(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102833748 A
(43)申请公布日 2012.12.19

(21)申请号 201210349976.0

(22)申请日 2012.09.20

(71)申请人 北京邮电大学
地址 100876 北京市海淀区西土城路 10 号

(72)发明人 贾庆轩 郜盼盼 高欣 赵兵
翟峰 王鑫

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)

权利要求书 1 页 说明书 7 页 附图 1 页

(54)发明名称

一种基于数字证书的无线网络轻量级认证密钥协商协议

(57)摘要

本发明涉及一种可用于无线网络的轻量级认证密钥协商协议，基于“证书私钥－保护密钥”双重认证系统和“保护密钥”动态协商机制，结合公钥密码与共享动态保护密钥对用户身份进行双重认证，用户通过交换证书及私钥签名证明会话持有及私钥拥有性，进行第一重认证，通过共享保护密钥进行第二重认证。协议利用上次会话结束后双方共享保护密钥保护重要参数的交换，并使用本次会话新计算的保护密钥确认密钥的正确性，每轮通信在交换参数的同时即可验证其正确性。密钥组的协商及参数交换均采用简单的位运算，并通过Finished消息完成密钥更新的确认。协议设置会话ID来动态选择是否利用已共享的旧参数计算本次会话密钥，在保证安全高效的同时增强协议的灵活性。

CN 102833748 A

1. 一种基于数字证书的无线网络认证密钥协商协议，其特征在于包括以下步骤：

1) 使用数字证书及持有证书者的数字签名证明私钥拥有性，并结合共享对称密钥进行双重身份认证；

2) 利用新旧保护密钥结合的方法保护参与新会话密钥组计算的重要参数的交换；

3) 利用新协商的 MAC 密钥计算 MAC 值进行密钥确认，确保双方新会话密钥组以及保护密钥的动态同步更新。

2. 如权利要求 1 所述的无线网络轻量级认证密钥协商协议，其特征在于：

所述步骤 2) 中结合新旧密钥保护参与计算新会话密钥的重要参数交换的具体步骤是（假定通信双方为 Alice 和 Bob）：

2.1)Bob 首先验证 Alice 数字证书的有效性及私钥拥有性，验证成功后利用 Alice 的公钥加密参数 k，发送给 Alice；

2.2)Bob 利用上次会话双方已计算好的保护密钥来保护 n_B，具体计算过程见图 1，发送给 Alice；

2.3)Alice 接收后，通过共享的保护密钥 K_{1old} 计算得到 n_B，利用新计算出的 K_{1new} 来验证所接收到的 n_B 的正确性，若验证通过，则利用上次会话双方已共享的保护密钥来保护 n_A，发送给 Bob，具体计算过程见图 1；

2.4)Bob 接收后，通过共享的保护密钥 K_{2old} 计算得到 n_A，并利用新计算出的 K_{2new} 验证其正确性，具体计算过程见图 1。

其中新旧密钥保护重要参数的结合之处在于，使用公钥及旧保护密钥来保护参数，使用新保护密钥来验证所接收参数的正确性，新旧密钥相辅相承，参数的交换与正确性验证同时完成，使攻击者很难攻破三道防线，获得全部参数进而得到会话密钥或是篡改参数欺骗用户。

3. 如权利要求 1 所述的无线网络轻量级认证密钥协商协议，其特征在于：

所述步骤 3) 中密钥更新的具体步骤为：

3.1)Bob 在计算得到新会话密钥之后，利用 MAC 密钥及初始向量对上一步接收到的参数计算 MAC 值，之后将密钥更新为新协商的会话密钥组。同时令 $K_{1old} = K_{1new}$，$K_{2old} = K_{2new}$，把本次会话新计算出来的共享密钥更新为保护密钥．保护下次会话的参数交换。

3.2)Alice 在计算得到新会话密钥之后，利用 MAC 密钥及初始向量对上一步发送给 Bob 的参数计算 MAC 值，与接收到的 MAC 值进行比较，若两值相等，则将密钥更新为新协商的会话密钥组。同时令 $K_{1old} = K_{1new}$，$K_{2old} = K_{2new}$，把本次会话新计算出来的共享密钥更新为保护密钥，保护下次会话的参数交换。

一种基于数字证书的无线网络轻量级认证密钥协商协议

技术领域

[0001] 本发明涉及一种可用于无线互联网络的轻量级认证密钥协商协议，利用“证书私钥－保护密钥”双重认证系统和“保护密钥”动态协商机制，并采用新旧保护密钥相结合的方法保护重要参数的交换，会话密钥的运算均使用超轻量级运算符，最后结合 BAN 逻辑和非形式化分析方法对协议进行安全性分析，证明其在达到一级信仰和二级信仰的同时具有双向实体认证、完美的向前保密性等安全属性。本协议仅需要两次通信即可完成密钥协商阶段的参数交换，会话密钥组的计算使用运算量很小的位运算，具有传输高效、存储量小、计算量低等特点，适用于无线互联网用户间的身份认证，密钥协商和密钥更新，保密通信等领域。

背景技术

[0002] 在非对称密码体制出现之前，早期的认证协议都是基于对称密码体制设计，用户间不能协商会话密钥，后来伴随着公钥密码的发展，一些认证协议开始基于公钥密码体制或是公钥体制与对称密码相结合的方法设计。早期提出的如 Needham-Schroeder 协议、Woo-Lam 协议、Denning-Sacco 协议和 Fiat-Shamir 认证协议等著名协议后来被发现在重放攻击或已知密钥攻击下不安全。2002 年，Kim 等人 (Kim M, Kim K.A New Identification Scheme Based on the Bilinear Diffie-Hellman Group[C]. In Information security and privacy :7th Australasian Conference, ACISP 2002 Melbourne. Australia, July 3-5, 2002 :362-378.) 基于 BDHP 困难性问题提出一个认证协议，但是该协议的交互过程较复杂并存在安全漏洞。2003 年中国推出了自己的无线局域网国家标准 GB 15629.11(Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11 :Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications.GB 15629.11-2003.(in Chinese))，标准包含无线认证和保密基础设施 WAPI 机制，但该协议在认证环节缺乏私钥验证，密钥协商环节不具备前向安全性等安全属性，不能抵抗重放攻击及密钥非同步等攻击。2004 年，IEEE 标准批准 802.11i 安全规范 (IEEE P802.11i/D3.0, Specification for Enhanced Security[OL], http://standards.ieee.org/reading /ieee/std/lanman/rafts/P802.11i.pdf)， 由于 AP 端发送的“EAP-Success”消息为明文传送，很容易被攻击者伪造进行中间人攻击。 同 年 PoPescu(Popescu, C.A secure authenticated key agreement protocol. Electrotechnical Conference, 2004.MELECON 2004.Proceedings of the 12th IEEE Mediterranean.12-15 May 2004(2) :783-786.) 提出了一种认证密钥协商协议，该协议的安全性及执行效率都较好，但是由于参数的下确性确认完全依赖于协议参与者双方的长期共享密钥，故不具有密钥泄漏安全性。2005 年，Sui 等人 (Sui A, Hui L, Yiu S, Chow K, Tsang W, Chong C, et al.An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication.In IEEE wireless

and communications and networking conference(WCNC 2005),2005:2088-93.)提出了基于口令的椭圆曲线认证协议,该协议虽然计算开销较小,但不能抵抗离线口令穷举攻击。2007 年.Feng 等人(冯登国,陈伟东.基于口令的安全协议的模块化设计与分析[J].中国科学 E 辑,2007,37(2):223-237.)提出了基于口令的模块化认证协议,但是由于协议在通信及计算上的开销都较大,不适用于无线互联网络。2010 年,Lo 等人(Lo J-W,Lee C-C,Hwang M-S.A secure and efficient ECC-based AKA protocol for wireless mobile communications.Int J Innovat Comput Inform Control 2010,6(11):5249-58.)利用 ECC 算法提出了基于口令的认证密钥协商协议,2011 年 He(He D.Weakness in an ECC-based AKA protocol for wireless mobile communications.Cryptology ePrint Archive,Report 2011/336,2011.)指出 Lo 等人的协议并不能抵抗离线口令穷举攻击。2012 年,Jonathan 等人(Jonathan Katz,Philip MacKenzie,Gelareh Taban,Virgil Gligor.Two-server password-only authenticated key exchange[J].Journal of Computer and System Sciences,March 2012,78(2):651-669)设计了一个双服务器认证密钥协商协议,但以上协议由于其通信计算量开销过大或抗攻击能力不够导致它们并不适合应用于无线网络。

发明内容

[0003] 基于上述,本发明提出一种应用于无线网络的轻量级认证密钥协商协议,该协议中保护重要参数交换的保护密钥动态变化,弥补了上述协议的不足,不仅具有完备的安全属性,抵抗多种攻击,而且满足无线网对于通信次数少和计算开销小的需求,通过结合 BAN 逻辑形式化分析和非形式化分析方法对协议进行分析,证明其能够在保证安全的情况下高效的完成用户间的保密通信。

[0004] 为了实现此目的,本发明设计了基于数字证书的无线网络轻量级认证密钥协商协议,其具体交互流程如图 1 所示。

[0005] 协议中的符号定义:

[0006] K_a,K_b:Alice,Bob 的公钥。

[0007] $K_{a^{-1}}$,$K_{b^{-1}}$:Alice,Bob 的私钥。

[0008] Rot(x,y):x 循环左移 f(y) 位。

[0009] Mixbits(x,y) 算法描述:

[0010] z ← x

[0011] for i = 1 to 32 do

[0012] $z \leftarrow (\frac{z}{2} + z + z + y) \bmod 2^L$

[0013] end for

[0014] return z

[0015] $\oplus$:按位进行异或运算

[0016] $\vee$:按位进行或运算

[0017] 本发明的优点在于:通信次数少,计算量小,安全性较高,能够实现双向实体认证,密钥协商,具有完美的向前保密性 (PFS),并且能够抵抗重放攻击,非同步攻击,已知密钥攻

击等攻击，为用户间的快速双向认证和密钥协商提供了高效安全的解决方案，适用于无线互联网络。

附图说明

[0018] 图 1 为本发明中所设计的基于数字证书的无线网络轻量级认证密钥协商协议的具体交互过程；

具体实施方式

[0019] （一）实施步骤

[0020] 协议包含了身份认证、密钥协商和密钥更新三个阶段，现将协议中用户 Alice 和 Bob 的具体交互过程描述如下：

[0021] 1. Alice 向 Bob 发送 Hello 消息挑起会话，并在 Hello 消息之后附上 Alice 的数字证书及会话 ID，计算消息摘要并用 A 的私钥加密生成数字签名。注意当会话 ID 为非 0 时，表示用户希望恢复之前会话的参数，在计算新密钥时使用已保存的上次会话的 k。

[0022] 2. Bob 在收到 A 的 Hello 消息后，检查 A 的数字证书有效性，进行身份认证，提取出 Alice 的公钥，验证 A 的数字签名，检查消息完整性，证明 A 确实为此次会话持有者。

[0023] 3. Bob 生成随机数 k，n_B，将两个参数与旧保护密钥 K_{1old} 一起计算 α，K_{1new}，K_{2new}，β 如图 1 所示，用 Alice 的公钥加密 k，发送 $session\ ID \| Certificate\ B \| [k]_{Ka} \| \alpha \| \beta \| [H]_{Kb^{-1}}$ 给 Alice，其中 $[H]_{Kb^{-1}}$ 为使用 Bob 的私钥加密消息前面几个部分的消息摘要生成的数字签名。在这一步骤中，若 Bob 同意恢复之前的会话，则回复与 Alice 相同的会话 ID，表示同意在计算新密钥时复用之前会话中的 k，给 Alice 发送的信息中无须包含 $[k]_{Ka}$，省去了公钥加解密的开销。

[0024] 4. Alice 收到消息后，首先检查证书的有效性，对 Bob 进行身份认证，若证书中的身份信息与 Bob 的身份吻合，则提取出公钥验证 Bob 的数字签名，检查信息的完整性，证明 Bob 确实为此次会话持有者。

[0025] 5. 若 Alice 在第 4 步检查信息的完整性通过，则用自己的私钥解密 $[k]_{Ka}$，得到 k，由旧保护密钥 K_{1old} 和 α 解出 n_B，根据 k 和 n_B 计算出新保护密钥 K_{1new}，由 n_B 和 K_{1new} 计算得到 β′，比较 β′ 与 β 是否相等。若相等，执行第 6 步。

[0026] 6. 生成随机数 n_A，使用新旧保护密钥由 K_{2new}，K_{2old}，n_A 计算得到 γ，δ 如图所示，并发送 γ ‖ δ 给 Bob。

[0027] 7. Bob 收到消息后，根据 γ，K_{2old} 算出 n_A，由新保护密钥 K_{2new}，n_A 计算得到 δ′，根据 K_{1new}，K_{2new}，n_A，n_B 计算得到新会话密钥组 K_{AB}。比较 δ′ 与 δ 是否相等，若相等，则将密钥更新为 K_{AB}。

[0028] 8. 将会话密钥组 K_{AB} 截为六段，依次为 A 方加密密钥，B 方加密密钥，A 方 MAC 密钥，B 方 MAC 密钥，A 方初始向量，B 方初始向量。使用 MAC 密钥及初始向量对第 7 步中收到的 γ ‖ δ 计算 MAC 值作为 Finished 消息发送给 Alice，供 Alice 进行密钥确认。之后将自己的密钥更新为新协商的会话密钥组 K_{AB}。同时更新共享保护密钥，令 $K_{1old} = K_{1new}$，$K_{2old} = K_{2new}$，保护下次会话的参数交换。

[0029] 9. Alice 计算会话密钥组 K_{AB}，并用同样的方法截取为六段，使用 MAC 密钥及初始向

量对第 6 步中计算的 γ ‖ δ 计算 MAC 值，与收到的 Finished 消息进行比较，若一致，则将自己的密钥更新为新协商的会话密钥组 K_{AB}。同时更新共享保护密钥，令 $K_{1old} = K_{1new}$，$K_{2old} = K_{2new}$，保护下次会话的参数交换。至此身份认证及密钥协商阶段结束，之后可以开始使用协商好的密钥加密应用数据。

[0030] （二）BAN 逻辑形式化分析

[0031] 首先利用 BAN 逻辑形式化分析方法对本发明所提出的轻量级无线网络认证密钥协商协议进行形式化分析，分析过程严格按照 BAN 逻辑要求的分析步骤进行。

[0032] 协议的认证目的：

[0033] 一级信仰：$A|\equiv A\xleftarrow{K_{AB}}B,\ B|\equiv A\xleftarrow{K_{AB}}B$

[0034] 二级信仰：$A|\equiv B|\equiv A\xleftarrow{K_{AB}}B,\ B|\equiv A|\equiv A\xleftarrow{K_{AB}}B$

[0035] 协议的描述：

[0036] A → B：{Certificate A, Session ID}

[0037]

$$B\rightarrow A:\left\{Certificate\ B, Session\ ID, \{k\}_{K_A}, K_{1old}\oplus n_B, [Rot(k,k)\vee Rot(n_B,n_B]\oplus\overline{n_B}\right\}_{K_{B^{-1}}}$$

[0038] $A\rightarrow B:\{K_{2old}\oplus n_A, Mixbits(n_B,k)\oplus\overline{n_A}\}$

[0039] $B\rightarrow A:\{K_{2old}\oplus n_A, Mixbits(n_B,k)\oplus\overline{n_A}\}_{K_{AB}}$

[0040] 协议理想化：

[0041] 省略消息 1，因为它对分析协议的逻辑属性没有作用。

[0042] 消息 2：$B\rightarrow A:\left\{\xrightarrow{K_B}B, \{k\}_{K_A}, \{n_B\}_{K_{1old}}, (k,n_B)\right\}_{K_{B^{-1}}}$

[0043] 消息 3：$A\rightarrow B:\{n_A, A\xleftarrow{K_{AB}}B\}_{K_{2old}}$

[0044] 消息 4：$B\rightarrow A:\{n_A, A\xleftarrow{K_{AB}}B\}_{K_{AB}}$

[0045] 初始化假设：

[0046] (1) $A|\equiv\#(k, n_B)$

[0047] (2) $B|\equiv\#(n_A)$

[0048] (3) $B|\equiv\xrightarrow{K_A}A$

[0049] (4) $A|\equiv\xrightarrow{K_B}B$

[0050] (5) $A|\equiv(B|\Rightarrow(k,n_B))$

[0051] (6) $B|\equiv A\xleftarrow{K_{2old}}B$

[0052] (7) $B|\equiv A\Rightarrow(n_A, A\xleftarrow{K_{AB}}B)\}$

[0053] (8) $A|\equiv n_A$

[0054] 逻辑推理：

[0055]

$$A\triangleleft\left\{\xrightarrow{K_B}B, \{k\}_{K_A}, \{n_B\}_{K_{1old}}, (k,n_B)\right\}_{K_{B^{-1}}} \qquad (1\text{-a})$$

[0056] 由公式 (1-a) 和假设 (4)，应用消息含义中的公钥规则得到

[0057] $A|\equiv B|\sim\left\{\xrightarrow{K_B}B,\{k\}_{K_A},\{n_B\}_{K_{1old}},(k,n_B)\right\}$ (1-b)

[0058] 由公式 (1-b)，应用发送规则，可得

[0059] $A|\equiv B|\sim(k,n_B)$ (1-c)

[0060] 由公式 (1-c) 和假设 (1)，应用临时值验证规则，可得

[0061] $A|\equiv B|\equiv(k,n_B)$ (1-d)

[0062] 由公式 (1-d) 和假设 (5)，应用仲裁规则，可得

[0063] $A|\equiv(k,n_B)$ (1-e)

[0064] 由公式 (1-e) 和假设 (8)，应用信仰规则，得到

[0065] $A|\equiv(k,n_B,n_A)$，即 $A|\equiv A\xleftarrow{K_{AB}}B$ (a)

[0066] 由消息 3 可得

[0067] $$B\triangleleft\{n_A,A\xleftarrow{K_{AB}}B\}_{K_{2old}}$$ (2-a)

[0068] 由公式 (2-a) 假设 (6)，应用消息含义中的共享密钥规则，得到

[0069] $B|\equiv A\sim(n_A,A\xleftarrow{K_{AB}}B)$ (2-b)

[0070] 由假设 (2)，应用新鲜性规则，得到

[0071] $B|\equiv\#(n_A,A\xleftarrow{K_{AB}}B)$ (2-c)

[0072] 由公式 (2-b) 和公式 (2-c)，应用临时值验证规则，得到

[0073] $B|\equiv A|\equiv(n_A,A\xleftarrow{K_{AB}}B)$ (2-d)

[0074] 由公式 (2-d)，应用信仰规则，得到

[0075] $B|\equiv A|\equiv A\xleftarrow{K_{AB}}B$ (b)

[0076] 由公式 (2-d) 和假设 (7)，应用仲裁规则，得到

[0077] $B|\equiv(n_A,A\xleftarrow{K_{AB}}B)$ (2-e)

[0078] 由公式 (2-e)，应用信仰规则，得到

[0079] $B|\equiv A\xleftarrow{K_{AB}}B$ (c)

[0080] 由消息 4 可得

[0081] $$A\triangleleft\{n_A,A\xleftarrow{K_{AB}}B\}_{K_{AB}}$$ (3-a)

[0082] 由公式 (a) 和 (3-a)，应用消息含义中的共享密钥规则，可得

[0083] $A|\equiv B|\sim\{n_A,A\xleftarrow{K_{AB}}B\}$ (3-b)

[0084] 由假设 (1)，应用新鲜性规则，得到

[0085] $A|\equiv\#\{n_A,A\xleftarrow{K_{AB}}B\}$ (3-c)

[0086] 由公式 (3-b) 和 (3-c)，应用临时值验证规则，可得

[0087] $A|\equiv B|\equiv\{n_A,A\xleftarrow{K_{AB}}B\}$ (3-d)

[0088] 由公式 (3-d)，应用信仰规则，可得

[0089] $A|\equiv B|\equiv A\xleftarrow{K_{AB}}B$ (d)

[0090] 由以上分析可知该协议符合最终的目标，达到认证的目的，即一级信仰 (a) 和

(c)，二级信仰 (b) 和 (d)。但需要说明，协议的安全性以与用户证书配套的私钥安全为前提。

[0091] （三）安全属性及抗攻击能力分析

[0092] 由于 BAN 逻辑本身的一些缺陷，可能无法探测针对协议的某些攻击及协议的一些安全属性，因此本文结合非形式化分析方法，从攻击及保密性方面对协议进行进一步分析。

[0093] 1. 双向实体认证

[0094] Alice 和 Bob 通过发送数字证书以及对发送信息的数字签名来实现身份认证。由于数字证书中所包含的身份信息有 CA 权威第三方的签名，用户首先可以通过检查身份信息来进行第一重身份认证，之后 Bob 可以提取出证书中 Alice 的公钥信息验证 Alice 的签名，从而证明 Alice 确实为会话持有者。同理，Bob 也是一样。由于 Alice 与 Bob 共享保护密钥，所以在交换随机数的同时可以起到第二重身份认证的作用。经过两重身份认证之后即可实现用户间的双向实体认证。

[0095] 2. 密钥协商

[0096] Alice 和 Bob 之间的会话密钥组及保护密钥是由 k，n_A，n_B 三个参数经过相关计算生成的，其中 n_A 由 Alice 随机生成，而 k，n_B 由 Bob 随机生成，且 k 以公钥加密方式传输，n_A，n_B 也都分别在旧保护密钥 K_{1old}，K_{2old} 的保护下隐蔽传输，并且利用新保护密钥 K_{1new}，K_{2new} 进行正确性确认，只有 Alice，Bob 可以计算得到，最后 Alice 通过 Bob 发送的 Finished 消息进行密钥的一致性确认，故最终的会话密钥组及保护密钥只有 Alice 和 Bob 可以获得。

[0097] 3. 完美的向前保密性 (PFS)

[0098] 在会话密钥组的协商及更新过程中，攻击者即使掌握了双方当前的会话密钥，也不会对下次的密钥协商造成威胁。因为参与每次会话密钥组计算的三个随机数都是重新生成的，并且分别加密传输，只有同时持有私钥及共享保护密钥的用户才能得到，而且在会话密钥组及保护密钥更新时新旧密钥之间不存在关联等式，因此本协议具有 PFS 性质。

[0099] 4. 抗重放攻击

[0100] 当攻击者在协议中重放之前的消息时，这些篡改造成的错误都会在协议中逐步累积，Bob 计算 n_A 并比较其正确性时就会发现遭受攻击。即使没有发现，最终导致通信双方更新密钥时计算出来的值不同步，由于 Finished 消息是用新协商好的 MAC 密钥计算出来，所以如果双方最终更新的密钥不同步或不一致，那么 Alice 在比较 Finished 值时就会发现。

[0101] 5. 抗非同步攻击

[0102] Bob 在进行密钥更新之后会用新得到的 MAC 密钥对收到的 $\gamma \| \delta$ 计算 MAC 值构成 Finished 消息发送给 Alice，A 收到消息后也用新计算得到的 MAC 密钥对自己上一步发出的 $\gamma \| \delta$ 计算 MAC 值，比较两个值是否一致，若相同，则密钥协商成功，若不同，则说明密钥更新不同步，可能受到攻击。故本协议可以抵抗非同步攻击。

[0103] （四）性能比较

[0104] 将本发明所提出的轻量级认证密钥协商协议与现有的其它两种协议进行性能比较如表 1 所示。

[0105] 表 1 与同类协议的性能比较

[0106]

协议	计算开销				通信次数
	公钥加/解密	指数运算	签名/验证	对称加/解密	
EAP-TLS[9]	1(1/0)	2	2(1/1)	0	10
WAPI[8]	2(1/i)	0	2(1/1)	0	7
本协议	1(0/1)	0	2(1/1)	0	4

[0107] 注：1. 计算性能所述各项均指 Alice 的计算量

[0108] 2. 2(1/1) 表示一共进行了 2 次该类型，包括 1 次加密运算和 1 次解密运算。

[0109] WAPI 协议的认证环节与密钥协商阶段是分开的，在认证环节缺乏私钥认证，密钥协商阶段缺乏密钥确认过程，如果考虑相应的私钥认证以及密钥确认过程的话，其交互轮数将会增加。由表 1 可以看出本文所提的基于数字证书的轻量级认证密钥协商协议，在性能上明显优于 EAP-TLS 和 WAPI 协议。本协议中仅有的一次公钥加密的运算开销是可选的，当使用会话 ID 选择复用上次会话的参数时，即可节省此次公钥解密的开销，具有灵活性，从而更适合应用于无线网络中用户的安全认证与密钥协商。

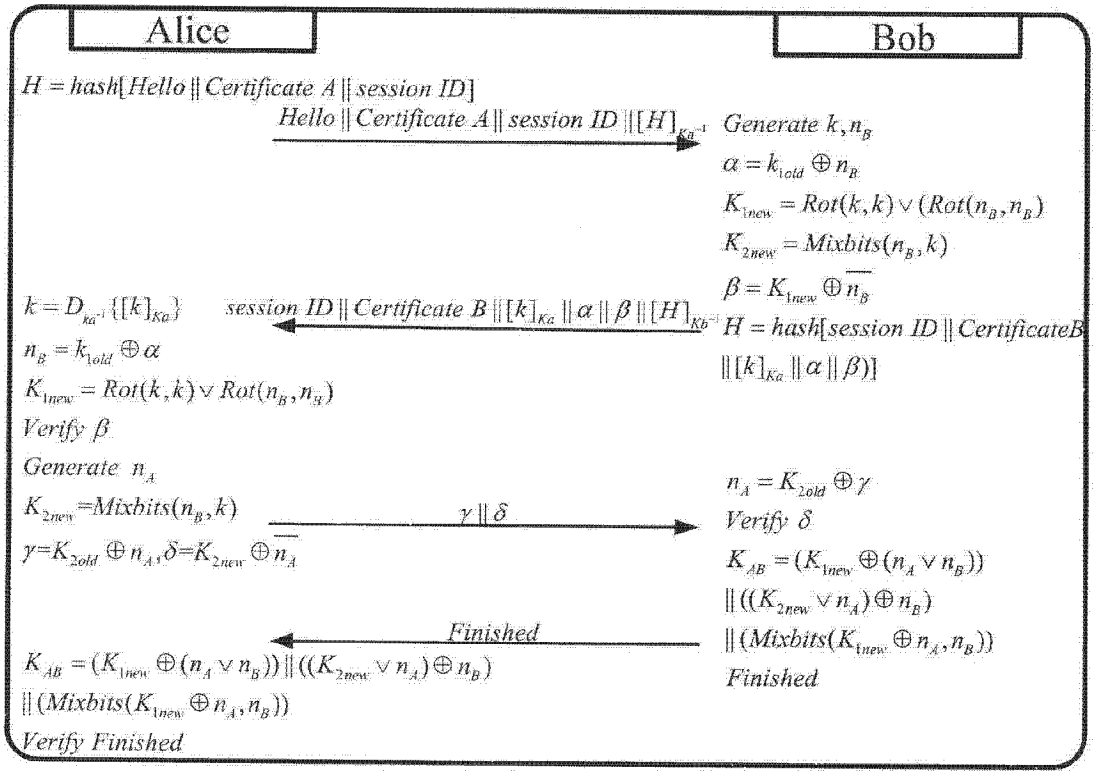
Alice
Bob
$H = hash[Hello \| Certificate\ A \| session\ ID]$
$Hello \| Certificate\ A \| session\ ID \| [H]_{Ka^{-1}}$
Generate k, n_B
$\alpha = k_{1old} \oplus n_B$
$K_{1new} = Rot(k,k) \vee (Rot(n_B, n_B)$
$K_{2new} = Mixbits(n_B, k)$
$\beta = K_{1new} \oplus \overline{n_B}$
$k = D_{Ka^{-1}}\{[k]_{Ka}\}$
$session\ ID \| Certificate\ B \| [k]_{Ka} \| \alpha \| \beta \| [H]_{Kb^{-1}}$
$H = hash[session\ ID \| CertificateB$
$\| [k]_{Ka} \| \alpha \| \beta)]$
$n_B = k_{1old} \oplus \alpha$
$K_{1new} = Rot(k,k) \vee Rot(n_B, n_B)$
Verify β
Generate n_A
K_{2new}=Mixbits(n_B, k)
$\gamma \| \delta$
$\gamma = K_{2old} \oplus n_A, \delta = K_{2new} \oplus \overline{n_A}$
$n_A = K_{2old} \oplus \gamma$
Verify δ
$K_{AB} = (K_{1new} \oplus (n_A \vee n_B))$
$\| ((K_{2new} \vee n_A) \oplus n_B)$
$\| (Mixbits(K_{1new} \oplus n_A, n_B))$
Finished
Finished
$K_{AB} = (K_{1new} \oplus (n_A \vee n_B)) \| ((K_{2new} \vee n_A) \oplus n_B)$
$\| (Mixbits(K_{1new} \oplus n_A, n_B))$
Verify Finished

图 1