一种有效可证安全的基于身份代理聚合签名方案

孙 华[1] 郭 磊[1] 郑雪峰[2] 韩晓光[2]
(安阳师范学院计算机与信息工程学院 安阳 455000)[1] (北京科技大学信息工程学院 北京 100083)[2]

摘 要 基于计算Diffie-Hellman问题的困难假设,构造了一个基于身份的代理聚合签名方案。该方案不仅满足代理签名的各种安全性要求,而且具有聚合签名的优点。最后,利用双线性技术对方案的正确性进行了严格的证明,并给出了方案安全性的详细证明。结果表明方案是可证安全的和可靠的,是一种安全有效的方案。

关键词 代理聚合签名,基于身份的密码,双线性对,计算Diffie-Hellman问题
中图法分类号 TP309 **文献标识码** A

Efficient and Provably Secure Identity-based Proxy Aggregate Signature Scheme

SUN Hua[1] GUO Lei[1] ZHENG Xue-feng[2] HAN Xiao-guang[2]
(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract Based on the hardness of the computational Diffie-Hellman problem, this paper proposed an identity-based proxy aggregate signature. The scheme not only owns all the secure properties of proxy signature, but also has merit of the aggregate signature. At last, the scheme's correctness was exactly proven in terms of bilinear pairing technique, and its security analysis was given in detail. It is indicated that this scheme is proven secure and reliable. Therefore, this scheme is secure and efficient.

Keywords Proxy aggregate signature, Identity based cryptography, Bilinear pairing, Computational Diffie-Hellman problem

1984年,Shamir[1]首先提出了基于身份的公钥密码体制,用以解决传统公钥密码体制中的证书管理。在基于身份的密码体制中,用户的公钥为能够标识用户身份的信息,如E-mail地址或IP地址,而其私钥则由可信第三方生成。2001年,Boneh和Franklin[2]利用双线性对技术提出了第一个实用的基于身份的加密方案,随后人们提出了一些基于身份的签名方案[3,4]。

为了实现数字签名权利的委托,1996年Mambo等人[5]提出了代理签名的概念。通常,在一个代理签名方案中包含原始签名人、代理签名人和验证者,由原始签名人将其签名权委托给代理签名人,代理签名人代表原始签名人生成有效的数字签名。代理签名可以应用到许多领域,例如分布式系统、网格计算、分布式网络和移动通信等。由于代理签名的广泛应用,因此,它一提出就一直受到密码学界的广泛关注。

代理签名与基于身份的密码体制相结合形成了基于身份的代理签名。2003年,Zhang和Kim[6]提出了第一个基于身份的代理签名(IBPS)方案,不过文献中只是对方案做了简单的安全分析。随后,人们又陆续提出了一些基于身份的代理签名方案[7,8]。

尽管基于双线性对的身份签名有一些优点,可是效率方面的问题限制了它的使用,尤其是在电子商务和银行服务环境中,当需要对许多签名同时进行验证时,这个问题显得尤为突出。

2003年,Boneh[9]等人提出了第一个聚合签名方案,即将n个不同签名者对n个消息m的签名聚合成一个单一的签名,而验证方只需对合成后的签名进行验证就能够确信签名是否来自指定的用户。聚合签名的概念非常重要,许多应用中都要求能够在较短的时间里对多个签名进行验证。

2004年,Cheon[10]等人利用Pointcheval和Stern[11]的分叉引理提出了第一个基于身份的聚合签名方案,然而方案本身对安全性证明所进行的规约就是不安全的。后来Herranz[12]提出了确定性的部分聚合身份签名,即对同一个签名者的多个签名进行聚合时,其聚合签名的长度是个常量。Camenisch[13]等人提出了对短签名进行批处理验证的方案。

本文提出了一个在随机预言模型下可证安全的基于身份的代理聚合签名方案。利用计算Diffie-Hellman问题的困难性,证明了方案在适应性选择消息和目标身份攻击下的安全性和不可伪造性,同时方案中代理聚合签名的长度仅和单个签名的长度相当,且可以有效地对它们进行验证。

到稿日期:2011-05-12 返修日期:2011-07-29 本文受国家自然科学基金项目(61075039,61170244),河南省科技攻关计划项目(112102210370)资助。

孙 华(1980—),男,博士生,主要研究方向为密码学与信息安全;郭 磊(1976—),男,讲师,主要研究方向为信息安全理论与技术;郑雪峰(1951—),男,教授,主要研究方向为信息安全技术;韩晓光(1982—),男,博士生,主要研究方向为网络安全、云计算。

1 预备知识

1.1 双线性对

设 G、G_T 是两个阶为素数 q 的循环加法群和循环乘法群，g 是群 G 的生成元，双线性对 $e:G\times G\to G_T$ 是具有如下性质的映射：

1. 双线性：对于所有的 $P,Q\in G$ 与 $a,b\in Z^*$，都有 $e(aP,bQ)=e(P,Q)^{ab}$；

2. 非退化性：$e(g,g)\neq 1$；

3. 可计算性：存在一个有效的算法计算 $e(P,Q)$，其中 $P,Q\in G$。

1.2 困难问题假设

DDH 问题：已知 G 是阶为素数 q 的循环群，P 是群 G 的生成元，给定 $P,aP,bP,cP\in G,a,b,c\in_R Z_q^*$，判定是否 $c=ab$。

CDH 问题：已知 G 是阶为素数 q 的循环群，P 是群 G 的生成元，给定 $P,aP,bP\in G,a,b\in_R Z_p^*$，计算 abP。

定义 1 如果群 G 上的 DDH 问题容易计算而 CDH 问题是困难的，且不存在运行时间至多为 t、解决群 G 的 CDH 问题的概率至少为 ϵ 的算法，则群 G 是一个 (t,ϵ)-GDH 群。

2 IBPAS 体制定义

2.1 IBPAS 的形式化定义

定义 2 设 P_A 是原始签名人，$PS=\{P_1,P_2,\cdots,P_n\}$ 是由代理人组成的代理签名群，则基于身份的代理聚合签名方案可表示成 IBPAS=(G,ε,S,V,(AD,AP),APS,PS,PV)。

1. G 是系统参数生成算法，用于生成系统参数。

2. ε 是用户私钥生成算法，用于生成参加签名用户的密钥对。

3. S 是标准签名生成算法，用于生成用户的签名。

4. V 是标准签名验证算法，用于验证用户的签名。

5. (AD,AP)是代理指定协议，AD 把原始签名人 P_A 的签名权委托给代理签名组的各个成员 $P_i(i=1,\cdots,n)$，AP 产生各代理签名人的代理签名私钥。

6. APS 是部分代理签名生成算法，用于生成各代理签名人的代理签名。

7. PS 是代理签名生成算法，用于生成代理聚合签名。

8. PV 是代理签名验证算法，用于验证代理聚合签名的正确性。

2.2 IBPAS 的安全要求

基于身份的代理聚合签名方案应满足如下安全性要求：

1)可区分性：任何人都可以区分标准签名和代理签名。

2)可验证性：根据代理签名，验证人能确信原始签名人认可代理签名人所签的签名。

3)强可识别性：根据代理签名，任何人都可确定相应的代理签名人的身份。

4)强不可伪造性：代理签名人能代表原始签名人产生有效的部分代理签名，而原始签名人和其他没有被指定为代理签名人的第三方都不能产生有效的部分代理签名。

5)强不可否认性：如果代理签名人代表原始签名人产生了有效的部分代理签名，他就不能否认他产生的部分代理签名；如果代理签名组代表原始签名人产生了有效的代理聚合签名，他们就不能否认其所产生的代理聚合签名。

6)抗滥用性：代理签名人不能将代理私钥用于除产生有效代理签名外的其他目的。代理签名人若滥用了代理私钥，则能确定代理签名人的责任。

3 本文的 IBPAS 方案

3.1 方案描述

设 P_A 是原始签名人，身份为 ID_A，$PS=\{P_1,\cdots,P_n\}$ 是一个代理人组成的代理签名群，相应身份为 $ID_i(i=1,\cdots,n)$，$M=(m_1,\cdots,m_n)$ 为待签消息的集合，W 是授权文件(包括原始签名人和代理签名人的身份信息，代理签名的消息空间以及代理签名的有效期等)。方案由如下几部分构成。

(1)系统参数生成算法 G

令 G、G_T 是阶为素数 q 的循环群，P 和 Q 为群 G 的两个不同生成元，双线性映射为 $e:G\times G\to G_T$，随机选取 $s\in Z_q^*$，计算 $P_{pub}=sP$ 作为公钥。选取两个 Hash 函数 $H_1:\{0,1\}^*\times G\to Z_q^*$ 和 $H_2:\{0,1\}^*\to G$，则系统参数为 $param=(G,G_T,e,P,Q,P_{pub},H_1,H_2)$，主密钥为 s。

(2)用户私钥生成算法 ε

给定用户身份 ID，该算法计算 $Q_{ID}=H_2(ID)$ 和 $S_{ID}=sQ_{ID}$，输出 S_{ID} 作为身份 ID 的私钥，Q_{ID} 为公钥。

(3)标准签名生成算法 S

给定用户身份 ID 的私钥 S_{ID} 和待签消息 m，随机选取 $r\in Z_q^*$，计算 $U=rP,h=H_1(m,U),V=rQ+hS_{ID}$，则在身份 ID 下对消息 m 的签名为 $\sigma=(U,V)$。

(4)标准签名验证算法 V

通过下面等式验证签名 $\sigma=(U,V)$ 的有效性：

$e(P,V)=e(Q,U)e(P_{pub},hQ_{ID})$

(5)代理指定协议(AD,AP)

AD：已知授权文件 W，原始签名人 P_A 的私钥为 S_{ID_A}，随机选择 $r_A\in Z_q^*$，并计算 $U_A=r_AP,h_A=H_1(W,U_A),V_A=r_AQ+h_AS_{ID_A}$，然后原始签名人 P_A 发送 (W,σ_W) 给每个代理成员 $P_i(i=1,\cdots,n)$，其中 $\sigma_W=(U_A,V_A)$ 是原始签名人 P_A 产生的授权证书。

AP：代理签名人 P_i 通过验证下式判断 (W,σ_W) 是否有效：

$e(P,V_A)=e(Q,U_A)e(P_{pub},h_AQ_{ID_A})$

如果成立，代理签名人 P_i 计算 $S_{P_i}=V_A+S_{ID_i}$ 作为代表原始签名人 P_A 的代理签名密钥。

(6)部分代理签名生成算法 APS

给定代理签名人 P_i 的私钥 S_{P_i} 和待签消息 m_i，随机选取 $r_i\in Z_q^*$，P_i 计算 $U_i=r_iP,h_i=H_1(m_i,U_i),V_i=r_iQ+h_iS_{P_i}$，则 $\sigma_i=(W,U_A,U_i,V_i)$ 为其产生的部分代理签名。

(7)代理签名生成算法 PS

首先验证代理签名人 P_i 代表原始签名人 P_A 生成的部分代理签名 σ_i 的有效性，验证等式为 $e(P,V_i)=e(Q,U_i)e(P_{pub},h_iQ_{ID_i})e(h_iQ,U_A)e(P_{pub},h_ih_AQ_{ID_A})$，若部分代理签名 $\sigma_i(i=1,\cdots,n)$ 通过验证，计算 $U=\sum_{i=1}^{n}U_i,V=\sum_{i=1}^{n}V_i$，则产生在代理人集合 PS 下的聚合签名 $\sigma=(W,U_A,U,V)$。

(8)代理签名验证算法 PV

给定验证者代理聚合签名 σ、各代理签名者的身份 ID_i

和其代理签名的消息 m_i，验证者计算 $Q_{ID_i}=H_2(ID_i)$ 和 $h_i=H_1(m_i,U_i)$，$1\leqslant i\leqslant n$，如果等式 $e(P,V)=e(Q,U)e(P_{pub},\sum_{i=1}^{n}h_iQ_{ID_i})e(U_A,\sum_{i=1}^{n}h_iQ)e(P_{pub},\sum_{i=1}^{n}h_ih_AQ_{ID_A})$ 成立，则 σ 为一个有效的代理聚合签名。

3.2 方案正确性

$$\begin{aligned}e(P,V)&=e(P,\sum_{i=1}^{n}V_i)=e(P,\sum_{i=1}^{n}r_iQ)e(P,\sum_{i=1}^{n}h_iS_{P_i})\\&=e(Q,\sum_{i=1}^{n}r_iP)e(P,\sum_{i=1}^{n}h_iS_{ID_i})e(P,\sum_{i=1}^{n}h_ir_AQ)e(P,\\&\quad\sum_{i=1}^{n}h_ih_AS_{ID_A})\\&=e(Q,U)e(P_{pub},\sum_{i=1}^{n}h_iQ_{ID_i})e(U_A,\sum_{i=1}^{n}h_iQ)e(P_{pub},\\&\quad\sum_{i=1}^{n}h_ih_AQ_{ID_A})\end{aligned}$$

因此，本方案是正确的。

3.3 方案安全性

由于在一个有效代理签名中包含一个授权文件、原始签名人身份、代理签名人身份，而在代理签名验证等式中授权文件、原始签名人身份、代理签名人身份均同时出现，因此，很容易证明本方案满足可区分性、可验证性、强可识别行、强不可否认性和抗滥用性。下面讨论本方案满足强不可伪造性。

定义 3 一个代理聚合签名伪造者 A $(t,q_{H_1},q_{H_2},q_E,q_S,N,\varepsilon)$-攻破一个 N 用户的代理聚合签名方案，如果 A 的运行时间至多为 t，并且 A 提出至多 q_{H_i} $(i=1,2)$ 次 Hash 函数询问，至多 q_E 次私钥询问，至多 q_S 次签名询问，获得的优势至少为 ε。如果敌手 A 没有攻破它，则该基于身份的代理聚合签名方案是 $(t,q_{H_1},q_{H_2},q_E,q_S,N,\varepsilon)$-抗存在性伪造安全的。

定理 1 假设 G 是一个阶为素数 q 的 (t',ε')-GDH 群，P 是群 G 的生成元，$e:G\times G\to G_T$ 是一个双线性映射，那么本文方案是 $(t,q_{H_1},q_{H_2},q_E,q_S,N,\varepsilon)$-抗存在性伪造安全的，并且有

$$\varepsilon\geqslant e(q_E+N)\varepsilon'$$

$$t\leqslant t'-C_{G_1}(q_{H_1}+q_{H_2}+q_E+4q_S+N+2)$$

式中，e 是自然对数的底，C_{G_1} 是群中计算乘法和求逆运算所需要的时间。

证明：假定 A 是一个攻破该方案的签名伪造者，那么我们可以构造一个算法 B，它能够以运行时间至多 t'、至少为 ε' 的概率解决群 G 上的 CDH 问题，其中 (P,aP,bP) 是 CDH 问题的一个实例，而这与 G 是一个 (t',ε') 群相矛盾。

我们假定 A 在对身份 ID_i 进行用户私钥询问前需先进行 H_2 询问，同样，以身份 ID_i 对消息 m_i 进行签名询问前需先进行 H_1 询问。算法 B 模仿挑战者与敌手伪造者交互如下：

系统建立：算法 B 随机选取 $t\in Z_q^*$，计算 $Q=tP$，令 $P_{pub}=aP$ 为系统公钥，随机选取目标身份 ID^*，不妨令 $ID^*=ID_1$，并将系统参数及目标身份发送给敌手 A。

询问：当敌手 A 发起私钥询问和签名询问时，算法 B 做如下响应：

①H_1-询问：为响应对随机预言机 H_1 的询问，算法 B 维护一张三元组 (m_i,U_i,v_i) 的列表 L_1。当敌手 A 对 m_i 和 U_i 进行 H_1 询问时，算法 B 响应如下：

1. 如果 (m_i,U_i) 已存在于列表 L_1 的三元组中，则算法 B 响应 $H_1(m_i,U_i)=v_i$。

2. 否则，算法 B 随机选取 $v_i\in Z_q^*$，把三元组 (m_i,U_i,v_i) 添加到列表 L_1 中，并把 $H_1(m_i,U_i)=v_i$ 发送给敌手 A。

②H_2-询问：在任何时刻敌手 A 可以向 H_2 发出询问。为了响应询问，算法 B 维护一张四元组 (ID_i,w_i,x_i,y_i) 的列表 L_2，它初始的时候是空的。当敌手对 ID_i 进行 H_2 询问时，算法 B 响应如下：

1. 如果 ID_i 已经存在于列表 L_2 的某个四元组 (ID_i,w_i,x_i,y_i) 中，则算法 B 响应 $H_2(ID_i)=w_i$。

2. 否则，算法 B 生成一个随机值 $y_i\in(0,1)$，且 $\Pr[y_i=0]=1/(q_E+N)$。

3. 算法 B 随机选取 $x_i\in Z_q^*$。如果 $y_i=0$，B 计算 $w_i=x_i(bP)$，如果 $y_i=1$，则 B 计算 $w_i=x_iP$。

4. 算法 B 把四元组 (ID_i,w_i,x_i,y_i) 添加到列表 L_2 中，并把 $H_2(ID_i)=w_i$ 发送给敌手 A。

③用户私钥询问：当敌手 A 询问身份 ID_i 的私钥时，算法 B 查找列表 L_2 中的四元组。如果 $y_i=0$，则算法失败退出。否则，算法 B 计算 $x_iP_{pub}=x_i(aP)\in G$ 作为其私钥，并发送给敌手。

④普通签名询问：当敌手 A 询问消息 m_i 在身份 ID_i 下的签名时，算法 B 首先从列表 L_2 查找相应的四元组，然后作如下处理：

1. 如果 $y_i=0$，则算法 B 失败并停止。

2. 否则，表明 $H_2(ID_i)=x_iP$。算法 B 随机选取 $r_i\in Z_q^*$，计算 $U_i=r_iP$。如果三元组 (m_i,U_i,v_i) 在列表 L_1 中，那么算法 B 从中取得 v_i，否则，随机选取 $v\in Z_q^*$，并把 (m_i,U_i,v) 加入列表 L_1 中。

3. 算法 B 计算 $V_i=r_iQ+v_i(x_iP_{pub})$，并把 $\sigma_i=(U_i,V_i)$ 发送给敌手 A，可知 σ_i 是消息 m_i 在身份 ID_i 下的一个有效签名。

⑤代理授权询问Ⅰ：敌手 A 提交原始签名人身份 ID_A 和代理签名人身份 $ID_i(i=1,\cdots,n)$ 和授权文件 W，A 扮演原始签名人 ID_A，运行算法 AD 并产生授权证书 σ_W。敌手 A 首先从列表 L_2 查找相应的四元组 (ID_A,w_A,x_A,y_A)，然后作如下处理：

1. 如果 $y_A=0$，则算法 B 失败并停止。否则，表明 $H_2(ID_A)=x_AP$，并且敌手 A 计算 x_AP_{pub} 作为其私钥。

2. 敌手 A 随机选取 $r_A\in Z_q^*$，计算 $U_A=r_AP$。如果三元组 (W,U_A,v_A) 在列表 L_1 中，那么敌手 A 取得 v_A，否则，敌手 A 发出 H_1 询问，算法 B 随机选取 $v_A\in Z_q^*$，并把 (W,U_A,v_A) 加入列表 L_1 中。

3. 敌手 A 计算 $V_A=r_AQ+v_A(x_AP_{pub})$，并将 (W,σ_W) 发送给 B，其中 $\sigma_W=(U_A,V_A)$。

4. 算法 B 首先从列表 L_2 查找相应的四元组 (ID_i,w_i,x_i,y_i)，如果 $y_i=0$，则算法 B 失败并退出；否则，算法 B 计算 x_iP_{pub} 作为代理签名人 ID_i 的私钥。然后算法 B 运行 AP 算法产生代理签名私钥 $S_{P_i}=V_A+S_{ID_i}$。

⑥代理授权询问Ⅱ：敌手 A 提交原始签名人身份 ID_A 和代理签名人身份 $ID_i(i=1,\cdots,n)$ 和授权文件 W，A 扮演代理签名人 ID_i，算法 B 运行算法 AD 并产生授权证书 σ_W。算法 B 首先从列表 L_2 查找相应的四元组 (ID_i,w_i,x_i,y_i)，然后作

如下处理：

1. 如果 $y_i=0$，则算法 B 失败并停止。否则，表明 $H_2(ID_i)=x_iP$，并且计算 x_iP_{pub} 作为其私钥。

2. 算法 B 随机选取 $r_i\in Z_q^*$，计算 $U_i=r_iP$。如果三元组 (W,U_i,v_i) 在列表 L_1 中，那么取得 v_i，否则，算法 B 随机选取 $v_i\in Z_q^*$，并把 (W,U_i,v_i) 加入列表 L_1 中。

3. 算法 B 计算 $V_i=r_iQ+v_i(x_iP_{pub})$，并且将 (W,σ_W) 发送给敌手 A，其中 $\sigma_W=(U_i,V_i)$。

⑦部分代理签名询问：敌手 A 提交原始签名人身份 ID_A 和代理签名人身份 $ID_i(i=1,\cdots,n)$、授权文件 W 和消息 $m_i(i=1,\cdots,n)$，A 扮演原始签名人 ID_A。敌手 A 首先从列表 L_2 查找相应的四元组 (ID_A,w_A,x_A,y_A)，然后作如下处理：

1. 如果 $y_A\neq 0$，敌手 A 运行算法 AD 产生授权证书 σ_W，并将 (W,σ_W) 发送给 B；否则，失败退出。

2. 算法 B 从列表 L_2 查找相应的四元组 (ID_i,w_i,x_i,y_i)，如果 $y_i\neq 0$，算法 B 运行 AP 算法产生代理签名私钥 $S_{P_i}=V_A+S_{ID_i}$。

3. 算法 B 随机选取 $r_i\in Z_q^*$，计算 $U_i=r_iP$，然后从三元组 (m_i,U_i,v_i) 列表 L_1 中取得 v_i，计算 $V_i=r_iQ+v_iS_{P_i}$，则 $\sigma_i=(W,U_A,U_i,V_i)$ 为产生的部分代理签名。

⑧代理签名询问：敌手 A 提交原始签名人身份 ID_A 和代理签名组身份 $(ID_i,\cdots,ID_n)$、授权文件 W 和消息 $M=(m_1,\cdots,m_n)$。A 扮演原始签名人 ID_A，运行 AD 算法并产生授权证书 σ_W，发送 (W,σ_W) 给 B。B 首先运行算法 AP，产生所有代理人的代理签名密钥，然后通过部分代理签名询问的方法产生各个代理人的部分签名，最后运行代理签名生成算法，生成代理聚合签名。

伪造：或者算法 B 失败退出，或者敌手 A 输出在原始签名人身份 ID_A、代理签名人身份 $ID_1,\cdots,ID_n$ 和授权文件 W 下对消息 $m_1,\cdots,m_n$ 的一个有效代理聚合签名 σ，并且敌手没有询问消息 m_1 在身份 ID_1 下的签名。

当且仅当 $y_1=0,y_i=1,2\leqslant i\leqslant n$ 时，算法 B 没有失败退出。因 $y_1=0$，得 $H_2(ID_1)=x_1(bP)$，而 $i\geqslant 2$ 时，由 $y_i=1$，得 $H_2(ID_i)=x_iP$。由聚合签名 σ 满足等式

$$e(P,V)=e(Q,U)e(P_{pub},\sum_{i=1}^{n}h_iQ_{ID_i})e(U_A,\sum_{i=1}^{n}h_iQ)e(P_{pub},\sum_{i=1}^{n}h_ih_AQ_{ID_A})$$

算法 B 从列表 L_1 中查找这 $n-1$ 个 (m_i,U_i,v_i) 以及 (W,U_A,v_A)，令 $V_i=tU_i+v_itU_A+v_ix_iP_{pub}+v_iv_Ax_AP_{pub}$，$Q=tP$，则有

$$\begin{aligned}e(P,V_i)&=e(P,tU_i+v_itU_A+v_ix_iP_{pub}+v_iv_Ax_AP_{pub})\\&=e(Q,U_i)e(P_{pub},v_iQ_{ID_i})e(v_iQ,U_A)e(P_{pub},v_iv_AQ_{ID_A})\end{aligned}$$

因此，$\sigma_i=(W,U_A,U_i,V_i)$ 是在代理身份 ID_i 下消息 m_i 的有效签名。令 $V_1=V-\sum_{i=2}^{n}V_i$，可以得到

$$\begin{aligned}e(P,V_1)&=e(P,V-\textstyle\sum_{i=2}^{n}V_i)\\&=\prod_{i=1}^{n}e(Q,U_i)e(P_{pub},v_iQ_{ID_i})e(v_iQ,U_A)e(P_{pub},v_iv_AQ_{ID_A})\cdot\prod_{i=1}^{n}e(Q,U_i)^{-1}e(P_{pub},v_iQ_{ID_i})^{-1}e(v_iQ,U_A)^{-1}e(P_{pub},v_iv_AQ_{ID_A})^{-1}\\&=e(Q,U_1)e(P_{pub},v_1Q_{ID_1})e(v_1Q,U_A)e(P_{pub},v_1v_AQ_{ID_A})\\&=e(P,tU_1+tv_1U_A)e(P,v_1x_1abP+v_1v_Ax_AabP)\end{aligned}$$

因此，算法 B 可以计算

$$abP=(v_1x_1+v_1v_Ax_A)^{-1}(V_1-tU_1-tv_1U_A)$$

最后，据分析可知，算法 B 将至少以概率 ϵ' 解决给定的 CDH 问题。首先分析算法 B 成功的 4 个事件：

E_1：B 没有因为 A 的私钥询问而失败退出。

E_2：B 没有因为 A 的签名询问而失败退出。

E_3：A 伪造一个有效的聚合签名 $\sigma=(W,U_A,U,V)$。

E_4：事件 E_3 发生，同时有 $y_1=0,y_i=1,2\leqslant i\leqslant n$ 成立，这里 y_i 为列表 L_2 中四元组中的值。

当所有这 4 个事件发生时，算法 B 获得成功，其成功概率可记作：

$$P_r[E_1\wedge E_2\wedge E_3\wedge E_4]=P_r[E_1]\cdot P_r[E_2|E_1]\cdot P_r[E_3|E_1\wedge E_2]\cdot P_r[E_4|E_1\wedge E_2\wedge E_3]$$

推论 1 算法 B 没有因为 A 的私钥询问而失败退出的概率至少为 $P_r[E_1]\geqslant(1-1/(q_E+N))^{q_E}$。

证明：由 $\Pr[y=0]=1/(q_E+N)$ 可知，对于一个私钥询问，算法 B 不失败退出的概率是 $1-1/(q_E+N)$。因敌手 A 至多进行 q_E 次私钥询问，所以事件 E_1 的概率至少为 $(1-1/(q_E+N))^{q_E}$。

推论 2 B 没有因为 A 的签名询问而失败退出的概率为 1。

证明：只有在 A 的私钥询问下 B 没有失败退出，该过程才是可以模拟的，因此，$P_r[E_2|E_1]=1$。

推论 3 如果算法 B 没有因 A 的私钥询问和签名询问而退出，那么敌手 A 的视图与真实世界里的攻击是一致的，因此，$P_r[E_3|E_1\wedge E_2]\geqslant\epsilon$。

推论 4 算法 B 在敌手 A 输出一个有效的伪造签名后而没有失败退出的概率为

$$P_r[E_4|E_1\wedge E_2\wedge E_3]\geqslant(1-1/(q_E+N))^{N-1}\cdot 1/(q_E+N)$$

证明：在事件 E_1,E_2,E_3 发生的情况下，算法 B 生成一个有效的伪造签名。由 $y_1=0,\Pr[y=0]=1/(q_E+N)$，得 $y_i=1,2\leqslant i\leqslant n$ 的概率为

$$(1-1/(q_E+N))^{k-1}\geqslant(1-1/(q_E+N))^{N-1}$$

因此，可得

$$P_r[E_4|E_1\wedge E_2\wedge E_3]\geqslant(1-1/(q_E+N))^{N-1}\cdot 1/(q_E+N)$$

综上所述，算法 B 解决 CDH 问题的概率为

$$(1-1/(q_E+N))^{q_E}\cdot\epsilon\cdot(1-1/(q_E+N))^{N-1}\cdot 1/(q_E+N)\geqslant\epsilon/e(q_E+N)\geqslant\epsilon'$$

可得 $\epsilon\geqslant e(q_E+N)\epsilon'$。

这里，我们来分析一下算法的时间复杂度。算法 B 的运行时间为 A 的运行时间加上 (q_{H_1},q_{H_2},q_S) 次 Hash 询问、q_E 次私钥询问、q_S 次签名询问的响应时间以及将 A 的伪造签名转化为 CDH 问题的时间。因此，总的运行时间至多为 $t\leqslant t'-C_{G_1}(q_{H_1}+q_{H_2}+q_E+4q_S+N+2)$。

3.4 方案效率

当需要对消息 $m_1,\cdots,m_n$ 在身份 $ID_1,ID_2,\cdots,ID_n$ 下的 n 个代理签名进行验证时，只需要进行聚合签名验证即可。由等式

（下转第 52 页）

法的预测误差和直接使用 ARIMA 模型所得到的预测误差如表 3 所列。

表 3 预测误差的比较

不同方法	e
基于 NMF 的预测	0.0651
直接预测	0.069

从表 3 中可以看出，基于 NMF 的预测方法和直接采用 ARIMA 模型的预测方法，其预测误差十分接近，但本文中的方法相对于直接预测方法来说省去了 4 路数据的建模开销，具有更低的计算复杂度。

结束语 本文针对宽带多媒体卫星通信系统中多路流量的预测问题，提出了一种基于非负矩阵分解的流量预测方法。通过非负矩阵分解，将原始多路流量数据投影到一个低维子空间，可降低预测数据量，提高整个预测系统的预测效率。通过实验表明，基于非负矩阵分解的流量预测方法与直接流量预测方法相比，预测误差十分接近，但预测计算复杂度更低。

参 考 文 献

[1] Secchi R, Barsocchi P, Davoli F. Linear quadratic control of service rate allocation in a satellite network[J]. Communications, IET, 2010, 4(13): 1580-1593

[2] Yueqiu J, Hang L. Study on bandwidth allocation of broadband multimedia communication satellite system[C]// Proceedings of the 3rd International Conference on Intelligent Networks and Intelligent Systems. 2010: 506-508

[3] Delli Priscoli F, Pompili D. A demand-assignment algorithm based on a Markov modulated chain prediction model for satellite bandwidth allocation[J]. Wirel. Netw., 2009, 15: 999-1012

[4] 王升辉，裘正定. 结合多重分形的网络流量非线性预测[J]. 通信学报，2007，28(2)：45-50

[5] Satsri S, Ardhan S, Chutchavong V, et al. ANN based NGN IP traffic prediction in Thailand[C]// Proceedings of the International Conference on Control, Automation and Systems. 2007: 2154-2157

[6] Li R, Chen J, Liu Y, et al. WPANFIS: combine fuzzy neural network with multiresolution for network traffic prediction[J]. The Journal of China Universities of Posts and Telecommunications, 2010, 17(4): 88-93

[7] 王俊松，高志伟. 基于 RBF 神经网络的网络流量建模及预测[J]. 计算机工程与应用，2008，44(13)：6-11

[8] 单佩韦，李明. 基于 EMD 的自相似流量 Hurst 指数估计[J]. 计算机工程，2008，34(23)：128-129

[9] 高波，张钦宇，梁永生，等. 基于 EMD 及 ARMA 的自相似网络流量预测[J]. 通信学报，2011，32(4)：47-56

[10] 姜伟，杨炳儒，隋海峰. 局部敏感非负矩阵分解[J]. 计算机科学，2010，27(12)：211-214

[11] Lee D D, Seung H S. Learning the parts of objects by non-negative matrix factorization[J]. Nature, 1999, 401(6755): 788-791

[12] Daniel D, Lee H. Sebastian Seung. Algorithms for non-negative matrix factorization[C]// Proceedings of the Conference on Advances in Neural Information Processing Systems. 2000: 556-562

[13] Tuomas V. Monaural sound source separation by nonnegative matrix factorization with temporal continuity and sparseness criteria[J]. IEEE Transactions on Audio, Speech, and Language Processing, 2007, 15(3): 1066-1074

(上接第 47 页)

$$e(P,V)=e(Q,U)e(P_{pub},\sum_{i=1}^{n}h_iQ_{ID_i})e(U_A,\sum_{i=1}^{n}h_iQ)e(P_{pub},\sum_{i=1}^{n}h_ih_AQ_{ID_A})$$

可知，我们只需要计算 $V=\sum_{i=1}^{n}V_i$，$U=\sum_{i=1}^{n}U_i$，而不需要单独验证各个签名 $\sigma_i=(W,U_A,U_i,V_i)$。签名长度的压缩率为 $1/n$，即与单个签名的长度相当，同时，整个签名验证过程只需要 5 个双线性对计算，因此具有较高的效率。

结束语 本文利用双线性对提出了一个基于身份的代理聚合签名方案。方案中聚合签名的长度仅与单个签名的长度相当，而签名的验证仅需要 5 个双线性对和 $3n$ 个群元素的标量乘计算，因而具有较高的效率。最后利用计算 CDH 问题的困难性证明了方案在随机预言模型下的不可伪造性。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Blakley G, Chaum D, eds. Proceedings of Crypto 1984, volume 196 of LNCS. 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Joe Kilian, ed. Proceedings of Crypto 2001. volume 2139 of LNCS. 2001: 213-229

[3] Hess F. Efficient identity based signature schemes based on pairings[C]// Kaisa Nyberg, Howard M, eds. Proceedings of SAC 2002. volume 2595 of LNCS. 2002: 310-324

[4] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]// Proceedings of ACISP 2006. volume 4058 of LNCS. 2006: 207-222

[5] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]// Proceedings of the 3rd ACM Conference on Computer and Communications Security. New York: ACM, 1996: 48-57

[6] Zhang F, Kim K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C]// Proceedings of the 8th Australasian Conference on Information Security and Privacy. volume 2727 of LNCS. 2003: 312-323

[7] Wu W, Mu Y, Susilo W, et al. Identity-based proxy signature from pairings[C]// Proceedings of the 4th International Conference on Autonomic and Trusted Computing. volume 4610 of LNCS. 2007: 22-31

[8] 李明祥，韩伯涛，朱建勇，等. 在标准模型下安全的基于身份的代理签名方案[J]. 华南理工大学学报：自然科学版，2009，37(5)：118-122

[9] Boneh D, Gentry C. Aggregate and verifiably encrypted signatures from bilinear maps[C]// Advances in Cryptography-Eurocrypt 2003. volume 2656 of LNCS. 2003: 416-432

[10] Cheon J H, Kim Y, Yoon H J. A new ID-based aggregate signature with batch verification[OL]. http://eprint.iacr.org/2004/131

[11] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396

[12] Herranz J. Deterministic identity-based signatures for partial aggregation[J]. Computer Journal, 2006, 49(3): 322-330

[13] Camenisch J, Hohenberger S, Pedersen M O. Batch Verification of short signatures[C]// Advances in Cryptography- Eurocrypt 2007. volume 4515 of LNCS. 2007: 246-263