一之间的信道。在优选实施例中，可以在第三设备保留了特定值的基础上，适当地设置这样 的认证闭合协议。特别地，在建立通信信道之前已经发生了认证之后，第三设备（在图 1 的示例中，设备 14）保持值 $y_D P+e_D R_D$、R_D、R_B、e_D、e_B。设备 12 保留值 R_D、R_B、e_D、e_B、h。在表 2 中，阐明了用于以下情况的认证过程：设备 14 已经认证了设备 12，如上所述，并且设备 12 寻求闭合通信信道。

[0111]

设备 14	设备 12
	设备 12 发起闭合与设备 14 的连接。选取随机 r_C，$1 < r_C < p-1$ 计算 $R_C = r_C P$ 在 $R_C == R_B$ or $R_C == R_B$ 时，则选择另一 R_C。将 R_C 发送到设备 14。
在 R_C ==无限点或 $R_C == R_B$ 或 $R_C == R_D$ 时，则 R_C = rand()。产生随机 e_C，$1 < e_C < p-1$ 在 $e_C == e_D$ 或 $e_C == e_B$ 时，则选择另一 e_C。将 e_C 发送到设备 12。	
	在 $e_C == 0$ 或 $e_C == e_D$ 或 $e_C == e_B$ 时，则 e_C = rand()。计算 $y_C = h - e_C r_C \mod p$ 将 y_C 发送到设备 14。
如果 $y_C P + e_C R_C$ ！ = $y_D P + e_D R_D$，则拒绝	

[0112] 如从以上所看到的，对闭合协议的认证是可用的，即使设备 14（第三设备未处理或直接使用密值 s 或散列值 h。在这种情况下，该认证根据如上所述的设备（在所给出的示例中的设备 12、14）所保留的值，遵循 Schnorr 标识策略。作为使用上述认证过程的结果，这些值可用于第三设备。

[0113] 因此，作为示例已经描述了本发明的各种实施例。本领域的技术人员将会理解：在不脱离本发明的情况下，可以进行各种变化和修改。本发明包括落在所附权利要求的范围内的所有这样的变体和修改。

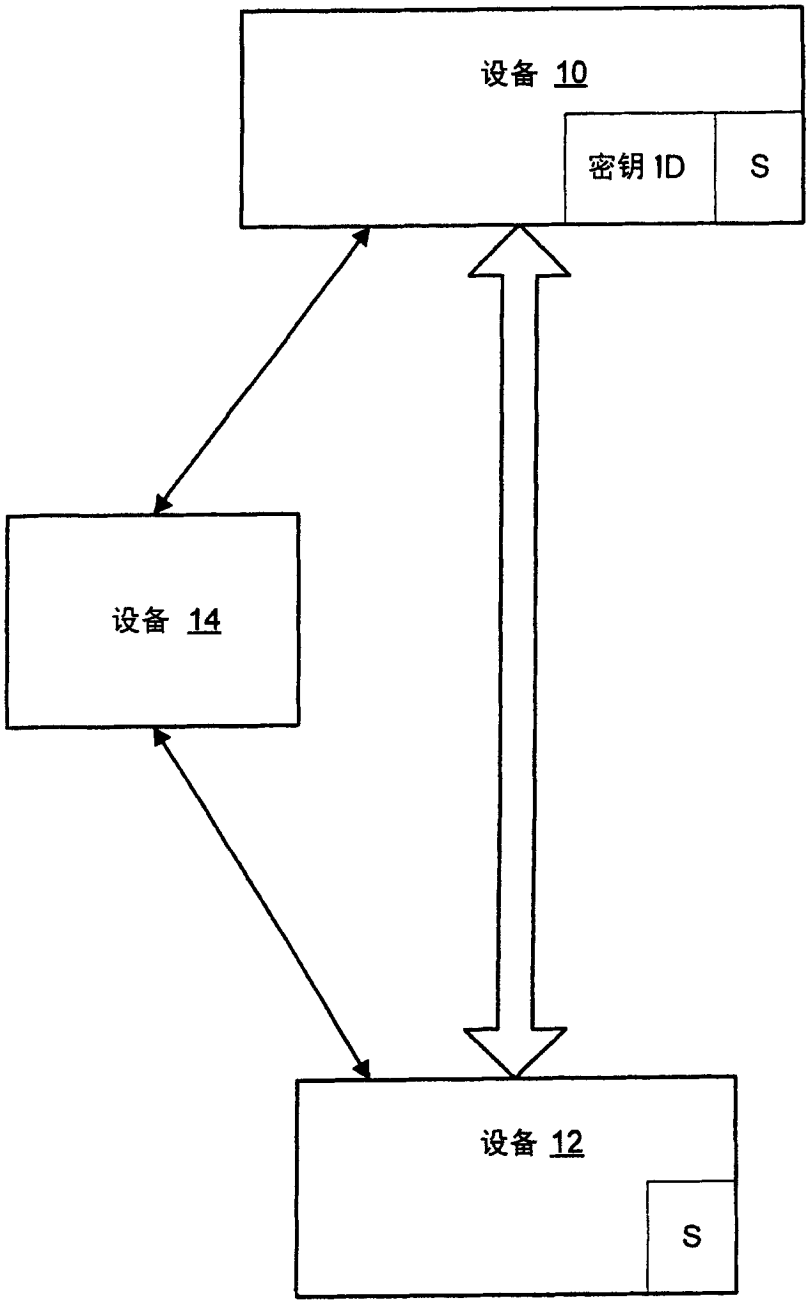


图 1