

文章编号:1001-9081(2007)06-1343-02

移动通信系统中的认证与密钥协商协议

谭利平, 李方伟

(重庆邮电大学 移动通信重点实验室, 重庆 400065)

(tanliping4512@163.com)

摘 要:提出了一种新的身份认证与密钥协商协议,该协议可以实现通信双方的相互认证,并通过协商产生安全的会话密钥。协议将对称密码体制和非对称密码体制有机地结合起来,非对称密码体制采用密钥比特少且安全性高的椭圆曲线密码体制。经过性能分析,该协议安全、有效,比较适合在移动通信系统中使用。

关键词:认证;密钥协商;会话密钥;椭圆曲线密码体制

中图分类号: TP393.08 **文献标识码:** A

Authentication and key agreement protocol in mobile communication system

TAN Li-ping, LI Fang-wei

(Key Laboratory of Mobile Communication Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: This paper proposed a new authentication and key agreement protocol which can realize mutual authentication and generate a secure session key agreed by both sides of communication. The protocol combines the symmetric with non-symmetric cryptography. Non-symmetric cryptography adopts Elliptic Curve Cryptosystem with greater security and shorter keys. Performance analysis shows this protocol is more secure and efficient. Therefore, it is suitable for mobile communication system.

Key words: authentication; key agreement; session key; ECC

0 引言

随着移动通信应用领域的不断扩大,特别是移动电子商务的发展,用户和网络运营商将会对移动通信网络的安全性、可靠性提出更高、更迫切的要求。为了保证移动通信网络的安全,实现正常安全通信,除了采用安全的加密技术保密机密信息外,还需要安全有效的身份认证与密钥协商协议保护用户与运营商的利益。身份认证与密钥协商协议作为呼叫建立过程的一部分,在移动通信网络中扮演着举足轻重的角色。一旦身份认证与密钥协商协议出现安全漏洞,整个通信就没有安全性可言。

在移动通信系统中,由于移动端的计算能力较低且计算资源较差,因此设计认证与密钥协商协议时应尽量减少移动端的计算量,采用计算简单的密码算法。此外,由于移动端与网络端之间采用无线通信,用户的身份认证必须通过无线信道进行,因此其身份、位置等敏感信息易受截获、窃听和攻击,认证时采用临时身份是解决上述问题的有效方法。文献[1]首先提出了基于对称密码体制的身份认证与密钥协商协议,该协议算法简单高效,但没有实现用户的匿名性。此后,许多基于对称密码体制^[2,3]和基于非对称密码体制^[4-6]的认证与密钥协商协议被提出来。文献[6]提出了一种基于离散对数的适用于移动通信的认证与密钥协商协议,该方案实现了匿名性,并通过为用户颁发临时签名私钥和匿名数字证书来提供不可否认服务。文献[7]指出该方案存在假冒攻击,且移

动端的计算量大。本文提出了一种新的身份认证与密钥协商协议,该方案移动用户与拜访网络之间采用单钥密码体制,而拜访网络与归属网络之间采用椭圆曲线密码体制。协议减少了移动端的计算量,同时提供了匿名性服务,有效地防止了假冒攻击。

1 认证与密钥协商协议

1.1 基本标识符

本文采用如下的标识符来描述协议:

$A \rightarrow B: X$: A 向 B 发送消息 X ; TID_M : 移动用户的一次性临时身份标识符; $E_K\{X\}$: 用对称密钥 K 对消息 X 加密得到的密文; PK_A, SK_A : A 的公钥/私钥对; $\{X\}_{SK_A}$: 用 A 的私钥对 X 签名得到的签名消息; $\{X\}_{PK_A}$: 用 A 的公钥对消息 X 加密得到的密文; $CertA$: 证书权威机构颁发给 A 的公钥证书; M : 移动用户的真实身份标识; H, V : 移动用户 M 的归属网络和拜访网络的身份标识; K_{MH} : M 与 H 之间共享的对称密钥; N_{MH} : M 与 H 之间共享的随机数; T_A : 由 A 产生的时间戳; $Mac_{K_{MH}}$: 带密钥 K_{MH} 的消息认证码; h_1, h_2, h_3 : 三个不同的单向哈希函数。记号 \parallel 表示两个比特串级联, $(A)_x$ 表示椭圆曲线上点 A 的横坐标。

1.2 协议描述

本协议假设通信前, M 已经知道了 VLR 的身份信息 V, M 的智能卡中已经存储了 M 的临时身份 TID_M 、与 H 共享的随机数 N_{MH} , 并且具有一定的安全访问机制和计算能力。 H 保存了共享随机数 N_{MH} , 以及用户的临时身份与真实身份的对应关

收稿日期: 2006-12-15; 修订日期: 2006-03-07

基金项目: 重庆市发改委资金资助项目(20041072); 重庆市教委科学技术研究项目(KJ060510)

作者简介: 谭利平(1980-), 男, 河北邯郸人, 硕士研究生, 主要研究方向: 移动通信技术; 李方伟(1960-), 男, 重庆人, 教授, 博士, 主要研究方向: 移动通信技术。

系。协议中 V 和 H 之间采用的公钥密码体制都是基于椭圆曲线离散对数难题的,系统参数为 (F_q, E, G, n) , 其中 E 是有限域 F_q 上的椭圆曲线, G 是 E 上的一个基点,素数 n 是 G 的阶。归属网络 H 的私钥为 SK_H , 对应的公钥为 $PK_H = SK_H \cdot G$; 而拜访网络的私钥为 SK_V , 对应的公钥为 $PK_V = SK_V \cdot G$ 。

协议流程如下:

- 1) $M \rightarrow V: TID_M, E_{K_{MH}}\{a, r_M, N_{MH}\}, H$
- 2) $V \rightarrow H: TID_M, E_{K_{MH}}\{a, r_M, N_{MH}\}, \{r_V, V\}_{SK_V}, T_V, CertV$
- 3) $H \rightarrow V: \{E_{K_{MH}}\{TID_M', N_{MH}', r_H, (R)_x\}, Mac_{K_{MH}}(r_M, TID_M', N_{MH}'), r_M, r_H, \{r_H, (R')_x\}_{SK_H}\}_{PK_V}, T_H, CertH, R'$
- 4) $V \rightarrow M: E_{K_{MH}}\{TID_M', N_{MH}', r_H, (R)_x\}, Mac_{K_{MH}}(r_M, TID_M', N_{MH}'), E_K\{r_M, V\}$
- 5) $M \rightarrow V: h_3(r_H, TID_M, K)$

下面,对上述协议进行详细描述:

1) 移动用户 M 产生一个 k bit 的随机数 r_M , 和一个 160 bit 的随机数 a , 并用 M 与 H 之间的共享密钥 K_{MH} 加密 a, r_M, N_{MH} 得 $E_{K_{MH}}\{a, r_M, N_{MH}\}$, 其中 $K_{MH} = h_1(TID_M, M, N_{MH}, V)$, 把 $TID_M, E_{K_{MH}}\{a, r_M, N_{MH}\}$ 和 H 一同发送给 V 。

2) V 收到报文后, 产生一个随机数 r_V 和时间戳 T_V , 并用私钥 SK_V 对 r_V 和 V 签名得到 $\{r_V, V\}_{SK_V}$, 发送 $TID_M, E_{K_{MH}}\{a, r_M, N_{MH}\}, \{r_V, V\}_{SK_V}, T_V, CertV$ 给 H 。

3) H 接收到来自 V 的报文后, 首先验证其中证书的合法性, 然后查看 T_V 与当前系统的时间误差是否在一个合理的范围内。 H 从 V 的公钥证书中获取 V 的身份信息和公钥 PK_V 验证数字签名的合法性。验证通过后, 根据 TID_M 查找用户的真实身份 M 和共享随机数 N_{MH} , 计算共享密钥 $K_{MH} = h_1(TID_M, M, N_{MH}, V)$, 解密 $E_{K_{MH}}\{a, r_M, N_{MH}\}$ 得到 a, r_M, N_{MH} , 比较 N_{MH} 与自己存储的 N_{MH} 是否一致, 以实现 H 对 M 的认证。

上述验证均通过后, H 将执行下列操作。随机产生新的用户临时身份 TID_M' 和共享随机数 N_{MH}' , 同时产生一个 160 - k bit 的随机数 r_H , 计算 $R' = a \cdot G, R = a \cdot PK_V$ 和消息认证码 $Mac_{K_{MH}}(r_M, TID_M', N_{MH}')$, 并用 K_{MH} 对 $TID_M', N_{MH}', r_H, (R)_x$ 加密得到密文, 然后再用 V 的公钥 PK_V 对 H 的签名 $\{r_H, (R')_x\}_{SK_H}, r_M, r_H, Mac_{K_{MH}}(r_M, TID_M', N_{MH}')$ 以及得到的密文加密, 最后附上自己的时间戳 T_H 、证书 $CertH$ 以及参数 R' 组成报文发给 V 。

4) V 收到 H 的报文后, 首先验证其中证书的合法性, 然后查看 T_H 与当前系统的时间差是否在一个合理的范围内。而后从公钥证书中获取 H 的公钥 PK_H , 验证签名的合法性。验证通过之后, 用自己的私钥 SK_V 解密消息流中的密文得到计算会话密钥 K 所需的 r_M 和 r_H , 计算 $R = R' \cdot SK_V$ 和会话密钥 $K = h_2((r_M \parallel r_H) \oplus (R)_x)$, 并把 $E_{K_{MH}}\{TID_M', N_{MH}', r_H, (R)_x\}, Mac_{K_{MH}}(r_M, TID_M', N_{MH}')$ 和 $E_K\{r_M, V\}$ 发送给 M 。

5) 用户收到报文后, 用 K_{MH} 对第一段报文进行解密得到 $TID_M', N_{MH}', r_H, (R)_x$, 计算 $Mac_{K_{MH}}(r_M, TID_M', N_{MH}')$, 并与收到的消息认证码比较以验证报文的有效性, 实现对 H 的认证。验证通过后, 计算会话密钥 $K = h_2((r_M \parallel r_H) \oplus (R)_x)$, 用 K 解密 $E_K\{r_M, V\}$ 得到 r_M , 并与原先产生的 r_M 比较。若相等, 则用户保存 TID_M' 和 N_{MH}' 以备下次使用。同时, 用户发送 $h_3(r_H, TID_M, K)$ 给 V 。 V 收到消息后用存储的 r_H, TID_M 和先前计算的会话密钥 K 验证 $h_3(r_H, TID_M, K)$ 的有效性, 从而判断是否与自己拥有相同的会话密钥 K 。会话密钥通过双方确认后, M 和 H 将注销 TID_M 和 N_{MH} 。

2 协议的性能分析

2.1 协议实现的功能

1) 双向认证: 建立会话密钥的双方 V 和 M 对彼此的身份进行了认证。 V 对 M 的认证是通过 V 对 H 的认证以及 H 对 M 的认证来间接实现的。 H 与 V 之间的相互认证是通过公钥证书以及签名实现的。 H 根据用户的临时身份 TID_M 与其真实身份 M 的对应关系可以认证 M , 并且通过比较解密出的 N_{MH} 与自己存储的 N_{MH} 是否一致进一步认证了 M 的身份。这是因为只有知道共享随机数 N_{MH} 以及临时身份与真实身份的对应关系的 M 和 H 才可以计算出共享密钥 K_{MH} 。而 M 对 V 的认证是通过 M 对 H 的认证以及 H 对 V 的认证来间接实现的。 M 通过验证消息认证码 $Mac_{K_{MH}}(r_M, TID_M', N_{MH}')$ 的有效性, 实现对 H 的认证, 因为只有 M 和 H 知道 r_M, TID_M' 和 N_{MH}' 。

2) 移动用户的匿名性: 协议使用了一次性临时身份完成对移动用户的认证, 只有移动用户 M 和归属网络 H 知道用户临时身份与真实身份的对应关系。因此实现了移动用户的匿名性, 有效地防止了移动用户被跟踪。

3) 密钥协商与双向密钥控制: 协议中 M 和 V 之间的会话密钥 $K = h_2((r_M \parallel r_H) \oplus (R)_x)$ 是由 M 和 V 双方协商得到的。参数 r_M, r_H 和 $(R)_x$ 是以密文形式传送的, 并且要获得参数 R 必须知道 V 的私钥或者随机数 a , a 又是以密文传送的, 所以只有用户和访问网络协商才可以计算出会话密钥, 任何一方都不能单独计算出会话密钥。

4) 会话密钥的新鲜性: 产生的会话密钥的参数 r_M, a 和 r_H 都是由用户和网络随机生成的, 每次通信时都不相同, 因此保证了会话密钥的新鲜性。

5) 双向会话密钥的确认: 移动用户通过解密 $E_K\{r_M, V\}$ 得到 r_M , 并与自己原先生成的 r_M 比较, 以确信网络端拥有正确的会话密钥; 而移动用户用会话密钥 K, r_H 和用户的临时身份 TID_M 计算哈希值 $h_3(r_H, TID_M, K)$, 并发送给网络端, 网络端通过验证收到的哈希值是否与自己计算的相等, 以确认用户拥有正确的会话密钥。

2.2 协议的安全性

本协议的安全前提是协议所使用的单钥密码技术和哈希函数是安全的, 且 V 和 H 之间采用的公钥密码体制是基于椭圆曲线离散对数难题的。

1) 用户身份得到了保护: 协议中使用了临时身份 TID_M 实现其匿名性, 在 H 对用户认证后, 产生一个新的临时身份 TID_M' 和随机数 N_{MH}' 并以密文形式传送给 M 备下次使用。除 M 和 H 外, 任何攻击者都不知道用户的临时身份与真实身份的对应关系。因此, 该协议有效的保护了用户的身份。

2) 产生的会话密钥是安全的: 产生会话密钥的参数是以密文形式传送的, 只有拥有共享密钥的人才可以正确解密。此外, 即使攻击者截获了 $R' = a \cdot G$ 也无法计算出 a , 因为这将面临求解椭圆曲线离散对数难题。

3) 抗重放攻击: 本协议在无线接口 M 和 V 之间传送的消息中含有的 TID_M, a, r_M, r_H 等参数都是随机产生的, 每次通信都不一样, 有效的防止了重放攻击。而 V 和 H 之间使用时间戳 T_V 和 T_H 以抵抗重放攻击。

4) 抗中间人攻击: 协议中 M 和 H 共享随机数 N_{MH} , 且只有 M 和 H 知道 M 的真实身份, 因此只有 M 和 H 才能计算出他们共享的对称密钥 K_{MH} , 任何人想伪造 M 或 H 进行通信都是不

(下转第 1348 页)

的隐蔽性。图 7(e) 是嵌入水印后的伪装 DEM 数据, 图 7(f) 是提取水印后的伪装 DEM 数据, 图 7(g) 是由种子再现的 DEM 数据, 图 7(h) 是恢复出的秘密 DEM 数据, 与原始秘密 DEM 数据完全相同。

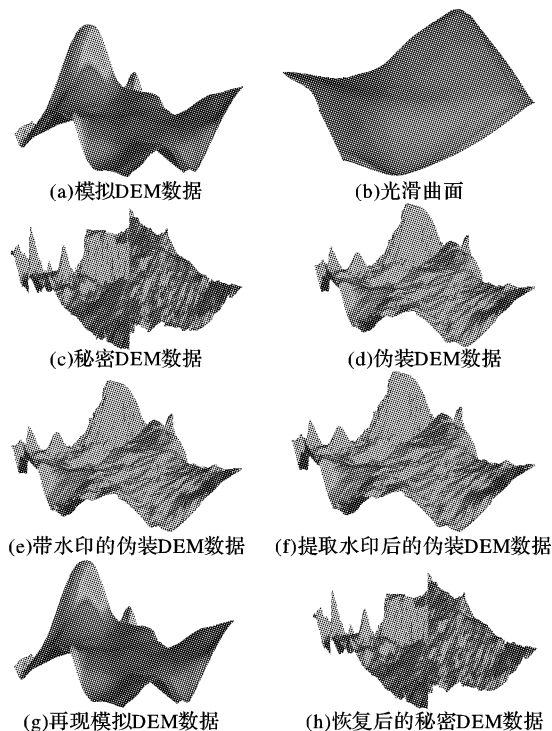


图 7 实验结果

3.2 安全性分析

本文用到的 SHA-256 单向 Hash 函数算法是公开的, 但如果没有种子和密钥, 将无法再现随机序列, 从而也不能获取秘密 DEM 数据。而 SHA-256 单向 Hash 函数的计算复杂度大于生日碰撞的复杂度 2^{128} , 也即意味着现有的硬件设备难以成功攻破该算法。

4 结语

本文提出了一种全新的基于经验模态分解的 DEM 数据

伪装技术, 不但可以很好地伪装秘密 DEM 数据, 而且利用可逆水印能够对 DEM 数据进行版权保护。由于构造了 SHA-256 单向 Hash 函数, 通过种子可以再现用于伪装的 DEM 数据, 从而可以完全恢复出秘密 DEM 数据。本文算法能够很好地保护 DEM 数据的版权, 安全性高, 可实现用户权限的多级管理。

参考文献:

- [1] 江早. 信息伪装——一种崭新的信息安全技术[J]. 中国图象图形学报, 1998, 3(1): 83-86.
- [2] 张雷. 平西建, 张涛. 一阶统计特征保持的图像信息伪装算法[J]. 计算机辅助设计与图形学学报, 2005, 17(1): 99-104.
- [3] 张涛. 平西建. 基于差分直方图实现 LSB 信息伪装的可靠检测[J]. 软件学报, 2004, 15(1): 151-158.
- [4] 杨尚英, 朱虹, 李永盛. 一种数字图像的信息伪装技术[A]. 信息隐藏[C]. 西安: 西安电子科技大学出版社, 2001: 170-174.
- [5] 罗永, 成礼智, 陈波, 等. 基于模糊关系的 DEM 数据信息伪装技术研究[J]. 模糊系统与数学, 2004, 18(3): 116-120.
- [6] CELIK MU, SHARMA G, TEKALP AM, et al. Lossless Watermarking for Image Authentication: A New Framework and an Implementation[J]. IEEE Transactions on Image Processing, 2006, 15(4): 1042-1049.
- [7] NI Z, SHI Y-Q, ANSARI N, et al. Reversible Data Hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354-362.
- [8] HANDSHUH H, GILBERT H. Evaluation Report Security Level of Cryptography SHA-256[R]. Technical Report, Issy-les-Moulineaux, 2002.
- [9] GILBERT H, HANDSHUH H. Security Analysis of SHA-256 and Sisters[A]. Lecture Notes in Computer Science[C]. 3006. 175-193.
- [10] HUANG NE, SHEN Z, LONG SR. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis[J]. Proceedings of the Royal Society of London, A, 1998, 454: 903-995.
- [11] DAMERVAL C, MEIGNEN S. A fast algorithm for bidimensional EMD[J]. IEEE Signal Processing Letters, 2005, 12(10): 701-704.

(上接第 1344 页)

可能的。又因为共享密钥 $K_{MH} = h_1(TID_M, M, N_{MH}, V)$ 中含有 V 的身份信息, 攻击者伪造 V 进行通信, 在协议的第三步 H 对 M 认证的同时就会对 V 进行认证, 从而识别出攻击者。

2.3 协议的效率

协议采用下列方法减少移动端的计算量: 1) 移动端采用算法比较简单, 计算量比较小的对称密码技术; 2) 将产生会话密钥的参数 $R = a \cdot PK_V$ 交给 H 计算, 并用共享密钥 K_{MH} 加密后传给 M ; 3) 移动端可以对 K_{MH} 进行预计算。

3 结语

移动通信系统中的身份认证与密钥协商协议一直以来都是人们研究的热点与难点。随着移动通信系统中多媒体、电子商务和网上银行等业务的发展, 身份认证与密钥协商协议就显得尤为重要。本文提出了一种双向身份认证与密钥协商协议, 协议将单钥密码体制与椭圆曲线密码体制结合起来, 既能实现通信双方的相互认证, 又能为通信双方协商一个新鲜、公正和经过双方确认的会话密钥。此外, 协议通过使用一次

性随机临时身份和随机共享密钥, 最大限度地保证了用户身份信息的机密性。性能分析表明, 协议安全有效且移动端计算量小, 适合移动通信环境。

参考文献:

- [1] BELLER MJ, CHANG LF, YACOBI Y. Privacy and Authentication on a Portable Communications system[J]. IEEEJSAC, 1993, 11(6): 821-829.
- [2] 余斌霄, 王新梅. 移动通信网中的认证与密钥建立协议[J]. 西安电子科技大学学报, 2004, 31(1): 124-128.
- [3] 文静华, 张梅, 李祥. 一个新的认证协议及其形式化分析[J]. 计算机工程, 2006, 32(8): 159-161.
- [4] 陈广辉, 李方伟, 李朔. 适用于移动通信系统的公钥加密认证方案[J]. 电子科技大学学报, 2005, 34(2): 183-185.
- [5] 邓方民, 许春香, 张娟. 基于 ECC 的移动通信认证与密钥协商协议[J]. 计算机应用与软件, 2006, 23(3): 125-126.
- [6] 邓所云, 胡正名, 钮心忻, 等. 一个无线双向认证和密钥协商协议[J]. 电子学报, 2003, 31(1): 135-138.
- [7] 冯国柱, 李超, 吴翊. 一个高效的无线匿名认证和密钥协商协议[J]. 计算机工程与应用, 2006, 42(19): 4-7.