可传递签名研究综述*)

张国印　王玲玲　马春光
（哈尔滨工程大学计算机科学与技术学院　哈尔滨 150001）

摘　要　可传递签名是由 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。本文综述了可传递签名的研究现状，描述了可传递签名的定义、模型及其安全性，概括了现有的可传递签名方案，包括无向传递签名方案和有向传递签名方案。最后对可传递签名的研究前景进行了展望。

关键词　密码学，数字签名，可传递签名，无向传递签名，有向传递签名

Survey on Transitive Signature Schemes

ZHANG Guo-Yin　WANG Ling-Ling　MA Chun-Guang
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)

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. In this paper, research actuality of transitive signatures is presented. The definition, the security and a model of transitive signatures are described. Two classes of transitive signature schemes, which are undirected transitive signature schemes and directed transitive signature schemes, are also described in details. Finally, some related problems about transitive signatures are summarized.

Keywords　Cryptography, Digital signatures, Transitive signatures, Undirected transitive signatures, Directed transitive signatures

1　引言

数字签名技术正以惊人的速度发展，它已成为人们在电子交易过程中必不可缺的一部分。应用于不同领域的签名方案也层出不穷。然而，一般的签名方案对于某些特殊的情况，其效率不尽人意。例如，在军事指挥系统中，当上级 A 向下级 B 下达命令时，为了保证命令的合法性，上级 A 必须向下级 B 证明它有权向其下达命令，即要求 A 提供一个权威 T 的签名(比如说是司令部的签名)，用来证明“A 是 B 的上级”。对于这个问题有两种做法：一种是由 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，这可能会增加许多签名。对于一个动态增长的群体来说，这样做的效率太低。另一种做法就是使用命令链。军长 A 与连长 B 中间还有师长 C、团长 D、营长 E、当 A 要向 B 下达命令时，他向 B 提供这样一个签名链：“A 是 C 的上级”、“C 是 D 的上级”、“D 是 E 的上级”、“E 是 B 的上级”。用这样的方式可以减少签名量，但又会带来另一个问题，这就是命令链会泄露一些不必要的细节，比如会泄露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似的还有 PKI 中的证书链，电子政务中也有类似的情形。因此，构造高效安全的特殊签名方案就成了所关注的问题。

可传递签名的概念最早是 2000 年由 Rivest 在他的一次报告[1]中提出的。在该观点提出两年后，许多学者应用这一观点构造了许多具体签名方案，如同态签名方案[2]、内容压缩签名方案[3]、可编辑签名[2]和前缀操作签名[4]等。2002 年，Micali 和 Rivest[5]正式提出了可传递签名的概念。他们在提出概念的同时，也给出了第一个可传递签名方案：MRTS 方案。稍后，在同一年，Bellare 和 Neven[6]在 ASIACYPT'02 上提出了“结点签名范例”的概念，这对于构造大部分传递签名方案是很有用的。Bellare 和 Neven 也给出了基于素数因子分解和 RSA 的传递签名方案：FBTS 方案和 RSATS 方案。

2003 年，Hohenberger[7]提出了设计和分析可传递签名方案的一般框架，同时指出构造有向传递签名方案存在困难的一些原因。同年，Kuwakado[8]首次提出了一个针对于有向树的有向传递签名方案：DTS-HK 方案。同时，Kuwakado 还指出可以通过失败-停止签名方案[9]来构造无向传递签名方案。

2004 年，Zhou[10]针对“结点签名范例”中标准签名方案的选择问题，提出了一种选择标准签名方案的原则。同年，Zhu[11]指出了“结点签名范例”对于构造有向传递签名方案的局限性，提出了不同于“结点签名范例”的构造可传递签名方案的新模型。

2005 年，Shahandashti, Salmasizadeh 和 Mohajeri[12]构造了一个基于双线性对偶的、高效简洁的传递签名方案：BGPTS 方案，并且指出该方案在 CDH 假设下是安全的。然而，在该方案提出不久，Bellare 和 Neven 在文[13]中指出了 BGPTS 方案的安全漏洞，并且证明了只有在 one-more CDH 假设下 BGPTS 方案才是安全的。Bellare 和 Neven 除做了以上工作之外，他们对 2002 年提出的各方案[6]给出了更加详细的

*)黑龙江省自然科学基金(F2004-06)；哈尔滨工程大学基础研究基金(HEUFT05067)。张国印　CCF 会员，教授，博士生导师，主要研究方向：信息安全、嵌入式系统；王玲玲　博士研究生，主要研究方向：密码学、信息安全；马春光　副教授，主要研究方向：密码学、网络与信息安全。

安全性证明，同时给出了 MRTS 的改进方案(DLTS-1M 方案)和基于 Gap Diffie Hellman 问题的两个新方案：GapTS-1 和 GapTS-2 方案。这些方案的提出极大丰富了无向传递签名方案的内容。同年，针对有向传递签名方案这个公开问题，黄振杰[14]提出了一个高效的全序有向传递签名方案：DTS-H 方案。他又将 DTS-H 方案与 MRTS 方案结合，提出了一个可对任何有向二元关系进行签名的方案：DTS-G 方案。遗憾的是，DTS-G 方案对于复杂的偏序关系(有向图)来说效率不是太高。因此针对有向传递签名方案这一方面的工作还有待进一步地展开。

2006 年，马春光在文[15]中，通过对 FBTS-1 方案和 RSATS-1 方案进行改进，提出了两种无状态无向传递签名方案：TS-FB 方案和 TS-RSA 方案。

从传递签名发展的整个过程来看，它的发展经历了 3 个阶段。

初期阶段：以 Rivest 提出可传递签名的观点为标志，这一阶段的工作主要是参考 Rivest 观点，提出具体的签名方案；

发展阶段：以 Micali 和 Rivest 正式提出可传递签名的概念为标志，这一时期涌现了很多新思想、新模型和新方案，是可传递签名发展的关键时期；

完善阶段：以 2005 年 Bellare 和 Neven 的文[13]的发表为代表，开始了可传递签名的完善时期。

本文第 2 节首先介绍了可传递签名方案的相关概念。其次，在综合分析了已搜集到的所有文献后，把现有的一些典型方案归纳为两类，即无向传递签名方案(第 3 节)和有向传递签名方案(第 4 节)。在每一类中，又将其细分为有状态方案和无状态方案。第 5 节提出了值得进一步研究的问题。

2 相关概念

2.1 图与可传递闭包图

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。一个图 $G=(V,E)$是由一个有限结点集 V 和一个有限边集 $E\subset V\times V$ 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；如果关系是非对称的，则需用有向边表示。若不考虑无向图还是有向图，都用有序对(u,v)来表示从结点 u 到 v 的边的话，那么对于无向图，存在边(u,v)，就一定存在边(v,u)。但在有向图中，存在(u,v)则不一定存在有向边(v,u)。对于那些具有传递性的图，才能考虑传递签名。一个图称为可传递的，如果它有一条从 u 到 v 的路，就一定有一条从 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$(u,v)\in E^*$ 当且仅当图中有一条从 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[16]。

2.2 可传递签名的相关定义

可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。下面给出可传递签名的一般性定义。

定义 1 一个可传递签名方案一般是由 4 个集合(K_S,K_P,M,S)和 4 个算法(TKG,TSig,TVer,Comp)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的二元关系)，S 是签名空间。4 个算法定义如下：

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(tpk,tsk)，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 tsk 和待签消息 m，输出签名 σ_m。

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 tpk 和被签消息 m 及签名 σ，当 σ 为 m 的有效签字时输出 1，否则输出 0。

Comp：$K_P\times M\times S\to\{S,\perp\}$是签名的合成算法，它是确定性的，输入公钥 tpk 和被签消息 m_1、m_2 及签名 σ_1、σ_2。当 σ_1、σ_2 是有效签名，则输出经过合成运算得到的签名 σ，否则输出$\perp$。

对于可传递签名方案，可以通过一个正确性判别试验来判断该签名方案的正确性。该实验[6]引入了两个布尔变量 *Legit* 和 *NotOK*，如果算法 A 进行了不合法的(如：算法 A 询问同一结点的边签名，或者算法 A 对不具有传递关系的两条边签名，等等)询问，则置 *Legit* 的值为 false；对于同一条边，如果用合成算法计算的签名值与用签名私钥直接签署的签名值不一致，则置 *NotOK* 的值为 true。试验最后的输出值为 $Legit\wedge NotOK$。只有当算法 A 进行了合法的询问，并且对同一条边的两个签名值不一致时，试验才返回“true”。下面是传递签名的正确性定义。

定义 2 一个传递签名是正确的，如果对于任意算法 A 和安全参数 k，正确性判别试验的输出结果是“true”的概率可以忽略的。

由于具有传递性，可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不可能产生新的有效签名。这样的安全性要求显然与传递签名的初衷相违背。传递签名方案提供了合成算法，使得任何人都可以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署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。

定义 3 一个可传递签名方案称为在选择明文攻击[17]下是安全的，如果在允许敌手任意选择明文请求的条件下，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[14]的有效签名的概率是可以忽略的，即任何敌手 A 的攻击优势(advantage)Adv A 是可以忽略的，这里

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

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。

2.3 可传递签名的性质及优点

通过分析可传递签名的正确性和安全性的定义，可以将可传递签名的几个重要性质总结如下[14]：(1)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。(2)可传递性。已知 m 和 n 的签名 σ_m 和 σ_n，则任何人无需知道私钥就可以产生签名 σ_x，使得 $\mathrm{TVer}(tpk,x,\sigma_x)=1$。(3)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。

可传递签名有以下几个主要优点：(1)使所需签名量达到最小；(2)隐藏关系链的中间细节；(3)特别适合动态增长的关

系图进行签名，每增加一个结点，只需要增加在传递简约中与其关联的边的签名，其它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。

3 无向传递签名方案

3.1 无向有状态传递签名方案

Bellare 和 Neven[6] 首次提出了“结点签名范例”的概念，这对于构造有状态的传递签名方案是很有用的。“结点签名范例”的具体内容是：签名人的密钥包含标准签名方案中的密钥。公钥除了有标准方案产生的公钥外，还包含一些额外的元素，如在 MRTS 方案中，公钥就包含 q 阶群 G_q 和群 G_q 的两个生成元。结点签名由公共标签 $L(i)$ 和用 SDS 对 $i \| L(i)$ 签署后的签名组成。边签名包含相关的两结点签名和该边的标签 δ。验证一条边的签名就是要对两个结点的公共标签进行计算，并且要验证用 SDS 所签的两个结点的签名值是否正确。签名合成就是对两个边签名进行代数运算，产生新的边签名。在该范例中，需要借助于标准签名方案来对结点进行签名。标准签名方案的种类有很多，在文[5,6,13]中所选择的标准签名方案都是可以抵抗自适应选择明文攻击的。在文[10]中，Zhou Sujing 为了提高方案的性能，提出了一种选择标准签名方案的新原则：只要能够保证，用该标准签名方案构造出来的可传递签名方案能够达到所要求的安全性，就可以选择它。这里，统一将标准签名方案表示为 SDS。它由三个算法组成：密钥生成算法 SKG、标准签名算法 SSign 和标准验证算法 SVf。

3.1.1 MRTS(DLTS)方案与 DLTS-1M 方案

Micali 和 Rivest 在文[5]中提出的 MRTS(DLTS)方案，为解决高效安全的数字签名问题迈出了巨大的一步，是数字签名领域的一个里程碑。MRTS(DLTS)方案是在求解离散对数问题困难性的安全性假设上提出的。方案的描述方式与本文给出的定义不尽相同，由五个步骤组成：用户设置、建立新结点、边签名、边签名验证以及合成边签名。其中点签名和边签名是分开的。Micali 和 Rivest[5] 在标准模型中证明了 MRTS(DLTS)方案的正确性和安全性。

为了对边进行签名，MRTS 方案使用了群 G_q 的两个生成元。Bellare 和 Neven 借鉴了 Schnorr[18] 的身份识别方案，提出了一个更简单的，仅需要使用一个生成元的 DLTS-1M 方案。该方案比 MRTS 方案的性能更好，减小了签名的大小和合成运算的时间。但是该方案需要更强的安全性假设，它是基于 one-more DLP 问题[19] 的。同样，DLTS-1M 方案满足定义 2，并且 Bellare 和 Neven 给出了该方案在标准模型中详尽的安全性证明。

3.1.2 RSATS-1 方案

RSATS-1 方案最早是由 Micali 和 Rivest[5] 提出的，但是文[5]并没有提供完整的方案，也没有给出该方案的安全性证明。Bellare 和 Neven 总结了 Micali 和 Rivest 的工作，并在文[6,13]中给出了 RSATS-1 方案的完全实现，还证明了该方案在标准 RSA 签名方案的安全性假设和 RSA 可以抵抗 one-more-inversion 攻击[19] 的假设下是可以抵抗自适应选择明文攻击的。

RSATS-1 方案使用了结点签名范例。同时引入了 RSA 密钥生成器 K_{rsa} 和 SDS。方案首先运行 SKG 生成密钥对 (spk, ssk)，通过 K_{rsa} 得到三元组 (N, e, d)；公钥为 (N, e, spk)，私钥为 (N, e, ssk)。其次，签名算法保存了所有被询问到的结点状态 $(V, \ell, L, \sum)$，其中结点集 $V \subseteq N$，$\ell: V \to Z_N^*$，是结点 $i \in V$ 的私有标签 $\ell(i)$ 的产生函数，$L: V \to Z_N^*$ 是公共标签 $L(i)$ 的产生函数，$\sum: V \to \{0,1\}^*$ 是准签名生成函数。当输入私钥 tsk 和结点 i, j 的信息时，表示要求产生边 (i, j) 的签名。具体执行步骤是：如果 $i > j$ 则交换 i, j。若 $i \notin V$，将 i 加入结点集 V 中，并对结点 i 进行签名，同时，$\ell(i) \xleftarrow{\$} Z_N^*$（表示从 Z_N^* 中随机选取一个值赋给 $\ell(i)$），$L(i) \leftarrow \ell(i)^e \bmod N$，$\sum(i) \leftarrow SSign(ssk, i \| L(i))$，则结点 i 的签名为 $C_i \leftarrow (i, L(i), \sum(i))$；同理，结点 j 的签名为 $C_j \leftarrow (j, L(j), \sum(i))$；边 (i, j) 的签名就是 $\sigma \leftarrow (C_i, C_j, \delta)$，其中 $\delta \leftarrow \ell(i)\ell(j)^{-1}$。验证签名时，当 $\delta^e \equiv L_i L_j^{-1} \bmod N$，并且结点签名也是正确的，则签名值是合法的。最后，通过 $\delta \leftarrow \delta_1 \delta_2 \bmod N$ 合成签名，这里要求 δ_1，δ_2 对应的边 (i, j)，(j, k) 的结点值满足 $i < j$，且 $j < k$。若不满足这样的大小关系，可通过交换结点，同时交换签名的方法达到此目的。

3.1.3 FactTS-1(FBTS-1)方案、FactTS-2(FBTS-2)方案和 FactTS-Z 方案

Bellare 和 Neven[6] 提出的 FactTS-1 方案、FactTS-2 方案和 Zhou[10] 提出的 FactTS-Z 方案，其安全性假设都是基于大因数分解困难性的。同 RSATS-1 方案类似，FactTS-1(FBTS-1)方案引入了模数生成器 K_{fact} 和 SDS。方案的具体描述严格按照定义的形式。类似证明 RSATS-1 方案正确性的方法可以用来证明 FactTS-1 方案是满足正确性定义 2 的。

FactTS-2 方案与 FactTS-1 方案不同的是：FactTS-2 方案为了去掉结点签名过程，而不使用结点签名范例。为了保证该方案的安全性，签名算法保存了结点状态，因此 FactTS-2 方案仍属于有状态签名方案。但是该方案可以通过改进，成为安全的无状态方案。同时，FactTS-2 方案引入了 Blum 模数产生器 K_{BW}，其目的是为了保证私有标签是 Z_N^* 中的一个平方剩余。

通过计算可知，FactTS-2 方案比 FactTS-1 方案在性能上得到了很大的提高，特别是签名尺寸减小了很多。Bellare 和 Neven 在文[13]中给出了 FactTS-1 方案在标准模型中的安全性证明，而 FactTS-2 方案的安全性证明需要在随机预言模型[20,21] 中讨论。

Zhou 在文[10]中提出了选择标准签名方案的原则。该原则的提出，使得标准签名方案的可选范围大大增加了。FactTS-Z 方案使用了新的标准签名方案，记作 SDS'。Zhou 证明了他所选择的 SDS' 在非自适应选择明文攻击下是安全的。该方案是在修改了 FactTS-1 方案的基础上得到的。就计算代价而言，Zhou 给出的 SDS' 小于一些强安全性的方案，如：Cramer-Shoup 方案[22] 和 Fischlin 方案[23]。这就使得，在不影响传递签名方案总的安全性能的前提下，可以通过选择类似 SDS' 的标准签名方案来提高传递签名的总体性能。文[10]证明了 FactTS-Z 方案在标准模型中是安全的。

3.1.4 GapTS-1 方案

GapTS-1 方案是 Bellare 和 Neven 在文[13]中首次提出的。该方案是关于 Gap Diffie Hellman 问题的，其安全性假设是基于 one-more CDH 问题[24] 的。该方案的大致过程与 RSATS-1 方案类似，不同的是该方案使用了一个 gap DH 群指示器 (K_{cg}, S_{ddh})，这里 S_{ddh} 是指多项式时间 DDH 算法；运行循环群生成器 K_{cg} 得到三元组 $(\langle G \rangle, g, q)$，同时 $x \xleftarrow{\$} Z_q$，且

$X \leftarrow g^x$；公钥为$(\langle \hat{G} \rangle, g, q, X, spk)$，私钥为$(\langle \hat{G} \rangle, g, q, X, ssk)$。其次，签名算法保存的结点状态值有所变化，这里，$\ell, L: V \to G$；结点的私有标签和公共标签为：$\ell(i) \leftarrow X^{y_i}$，$L(i) \leftarrow g^{y_i}$，$y_i$是从$Z_q$中随机选取的值。边$(i,j)$的签名是：$\delta \leftarrow \ell(i)\ell(j)^{-1}$。再次，验证签名时，只需验证等式：$S_{dth}(\langle \hat{G} \rangle, g, q, X, L_i L_j^{-1}, \delta) = 1$。与 RSATS-1 方案不同，该方案中所有的运算不再是模 N 运算，而是在循环群 $\hat{G}$ 中进行的。Bellare 和 Neven 在文[13]中证明了该方案满足正确性定义，并且证明了该方案在标准模型中是安全的。

3.1.5 UTS-HZ 方案

UTS-HZ 方案是 Zhu[11] 在提出新的无向传递签名模型的基础上，给出的一个实例。新模型把签名算法细分为独立的两个算法，分别是结点签名算法和边签名算法，并且这两个算法共享状态信息。这种模型对于分析无向传递签名的安全性很方便，而且便于以后对有向传递签名的研究。

UTS-HZ 方案没有使用 SDS，而是选择了 Cramer-Shoup 陷门杂凑方案[22] 作为标准签名方案。UTS-HZ 方案满足正确性定义 2。文[11]对于 UTS-HZ 方案的安全性给出了两种假设性证明。Zhu 在标准模型中证明了：如果 one-more-RSA 逆问题是困难的，离散对数问题仍然难解，并且 H 是无碰撞的杂凑函数，则 UTS-HZ 方案可以抵抗自适应选择明文攻击。

3.1.6 BGPTS 方案

Shahandashti, Salmasizadeh 和 Mohajeri[12] 为了构造高效简洁的传递签名方案，提出了 BGPTS 方案。该方案与文[10]类似，通过选择安全性要求较松的(可以抵抗已知明文攻击)标准签名方案来达到减小计算代价的目的，并且利用 GDH 群中双线性映射[25] 的代数性质[26,27] 得到简短的签名，从这两方面入手优化了传递签名方案的性能。与 2.1 节传递签名的一般定义不同，该方案的定义综合了文[3]和[2]的定义方式。BGPTS 方案将签名算法和验证算法分成了点签名(验证)算法和边签名(验证)算法。签名算法仍需要保存询问过结点的状态。不同于 MRTS 等方案，该方案没有使用固定公式(在 MRTS 中为：$v_n = g^{x_n} h^{y_n} \bmod p$)来计算结点的公开值，而是让结点签名算法随机选择一个值作为该结点的公开值。这种改进使得该方案在不影响安全性的前提下，为产生简短的结点签名提供了前提。

文[12]指出，如果在双线性群对中 CDH 问题是困难的，且 *SDS* 可以抵抗已知明文攻击，则 BGPTS 方案在自适应选择明文攻击下是安全的。然而，Bellare 和 Neven 在文[13]中指出了 BGPTS 方案存在的安全漏洞，并且详细证明了只有在 one-more CDH 假设下 BGPTS 方案才可以抵抗自适应选择明文攻击。

3.2 无向无状态传递签名方案

无向无状态传递签名方案的主要思想是通过杂凑函数去掉结点签名而直接对边签名，或通过伪随机函数等方法根据签名需要，随时计算结点的状态，使得签名算法不需要保存结点的状态，从而减小签名大小、减少计算代价。

在这一类签名方案中往往不再使用“结点签名范例”。因为，如上文所描述，对一条边签名会要求两次标准签名的计算。边的签名包含两个结点的签名和一个标准签名，所以即使结点签名很小，但是整个边的签名可能会很长，这样就使得签名大小不断增大，而且也增加了计算代价。Bellare 和 Neven 在文[6]中首次提出通过杂凑函数去掉结点签名的想法。后来 Bellare 和 Neven 在文[6]的基础上，在文[13]中提出了对于大多数有状态传递签名方案有效的，将其转化为无状态方案的一般方法。

该方法的主要思想是：根据签名的需要，使用伪随机函数[28] 产生两个随机数 ω_i, ω_j，分别用于计算两个结点的状态信息，再将计算出的结点状态信息用于产生边的签名。这样就不用在签名算法中始终保存所有结点的状态信息了，而是在签名需要时，随时计算。这种方法的缺点在于：仍然需要计算结点签名，只是减小了存储代价，计算代价没有改变，相对于通过杂凑函数来达到无状态的方法，其性能还是后者好。考虑到，并不是所有的有状态方案都可以通过杂凑函数法来达到无状态，所以这种方法也是一种从有状态方案向无状态方案转化的有效方法。

3.2.1 RSATS-2 方案

RSATS-2 方案是对 RSATS-1 方案改进后得到的。RSATS-2 方案不再使用 *SDS*，与 RSATS-1 方案不同的是：首先，输出公钥为(N,e)，私钥为(N,d)。其次，签名算法不再需要保存状态信息，通过杂凑函数来取代公共标签，边的签名为：$\delta \leftarrow [H_N(i) H_N(j)^{-1}]^d \bmod N$，同样要求 $i<j$。再次，验证算法需验证等式：$\delta^e \equiv H_N(i) H_N(j)^{-1} \bmod N$。

RSATS-2 方案的安全性证明是基于随机预言模型的。方案中的每一个算法乃至敌手都可以随机访问杂凑函数 H_N。Bellare 和 Neven 在文[13]中给出了详细的证明过程。

3.2.2 GapTS-2 方案

因为 GapTS-1 方案会提供陷门信息，使得敌手可以通过陷门信息计算出私有标签，因此 GapTS-1 方案必须保存结点状态信息确保方案的安全性。Bellare 和 Neven 对 GapTS-1 方案进行了改进，通过用杂凑函数计算边签名，从而去掉结点签名过程的方法，提出了无状态 GapTS-2 方案[13]。经对比分析可知，该方案所产生的签名尺寸是 Bellare 和 Neven[13] 提出的所有方案中最小的。

与文[26]中提到的简短签名方案类似，在 GapTS-2 方案里，对边的签名只用到了循环群 $\hat{G}$ 的一个元素 x。如果使用椭圆曲线来构造群 $\hat{G}$ 的话，仅需要 160 位的密钥就能达到 RSA 用 1024 比特才能及的安全性能。

GapTS-2 方案满足正确性定义，同时 Bellare 和 Neven[13] 在随机预言模型中证明了该方案是安全性的。

3.2.3 TS-FB 方案和 TS-RSA 方案

马春光[15] 通过改进 FBTS-1 方案和 RSATS-1 方案，分别提出了两个无状态方案：TS-FB 方案和 TS-RSA 方案。它们都是通过使用伪随机函数产生随机值，来随时计算结点状态的方法，达到了不需要保存结点状态的目的。

文[15]没有详细证明方案的安全性，只给出了安全性定理：令 MG 是模数生成器，*SDS* 是标准数字签名算法，H 是加密杂凑函数，如果关于 MG 的因数分解问题(one-more-RSA 逆问题)是困难的，并且 *SDS* 在自适应选择明文攻击下是安全的，则在随机预言模型中，TS-FB 方案(TS-RSA 方案)在自适应选择明文攻击下是安全的。

4 有向传递签名方案

已提出的大部分传递签名方案都是基于与无向图对应的等价关系的。随着学者们的研究发现，构造针对于有向图的传递签名方案存在着一定的复杂性，从而引发了为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的各种不同努力，主要表现在：

(1) 提出针对于特殊有向图(如有向树)的有向传递签名方案，如 DTS-HK 方案、DTS-H 方案。

(2) 在针对特殊情况的有向传递签名方案的基础上，结合已有的无向传递签名方案，产生出理论上适合于一般有向图的传递签名方案，如 DTS-G 方案。

这些有向传递签名方案的签名算法都需要保存结点状态信息，因此属于有向有状态传递签名方案。

4.1 DTS-HK 方案

Kuwakado[8]针对于有向图的特例——有向树[8]，提出了第一个有向传递签名方案：DTS-HK 方案。该方案使用了模数算法和整数算法，有向边的方向由签名值的符号来表示。负值在该方案中是不合法的。DTS-HK 方案与 MRTS 方案类似，分别引入了结点签名算法和边签名算法。任何安全的 SDS 都可以用于结点签名，文[8]主要讨论了针对边签名算法的方案。因为有向树是有向图的一个特例，因此该方案的提出并没有完全解决公开问题。

Kuwakado 没有给出 DTS-HK 方案详细的安全证明过程，只是说明了在安全参数 t 足够大的情况下，可以忽略验证算法接受伪造签名的概率。然而，X Yi[29] 指出了 DTS-HK 方案在某些特殊情况下是可以被伪造签名的。

4.2 DTS-H 方案和 DTS-G 方案

DTS-H 方案是黄振杰[14]提出的适用于明文空间为全序关系的有向传递签名方案，它是 MRTS 方案的改进方案。该方案选择了 SDS，其私钥空间 K_S 和公钥空间 K_P 就是 SDS 相应的私钥空间和公钥空间，并有以下两条假设：

(1)设 p,q 为满足 $q|(p-1)$ 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 h 关于基 g 的离散对数是不可行的。

(2)假设 M 是集合上 A 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 $w_v<w_u$。

DTS-H 方案的签名算法保存了结点状态信息，对于边 $(u,v)\in M$，如果结点 u、v 未在已被签名的消息中出现过，则随机选取 $y,x_u,x_v\in Z_q$，并计算：$V_u=g^{x_u}h^{y+w_u}\pmod p$，$V_v=g^{x_v}h^{y+w_v}\pmod p$，用 SDS 对 V_u，V_v 签名，得：$\sigma_u=SSign(k_s,(u,V_u))$，$\sigma_v=SSign(k_s,(v,V_v))$；计算 $\alpha_{uv}=x_u-x_v\pmod q$，$\beta_{uv}=w_u-w_v\pmod q$；最后可得边 (u,v) 的签名 $\sigma_{uv}=TSig(k_s,(u,v))=(\sigma_u,\sigma_v,\alpha_{uv},\beta_{uv})$。验证签名时，需要验证等式 $TVf(tpk,(u,v),\sigma_{uv})=1$ 是否成立。此时需分别验证：$SVf(tpk,(u,V_u),\sigma_u)=1$；$SVf(tpk,(v,V_v),\sigma_v)=1$；$V_u=V_vg^{\alpha_{uv}}h^{\beta_{uv}}\pmod p$；$\beta_{uv}\in(0,q/2)$。对于有传递关系的有向边可以进行合成签名运算。根据全序关系的特点(如：反对称性)，对于 $\forall(u,v),(s,t)\in M$，可以通过比较各结点的权值 w 来决定所合成的边签名的值。

黄振杰[14]证明了 DTS-H 方案在选择明文攻击下是安全的。

DTS-G 方案是将 DTS-H 方案和 MRTS 方案结合来提供偏序关系签名的一种解决方案。其主要是将偏序关系拆分成全序关系的并，这些全序关系的公共结点用等价关系表示。这样一来就可以用 DTS-H 方案对全序关系之并签名，用 MRTS 方案对等价关系签名，然后用签名组来表示所需的某个签名了。

偏序关系是反对称的，所对应的图不会出现有向圈。如果考虑最一般的有向图，对于同一有向圈上的结点，可视为一个等价点集，也可以使用 DTS-G 方案。但是 DTS-G 方案对于复杂的偏序关系效率不高，因此提出一个高效的适用于任意有向图的传递签名方案仍是一个需要深入研究的公开问题。

5 值得研究的问题

可传递签名是一种安全高效的签名机制。现在，许多学者都在发展和完善可传递签名机制，但是可传递签名仍然没有完全成熟和广为应用，而且还有很多问题有待解决。

(1) 提出有向传递签名方案。寻找构造有向传递签名方案可以依据的现实可行的数学难题；在现有少量针对特殊情况的有向传递签名方案的基础上，提出更多实际有效的适用于一般有向图的传递签名方案；研究多个方案的具体构造过程；提出构造针对所有有向图的传递签名方案的模型。

(2) 改进和优化现有方案。在保证安全性的前提下简化传递签名方案，特别是签名算法，使其计算代价和存贮代价越小越好；研究更多的方法，简化有状态传递签名方案的整体过程，或构造更多安全高效的无状态传递签名方案；在保证传递签名方案安全的前提下，扩大标准签名方案的选择范围，使得可依据用户的具体情况选择标准签名方案，这是构造高效方案的重要环节。

(3) 提高方案的可证安全性。提出新方法，使得方案不仅在随机预言模型中是可证安全的，而在现实标准模型中也可以讨论其安全性；提出更加简洁、易懂的用于证明传递签名方案安全性的形式化方法。

(4) 可传递签名方案的应用。可传递签名是应一些实际问题的要求而提出的特种签名机制，其在电子商务(如：电子现金[30]，电子支票系统[31])、电子政务和网络安全等方面有着积极的应用。

(5) 更安全高效的、基于新的数学难题的可传递签名方案的研究。解决数学难题的不可行性是构造安全有效的可传递签名方案的理论依据，寻找更多的可用于构造传递签名方案的数学难题，并交叉使用多个数学难题来构造可传递签名方案；根据用户要构造的可传递签名方案的不同目的，高效性有时候比不必要的强安全性更重要，而有时高效性会与安全性发生冲突，此时就需要研究高效安全的折中方案。

参 考 文 献

1 Rivest R. Two signature schemes. Slides from talk given at Cambridge University, October 17, 2000. Available from http://theory.lcs.mit.edu/~rivest/publications.html, 2000

2 Johnson R, et al. Homomorphic signature schemes. In: Preneel B, edi. Topics in Cryptology - CT-RSA 2002. Berlin: Springer-Verlag, 2002. LNCS 2271, 244~262

3 Steinfeld R, Bull L, Zheng Y L. Content extraction signatures. In: Kwangjo Kim, ed. Information Security and Cryptology - ICISC 2001. Berling: Springer-Verlag, 2002. LNCS 2288, 285~304

4 Chari S, Rabin T, Rivest R. An efficient signature scheme for route aggregation. Manuscript, Available at: http://theory.lcs.mit.edu/~rivest/publications.html, 2002

5 Micali S, Rivest R. Transitive signature schemes. In: Preneel B, ed. Topics in Cryptology - CT-RSA 2002. Berlin: Springer-Verlag, 2002. LNCS 2271, 236~243

6 Bellare M, Neven G. Transitive signatures based on factoring and RSA. In: Zheng Y. editor. Advances in Cryptology - ASIACRYPT 2002. Berlin: Springer-Verlag, 2002. LNCS 2501, 397~414

7 Hohenberger S. The cryptographic impact of groups with infeasi-

ble inversion: [Master's thesis]. Massachusetts Institute of Technology, available from http://theory.lcs.mit.edu/~cis/cis-theses.html, 2003
8 Kuwakado H, Tanaka H. Transitive signature scheme for directed trees. IEICE TransFundamental, 2003, E86-A(5): 1120~1126
9 Van Heijst E, Pedersen T P, Pfitzmann B. New constructions of fail-stop signatures and lower bounds. In: Crypto'92. Berlin: Springer-Verlag, 1993, LNCS 740: 15~30
10 Zhou S J. Transitive Signatures Based on Non-adaptive Standard Signatures. Cryptography ePrint Archive. Report 2004/044/
11 Zhu H. Model for undirected transitive signatures. IEE Proceedings Communications, 2004, 151(4): 312~315
12 Shahandashti S F, Salmasizadeh M, Mohajeri J. A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs. In: SCN 2004. Berling: Springer-Verlag, 2005, LNCS 3352: 60~76
13 Bellare M, Neven G. Transitive signatures: New Schemes and Proofs. IEEE Transactions on Information Theory, 2005, 51(6): 2133~2151
14 黄振杰，郝艳华. 一个高效的有向传递签名方案. 电子学报, 2005, 33(8): 1497~1501
15 Ma C G, Wu P, Gu G C. A New Method for the Design of Stateless Transitive Signature Schemes. In: APWeb Workshops 2006. Berlin: Springer-Verlag, 2006, LNCS 3842: 897~904
16 Aho A V, Garey M R, Ullman J. The transitive reduction of a directed graph [J]. SIAM Journal of Computing, 1972, 1(2): 131~137
17 Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 1988, 17(2): 281~308
18 Schnorr C P. Efficient identification and signatures for smartcards. In: Brassard G. editor. Advances in Cryptology - CRYPTO 1989. Berlin: Springer-Verlag, 1990, LNCS 435: 239~252
19 Bellare M, Namprempre C, Pointcheval D, et al. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. Journal of Cryptology, 2003, 16(3): 185~215
20 Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: ACM. editor. Proceedings of the First Conference on Computer and Communications Security. Fairfax, 1993. 62~73
21 Canetti R, Goldreich O, Halevi S. The Random Oracle Methodology, Revisited. Journal of the ACM, 2004, 51(4): 557~594
22 Cramer R, Shoup V, Signature schemes based on the strong RSA assumption. ACM Transactions on Information and System Security (ACM TISSEC), 2000, 3(3):161~185
23 Fischlin M. The Cramer-Shoup Strong-RSA signature scheme revisited. In: Public Key Cryptography - PKC'03. Berlin: Springer, 2003, LNCS 2567: 116~129
24 Boldyreva A. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie Hellman- group signature scheme. In: Desmedt Y. editor. Advances in Cryptology - Public-Key Cryptography 2003. Berlin: Springer-Verlag, 2003, LNCS 2567: 31~46
25 Boneh D, Franklin M. Identity Based Encryption from the Weil Pairing. SIAM Journal of Computing, 2001,32 (3) :586~615
26 Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Boyd C. editor. Advances in Cryptology - ASIACRYPT 2001. Berlin: Springer-Verlag, 2001, LNCS 2248: 514~532
27 Boneh D, Mironov I, Shoup V. A Secure Signature Scheme from Bilinear Maps. In: Proceedings of RSA-CT'03, Berlin: Springer-Verlag, 2003, LNCS 2612: 98~110
28 Goldreich O, Goldwasser S, Micali S. How to construct random functions. Journal of the ACM, 1986, 33(4): 792~807
29 Yi X, Tan C H, Okamoto E. Security of Kuwakado-Tanaka Transitive Signature Scheme for Directed Trees. IEICE Transactions on Fundamentals, 2004, E87-A(4): 955~957
30 马春光，杨义先. 可转移离线电子现金. 计算机学报, 2005, 28(3): 301~308
31 马春光，杨义先，胡正名，等. 可直接花费余额的电子支票系统. 电子学报, 2005, 33(9): 1562~1566

(上接第 5 页)

31 Giannella C, et al. Mining frequent patterns in data streams at multiple time granularities. In: Next Generation Data Mining, 2003. 191~212
32 Guha S, et al. Clustering Data Streams. In: Proc of the 41st Annual Symposium on Foundations of Computer Science, 2000. 359~366
33 Zhang T, Ramakrishnan R, Livny M. BIRCH: An Efficient Data Clustering Method for Very Large Databases. In: Proc of the 1996 ACM SIGMOD Intl Conf on Management of Data, 1996. 103~114
34 Park N H, Lee W S. Statistical Grid-Based Clustering over Data Streams. ACM SIGMOD Record, 2004, 33(1): 32~37
35 Lu Y, et al. A Grid-Based Clustering Algorithm for High-Dimensional Data Streams. In: Proc of the 1st Intl Conf on Advanced Data Mining and Applications (ADMA), 2005. 824~831
36 Wang Z, et al. Clustering Data Streams on the Two-Tier Structure. In: Advanced Web Technologies and Applications: 6th Asia-Pacific Web Conf (APWeb 2004), 2004. 416~425
37 Ordonez C. Clustering Binary Data Streams with K-Means. In: Proc of the 8th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, 2003. 12~19
38 Babcock B, et al. Maintaining Variance and k-Medians over Data Stream Windows. In: Proc of the twenty-second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, 2003. 234~243
39 Dong G, et al. Online Mining of Changes from Data Streams: Research Problems and Preliminary Results. Proc of the 2003 ACM SIGMOD Workshop on Management and Processing of Data Streams. 2003
40 Widmer G. Tracking Context Changes through Meta- Learning. Machine Learning, 1997, 27(3): 259~286
41 Widmer G, Kubat M. Learning in the Presence of Concept Drift and Hidden Contexts. Machine Learning, 1996, 23(1): 69~101
42 Bartlett P L, Ben-David S, Kulkarni S R. Learning Changing Concepts by Exploiting the Structure of Change. Machine Learning, 2000, 41(2): 153~174
43 Harries M, Horn K. Learning Stable Concepts in a Changing World. In: Selected Papers from the Workshop on Reasoning with Incomplete and Changing Information and on Inducing Complex Representations, 1996. 106~122
44 Gerencser L, Molnar-Saska G. Change detection of Hidden Markov Models. In: 43rd IEEE Conf on Decision and Control, 2004. 1754~1758
45 Keogh E, Kasetty S. On the Need for Time Series Data Mining Benchmarks: A Survey and Empirical Demonstration. Data Mining and Knowledge Discovery, 2003, 7(4): 349~371
46 Yamanishi K, Takeuchi J-I. A Unifying Framework for Detecting Outliers and Change Points from Non-Stationary Time Series Data. In: Proc of the 8th ACM SIGKDD Intl Conf on Knowledge Discovery and Data Mining, 2002. 676~681
47 Fan W. Systematic Data Selection to Mine Concept-Drifting Data Streams. In: Proc of the 10th ACM SIGKDD Intl Conf on Knowledge Discovery and Data Mining, 2004. 128~137
48 Aggarwal C C. A Framework for Diagnosing Changes in Evolving Data Streams. In: Proc of the 2003 ACM SIGMOD Intl Conf on Management of Data, 2003. 575~586
49 Batu T, et al. Testing That Distributions are Close. In: Proc of the 41st Annual Symposium on Foundations of Computer Science, 2000. 259~269
50 Kifer D, Ben-David S, Gehrke J. Detecting Change in Data Streams. In: Proc of the 30th VLDB Conf, 2004. 180~191
51 Wang H, Pei J. A Random Method for Quantifying Changing Distributions in Data Streams. The 9th European Conf on Principles and Practice of Knowledge Discovery in Databases (PKDD). 2005