安全高效的移动终端数字签名方案①

隋晓芹, 刘培顺

(中国海洋大学 信息科学与工程学院, 青岛 266000)

摘 要: 终端数字签名技术是保证终端应用安全的重要手段, 由于移动终端上使用的计算资源有限和安全限制, 移动终端不能保证私钥的安全. 本文在身份门限签名的数字签名技术的基础上, 将移动终端与签名服务器相结合, 设计出一种安全高效的解决方案. 该方案将密钥分发成 2 部分, 其中 1 份存储在签名服务器上, 另外 1 份分发给移动终端, 签名需要这两部分合作完成签名. 通过基于身份的门限签名技术, 有效实现移动终端在私钥不能保证安全的情况下的安全数字签名.

关键词: 移动终端; 数字签名; 门限签名; 基于身份的密码

Safe and Efficient Mobile Terminal Digital Signature Scheme

SUI Xiao-Qin, LIU Pei-Shun

(College of Information Science and Engineering, Ocean University of China, Qingdao 266000, China)

Abstract: Digital signature technology is an important way to ensure the safety of terminal application. But due to the limited computing resources and security constraints on the mobile terminal, the mobile terminal can not guarantee the security of the private key. This paper designs a safe and efficient solution based on the digital signature technology, combining mobile terminal with signature server. The key is distributed into two parts, one part is stored in the signature server and the other is distributed to mobile terminals, the signature must include the two parts. Through this identity-based threshold signature technology, we realize the secure mobile terminal digital signature in the case of signature key can't guarantee safety.

Key words: mobile terminal; digital signature; threshold signature; identity-based cryptography

1 引言

随着移动互联网的发展, 智能移动终端在电子商务, 移动办公中的应用越来越广泛. 移动终端一般是通过无线方式与其他设备进行交互. 目前针对移动终端的攻击越来越多, 许多恶意应用能够窃取用户存储在终端上的私有数据, 攻击终端与服务器的通信. 在移动办公中, 必须保证电子公文的真实性、完整性和不可抵赖性. 在文献[1]中, 为了保证数字签名过程中私钥的安全, 采用 USB 密码钥匙(USB key)作为客户端装置来存储私钥. 但使用 USB 密码钥匙需要主机拥有 USB 接口, 虽然目前出现了带有蓝牙接口或音频接口的 USB 密码钥匙, 但上述设备仍存在如下缺点: 由于蓝牙协议的开放性, 无法保证蓝牙 USB 密码钥匙设备与主机通讯的安全性; 带音频接口的 USB 密码钥匙设备, 无法解决不同移动终端间音频接口的兼容性问题.

1984 年, 基于身份的密码体制[2]第一次被 Shamir 提出, 即将用户的私人信息作为身份识别标识, 来加强对密钥的管理. 随后, 不同基于身份的安全模型被相继提出, 如文献[3]中, Hess F 等人提出了基于身份的双线性对加密方案, 采用双线性对技术, 但存在计算上的复杂性. 文献[4~7]中分别是对基于身份的门限签名方案的优化及证明, 其中文献[7]中对公钥的产生方式虽然通过所参与签名的成员身份来定, 而共享密

① 基金项目:微智慧移动互联系统信息安全技术服务(20140500)

收稿时间:2016-03-26;收到修改稿时间:2016-05-12 [doi: 10.15888/j.cnki.csa.005515]

钥是系统的主密钥保存在 PKG 上, 这样只有 PKG 知道完整的共享密钥, 在设计上存在不完整性. 本文在基于身份门限签名的基础上进行改进, 提出了可以应用到移动终端上的一种更加高效安全的数字签名方案.

本方案的主要方法是通过将移动终端与签名服务器相结合, 密钥分发成 m 份, 其中 1 份作为主要部分密钥存储在签名服务器上, 另外 m-1 份分发给用户所持有的不同移动终端. 有效签名, 则必须由签名服务器与用户所持有的任一移动终端上的密钥结合生成; 在生成签名时, 签名服务器首先通过身份口令验证用户终端传来的密钥是否为 PKG 分发给用户的部分私钥, 验证成功后再与之结合生成门限签名. 这样即使攻击者获取了移动终端上的部分密钥, 也无法通过签名服务器上的验证, 从而无法获得完整的密钥, 保证了移动终端上数字签名的安全.

2 基于身份的门限签名方案

鉴于移动终端自身的一些局限性, 用户私钥保存在移动终端上并不能保证足够的安全性, 本文提出了一种基于身份门限签名的数字签名方案, 不仅能够保证信息来源的正确性和完整性, 更能在移动终端上签名私钥不能保证安全的情况下实现安全的数字签名. 图 1 描述了该方案的基本实现过程. 由图可看出门限签名的基本过程主要包括在签名方进行: 系统参数建立、PKG 产生密钥并分发、验证及生成门限签名(验证终端部分密钥的有效性); 在验证方进行公钥解密和结果验证.

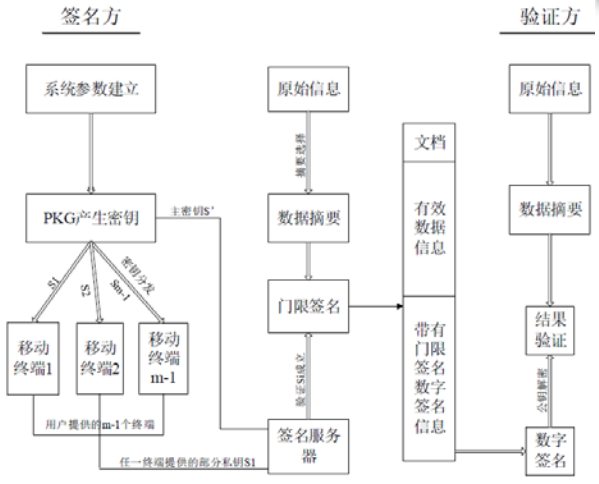

图 1 基于身份门限签名的数字签名过程

2.1 系统参数建立

令 *G1* 为 *q* 阶的加法循环群, *G2* 为 *q* 阶的乘法循环群, 其中 *q* 为大素数, 设 *g* 为 *G1* 的生成元, 由密钥管理中心 PKG 随机从 Z_q^* 中选择一个随机数 *r*, 计算 $g'=g^r, g''=g'^a$ (*a* 是从 *Zq* 中随机选取的随机数),并将 g'' 作为系统主密钥进行保存. 另存在一个双线性映射 $e: G_1\times G_1\to G_2$, 且存在两个单向哈希函数 $Hash: H_1: \{0,1\}^*\times G_1\to Z_q^*$ 和 $H_2: \{0,1\}^*\to\{0,1\}^{n_\mu}$. 随机选取 $\mu', \mu_i\in G_1$, 长度为 n_μ 的向量 $\mu=(\mu_i)$, 选择基点 $P\in G_1$, 计算 $P_{pub}=g''\cdot P$ 并将其作为系统公钥. 最后由 PKG 公开系统参数为 $params=(G_1, G_2, e, g, g', \mu', \mu, P_{pub})$.

2.2 密钥的生成和分发

门限密钥的生成算法由两部分构成, 即存储在签名服务器上的主要部分密钥 *S'* 和分发给用户持有的不同移动终端的部分密钥 *S1, S2...Sm-1*. 其中分发给不同移动终端的部分密钥的生成是由 PKG 根据用户所持有的移动终端的手机号码 *T* 作为身份 *ID* 并结合用户名来产生的, 其中 *N'* 代表用户名的数值表示形式. 主要部分密钥将由系统主密钥 *g''* 生成并存储在签名服务器上.

① 主要部分密钥的生成算法:

主要部分密钥由系统主密钥来确定, 结合 PKG 公布的公开参数, 利用双线性对计算得出主要部分密钥 $S'=e(g'', g')$, 并将其存储在签名服务器上.

② 部分密钥的生成算法:

设用户持有 *n* 个移动终端, 分别为 *R1, R2, ...Rn*, 另设移动终端的身份 *IDi* 是一个长度为 n_μ 的二进制串, 用集合 *W* 来表示身份 *ID* 中比特值为 1 的位置, 即集合 $W\subseteq\{1,2,3\cdots n_\mu\}$. 由 PKG 随机选取一个 $d\in Z_q^*$, 计算出每个移动终端持有的部分密钥为:

$$S_i=(S_{i1}, S_{i2})=(g^{N'}\cdot(\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}}, g') \quad (k\in W_i, i\in\{1,2,3....n\}) .$$

计算 $P_i=e(g,g')^{N'}$ 并将其公开, 然后将 S_i 通过安全通道传送给 *Ri*, 同时将移动终端的登录密码 *r'* 传送到签名服务器上保存. 另外当用户有新的移动终端加入时, 只需要用户名及移动终端的手机号码就可以生成部分密钥, 实现动态签名.

2.3 验证及门限签名的生成

本文中进行门限签名的签名密钥由签名服务器上存储的主要部分密钥和用户持有的任一移动终端上的

部分密钥组成, 因此在进行门限签名之前, 首先需要对用户移动终端进行判别, 即通过签名服务器上存有的该终端的登录密码 r' 来确保该终端是否具有进行签名的权限; 若验证成功, 证明该终端具有进行签名的权限后, 再对其部分密钥进行验证, 验证传来的部分密钥是否为 PKG 分发给用户的部分密钥. 根据等式 $e(S_{i1},g')=P_i\cdot e((\mu'\prod_{k\in W_i}u_k)^{d_{\mu i}},S_{i2})$, 若等式成立, 则签名服务器接受该部分密钥并进行签名; 若不成立, 则签名服务器拒绝签名请求, 并通知 PKG 重新生成部分密钥.

进行门限签名的合成者必须是由签名服务器和任一移动终端组成. 通过计算得出:

$\sigma_1=\prod_{i\in W}S_{i1}^{L_i},\sigma_2=\prod_{i\in W}(S'\cdot M')^{L_i},\sigma_3=\prod_{i\in W}S_{i2}^{L_i}$, 其中 $L_i=\prod_{i\neq j}\frac{j}{j-i}$

则最终门限签名为:

$$\begin{aligned}\sigma&=(\sigma_1,\sigma_2,\sigma_3)\\&=(\prod_{i\in W}S_{i1}^{L_i},\prod_{i\in W}(S'\cdot M')^{L_i},\prod_{i\in W}S_{i2}^{L_i})\\&=(\prod_{i\in W}(g^{N'}\cdot(\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}})^{L_i},\prod_{i\in W}(e(g'',g')\cdot M')^{L_i},\prod_{i\in W}g'^{L_i})\end{aligned}$$

数字签名为: $E_\sigma(M',M)$. 当接收方(验证方)收到签名后, 用公钥 P_{pub} 解密得到门限签名, 再根据公开参数及参与签名的移动终端身份对消息 M 的签名进行验证, 若满足等式:

$e(\sigma_1,g')=\prod_{i\in W}e(\mu'\prod_{k\in W_i}\mu_k,S_{i2})^{L_i}\cdot e(g^{N'},\sigma_3)$ 则验证方接受该签名, 即签名有效; 否则将拒绝, 即认为签名无效.

3 方案的分析

3.1 正确性

本方案通过对门限签名生成算法[8]进行验证, 证明方案的正确性, 具体步骤如下:

① 部分密钥的验证:

$$\begin{aligned}&e(S_{i1},g')\\&=e(g^{N'}\cdot(\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}},g')\\&=e(g^{N'},g')\cdot e((\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},g')\\&=e(g,g')^{N'}\cdot e((\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},g')\\&=P_i\cdot e((\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},S_{i2})\end{aligned}$$

② 门限签名算法的验证:

$$\begin{aligned}&e(\sigma_1,g')\\&=e(\prod_{i\in W}S_{i2}^{L_i},g')\\&=e(\prod_{i\in W}(g^{N'}\cdot(\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}})^{L_i},g')\\&=\prod_{i\in W}e(g^{N'}\cdot(\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}}),g')^{L_i}\\&=\prod_{i\in W}e(g^{N'},g')^{L_i}\cdot e((\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}}),g')^{L_i}\\&=\prod_{i\in W}e((\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}}),S_{i2})^{L_i}\cdot e(g^{N'},\prod_{i\in W}g'^{L_i})\\&=\prod_{i\in W}e((\mu'\prod_{k\in W_i}\mu_k)^{d_{ui}}),S_{i2})^{L_i}\cdot e(g^{N'},\sigma_3)\end{aligned}$$

3.2 安全性

定理 1[9]. 如果基本签名方案是不可伪造的安全方案, 且相应的门限签名方案是可模拟的, 则可证明此门限签名是不可伪造的.

定义 1. 如果门限签名方案可模拟, 需要满足以下性质:

(1) 密钥生成及分发的过程是可模拟的. 输入公钥、公开的系统参数以及移动终端的身份 ID 和用户名数值表示形式 N', 存在一个模拟器能够模拟攻击者 A' 在密钥生成及分发中输出公钥的视图.

(2) 签名过程是可模拟的. 输入公钥、公开的系统参数、消息摘要 M' 以及任一个终端的登录密码 r' 和某个移动终端的部分密钥, 存在一个模拟器能够模拟攻击者进行签名的视图.

定理 2. 本文提出的基于身份门限签名方案是可模拟的.

证明: (1) 密钥生成及分发过程: 给定公开的系统参数、移动终端的身份 ID, 即手机号 T, 以及用户名的数值表示形式 N', 则攻击者 A' 可以计算得出:

$e(\prod_{i\in W}S_{i1}^{d_{\mu i}},g')=e(g,g')^{N'}\cdot\prod_{i\in W}e(\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},S_{i2})^{d_{\mu i}}$ 而 $e(\prod_{i\in W}S_{i1}^{d_{\mu i}},g')=\prod_{i\in W}e(S_{i1},g')^{d_{\mu i}}$, 因此整理上式可得:

$$\begin{aligned}e(\prod_{i\in W}S_{i1}^{d_{\mu i}},g')&=e(g,g')^{N'}\cdot\prod_{i\in W}e(\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},S_{i2})^{d_{\mu i}}\\&=\prod_{i\in W}(e(g,g')^{N'}\cdot e(\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},S_{i2}))^{d_{\mu i}}\\&=\prod_{i\in W}e(S_{i1},g')^{d_{\mu i}}\end{aligned}$$

进而得到: $e(S_{i1},g')=e(g,g')^{N'}\cdot e((\mu'\prod_{k\in W_i}\mu_k)^{d_{\mu i}},S_{i2})$, 可获得密钥生成及分发时的公钥 $P_i=e(g,g')^{N'}$. 因此, 密钥生成及分发过程是可模拟的.

(2) 签名过程: 给定系统公钥、公开的系统参数、消息摘要 M' 以及任一个终端的登录密码 r' 和某个移

动终端的部分密钥. 通过正确的登录密码 r'，可以获取签名的权限. 由部分密钥 $S_i=(S_{i1},S_{i2})$ 及 $\sigma_1=\prod_{i\in W}S_{i1}^{L_i},\sigma_3=\prod_{i\in W}S_{i2}^{L_i}$ 等，攻击者可以满足等式：$e(\sigma_1,g')=\prod_{i\in W}e(\mu'\prod_{k\in W_i}\mu_k,S_{i2})^{L_i}\cdot e(g^{N'},\sigma_3)$，从而获得签名服务器上的主要部分密钥 S'，计算得出 $\sigma_2=\prod_{i\in W}(S'\cdot M')^{L_i}$，最终得到签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$. 因此，签名过程也是可模拟的.

定理 3. 本文提出的基于身份门限签名方案是安全的.

证明：由定理 2 可知本文的门限签名方案是可模拟的，再根据定理 1 可知本方案是不可伪造的. 另外，基于用户的身份进行数字签名，能够实现对发送消息用户身份的认证，同时接收消息的用户也能对接收的消息及数字签名进行验证. 从而保证了移动终端在通信中信息的完整性、用户的身份认证以及通信的不可抵赖性.

由此证明本文所提出的基于身份门限签名的方案在移动终端数字签名中是安全的，值得应用.

3.3 高效性

本方案中 $e(g'',g')$ 能够通过预先计算而得，因此减少了在验证部分的双线性对的计算次数，另外，本方案涉及到的系统参数也有所减少，使方案在计算上更加简化. 下面分析本方案与其他两个参考文献方案在高效性上的比较. 其中 L_e、L_m、L_p 分别表示一次指数运算、乘法运算和双线性对运算，n_m 和 n_u 分别表示一个消息 m 和身份 u 的比特位数. 如表 1 所示.

表 1 三种方案高效性比较

方案	签名算法时间	验证算法时间
文献[7]方案	$(\frac{n_m}{2}+1)\cdot L_m+2L$	$(\frac{n_m+n_u}{2}+2)\cdot L_m+3$
文献[9]方案	$2L_p+\frac{n_u+1}{2}(L_e+L_m$	$2L_p+\frac{n_u+1}{2}(L_e+$
本文方案	$L_p+L_e+L_m$	$2L_e+L_m$

4 结语

综上本文中提出的数字签名方案具有不可伪造性、健壮性和不可抵赖性，能够抵抗适应性选择消息攻击，有效解决移动终端密钥存储困难的难题，同时提高了移动终端在信息传输中的安全，该方案应用到移动终端上，将能够更好地实现移动终端的数字签名.

参考文献

1 王芸,赵长江.安全的移动终端数字签名方案.中国科技信息,2015,(22):52–54.

2 Shamir A. Identity-Based Cryptosystems and Signature Schemes. New York: Springer-Verlag, 1984: 47–53.

3 Hess F. Effcient identity based signature schemes based on pairings. SAC'02, LNCS 2595. Springer-Verlag. 2003. 310–324.

4 黄梅娟.新的基于身份的门限签名方案.计算机与数字工程,2013,(4):625–626.

5 郝立峰.移动终端上一种基于身份数字签名方案的研究[硕士学位论文].武汉:华中科技大学,2011.

6 吕鑫,王志坚,许峰.基于双线性对的新型门限签名方案.计算机科学,2011,38(4):111–114.

7 张建中,高欢欢,赵柄翼.标准模型下基于身份的模型签名方案.计算机工程与应用,2012,48(23):77–80.

8 徐静.标准模型下可证安全的门限签名方案.计算机学报,2006,29(9):1636–1640.

9 郑广亮,魏立线.高效的基于身份的门限签名方案.计算机工程与科学,2013,(8):37–38.