计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(4):574~580, 2007

一个基于双线性映射的前向安全门限签名方案

彭华熹　　冯登国
(中国科学院软件研究所信息安全国家重点实验室　北京　100080)
(huaxi01@ios.cn)

A Forward Secure Threshold Signature Scheme from Bilinear Pairing

Peng Huaxi and Feng Dengguo
(*State Key Laboratory of Information Security*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100080)

Abstract　A forward secure threshold signature scheme from bilinear pairing is proposed by combining the concept of forward security with threshold signature from bilinear pairing. In the scheme proposed the signature key is distributed into the whole group and is updated by means of updating partial keys. So the security of the signature key is enhanced and the scheme has the characters of forward security. Furthermore, for the character of partial keys-update, the scheme can prevent the mobile adversaries. The security of the scheme is also analyzed. It is shown that the proposed scheme is secure and effective.

Key words　threshold signature; bilinear pairing; forward secure; ID-based cryptography

摘　要　将前向安全的概念引入到基于双线性映射的门限签名方案中,提出了一个基于双线性映射的前向安全的门限签名方案. 该方案将签名密钥分散到签名成员集合中,采用各成员部分密钥前向更新的方式实现了签名密钥的前向更新,增强了签名密钥的安全性,使得签名方案具有前向安全性. 另外,由于部分密钥具有前向更新的特性,从而方案有效防止了移动攻击. 对该方案的安全性进行了分析,分析表明,该方案是安全、有效的.

关键词　门限签名;双线性映射;前向安全;基于身份的密码体制

中图法分类号　TP309

在两个组织之间的网络通信中,为了能安全地生成签名,实现签名的权利分配,避免滥用职权,增加内部和外部攻击者对签名密钥的攻击难度,签名者将签名密钥分布式分散给多人管理,只有在足够多的成员参与的情况下才能产生正确的签名,这就需要用到门限签名技术.

门限签名是门限密码学的一个主要研究内容,是普通数字签名的一个扩展. 在一个(t,n)的门限签名方案中,签名密钥分散到 n 个成员的签名成员集合中,签名密钥不直接参与签名过程,由不少于 t 个成员的成员子集使用各自所拥有的部分密钥共同产生最终的签名结果,而任何小于 t 个成员的子集都无法恢复密钥或者计算正确的签名结果.

门限签名方案的安全性很大程度上取决于签名密钥的安全性,现有的基于双线性映射[1]的门限签名的方案[2-4],采用秘密信息共享技术分散签名密钥来保护签名密钥的安全,如文献[3]基于 Hess[5] 签名方案提出了一个可验证的门限签名方案,并给出了详细的证明,但该方案在签名过程中签名成员集合需要多次使用秘密共享技术协商参数和计算部分签名,因此该方案过程复杂,效率较低. 虽然这些方案通过门限技术提高签名密钥的安全性,但存在

收稿日期:2006-07-17;修回日期:2006-11-13
基金项目:国家自然科学基金项目(60273027);国家"九七三"重点基础研究发展规划基金项目(G1999035802);国家杰出青年基金项目(60025205)

以下一些问题:1)当大于或等于 t 个成员的部分密钥泄漏,那么攻击者就能恢复密钥伪造签名,从而签名者在此之前的所有签名将变成无效;2)在这些门限签名方案中,由于成员集合的部分密钥不会定期更新,因此可能遭受移动攻击[6],即攻击者虽然在某一段时间内只能入侵并获得少于 t 个成员的部分密钥,但攻击者可以在很长一段时间入侵更多的成员集合成员,使得获得的部分密钥的个数达到并超过门限值 t,从而威胁签名密钥的安全.

针对现有基于双线性映射门限签名的一些问题,本文提出了一个基于双线性映射的前向安全的门限签名方案. 方案将前向安全的概念引入到门限签名方案中,采用对部分密钥的前向更新实现了签名密钥的前向更新,使得即使所有的部分密钥泄漏,也不会影响到以前产生的签名的有效性. 另外,由于部分密钥的前向安全性和定期更新性,因此能有效地防止移动攻击.

1 相关背景

1.1 基于身份的密码体制和双线性映射

Shamir[7]提出了基于身份的密码体制(ID-based public key cryptography, IDPKC),使用用户的名称、Email 地址等任意的字符串用于计算公钥,委托密钥中心 KGC 产生该 ID 所对应的私钥. IDPKC 的优点在于可以避免传统的基于证书的 PKI 系统中使用证书带来的维护成本高,证书链处理过于繁琐等弊端. 2001 年,Boneh 和 Franklin 提出了一个实用的基于身份的加密方案[1](identity-based encryption, IBE).

双线性映射[1]是基于身份的密码体制中非常重要的概念,双线性映射可以从椭圆曲线中的 Weil Pairing 或 Tate Pairing 构造得到.

设 G_1 是一个阶为 q,生成元为 P 的加法循环群,设 G_2 是阶为 q 的乘法循环群,其中 q 是一个大素数. 映射 $\hat{e}:G_1\times G_1\rightarrow G_2$ 称为双线性映射,如果满足以下 3 个条件:

1) 双线性

$\hat{e}(P_1+P_2,Q)=\hat{e}(P_1,Q)\cdot\hat{e}(P_2,Q)$,

$\hat{e}(P,Q_1+Q_2)=\hat{e}(P,Q_1)\cdot\hat{e}(P,Q_2)$,

$\hat{e}(aP,bP)=\hat{e}(P,Q)^{ab}$.

2) 非退化性

如果 P 是 G_1 的生成元,那么 $\hat{e}(P,P)$ 是 G_2 的生成元,即 $\hat{e}(P,P)\neq 1$.

3) 可计算性

$\hat{e}(P,Q)$ 可有效地计算.

同时 IDPKC 中有以下一些难解问题:

1) DLP 问题. 设 P 和 Q 是 G_1 中的两个元素,找到一个整数 n,满足 $Q=nP$.

2) CDH 问题. 设 $a,b\in Z_q^*$,给定 P,aP,bP,计算 abP.

3) BDH 问题. 设 $a,b,c\in Z_q^*$,给定 P,aP,bP,cP,计算 $\hat{e}(P,P)^{abc}$.

1.2 Hess 的基于身份的签名方案

Hess 的基于身份的签名方案[5]的安全性建立在 CDH 问题难解的基础上,且已在 Random Oracle 模型下证明是 CPA(选择明文攻击)安全的. 本文的门限签名方案基于 Hess 的签名方案,并对该签名方案进行了扩展. 下面简单介绍该签名方案.

1.2.1 系统建立

KGC 分别选定阶为 q 的加法群 G_1 和乘法群 G_2,G_1 的生成元为 P,线性映射为 $\hat{e}:G_1\times G_1\rightarrow G_2$,选择两个安全的 Hash 函数 $H_1:\{0,1\}^*\rightarrow Z_q$ 和 $H_2:\{0,1\}^*\rightarrow G_1$. KGC 随机选定作为其主密钥,计算 $P_{\text{pub}}=s\cdot P$ 作为其公钥. KGC 秘密保存 s,公布 $params=\{G_1,G_2,\hat{e},q,P,P_{\text{pub}},H_1,H_2\}$ 作为其公共参数.

1.2.2 密钥生成

假设一个用户的身份标识符为 ID,那么该用户的公钥为 $Q_{ID}=H_2(ID)$,KGC 计算该用户的私钥为 $S_{ID}=s\cdot Q_{ID}$,KGC 通过安全渠道将 S_{ID} 颁发给用户,可以看出 $Q_{ID},S_{ID}\in G_1$.

1.2.3 签名

若该用户要对消息 M 签名,那么随机选取 $w\in_R Z_q^*$,计算 $\gamma=\hat{e}(P,P)^w$,得到消息 M 的 Hash 值 $v=H_1(M||\gamma)$,计算签名结果

$$U=vS_{ID}+wP, \tag{1}$$

则对消息 M 的签名为 (U,v).

1.2.4 验证

验证者收到消息 M 和签名 (U,v) 后,计算 $\gamma'=\hat{e}(U,P)\hat{e}(Q_{ID},-P_{\text{pub}})^v$,当且仅当 $v=H_1(M||\gamma')$ 时接受该签名.

1.3 签名的前向安全性

前向安全的签名就是把密钥的有效期分为若干个时间段,在每个时间段内都使用不同的密钥签名,即使某个时间段的密钥泄漏,也不会影响之前时间段签名的有效性. 现有的基于双线性映射的前向安

全方案[8-10]的思想都是来源于文献[11]的方案,文献[11]的方案并不具有前向安全的性质,只是使用一个 ID 身份链实现了多层次 KGC 的密钥分发. 基于文献[11]的方案,Canetti 等人在文献[8]中提出了一个基于双线性映射的前向安全加密方案,使用树形结构的时间段表示方法,各个时间段内使用不同的密钥加密,实现了加密的前向安全性. 文献[9]也使用时间段的树形结构表示法,实现了基于双线性映射的前向签名方案.

在本文的方案中,将签名密钥 S_{ID} 的有效时间分为若干个段,即 $t_1,t_2\cdots,t_i,\cdots,t_n$. t_1 时间段内使用 S_1,t_i 时间段内使用 S_i,其中 S_i 由前一个时间段的密钥 S_{i-1} 通过单向函数计算产生. 因此有由 S_{i-1} 能够计算 S_i,但是由 S_i 计算 S_{i-1} 是非常困难的. 成员集合将密钥更新以后,将删除前一个时间段的私钥 S_{i-1}. 这样,即使攻击者在某个时间段 t_i 获得了 S_i,他也无法计算以前的所有私钥,无法伪造该用户以前的签名. 同时,S_i 是分布式存在和更新的,因此任何成员都不知道 S_i 和其他成员的部分密钥.

本文将前向安全的概念扩展到门限签名的方案中,使用部分密钥的前向更新的方式实现了成员集合签名密钥的前向更新,使得任何成员都不可能单独控制签名密钥的前向更新. 从而使得部分密钥和签名密钥都具有前向安全性,同时也有效地解决了门限方案中的移动攻击问题.

2 基于双线性映射的前向安全门限签名方案

按照第 1.2.1 节中的方法建立系统,设签名用户 Dealer 的标识符为 ID,那么其公钥为 $Q_{ID}=H_2(ID)$,KGC 计算其私钥即签名密钥为 $S_{ID}=s\cdot Q_{ID}$,KGC 通过安全渠道将 S_{ID} 发送给 Dealer.

设 $u=\{u_1,u_2,\cdots,u_n\}$ 为 Dealer 的 n 个成员的授权签名成员集合,不妨设成员集合 $u=\{u_1,u_2,\cdots,u_n\}$ 中各个成员的 ID 分别为 $1,2,\cdots,n$. 在该方案中,Dealer 是诚实可信的,不直接参与签名过程,只参与初始化阶段将密钥 S_{ID} 分散到该成员集合中,由该成员集合采用 (t,n) 的门限方案完成消息的签名. 签名密钥的更新由成员集合中的各个成员分别进行更新,有利于实现密钥的前向安全性.

签名中心(SC)负责收集各个成员的部分签名计算得到最后的签名结果,在方案中,SC 是无法得到密钥以及各个成员的部分密钥的. 该方案需要一个公告牌用于发布一些公开信息,任何人都可以查看该公告牌上的信息,但只有 SC 能修改和更新.

2.1 初始化阶段

1) Dealer 随机选取 $A_i\in_R G_1$,其中 $i=1,\cdots,t-1$,令 $A_0=S_{ID}$,构造多项式 $F(x)=\sum_{i=0}^{t-1}A_ix^i$. Dealer 对所有的成员计算其部分密钥 $S_{i0}=F(i)$,其中 $i=1,2,\cdots,n$,将 S_{i0} 通过秘密信道发送给 u_i. 计算 $\hat{e}(A_j,P)$ 用于验证部分密钥的正确性,其中 $j=0,1,\cdots,t-1$,将 $\hat{e}(A_j,P)$ 广播出去. 另外,Dealer 计算 $\hat{e}(S_{i0},P)$ 发送给 SC,用于 SC 在密钥更新阶段验证签名成员部分密钥更新的正确性.

2) u_i 接收到 S_{i0} 后,验证

$$\hat{e}(S_{i0},P)=\prod_{j=0}^{t-1}\hat{e}(A_j,P)^{i^j},\tag{2}$$

若式(2)成立则接受并秘密保存该部分密钥,否则返回失败信息,要求重新分发部分密钥.

初始化阶段后,各个成员得到的都是初始部分密钥,即时间段 t_0 的部分密钥.

2.2 密钥更新

当从时间段 t_{k-1} 过渡到时间段 t_k 时,授权签名集合成员更新密钥方法如下:

1) u_i 随机选取 $a_{ij}\in_R Z_q^*$,其中 $j=0,1,\cdots,t-1$,构造多项式 $f_i(x)=\sum_{j=0}^{t-1}a_{ij}x^j$. 对所有其他成员计算 $f_i(j)$,其中 $j=1,\cdots,n$ 且 $j\neq i$,将 $f_i(j)$ 通过秘密信道发送给 u_j. 计算 $\alpha_{il}=a_{il}P$ 用于验证 $f_i(j)$ 的正确性,其中 $l=0,1,\cdots,t-1$,将 α_{il} 广播出去.

2) u_j 接收到 $f_i(j)$ 后,验证

$$f_i(j)\cdot P=\sum_{l=0}^{t-1}\alpha_{il}\cdot j^l.\tag{3}$$

若式(3)验证正确则接受,否则返回失败信息,要求重新计算该秘密值. 若验证通过,u_j 计算其部分密钥更新参数 $r_{jk}=\sum_{i=1}^{n}f_i(j)$. 这样,在成员集合中存在一个多项式 $g(x)=\sum_{i=0}^{t-1}b_ix^i$,其中 $b_i=\sum_{l=1}^{n}a_{li}$,虽然成员集合中任何一个成员都不知道该多项式,但不难知 $r_{jk}=g(j)$.

3) 因此,u_i 更新其部分密钥 $S_{ik}=S_{i,k-1}+r_{ik}H_2(t_k)$,即有

$$S_{ik}=S_{i0}+\sum_{j=1}^{k}r_{ij}H_2(t_j),\tag{4}$$

计算 $\hat{e}(S_{ik},P)$ 用于 SC 验证部分密钥. u_i 将 $\hat{e}(S_{ik},$

P)发送给 SC.

4) SC 接收到 $\hat{e}(S_{ik},P)$后,取出 u_i 上一个时间段的部分密钥验证参数 $\hat{e}(S_{i,k-1},P)$,计算密钥更新的部分公开信息 $R_{ik}=\sum_{j=1}^{n}\sum_{l=0}^{t-1}\alpha_{jl}\cdot i^l$,由 r_{ik}的计算方法和式(3),显然有 $R_{ik}=r_{ik}P$. 验证该部分密钥的正确性:

$$\hat{e}(S_{ik},P)=\hat{e}(S_{i,k-1},P)\hat{e}(H_2(t_k),R_{ik}),\quad(5)$$

若式(5)正确则进入下一步,否则返回失败信息,并检查该成员是否已被攻击.

5) SC 接收 n 个成员的验证消息并验证,未通过验证的成员被认为已被攻击,排除出成员集合之外. 若验证通过的成员个数$\geqslant t$,SC 则选择其中的 t 个成员,不妨设其 ID 分别为 $1,\cdots,t$,计算密钥更新的公开信息 $R_k=\sum_{i=1}^{t}R_{ik}\eta_i$,其中 $\eta_i=\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}$ 为 Lagrange 系数. 这样,在成员集合中存在 $r_k=\sum_{i=1}^{t}r_{ik}\eta_i$,虽然任何一个成员都不知道 r_k,但不难知 $R_k=r_kP$. 为了保证更新后的密钥和以前的密钥没有重复,SC 计算 $R_k'=\prod_{i=1}^{k}\hat{e}(H_2(t_i),R_i)$,验证 R_k' 与保存的$R_i'(i<k)$是否有重复,若有则更新的密钥和以前产生的密钥有重复,要求重新更新密钥,回到步骤 1). 否则密钥更新成功,SC 在公告牌上公布 R_k 和部分密钥验证参数$\hat{e}(S_{ik},P)$,保存 R_k' 用于以后验证,向成员集合发送密钥更新成功信息. 不难知时间段 t_k 签名授权成员集合的签名密钥为

$$S_k=\sum_{i=1}^{t}S_{ik}\eta_i,\text{即 }S_k=S_{ID}+\sum_{j=1}^{k}r_jH_2(t_j).\quad(6)$$

6) 签名授权集合成员 u_i 接收到密钥更新成功信息后,秘密保存 S_{ik}作为时间段 t_k 的新的部分密钥,销毁上一个时间段 t_{k-1}的部分密钥 $S_{i,k-1}$以及更新参数 r_{ik}.

这样,步骤 5)中验证成功的各个成员部分密钥更新为 t_k 时间段的部分密钥,总的签名密钥也因为部分密钥的更新而更新为时间段 t_k 的密钥.

2.3 部分签名生成

在时间段 t_k 内,成员集合为了完成对消息 M 的签名,签名成员集合进行以下步骤:

1) 首先,SC 随即选取 $w\in_R Z_q^*$,$P_1\in_R G_1$($P_1\neq P$),计算 $\gamma=\hat{e}(P,P)^w$,将消息 M 做 Hash 值 $v=H_1(M||\gamma)$,将 v,P_1 发布在公告牌上,并启动签名过程.

2) u_i 从公告牌上查询得到 v,P_1,随机选取 $w_i\in_R Z_q^*$,计算 $\gamma_i=w_iP$ 和部分签名

$$U_i=vS_{ik}+w_iP_1,\quad(7)$$

将(U_i,γ_i)发送给 SC.

2.4 最终签名生成

SC 接收到(U_i,γ_i)后,首先验证收到的部分签名,从公告牌上获得第 2.2 节步骤 5)保存的部分密钥验证参数 $\hat{e}(S_{ik},P)$,验证下面等式是否成立:

$$\hat{e}(P_1,\gamma_i)=\hat{e}(U_i,P)\hat{e}(S_{ik},P)^{-v},\quad(8)$$

由于

$$\hat{e}(U_i,P)\hat{e}(S_{ik},P)^{-v}=\hat{e}(vS_{ik}+w_iP_1,P)\cdot\hat{e}(-vS_{ik},P)=\hat{e}(vS_{ik},P)\hat{e}(w_iP_1,P)\cdot\hat{e}(-vS_{ik},P)=\hat{e}(P_1,\gamma_i),$$

因此有式(8)成立. 若验证不通过则拒绝该部分签名.

SC 从$\geqslant t$ 个通过验证的成员中选取 t 个 U_i,不妨设这 t 个成员的 ID 分别为 $1,\cdots,t$,计算

$$U=\sum_{i=1}^{t}U_i\eta_i+wP,R=\sum_{i=1}^{t}\gamma_i\eta_i,\quad(9)$$

其中 $\eta_i=\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}$ 为 Lagrange 系数.

因此最终的签名结果为(M,U,R,v,Q_{ID},k),其中 k 表示该签名是在时间段 t_k 内产生的.

2.5 前向安全的签名验证

签名验证者收到签名结果(M,U,R,v,Q_{ID},k)后,首先在公告牌上查询到签名者在时间段 t_k 以前的密钥公开信息为 $R_1,R_2,\cdots,R_k$,计算

$$\gamma'=\frac{\hat{e}(R,-P_1)\hat{e}(U,P)\hat{e}(Q_{ID},-P_{pub})^v}{\left(\prod_{j=1}^{k}\hat{e}(H_2(t_j),R_j)\right)^v}.\quad(10)$$

验证 $v=H_1(M||\gamma')$是否成立,如果成立则接受该签名,否则拒绝该签名.

3 安全性分析

3.1 (M,U,R,v,Q_{ID},k)是有效的前向安全签名

要证明(M,U,R,v,Q_{ID},k)是有效的前向安全签名,则需要证明 $v=H_1(M||\gamma')$成立,由式(4)(7)(9)(10)以及第 2.2 节中 r_k 和第 2.3 节中 γ 的生成方法,得

$$\gamma'=\left(\hat{e}\left(\sum_{i=1}^{t}\eta_i\left(vS_{i0}+v\sum_{j=1}^{k}r_{ij}H_2(t_j)+w_iP_1\right)+wP,P\right)\right)\Big/\left(\hat{e}\left(\sum_{j=1}^{k}r_jH_2(t_j),P\right)^v\right)\cdot$$

$$\hat{e}\left(\sum_{i=1}^{t}\gamma_i\eta_i,-P_1\right)\hat{e}(S_{ID},P)^{-v}=\hat{e}(P,P)^{w},$$

根据 $\gamma=\hat{e}(P,P)^{w}$ 以及上式可得

$$v=H_1(M\|\gamma')=H_1(M\|\hat{e}(P,P)^{w})=H_1(M\|\gamma),$$

因此有(M,U,R,v,Q_{ID},k)是有效的前向安全签名. 另外,由第 2.3 节可以看出,部分签名的生成不需要集合成员的多次交互,相比文献[3]的门限签名方案,本方案更高效.

3.2 方案具有前向安全性

假设某一攻击者已获得时间段 t_k 成员集合中 t 个成员的密钥 S_{ik},不妨设 $i=1,\cdots,t$,企图通过 $R_{ik}=r_{ik}P$,$S_{ik}=S_{i,k-1}+r_{ik}H_2(t_k)$计算以前的密钥 $S_{ij}(j<k)$. 由于由 R_{ik}求 r_{ik}是 DLP 难解问题,因此攻击者无法直接求得 r_{ik}来计算 $S_{i,k-1}$. 又由于通过 $R_{ik}=r_{ik}P$ 和 $H_2(t_k)$来计算 $r_{ik}H_2(t_k)$是 CDH 难解问题,因此攻击者也无法通过求 $r_{ik}H_2(t_k)$来计算 $S_{i,k-1}$. 因此签名方案的前向安全性建立在 CDH 问题难解的基础上,攻击者无法通过时间段 t_k 的部分密钥 S_{ik}求得以前的部分密钥 $S_{ij}(j<k)$,由定理 1 可知攻击者也无法伪造签名者以前的签名,从而方案具有前向安全的特性.

定理 1. 即使攻击者获得了时间段 t_k 超过 t 个成员的密钥 S_{ik},也不能伪造时间段 $t_j(j<k)$的签名.

证明. 攻击者选择随机参数 $w\in_R Z_q^*$,$P_1\in_R G_1(P_1\neq P)$,计算 $\gamma=\hat{e}(P,P)^{w}$ 和消息 M 的 Hash 值 $v=H_1(M\|\gamma)$,重复第 2.3 节和第 2.4 节中的步骤计算得到签名结果为 $U=\sum_{i=1}^{t}U_i\eta_i+wP$,$R=\sum_{i=1}^{t}\gamma_i\eta_i$,因此伪造的时间段 t_j 消息 M 的签名为 (M,U,R,v,Q_{ID},j).

由于

$$\gamma'=\left(\prod_{i=j+1}^{k}\hat{e}(r_iH_2(t_i),P)\right)^{v}\hat{e}(P,P)^{w}=\hat{e}\left(v\sum_{i=j+1}^{k}r_iH_2(t_i)+wP,P\right).$$

如果该伪造的签名结果能通过第 2.5 节的验证,则有 $\hat{e}\left(v\sum_{i=j+1}^{k}r_iH_2(t_i)+wP,P\right)=\hat{e}(P,P)^{w}$. 要使该式成立,由非退化性,那么一定有 $v\sum_{i=j+1}^{k}r_iH_2(t_i)=O$,其中 O 为 G_1 的原点. 两边同时点乘 v^{-1},因此有

$$\sum_{i=j+1}^{k}r_iH_2(t_i)=O. \tag{11}$$

而在第 2.2 节的步骤 5)中,$\forall j<k$ 有 $R_j'\neq R_k'$,即 $\prod_{i=1}^{j}\hat{e}(H_2(t_i),R_i)\neq\prod_{i=1}^{k}\hat{e}(H_2(t_i),R_i)$,要使该式成立,那么一定有 $\sum_{i=j+1}^{k}r_iH_2(t_i)\neq O$,与式(11)矛盾. 因此即使攻击者获得了时间段 t_k 中 t 个成员的密钥 S_{ik},也不能伪造时间段 $t_j(j<k)$的签名.

证毕.

3.3 方案可防止欺诈

在初始化阶段,若攻击者企图发送伪造的部分密钥欺骗 u_i,那么 u_i 可以通过验证式(2)发现伪造的部分密钥. 在密钥更新阶段,u_i 可以通过验证式(3)发现不诚实的内部欺骗者,防止产生错误的密钥更新参数 r_{ik}. SC 也可以通过验证式(5)发现错误的密钥更新,防止攻击者伪造错误的部分更新密钥. 在最终签名生成阶段,SC 通过验证式(8)能即时发现错误的部分签名和参数 γ_i,发现内部欺骗者. 另外,在每一次验证过程中,诚实的内部成员或者 SC 都可以根据失败信息发现产生错误的欺骗者,保证密钥更新和签名的正常进行.

3.4 方案可抵抗伪造攻击

定理 2. 攻击者若已知部分签名或成员集合签名,求解部分密钥或签名密钥的难度等价于破解 Hess 的签名方案.

证明. 若攻击者 A 获得了部分签名即已知$(U_i,v,R_{ik},M,\gamma_i)$,企图获得部分私钥,由于通过 $\gamma_i=w_iP$ 计算 w_i 是 DLP 难题,通过 $\gamma_i=w_iP$ 和 P_1 计算 w_iP_1 是 CDH 难题,因此 A 不能利用 $U_i=vS_{ik}+w_iP_1$ 计算出部分签名,与 Hess[5] 的签名计算式(1)比较可知攻击者已知部分签名求部分密钥 S_{ik} 的难度等价于破解 Hess 的签名方案. 同理,若攻击者 A 已知成员集合的签名,即$(U,v,R_k,R,M,\gamma,Q_{ID})$,由式(9)以及 $S_k=\sum_{i=1}^{t}S_{ik}\eta_i$ 可得 $U=vS_k+\sum_{i=1}^{t}\eta_iw_iP_1+wP$,与式(1)比较可知求解时间段 t_k 密钥 S_k 的难度等价于破解 Hess 的签名方案. 证毕.

定理 3. 在时间段 t_k 的部分签名生成阶段,一个不知道成员 u_i 部分密钥的攻击者 A 不能假冒该成员伪造一个正确的部分签名.

证明. 攻击者 A 企图假冒合法成员 u_i,但由于 A 不知道 u_i 的部分密钥 S_{ik},也就无法通过式(7)计

算能通过验证式(8)的部分签名结果 U_i,攻击者 A 只能依靠猜测 S_{ik} 来计算部分签名结果,由于系统建立时期 q 足够大(160b),猜出正确的 S_{ik} 的概率是非常低的.

Hess 签名方案[5] 已经证明攻击者若已获得合法签名,也不能为自己选定的一个消息通过式(1)伪造一个合法签名,比较部分密钥计算式(7)和 Hess 的签名计算式(1),可知本方案的部分签名的伪造难度等价于 Hess 的签名伪造难度. 因此攻击者无法产生正确的部分签名. 证毕.

由定理 2 可知攻击者通过公开信息以及签名来获得私钥,从而伪造签名是困难的. 由定理 3 可知未知部分密钥的攻击者无法伪造一个正确的签名. 因此综上所述,本方案的防伪造性和部分密钥以及签名授权集合密钥的安全性基于 Hess 的签名方案的安全性,本方案可抵抗伪造攻击.

3.5 方案可有效防止移动攻击(mobile adversaries)

移动攻击首先是由 Ostrovskey 和 Yung 在文献[6]中提出来的,文献[6]中指出在移动攻击模型中,一个攻击者可能在某一段时间内入侵不超过门限值 t 个的节点,即使系统发现了这些受攻击的节点,甚至将这些节点从系统中删除,但如果系统不再更新密钥的分布,那么攻击者可以在很长一段时间使得入侵节点的个数达到并超过门限值 t,从而威胁整个系统的安全.

针对移动攻击的问题,传统的门限方案一般采用定期重新分发密钥的方式解决. 在本文的方案中,采用部分密钥自我前向安全更新的方式有效解决了移动攻击的问题.

假设移动攻击者 A 在时间段 t_{k_1} 获得了不大于 t 个的部分密钥,不妨设为 $S_{1k_1}, S_{2k_1}, \cdots, S_{ik_1}$,其中 $i<t$. 在移动攻击模型中,SC 是可以通过检测发现密钥的泄漏情况的,因此 SC 将该部分成员排除出成员集合不参与密钥更新. 而攻击者 A 在另一个时间段 t_{k_2} 又获得了另外不大于 t 个的部分密钥,不妨设为 $S_{jk_2}, S_{j+1,k_2}, \cdots, S_{lk_2}$,其中 $l-j+1<t$. 显然,由于在时间段 t_{k_1} 到 t_{k_2} 内,虽然攻击者 A 所获得的部分密钥总数可能达到或超过 t,但是其所拥有的 $S_{1k_1}, S_{2k_1}, \cdots, S_{ik_1}$ 没有参与密钥更新过程. 由第 3.2 节的分析可知,对于 $\forall i$,由 R_{ik} 求 r_{ik} 是 DLP 难解问题,由 $R_{ik}=r_{ik}P$ 和 $H_2(t_k)$ 来计算 $r_{ik}H_2(t_k)$ 是 CDH 难解问题,因此,移动攻击者 A 无法求出 $S_{1k_2}, S_{2k_2}, \cdots, S_{ik_2}$,也无法求出 $S_{jk_1}, S_{j+1,k_1}, \cdots, S_{lk_1}$,也就是说无法得到超过 t 个的同一个时间段的部分密钥. 所以,移动攻击者即使在很长一段时间内获得了总数超过门限值 t 个的部分密钥,由于泄漏的部分密钥没有进行前向更新,仍然不能采用 $S_k=\sum_{i=1}^{t} S_{ik}\eta_i$ 计算出任何一个时间段的密钥,也不能伪造签名,有效地防止了移动攻击.

4 结束语

本文针对现有基于双线性映射门限签名的一些问题,提出了一个前向安全的门限签名方案. 该方案不仅具有门限方案的入侵容忍的性质,而且具有前向安全的特性,使得即使所有的部分密钥被泄漏,也不会影响到以前所产生的签名的有效性. 同时,本文也对方案的安全性进行了分析,分析结果表明,本方案可防止内部欺骗和抵抗伪造攻击,且能有效地防止移动攻击,是一个安全、有效的前向安全的门限数字签名方案.

参 考 文 献

[1] D Boneh, M Franklin. Identity-based encryption from the Weil pairing [G]. In: Advances in Cryptology-Crypto 2001, LNCS 2139. Berlin: Springer-Verlag, 2001. 213-229

[2] D L Vo, F Zhang, K Kim. A new threshold blind signature scheme from pairings [C]. In: SCIS2003. New York: ACM Press, 2003. 26-29

[3] J Baek, Y Zheng. Identity-based threshold signature scheme from the bilinear pairings [C]. In: IAS '04 Track of ITCC '04. Los Alamitos: IEEE Computer Society Press, 2004. 124-128

[4] Ma Chunbo, He Dake. A new Chameleon threshold signature on bilinear pairing [J]. Journal of Computer Research and Development, 2005, 42(8): 1427-1430 (in Chinese)
(马春波,何大可. 基于双线性映射的卡梅隆门限签名方案[J]. 计算机研究与发展, 2005, 42(8): 1427-1430)

[5] F Hess. Efficient identity based signature schemes based on pairings [G]. In: Selected Areas in Cryptography (SAC 2002), Lecture Notes in Computer Science 2595. Berlin: Springer-Verlag, 2002. 310-324

[6] R Ostrovsky, M Yung. How to withstand mobile virus attacks [C]. The 10th Annual Symp on Principles of Distributed Computing (PODC '91), Montreal, Quebec, Canada, 1991

[7] A Shamir. Identity-based cryptosystems and signature schemes [G]. In: Advances in Cryptology-Crypto '84, LNCS 196. Berlin: Springer-Verlag, 1984. 47-53

[8] R Canetti, S Halevi, J Katz. A forward-secure public-key encryption scheme [G]. In: Advances in Cryptology—Eurocrypt '03, LNCS 2656. Berlin: Springer-Verlay, 2003. 255-271

[9] F Hu, C-H Wu, J D Irwin. A new forward secure signature scheme using bilinear maps [R]. Cryptology ePrint Archive, Tech Rep: 2003/188, 2003

[10] Y Dodis, M Franklin, J Katz, *et al*. Intrusion resilient public-key encryption [G]. In: Topics in Cryptology CT-RSA 2003, Lecture Notes in Computer Science 2612. Berlin: Springer-Verlag, 2003. 19-32

[11] C Gentry, A Silverberg. Hierarchical ID-based cryptography [G]. In: Advances in Cryptology-Asiacrypt 2002, Lecture Notes in Computer Science 2501. Berlin: Springer-Verlag, 2002. 548-566

Peng Huaxi, born in 1978. Ph. D. candidate. His main research interests include information system and network security, PKI, etc.

彭华熹,1978 年生,博士研究生,主要研究方向为大型网络信息系统安全、PKI 技术等.

Feng Dengguo, born in 1965. Professor and Ph. D. supervisor. His main research interests include information and network security.

冯登国,1965 年生,研究员,博士生导师,主要研究方向为信息和网络安全.

Research Background

This work is partly supported by the National Natural Science Foundation of China under grant No. 60273027, the National Key Basic Research Program of China under grant No. G1999035802, and the National Foundation of China for Palmary Youth under grant No. 60025205.

Combining forward security and threshold cryptography can provide some security guarantees to the identity-based signature scheme. The adversary cannot forge the signature even if the adversary has taken control of all servers and has completely learned the secret. And lots of researchers pay an increasing attention to the forward secure threshold signature from bilinear pairing. In this paper, a forward secure threshold signature scheme from bilinear pairing is proposed. The signature key is distributed into the whole group and updated by means of the updating of partial keys. So the security of the identity-based signature scheme is enhanced and the character of forward security is provided. The scheme can prevent the mobile adversaries for the character of forward security. The security of our scheme is analyzed. The results show that the proposed scheme is secure and effective.