一个高效的有向传递签名方案

黄振杰[1,2,3], 郝艳华[2], 王育民[2], 陈克非[1]
(1. 上海交通大学计算机科学与工程系, 上海 200030; 2 西安电子科技大学综合业务网国家重点实验室, 陕西西安 710071;
3. 漳州师范学院数学与信息科学系, 福建漳州 363000)

摘 要: 传递签名是由 Micali 和 Rivest 在 2002 年首先提出的, 主要用于对二元传递关系进行签名. 已有的传递签名方案都是无向的, 只适用于对等价关系签名, 提出有向传递签名方案是个留待解决的公开问题. 该文提出一个高效的全序有向传递签名方案, 并证明该方案在选择明文攻击下是安全的. 在方案中, 签名的 β_{uv} 部分被限定在 0 和 $q/2$ 之间, 以防止敌手由 (u, v) 的签名伪造 (v, u) 的签名, 从而保证签名的有向性. 将该方案与无向传递签名方案结合, 提出一个可对任何有向二元传递关系进行签名的方案.

关键词: 数字签名; 传递签名; 有向传递签名; 序关系
中图分类号: TN918, TP309 文献标识码: A 文章编号: 0372-2112 (2005) 08-1497-05

Efficient Directed Transitive Signature Scheme

HUANG Zhen-jie[1,2,3], HAO Yan-hua[2], WANG Yu-min[2], CHEN Ke-fei[1]
(1. *Department of Computer Science and engineering, Shanghai Jiaotong University, Shanghai 200030, China;*
2. *National Key Lab of Integrated Service Networks, Xidian University, Shaanxi, Xi'an 710071, China;*
3. *Department of Mathematics and Information Science, Zhangzhou Normal University, Fujian, Zhangzhou 363000, China*)

Abstract: Transitive signature was first introduced by Micali and Rivest in 2002 to meet the need of certain applications like signing a chain of command, a chain of certificate or transitive binary relations. Unfortunately, all the transitive signature schemes available are undirected ones and can only be used in the case of equivalence relation. The problem of finding a directed transitive signature scheme remains a very interesting open problem. In this paper, an efficient total ordering directed transitive signature scheme is proposed and its security against adaptive chosen-message attack is proved. In the proposed scheme, the part β_{uv} of signature is limited from 0 to $q/2$ to prevent an adversary from forging (v, u)'s signature with the knowledge of (u, v)'s signature, and thus achieve the directed property. A solution for signing any directed transitive binary relation is presented by combining the proposed scheme with the undirected transitive signature schemes available.

Key words: digital signature; transitive signature; directed transitive signature; order relation

1 引言

传递签名是由 Micali 和 Rivest[1] 在 2002 年首先提出的, 主要用于对具有传递性的二元关系进行高效签名, 这在军事、政治和经济等领域都有重要应用. 以军事指挥系统为例, 当上级 A(比如说是军长) 向下级 B(比如说是连长) 下达命令时, 为了保证命令的合法性, 上级 A 必需向下级 B 证明他有权向其下达命令, 即要求 A 提供一个权威 T(比如说是司令部) 的签名, 用来证明"A 是 B 的上级". 一个平凡的做法是: 由 T 为每对有"命令"关系的成员对发布一个签名, 但这有一个明显的缺点, 就是 T 必须亲自产生很多签名, 而且每增加一个成员, 就得为该成员与其他成员间的所有"命令"关系进行签名, 这可能需要增加许多签名, 对于一个动态增长的群体来说, 这样做的效率太低. 另一种方法是使用命令链. 军长 A 与连长 B 中间还有师长 C_1、团长 C_2、营长 C_3, 当 A 要向 B 下命令时, 他向 B 提供这样的一个签名链: "A 是 C_1 的上级", "C_1 是 C_2 的上级", "C_2 是 C_3 的上级", "C_3 是 B 的上级", 用这种方式可以减少签名量, 但这又会带来另一个问题, 命令链会泄露一些不必要的细节, 比如会泄露该命令链的所有中间成员以及这些成员间的等级关系, 也就是说, 该部队组织结构会被泄露, 这将给机密性带来额外的威胁. 与军事指挥中的命令链相类似的还有 PKI 中的证书链, 电子政务中也有类似情形. 注意到这些二元关系都具有传递性, Micali 和 Rivest 提出传递签名来满足对这类问题进行高效和安全签名的要求.

我们知道二元关系可以用图来表示, 一个二元关系等价于一个图, 等价关系与无向传递图等价, 序关系与有向传递图等价, 因此在本文中对二元关系和图将不加区分. 一个图 $G=(V, E)$ 由一个有限结点集 V 和一个有限边集 $E \subseteq V \times V$ 组成. 结点代表成员, 连接两个结点的边则代表结点所对应的两个成员之间的关系, 如果这种关系是对称的就用无向边来表示,

收稿日期: 2004-02-03; 修回日期: 2005-03-25
基金项目: 国家自然科学基金(No. 60473027, No. 60273049); 国家 973 项目(No. G1999035803); 福建省教育厅科技项目(No. JA04250)

如果关系是非对称的则需用有向边才能表示. 不管对无向图还是有向图,本文都用有序对(u, v)来表示从结点u到v的边. 对于无向图, 存在边(u, v)就一定存在边(v, u),但在有向图中, 存在有向边(u, v)则不一定存在有向边(v, u). 传递签名所考虑的是具有传递性的图, 一个图称为是可传递的, 如果它有一条从u到v的路就一定有从u到v的边. 图$G=(V, E)$的传递闭包$G^*=(V^*, E^*)$是满足这样条件的图: $V^*=V$且边$(u, v)\in E^*$当且仅当中有一条从u到v的路. 图$G=(V, E)$的传递简约$G'=(V', E')$是和G有相同传递闭包的图类中边数最少的图. 有向图和无向图的传递简约都可有效求得[2]. 有关图和二元关系的其他概念请参见[3].

考虑一个表示可传递二元关系的图$G(V, E)$(无向或有向的), 传递签名(transitive signature)是这样的一种签名方案, 签名者Alice对图G的边进行签名,使得任何人只要得到Alice对边(u, v), (v, w)的签名, 无需知道签名私钥就可简单地计算出关于边(u, w)的签名,而且这样产生的签名与由Alice产生的签名是不可区分的, 这就是传递签名的传递性. 这样一来, 对一个传递图签名就只需对其某个传递简约签名即可,其主要优点是: 1. 使所需签名量达到最小; 2. 隐藏关系链的中间细节; 3. 特别适合对动态增长的关系图进行签名, 每增加一个结点, 只需增加在传递简约中与其关联的边的签名,其他边的签名可由传递性得到. 这几点对于提高签名与验证的效率以及提高安全性和保密性都有重要意义.

传递签名是2002年才提出的新概念,目前只有少数几个方案: Micali和Rivest[1]在提出传递签名概念的同时也给出了第一个传递签名方案, 我们记它为MR02方案; 稍后, 在同一年Bellare和Neven[4]在ASIACYPT'02上又提出基于素因子分解和RSA的传递签名方案. 遗憾的是已有的这些方案都只适用于无向图的情形, 称这些方案为无向传递签名方案, 而提出有向传递签名方案仍是一个急待解决的公开问题[1]. 也就是说,已提出的传递签名只适用于与无向图相对应的等价关系,提出适用于与其他传递关系(如偏序关系、全序关系等)相对应的有向图的有向传递签名方案仍是个留待解决的公开问题,上述的命令链和证书链的例子都属于后者, 因此这个公开问题的解决显得特别重要.

另外, Johnson等在[5]讨论了同态签名(homomorphic signature),其明文空间与签名空间是两个同态群, 签名算法是它们之间的同态映射. 如果将传递签名的拟二元运算(见第2节)看成二元运算,那么传递签名就是一种同态签名, 可见同态签名与传递签名关系密切. 同样地, 文[5]中也将提出有向同态签名方案, 称为半群同态签名(semigroup homomorphic signature),留作公开问题.

本文讨论有向传递签名,我们对MR02方案进行改进, 先提出一个适用于明文空间为全序关系的有向传递签名方案, 并证明该方案在选择明文攻击下是安全的, 在此基础上我们将该方案与MR02方案结合, 提出一个适用于任意有向图的有向传递签名的解决方案. 这样就使得传递签名不仅可对等价关系签名,还可对其他传递关系,如偏序关系、全序关系等进行签名,其适用范围扩大了很多.

本文的余下部分是这样安排的: 在第2节里, 我们给出一般传递签名及其安全性的定义, 对其性质作了说明; 在第3节我们介绍了Micali和Rivest提出的无向传递签名方案, 并为该方案的传递运算和合成运算给出更准确更详细的定义; 我们的有向传递签名方案在第4节里给出, 4.1小节给出一个适用明文空间为全序关系的有向传递签名方案, 并证明该方案在选择明文攻击下是安全的, 4.2小节是一个一般有向传递签名方案; 第5节是结论和进一步工作的可能方向.

2 传递签名

传递签名是对可传递二元关系的签名, 与标准数字签名相比其主要特点是具有传递性, 其明文空间和签名空间各自都带有一个拟二元运算. 我们称$+$为集合A上的一个拟二元运算,如果对于任意$a, b\in A$, 要么$a+b=c\in A$,要么$a+b=$ False. 也就是说,如果a和b可运算, 则其结果c一定也在A中,如果它们不可运算, 就得到一个表示错误的值"*False*".

这里我们参照[5]中同态签名的定义为传递签名给出一个一般性定义:

定义1 一个传递签名方案一般由4个集合(K_S, K_P, M, S), 2个运算$(\oplus, \otimes)$和3个算法(TKG, TSig, TVer)组成, 其中K_S是私钥空间, K_P是公钥空间, M是明文空间(它是某集合上的一个可传递二元关系), S是签名空间, 2个运算和3个算法定义如下:

® $\oplus$: $M\times M\to M$ 是M上的拟二元运算, 该运算定义M的传递性.

® $\otimes$: $S\times S\to S$ 是S上的拟二元运算, 称为合成运算, 用来产生传递签名.

® TKG: $\{0, 1\}^k\to K_S\times K_P$ 是用来生成密钥的一个随机算法, 输入1^k, 输出密钥对(k_s, k_p). k为安全参数.

® TSig: $K_S\times M\to S$ 是签名算法, 可以是确定性的也可以是随机性的, 输入私钥k_s和待签消息m, 输出签名σ_m. 而且, 对于任意取定的私钥k_s, TS_{igk_s}是$(M, \oplus)$到$(S, \otimes)$的同态映射.

® TVer: $K_P\times M\times S\to\{1, 0\}$ 是签名的验证算法, 它是确定性的, 输入公钥k_p和被签消息m及签名σ, 当σ为m的有效签名时输出1, 否则输出0.

由于具有传递性, 传递签名的安全性与标准签名的安全性是不一样的, 标准签名的安全性要求: 在基础安全假设下, 任何不知道私钥的敌手都是不可能产生新的有效签名. 这样的安全要求显然是与传递签名的初衷相违背的, 传递签名方案提供了合成运算$\otimes$使得任何人都可用它来产生新的签名, 而且合成得到的签名与签名人亲自签的签名是不可区分的, 因此标准签名的安全性要求不再适用于传递签名, 传递签名应有自己的安全性定义.

为定义传递签名的安全性, 我们需要张成集的概念, 设B为A的一个非空子集, $+$为A上的拟二元运算, B关于$+$的张成集$\mathrm{Span}_+(B)$是满足下列条件的集合:

(1) $B\subseteq\mathrm{Span}_+(B)$, 且$+$在$\mathrm{Span}_+(B)\cup\{\mathrm{False}\}$上封闭;

(2) 若A的子集R也符合(1), 则必有$\mathrm{Span}_+(B)\subseteq R$.

定义 2　一个传递签名称为在选择明文攻击下是安全的, 如果在允许敌手任意选择明文请求签名的条件下, 任何敌手 A 在多项式时间内产生一个不属于已有有效签名的张成集的有效签名的概率是可忽略的, 即任何敌手 A 的攻击优势(advantage) Adv A 是可忽略的, 这里

$$\mathrm{Adv}\ A = \Pr[A^{TSig(k,\cdot)} = (m, \sigma_m) \wedge TVer(m, \sigma_m) = 1 \wedge m \notin Span\{m_1, m_2, \cdots, m_q\}]$$

其中 $\{m_1, m_2, \cdots, m_q\}$ 为已签消息集, k 为签名方案的安全参数.

从上述定义我们可以知道传递签名具有这样的几个重要性质:

® 抗选择明文攻击: 在允许敌手任意选择明文请求签名的条件下, 任何敌手要伪造一个不在已有有效签名的张成集内的有效签名是不可能的.

® 可传递性: 已知 m 和 n 的签名 σ_m 和 σ_n, 如果 $m \oplus n = x$, 则任何人无需知道私钥就可产生签名 $\sigma_x = \sigma_m \otimes \sigma_n$, 使得 $TVer(k_p, x, \sigma_x) = 1$.

® 不可区分性: 任何人都不可能区分一个签名是签名人签的还是通过合成运算 $\otimes$ 合成而来的.

3　无向传递签名方案(MR02)

Micali 和 Rivest[1] 提出的无向传递签名方案是用于对表示等价关系的无向传递图进行签名的, 它由五个步骤组成, 它的点签名和边签名是分开的, 其方案描述方式也与本文给出的一般性形式不尽相同, 这里我们按其原有方式引述如下, 在第 4 节里我们将给出一个由其改进而来的有向传递签名方案, 那里将用本文的一般形式描述, 读者可从中看出两种描述之间的对应关系:

(1) 用户设置(User setup)　用户选择一个用于对结点进行签名的公钥签名方案(可抗选择明文攻击)和一对公钥/私钥对, 并发布公钥.

为对边进行签名, 选择如下参数并分布:

– 选择满足 $q \mid (p-1)$ 的大素数 p 和 q;

– 选择 Z_p^* 的 q 阶子群 G_q 的两个生成元 g 和 h 使得对其他人来说求 h 关于基 g 的离散对数是不可行的.

(2) 建立新结点(Creating a new vertex)　如果 Alice 要建立一个新的结点并将它加到图中, 她执行如下步骤:

– 设 n 为已建立的结点数, 将 n 加 1;

– 随机选择 $x_n, y_n \in Z_q$, 并计算 $v_n = g^{x_n} h^{g_n} \pmod p$;

– 签署并发布这样的一个陈述:"图中的第 n 个结点用值 v_n 表示."(这个消息用点签名算法签名, 在这里值 v_n 以明文形式给出, 值 x_n 和 y_n 作为秘密值由 Alice 保存)

(3) 边签名(Signing the edge(i, j))　为对连接第 i 个结点和第 j 个结点的边 (i, j) 签名, Alice 计算并发布如下的 4 元组:

$$(i, j, \alpha_{ij}, \beta_{ij})$$

其中　$\alpha_{ij} = x_i - x_j \pmod q$, $\beta_{ij} = y_i - y_j \pmod q$

(4) 边签名验证(Verifying an edge signature)　任何人可通过验证下面的等式来验证边 (i, j) 的签名

$$v_i = v_j g^{\alpha_{ij}} h^{\beta_{ij}} \pmod p$$

(5) 合成边签名(Composing edge signatures)　给定边 (i, j) 的签名 $(i, j, \alpha_{ij}, \beta_{ij})$ 和边 (j, k) 的签名 $(j, k, \alpha_{jk}, \beta_{jk})$, 任何人可计算边 (i, k) 的签名 $(i, k, \alpha_{ik}, \beta_{ik})$, 其中:

$$\alpha_{ik} = \alpha_{ij} + \alpha_{jk} \pmod q,\ \beta_{ik} = \beta_{ij} + \beta_{jk} \pmod q$$

注意到在等价关系(无向图)中边是对称的, 即边 (i, j) 和边 (j, i) 视为同一条边(它们的签名是等价的), 我们可以给出 MR02 方案中传递运算和合成运算更准确更详细的定义:

$$® (i, j) \oplus (k, l) = \begin{cases} (i, l), & j = k \\ (k, j), & i = l \\ (l, j), & i = k \\ (i, k), & j = l \\ \text{False}, & \text{Otherwise} \end{cases}$$

® $\sigma_{ij} \otimes \sigma_{kl} = \sigma_{xy} = (x, y, \alpha_{xy}, \beta_{xy})$, 其中

$$(x, y) = (i, j) \oplus (k, l)$$

$$\alpha_{xy} = \begin{cases} \alpha_{ij} + \alpha_{kl}, & j = k \vee i = 1 \\ \alpha_{ij} - \alpha_{kl}, & i = k \vee j = l \\ \text{False}, & \text{Otherwise} \end{cases} \pmod q$$

$$\beta_{xy} = \begin{cases} \beta_{ij} + \beta_{kl}, & j = k \vee i = l \\ \beta_{ij} - \beta_{kl}, & i = k \vee j = l \\ \text{False}, & \text{Otherwise} \end{cases} \pmod q$$

Micali 和 Rivest 在文[1]也给出了 MR02 方案的安全性证明, 他们证明了如下定理:

定理 1　MR02 方案在选择明文攻击下是安全的.

4　有向传递签名方案

本节我们先提出一个适用于明文空间为全序关系的有向传递签名方案, 简称为全序有向传递签名方案, 并证明它在选择明文攻击下是安全的, 然后将该方案与 MR02 方案结合, 提出一个适用于对任意有向图的进行签名的解决方案.

4.1　全序有向传递签名方案

本小节我们提出一个适用于明文空间为全序关系的有向传递签名方案, 它是 MR02 方案的改进方案, 下面我们按本文的传递签名的定义形式给出其详细描述:

设 p, q 为满足 $q \mid (p-1)$ 的大素数, g 和 h 都是 Z_p^* 的 q 阶子群 G_q 的生成元, 并使得求 h 关于基 g 的离散对数是不可行的.

假设 M 是集合 A 上的一个全序关系, 则 A 中的元素在 M 下是可排序的, 因此可为 A 中的每个元素赋予一个小于 $q/2$ 的随机权值 w, 并使得 $\forall (u, v) \in M$ 都有 $w_v < w_u$.

我们仍然需要一个可抗选择明文攻击的标准签名方案, 其明文空间为 $A \times Z_p$, 其签名空间为 B, 其密钥生成算法为 KG, 其签名算法为 Sig, 其验证算法为 Ver, 其安全参数为 k.

本方案的私钥空间 K_S 和公钥空间 K_P 就是所用标准签名方案的相应私钥空间和公钥空间, 明文空间 M 是集合 A 上的一个全序关系, 签名空间 $S = B \times B \times Z_q \times Z_q$,

® **TKG**: $\{0, 1\}^k \to K_S \times K_P$ 为所用标准签名方案的密钥生成算法 KG, 输入 1^k, 输出密钥对 (k_s, k_p), 其中 k_s 为私钥, k_p 为对应的公钥, 公布 k_p.

® **TSig**: 随机选取 $y \in Z_q$, 设$(u, v) \in M$ 为待签消息, Alice 随机选取 $x_u, x_v \in Z_q$, 并计算

$$V_u = g^{x_u} h^{y+w_u} (\mathrm{mod}\ p),\ V_v = g^{x_v} y^{y+w_v} (\mathrm{mod}\ p)$$

用标准签名算法对 V_u 和 V_v 签名得:

$$\sigma_u = \mathrm{Sig}(k_s, (u, V_u)),\ \sigma_v = \mathrm{Sig}(k_s, (v, V_v))$$

(若 u 或v 曾在已被签名的消息中出现过, 则不再重新计算相应的部分).

计算$\alpha_{uv} = x_u - x_v (\mathrm{mod}\ q)$, $\beta_{uv} = w_u - w_v (\mathrm{mod}\ q)$

得到(u, v) 的签名 $\sigma_{uv} = \mathrm{TSig}(k_s, (u, v)) = (\sigma_u, \sigma_v, \alpha_{uv}, \beta_{uv})$

® **TVer**

$\mathrm{TVer}(k_p, (u, v), \sigma_{uv}) = 1 \Leftrightarrow$

$\mathrm{Ver}(k_p, (u, V_u), \sigma_u) = 1 \wedge (\mathrm{Ver}(k_p, (v, V_v), \sigma_v) = 1$

$\wedge V_u = V_v g^{\alpha_{uv}} h^{\beta_{uv}} (\mathrm{mod}\ p) \wedge \beta_{uv} \in (0, q/2)$

® Θ为 M 上的传递运算, 对于$\forall (u, v), (s, t) \in M$,

$$(u, v) \Theta (x, t) = \begin{cases} (u, t), & v = s \\ (s, v), & u = t \\ (v, t), & u = s,\ w_v > w_t \\ (t, v), & u = s,\ w_t > w_v \\ (u, s), & v = t,\ w_u > w_s \\ (s, u), & v = t,\ w_s > w_u \\ \mathrm{False}, & \mathrm{Otherwise} \end{cases}$$

® $\odot$为合成运算, 对于$\forall \sigma_{uv}, \sigma_{st} \in S$, $\sigma_{uv} \odot \sigma_{st} = \sigma_{xy} = (\sigma_x, \sigma_y, \alpha_{xy}, \beta_{xy})$, 其中

$$(\sigma_x, \sigma_y) = \begin{cases} (\sigma_u, \sigma_t), & v = s \\ (\sigma_s, \sigma_v), & u = t \\ (\sigma_v, \sigma_t), & u = s,\ \beta_{st} > \beta_{uv} \\ (\sigma_t, \sigma_v), & u = s,\ \beta_{uv} > \beta_{st} \\ (\sigma_u, \sigma_s), & v = t,\ \beta_{uv} > \beta_{st} \\ (\sigma_s, \sigma_u), & v = t,\ \beta_{st} > \beta_{uv} \\ \mathrm{False}, & \mathrm{Otherwise} \end{cases}$$

$$\alpha_{xy} = \begin{cases} \alpha_{uv} + \alpha_{st}, & v = s \vee u = t \\ \alpha_{uv} - \alpha_{st}, & u = s \vee v = t,\ \beta_{uv} > \beta_{st} \\ \alpha_{st} - \alpha_{uv}, & u = s \vee v = t,\ \beta_{st} > \beta_{uv} \\ \mathrm{False}, & \mathrm{Otherwise} \end{cases} (\mathrm{mod}\ q)$$

$$\beta_{xy} = \begin{cases} \beta_{uv} + \beta_{st}, & v = s \vee u = t \\ \beta_{uv} - \beta_{st}, & u = s \vee v = t,\ \beta_{uv} > \beta_{st} \\ \beta_{st} - \beta_{uv}, & u = s \vee v = t,\ \beta_{st} > \beta_{uv} \\ \mathrm{False}, & \mathrm{Otherwise} \end{cases} (\mathrm{mod}\ q)$$

下面是本方案的安全性证明.

定理 2 上述有向传递签名方案在选择明文攻击下是安全的.

证明 首先, 本方案与 MR02 方案一样都选用了一个可抗选择明文攻击的标准签名方案, 在这一部分的安全性上两个方案是一样的; 其次, 在本方案中结点值 V_u 的形式为 $V_u = g^{x_u} h^{y+w_u}$, 其中 y, x_u 和w_u 都是随机选取的, 在 MR02 方案中结点值 v_n 的形式为$v_n = g^{x_n} h^{y_n}$, 它可改写为 $v_n = g^{x_n} h^{y_1 + \beta_{1n}}$, 这里的 y_1, x_n 和β_{1n}也都是随机选取的, 两者是一致的, 因此两个方案的边签名具有相同的随机性, 它们在签名空间中都是随机分布的; 再次, 比较两个方案的传递运算和合成运算可知, 在不考虑方向时, 对于相同的明文子集两个方案所得的张成集是相同的, 因此本方案在不考虑明文(u, v) 的方向时与MR02 方案是一样的, 它们的安全性相同.

唯一留待证明的是: 对于任何敌手来说, 要从(u, v) 的签名$(\sigma_u, \sigma_v, \alpha_{uv}, \beta_{uv})$ 伪造出其逆(v, u) 的签名$(\sigma_v, \sigma_u, \alpha_{vu}, \beta_{vu})$ 是不可行的. 要是他伪造出签名$(\sigma_v, \sigma_u, \alpha_{vu}, \beta_{vu})$, 那么: (1) 如果 $\alpha_{vu} = \alpha_{uv}^{-1}$, $\beta_{vu} = \beta_{uv}^{-1}$, 则由 $\beta_{uv} < q/2$, 有 $\beta_{vu} = \beta_{uv}^{-1} = q - \beta_{uv} > q/2$, 这个签名是无效的; (2) 如果 $\alpha_{vu} \neq \alpha_{uv}^{-1}$或$\beta_{vu} \neq \beta_{uv}^{-1}$, 那么他就可得到 $g^{\alpha_{vu} - \alpha_{uv}^{-1}} h^{\beta_{vu} - \beta_{uv}^{-1}} = 1$, 从而可计算出 $\log_g h = -(\alpha_{vu} - \alpha_{uv}^{-1})(\beta_{vu} - \beta_{uv}^{-1})^{-1}$, 这与不可能计算 h 关于g 的离散对数的假设矛盾.

由定理 1 和上述讨论可知: 本方案在选择明文攻击下是安全的. 证毕.

注: (1) 在传递关系中从(u, v) 和(v, w) 传递得到(u, w) 是很自然的, 但全序关系有其自身的特点, 比如, 如果(u, v) 和(u, w) 都在全序关系 M 中, 那么就一定有且只有(v, w), (w, v) 两者中的一个也在 M 中. 对于(u, v) 和(w, v) 也类似. 本方案中所定义的传递运算将后两种情况也包含进去, 正是全序关系的特点所决定的.

(2) 本方案要求明文空间是全序关系, 并不要求所签的消息全体也构成全序关系, 因此可对若干个子全序关系的并(这是一种特殊的偏序关系) 进行签名, 而且这些子关系都可动态增长, 还可动态地将两个子关系连接起来.

4.2 一般偏序关系的签名方案

上一小节所提出的有向签名方案不适用于对一般的偏序关系进行签名, 但它与 MR02 方案结合可提供偏序关系签名的解决方案, 这个解决方案对于较简单的偏序关系来说还是比较有效的. 其主要思路是将偏序关系拆分成全序关系的并, 这些全序关系是有公共结点的, 将这些公共结点用等价关系表示, 这样一来就可用上小节的方案对全序关系之并签名, 用 MR02 方案对等价关系签名, 然后就可用签名组来表示某个所需的签名了. 这里给出一个说明性的例子: 假设待签偏序关系的哈斯图①如图 1-a, 那么我们可将该偏序关系折分成 5 个全序关系的并(图 1-b), 其中偏序关系中的两交叉点 v_1 和 v_2 分别用两组各 3 个等价的点$\{v_{11}, v_{12}, v_{13}\}$ 和$\{v_{23}, v_{24}, v_{25}\}$ 表示. 签名可这样进行: 用上小节方案对 5 个全序关系的并进行签名, 同时用 MR02 方案对等价关系$\{\{v_{11}, v_{12}, v_{13}\}, \{v_{23},$

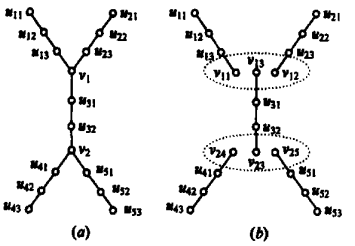


图 1 偏序关系及其拆分

① 哈斯图中结点位置的高低隐含着边的方向, 也就是说所有边都有从高指向低的方向, 但不画出来. 哈斯图本质上是个有向图, 参见[3].

v_{24}, v_{25}}} 签名, 这样偏序关系中的所有关系都可由一个签名组表示出来, 如可用$(\sigma_{u_{11}v_{11}}, \sigma_{v_{11}v_{13}}, \sigma_{v_{13}u_{32}})$作为对$(u_{11}, u_{32})$的签名.

偏序关系是反对称的, 所以对应的图不会出现有向圈, 如果考虑最一般的有向图, 则同一有向圈上的结点都是等价的, 它们构成一个等价点集, 使用本方案也没有问题.

这个解决方案虽然对于复杂的偏序关系(有向图)来说效率不是太高, 但也比对每个关系都单独签名要高效得多, 而且, 这个解决方案所得的签名对关系链的中间细节的泄露也是很少的, 总之, 这个解决方案对于解决提出传递签名时所要解决的两个问题都是较有成效的, 从理论上说它可对任何偏序关系进行签名, 就实际意义来说它可作为较简单偏序关系的有向传递签名方案.

5 结论

传递签名是近年来提出的用于对传递二元关系进行签名的签名方案, 已有的为数不多的传递签名方案都是无向传递签名方案, 而寻找有向传递签名方案是个留待解决的公开问题. 本文研究了有向传递签名, 提出一个适用于明文空间为全序关系的高效安全的有向签名方案, 并将之与 MR02 方案结合, 提出一个在理论上可对任意有向传递图进行签名的解决方案, 该解决方案对于较简单的有向图是实际可行的, 继续寻求对任意有向传递图实际可行的高效安全的有向传递签名方案是进一步工作的可能方向.

参考文献:

[1] Micali S, Rivest R. Transitive signature schemes[A]. Topics in Cryptology-CT-RSA'02[C]. LNCS 2271, Berlin: Springer-Verlag, 2002. 236-243.

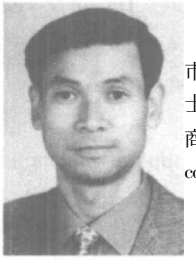
[2] Aho A V, et al. The transitive reduction of a directed graph[J]. SIAM J. Comput, 1972, 1: 131-137.

[3] 黄振杰, 离散数学[M]. 厦门: 厦门大学出版社, 2000. 8.

[4] Bellare M, Neven G. Transitive signature schemes based on factoring and RSA[A]. Advances in Cryptology-ASIACRYPT'02[C]. LNCS 2501, Berlin: Springer-Verlag, 2002. 397-414.

[5] Johnson R, et al. Homomorphic signature schemes[A]. Topics in Cryptology-CT-RSA'02[C]. LNCS 2271, Berlin: Springer-Verlag, 2002. 244-262.

作者简介:



黄振杰　男, 1964 年 11 月出生于福建龙海市, 现为上海交通大学计算机科学与工程系, 博士后, 漳州师范学院教授, 主要研究兴趣是电子商务安全和网络安全. E-mail: zhj-huang@163.com.

郝艳华　女, 1976 年 4 月出生于河南新乡市, 现为西安电子科技大学博士研究生, 主要研究兴趣是(超)椭圆曲线密码体制与电子商务安全.