(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 102739660 A
(43)申请公布日 2012.10.17

(21)申请号 201210200320.2

(22)申请日 2012.06.16

(71)申请人 华南师范大学
地址 510631 广东省广州市中山大道西 55 号
申请人 广州杰赛科技股份有限公司

(72)发明人 赵淦森 巴钟杰 李子柳 李惊生

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 谭英强

(51)Int.Cl.
H04L 29/06(2006.01)

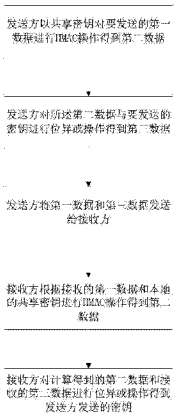
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

一种单点登录系统的密钥交换方法

(57)摘要

本发明公开了一种单点登录系统的密钥交换方法，应用于身份认证请求或者服务请求中交互的发送方和接收方之间的密钥交换，本发明方法通过发送方和接收方共享的共享密钥对交互的额外信息进行 HMAC 操作得到第二数据，并将第二数据与要交换的密钥进行位异或操作后的第三数据传送给接收方，接收方根据接收的第一数据和本地的共享密钥进行 HMAC 操作得到第二数据；接收方对计算得到的第二数据和接收的第三数据进行位异或操作得到发送方发送的密钥。本方法既减轻了密钥交互算法的复杂性，在保证密钥交互的时效性下又支持长密钥的交换，保证密钥换的安全性，适用于瘦终端间的密钥交换。



CN 102739660 A

1. 一种单点登录系统的密钥交换方法，应用于发送方与接收方之间的密钥交换，所述发送方与接收方之间存在双方共享的共享密钥，其特征在于，所述密钥交换包括以下步骤：

发送方以共享密钥对要发送的第一数据进行 HMAC 操作得到第二数据；

发送方对所述第二数据与要发送的密钥进行位异或操作得到第三数据；

发送方将第一数据和第三数据发送给接收方；

接收方根据接收的第一数据和本地的共享密钥进行 HMAC 操作得到第二数据；

接收方对计算得到的第二数据和接收的第三数据进行位异或操作得到发送方发送的密钥。

2. 根据权利要求 1 所述的一种单点登录系统的密钥交换方法，其特征在于：所述第一数据为密钥交换过程中参与交互的额外信息。

3. 根据权利要求 1 所述的一种单点登录系统的密钥交换方法，其特征在于：所述发送方或者接收方为身份认证请求或者服务请求中交互的客户端或者服务器。

一种单点登录系统的密钥交换方法

技术领域

[0001] 本发明涉及一种单点登录系统，尤其是一种单点登录系统的密钥交换方法。

背景技术

[0002] 单点登录(Single Sign On)：简称为SSO，是目前比较流行的企业业务整合的解决方案之一。SSO的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统，避免了用户每次请求一个服务时都要验证一次身份造成的性能损耗。为了实现单点登录，所有应用系统都共享一个身份认证系统。若在单点登录系统的整个认证或者服务交互过程中，长时间或者过多使用永久密码对消息进行加密，则容易导致密钥被攻击者获取，造成密钥的泄露。

[0003] 现有的密钥交换方法一般基于迪菲－赫尔曼密钥交换(Diffie－Hellman key exchange，简称“D-H”)协议，所述 D-H 协议是一种安全协议，它可以让双方在完全没有对方任何信息的条件下通过不安全信道建立起一个密钥。这个密钥可以在后续的通讯中作为对称密钥来加密通讯内容。在申请号为 CN03116619.9，专利名称为《一种基于公匙证书的密钥交换方法》的中国发明专利文献中公开了一种基于公匙证书的密钥交换方法，它从大素数域上的离散对数问题和 D-H 协议出发，辅以抗碰撞杂凑函数、公匙证书和数字签名的会话密钥交换方法。该 D-H 协议基于离散对数的应用，但是若出现了一个高效的解决离散对数问题的算法，那么则可以用来简化 a 或者 b 的计算，就可以解决迪菲－赫尔曼问题，使得该迪菲－赫尔曼密钥交换系统在内的很多公匙密码学系统变得不安全。

[0004] 在申请号为 CN200610103449.6，专利名称为《一种椭圆曲线密钥交换方法在 MANET 网络中的应用》的中国发明专利文献中公开了一种 MANET 网络安全保护过程的新型加密解密体制和密钥管理方法，该方法采用了椭圆形曲线密码体制，但椭圆形曲线加密的密钥交换方法对计算量要求很大，不适用于瘦终端。

发明内容

[0005] 本发明要解决的技术问题是：提供一种单点登录系统的密钥交换方法，该密钥交换方法对计算量的要求低且安全性高。

[0006] 为了解决上述技术问题，本发明所采用的技术方案是：

一种单点登录系统的密钥交换方法，应用于发送方与接收方之间的密钥交换，所述发送方与接收方之间存在双方共享的共享密钥，所述密钥交换包括以下步骤：

发送方以共享密钥对要发送的第一数据进行 HMAC 操作得到第二数据；

发送方对所述第二数据与要发送的密钥进行位异或操作得到第三数据；

发送方将第一数据和第三数据发送给接收方；

接收方根据接收的第一数据和本地的共享密钥进行 HMAC 操作得到第二数据；

接收方对计算得到的第二数据和接收的第三数据进行位异或操作得到发送方发送的密钥。

[0007] 进一步作为优选的实施方式，所述第一数据为密钥交换过程中参与交互的额外信息。

[0008] 进一步作为优选的实施方式，所述发送方或者接收方为身份认证请求或者服务请求中交互的客户端或者服务器。

[0009] 本发明的有益效果是：本发明单点登录系统的密钥交换方法，应用于身份认证请求或者服务请求中交互的发送方和接收方之间的密钥交换，本发明方法通过发送方和接收方共享的共享密钥对交互的额外信息进行 HMAC 操作得到第二数据，并将第二数据与要交换的密钥进行位异或操作后的结果传送给接收方，既减轻了密钥交互算法的复杂性，在保证密钥交互的时效性下又支持长密钥的交换，保证密钥换的安全性，适用于瘦终端间的密钥交换。

附图说明

[0010] 下面结合附图对本发明的具体实施方式作进一步说明：

图 1 是本发明单点登录系统的密钥交换方法的步骤流程图。

具体实施方式

[0011] 参照图 1，一种单点登录系统的密钥交换方法，应用于发送方与接收方之间的密钥交换，所述发送方或者接收方为身份认证请求或者服务请求中交互的客户端或者服务器。例如当发送方为客户端时，接收方为服务器；当发送方为服务器时，接收方为客户端。所述发送方与接收方之间共享的共享密钥为 sharekey。所述密钥交换包括以下步骤：

发送方用共享密钥 sharekey 对要发送的第一数据 content 进行 HMAC 操作得到第二数据 H(sharekey, content)，所述 H(sharekey, content) 是表示以 sharekey 为密钥，对消息 content 进行 HMAC 操作；

发送方对所述第二数据 H(sharekey, content) 与要发送的密钥 exchangkey 进行位异或操作 ⊕ 得到第三数据 H(sharekey, content) ⊕ exchangdkey；

发送方将第一数据 content 和第三数据 H(sharekey, content) ⊕ exchangdkey 发送给接收方；

接收方根据接收的第一数据 content 和本地的共享密钥 sharekey 进行 HMAC 操作得到第二数据 H(sharekey, content)；

接收方对计算得到的第二数据 H(sharekey, content) 和接收的第三数据 H(sharekey, content) ⊕ exchangdkey 进行位异或操作得到发送方发送的密钥 exchangkey。所述过程如下：

H(sharekey, content) ⊕ (H(sharekey, content) ⊕ exchangdkey) → exchangekey。

[0012] 所述 exchangkey 是指由一方创建或得知之后，交换或传递给另外一方的密钥；所述 content 是指在整个密钥交换过程中参与交互的额外信息，若 content 中有部分信息是已知的（标记为 share_content），那么以上的发送方发送的数据也可以表示为“partial_content, share_content_tips, H(sharekey, partial_content+share_content) ⊕ exchangdkey”，其中 share_content_tips 是表示要用到的共享消息的相关提示信息，

“+”表示与操作，与操作左边与右边的信息如何组织可以根据具体情况而定。

[0013] 以上是对本发明的较佳实施进行了具体说明，但本发明创造并不限于所述实施例，熟悉本领域的技术人员在不违背本发明精神的前提下还可以作出种种的等同变形或替换，这些等同的变形或替换均包含在本申请权利要求所限定的范围内。

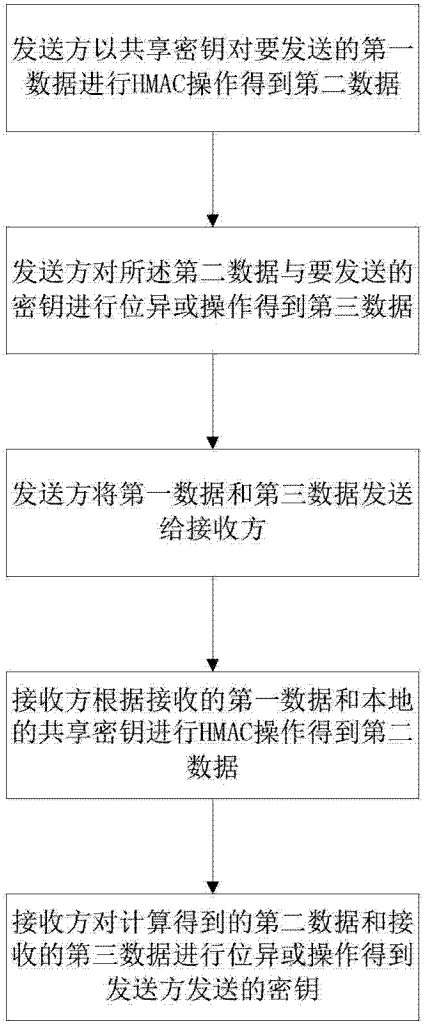

发送方以共享密钥对要发送的第一数据进行HMAC操作得到第二数据
发送方对所述第二数据与要发送的密钥进行位异或操作得到第三数据
发送方将第一数据和第三数据发送给接收方
接收方根据接收的第一数据和本地的共享密钥进行HMAC操作得到第二数据
接收方对计算得到的第二数据和接收的第三数据进行位异或操作得到发送方发送的密钥

图 1