一种安全有效的基于身份的聚合签名方案

孙 华 郑雪峰 于义科 周 芳
(北京科技大学信息工程学院 北京 100083)

摘 要 聚合签名是一种将 n 个来自于 n 不同签名者对 n 个不同消息 m 的签名聚合成一个单一签名的数字签名技术。利用双线性对技术,提出了一种有效的基于身份的聚合签名方案。同已有的基于身份的聚合签名方案相比,该方案在签名验证方面具有较低的计算成本。最后利用计算 Diffie-Hellman 问题的困难性在随机预言模型下证明了该方案在适应性选择消息和身份攻击下的不可伪造性。

关键词 身份签名,聚合签名,双线性对,计算 Diffie-Hellman 问题
中图法分类号 TP309 **文献标识码** A

Secure and Efficient Identity-based Aggregate Signature Scheme

SUN Hua ZHENG Xue-feng YU Yi-ke ZHOU Fang
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract An aggregate signature scheme is a digital signature that given n signatures on n distinct messages from n distinct users, it is possible to aggregate all these signatures into a single signature. We proposed an identity-based aggregate signature scheme based on the bilinear pairings, which has a lower verification cost compared with the existing identity-based aggregate signatures. We proved that the proposed signature scheme is secure against existential forgery under adaptively chosen message and ID attack in the random oracle model, assuming that the Computational Diffie-Hellman problem is hard to solve.

Keywords Identity-based signature, Aggregate signature, Bilinear pairings, Computational Diffie-Hellman problem

1984年,Shamir[1]首先提出了基于身份的签名思想,用以简化基于证书的PKI中的密钥管理。后来一些基于身份的加密和签名方案被相继提出,然而早期的方案因为计算过于复杂而很难推广。2001年Boneh和Franklin[2]利用双线性对技术提出了一个实用的基于身份的加密方案,随后人们又利用双线性对所特有的性质提出了一些基于身份的签名方案[3-5]。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[6]等人基于BLS[7]短签名方案提出了第一个聚合签名方案,即将 n 不同签名者对 n 个不同消息 m 的 n 个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。随后Lysyanskaya[8]和Ostrovsky[9]等人分别提出了相应的序列聚合签名方案。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。例如在邮件服务器中,为了减少服务器验证邮件签名的处理时间,需要一种快速的验证方案用以在很短的时间内对大量的签名进行验证。

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,并指出不能将某一种基于身份的签名方案简单地通过聚合技术来生成基于身份的聚合签名方案,虽然签名方案本身是安全的,可是由其得到的聚合签名方案则可能是不安全的,而Cheon[10]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,当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。Gentry[13]等人提出了基于身份的聚合签名。Camenisch[14]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聚合签名方案。方案利用计算Diffie-Hellman问题的困难性证明了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。

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 $e(aP, bQ)=e(P, Q)^{ab}$;

到稿日期:2009-06-08 返修日期:2009-09-10 本文受国家自然科学基金项目(No. 60674054)资助。
孙 华(1980—),男,博士生,研究方向为密码学与信息安全,E-mail:sh1227@163.com;郑雪峰(1951—),男,教授,研究方向为信息安全技术;于义科(1971—),男,副教授,研究方向为网络与信息安全;周 芳(1972—),女,讲师,研究方向为网络安全技术。

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 GDH 群

假设 G 是一个阶为素数 q 的循环群，P 是群 G 的生成元。

DDH 问题：给定 $P,aP,bP,cP\in G,a,b,c\in_R Z_p^*$，判定是否 $c=ab$。

CDH 问题：给定 $P,aP,bP\in G,a,b\in_R Z_p^*$，计算 abP。

定义 1 群 G 是一个 GDH 群，如果群 G 上的 DDH 问题是容易计算的而 CDH 问题是困难的。如果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 基于身份的聚合签名

2.1 形式化定义

一个基于身份的聚合签名方案由以下 5 个算法组成，即 Setup，KeyGen，Sign，Aggre 和 Verify。

1)Setup：给定安全参数 k，生成系统参数 $params$，公钥 pk 以及 PKG 的私钥 sk。

2)KeyGen：给定一个用户身份 ID_i，输入 sk 和 ID_i，输出身份 ID_i 的私钥 sk_i。

3)Sign：输入 sk_i、消息 m 和一些描述信息 w，输出一个基于身份的个体签名 σ_i。

4)Aggre：输入 pk,w，两个身份信息对 S_1 和 S_2 以及各自基于身份的(聚合)签名 σ_{S_1} 和 σ_{S_2}，如果等式 Verify$(pk,w,S_1,\sigma_{S_1})=accept$ 和 Verify$(pk,w,S_2,\sigma_{S_1})=accept$ 成立，则输出在身份信息对 $S_1\cup S_2$ 上的聚合签名 $\sigma_{S_1\cup S_2}$。

5)Verify：输入 pk,w，一个基于身份的聚合签名 σ_S 以及一个身份信息对 S 的描述，当且仅当 Verify$(pk,w,S,\sigma_S)=accept$ 时，σ_S 为一个有效的聚合签名。

2.2 安全模型

一个基于身份的聚合签名方案应该在适应性选择消息和身份攻击下是安全的且可以抵抗存在性伪造。可以通过一个挑战者 C 与敌手 A 之间的游戏，定义 IBAS 方案在适应性选择消息和身份攻击下抗存在性伪造的安全模型，这个游戏叙述如下。

Setup：挑战者运行签名方案的 KeyGen 算法得到系统参数 $params$ 和私钥 sk，并发送 $params$ 给敌手，保存 sk。

Queries：敌手可以适应性地向挑战者提出一定数量的询问。敌手可以选择身份 ID_i 并询问其私钥 sk_i，敌手也可以询问$(pk,w,S,\{m_i\}_{i=1}^{k-1})$上的聚合签名 σ_S，其中 $S=\{ID_i\}_{i=1}^{k-1}$。这里要求敌手不能询问$(pk,w,S',\{m_i'\}_{i=1}^{k-1})$上的聚合签名，其中 $ID_i\in S\cap S'$并且 $m_i'\neq m_i$。

Response：对于某个$(pk,\{ID_i\}_{i=1}^{l},\{m_i\}_{i=1}^{l})$，$l\leqslant n$，敌手输出在其上的聚合签名 σ_l。如果 σ_l 是$(pk,\{ID_i\}_{i=1}^{l},\{m_i\}_{i=1}^{l})$上的一个有效聚合签名且对于 $1\leqslant i\leqslant l$，敌手没有询问身份 ID_i 的私钥 sk_i 以及(ID_i,m_i)上的签名，则敌手获胜。

把敌手 A 在上面游戏中获胜的概率定义为 A 的优势。

在上面的游戏中，如果不存在运行时间至多为 t、优势至少为 ε 的敌手 A，且 A 进行 Hash 函数询问的次数最多为 q_H、KeyGen 询问的次数最多为 q_E、Sign 询问的次数最多为 q_s，则该 IBAS 方案是$(t,\varepsilon,q_H,q_E,q_S)$-EU-IBAS-CMIA 安全的。

3 一个安全有效的基于身份的聚合签名

3.1 方案描述

设 $\mathbb{U}$ 为签名者的集合，$S\subseteq\mathbb{U}$ 为生成聚合签名的签名者集合。每个签名者 $u\subseteq S$ 都有一签名密钥对(pk_i,sk_i)，可产生在所选消息 m_i 上的签名 σ_i。然后这些签名被聚合生成聚合签名。聚合签名的生成者可以是不同于 u 或者不被 u 信任的用户，它可以访问 u 的公钥，消息 m_i 及其签名 σ_i，但是不能访问其私钥 sk_i。给定聚合签名、参与生成聚合签名者的身份及其签名的消息，验证者可以确信各个签名者对其选择的消息进行了签名。方案由如下几部分构成：

Setup：给定群 G,G_T，群 G 的两个不同的生成元 P 和 Q 以及双线性对 $e:G\times G\to G_T$，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 $params=(G,G_T,e,P,Q,P_{pub},H_1,H_2)$，主密钥为 s。

Private key generation：给定身份 ID_i，该算法计算 $Q_{ID_i}=H_2(ID_i)$和 $S_{ID_i}=sQ_{ID_i}$，输出 S_{ID_i} 作为身份 ID_i 的私钥，Q_{ID_i} 为公钥。

Individual Signing：给定身份 ID_i 的私钥 S_{ID_i} 和消息 m_i，随机选取 $r_i\in Z_q$，计算 $U_i=r_iP$，$h=H_1(m_i,U_i)$，$V_i=r_iQ+hS_{ID_i}$，则在身份 ID_i 下对消息 m_i 的签名为 $\sigma_i=(U_i,V_i)$。

Verification：给定用户的公钥 Q_{ID_i}，消息 m_i 及其签名 σ_i，计算 $h=H_1(m_i,U_i)$，如果等式 $e(P,V_i)=e(Q,U_i)e(P_{pub},hQ_{ID_i})$成立，则 σ_i 是一个有效的用户签名。

Aggregation：设 $S\subseteq\mathbb{U}$ 为生成聚合签名的用户集合，$k=|S|$，(U_i,V_i)为用户在身份 ID_i 下对消息 m_i 的签名，计算 $V=\sum_{i=1}^{k}V_i$，则在用户集合 S 下生成的聚合签名为 $\sigma=(U_1,U_2,\cdots,U_k,V)$。

Aggregation Verification：给定验证者聚合签名 σ，各签名用户的身份 ID_i 和其签名的消息 m_i，验证者计算 $Q_{ID_i}=H_2(ID_i)$和 $h=H_1(m_i,U_i)$，$1\leqslant i\leqslant k$，如果等式 $e(P,V)=e(P_{pub},\sum_{i=1}^{k}hQ_{ID_i})e(Q,\sum_{i=1}^{k}U_i)$成立，则 σ 为一个有效的聚合签名。

3.2 方案正确性

1)个体签名的正确性：

$$e(P,V_i)=e(P,r_iQ+hS_{ID_i})=e(Q,r_iP)e(sP,hQ_{ID_i})=e(Q,U_i)e(P_{pub},hQ_{ID_i})$$

2)聚合签名的正确性：

$$e(P,V)=e(P,\sum_{i=1}^{k}V_i)=\prod_{i=1}^{k}e(P,V_i)=\prod_{i=1}^{k}e(P,r_iQ+hS_{ID_i})=\prod_{i=1}^{k}e(Q,U_i)e(P_{pub},hQ_{ID_i})=e(Q,\sum_{i=1}^{k}U_i)e(P_{pub},\sum_{i=1}^{k}hQ_{ID_i})$$

所以本方案是正确的。

3.3 方案安全性

在此定义基于身份的聚合签名方案的安全模型。在这个模型中，给定敌手一个目标身份 ID^*，敌手的目标是聚合签名的存在性伪造。允许聚合签名伪造者选择除目标身份 ID^* 外的任何身份 ID，并且可以询问在目标身份 ID^* 下的签名。如果敌手 A 能以不可忽略的优势攻击上面的方案，则能

够构造算法 B，B 可以利用 A 解决计算 Diffie-Hellman 问题。可以通过下面挑战者与敌手之间的游戏来定义敌手获得的优势 $Adv_{Agg,A}$。

Setup：挑战者运行方案的 Setup 算法，生成系统参数 *params*，随机选取目标身份 ID^*，并将它们发送给敌手。

Queries：对于敌手 A 发出的询问，挑战者 C 的处理方法如下：

①Hash query：挑战者计算给定输入的 Hash 函数值，并将它们发送给敌手。

②Extract query：给定身份 ID_i（$ID_i \neq ID^*$），挑战者通过运行 KeyGen 算法生成身份 ID_i 的私钥 S_{ID_i}，并将它发送给敌手。

③Sign query：给定身份 ID_i（包括目标身份 ID^*）及其选定签名的消息 m_i，挑战者通过运行 Sign 算法生成在身份 ID_i 下对消息 m_i 的签名，并将它发送给敌手。

Response：最后敌手输出 $k-1$ 个身份 $ID_2, ID_3, \cdots, ID_k$。这里假定 $ID_1 = ID^*$，$k \leqslant N$，N 是一个游戏参数。敌手同时输出 k 个消息 $m_1, m_2, \cdots, m_k$ 以及在这些身份和消息上的一个聚合签名 σ。

如果 σ 是消息 $m_1, m_2, \cdots, m_k$ 在身份 $ID_1, ID_2, ID_3, \cdots, ID_k$ 下的一个有效聚合签名，并且敌手没有询问消息 m_1 在身份 ID_1 下的签名，则说明敌手成功地伪造了一个基于身份的聚合签名。

定义 2 一个聚合签名伪造者 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。一个基于身份的聚合签名方案是 $(t, q_{H_1}, q_{H_2}, q_E, q_S, N, \varepsilon)$-抗存在性伪造安全的，如果没有聚合签名伪造者 $(t, q_{H_1}, q_{H_2}, q_E, q_S, N, \varepsilon)$-攻破它。

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，那么群 G 上的基于身份的聚合签名方案在上述安全模型下是 $(t, q_{H_1}, q_{H_2}, q_E, q_S, N, \varepsilon)$-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 $(t, q_{H_1}, q_{H_2}, q_E, q_S, N, \varepsilon)$-攻破签名方案的敌手伪造者，那么可以构造算法 B，它能够以运行时间至多为 EMBEDEquation. 3、至少为 ε' 的概率解决群 G 上的 CDH 问题，其中 $P, aP, bP \in G$ 已知，而这与 G 是一个 (t', ε') 群相矛盾。

假定 A 在对身份 ID_i 进行 Extract 询问前需先进行 H_2 询问，同样，在身份 ID_i 下对消息 m_i 进行 Sign 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：

Setup：算法 B 随机选取 $t \in \mathbb{Z}_q^*$，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。

H_1-Hash Query：为了响应对随机预言机 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) 已经存在于列表 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 $v \in Z_q^*$，把三元组 (m_i, U_i, v_i) 添加到列表 L_1 中，并把 $H_1(m_i, U_i) = v$ 发送给敌手 A。

H_2-Hash Query：在任何时刻 A 可以询问随机预言机 H_2。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 $y \in (0,1)$，且 $Pr[y=0] = 1/(q_E+N)$。

3）算法 B 随机选取 $x \in Z_q$。如果 $y=0$，B 计算 $w=x(bP) \in G$，如果 $y=1$，则 B 计算 $w=xP \in G$。

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。

Extract Query：当敌手 A 询问身份 ID_i 的私钥时，算法 B 查找列表 H_2 中的四元组对。如果 $y=0$，则算法输出"失败"并退出。否则，算法 B 计算 $xP_{pub} = x(aP) \in G$ 作为其私钥，并发送给敌手。

Sign Query：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。

Output：或者算法 B 失败退出，或者敌手 A 输出消息 $m_1, m_2, \cdots, m_k$ 在身份 $ID_1, ID_2, \cdots, ID_k$ 下的一个有效聚合签名 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 $y_1=0, y_i=1, 2 \leqslant i \leqslant k$ 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

$$e(P,V) = \prod_{i=1}^{k} e(Q,U_i)e(P_{pub}, hQ_{ID_i})$$

算法 B 从列表 L_1 中查找这 k 个 (m_i, U_i, v_i)，对 $i \geqslant 2$，令 $V_i = tU_i + v_ix_iP_{pub}$，有

$$e(P,V_i) = e(P, tU_i + v_ix_iP_{pub}) = e(Q,U_i)e(v_iQ_{ID_i}, P_{pub})$$

因此，$\sigma_i = (U_i, V_i)$ 是消息 m_i 在身份 ID_i 下的有效签名。令 $V_1 = V - \sum_{i=2}^{k} V_i$，可以得到

$$\begin{aligned} e(P,V_1) &= e(P, V - \textstyle\sum_{i=2}^{k} V_i) \\ &= \prod_{i=1}^{k} e(Q,U_i)e(P_{pub}, hQ_{ID_i}) \prod_{i=2}^{k} e(Q,U_i)^{-1} e(P_{pub}, hQ_{ID_i})^{-1} \\ &= e(Q,U_1)e(P_{pub}, hQ_{ID_1}) \\ &= e(P, tU_1)e(aP, v_1x_1(bP)) \end{aligned}$$

式中，$h = v_1$，因此算法 B 可以计算

$$abP = v_1^{-1}x_1^{-1}(V_1 - tU_1)$$

最后通过分析可知，算法 B 至少可以以概率 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 Extract Queries 而失败退出。

E_2：B 没有因为 A 的 Sign Queries 而失败退出。

E_3：A 伪造生成一个有效的聚合签名 $(U_1, U_2, \cdots, U_k, V)$。

E_4：事件 E_3 发生，同时有 $y_1=0, y_i=1, 2\leqslant i\leqslant k$ 成立，这里 y_i 为列表 L_2 的四元组中的值。

当所有这 4 个事件发生时，算法 B 获得成功，其成功概率可以记作：

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

推论 1 算法 B 没有因为 A 的 Extract Queries 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 Sign Queries 而失败退出的概率为 1。

证明：只有在 A 的 Extract Queries 下 B 没有失败退出，该过程才是可以模拟的，因此，$P_r[E_2 \mid E_1]=1$。

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，$P_r[E_3 \mid E_1 \wedge E_2]\geqslant\varepsilon$。

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

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

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 $y_1=0, Pr[y=0]=1/(q_E+N)$，则 $y_i=1, 2\leqslant i\leqslant k$ 的概率为

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

因此，可得

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

综上所述，算法 B 解决 CDH 问题的概率为

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

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

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 $m_1, m_2, \cdots, m_k$ 在身份 $ID_1, ID_2, \cdots, ID_k$ 下的 k 个签名进行验证时，只需要进行聚合签名验证即可。由等式 $e(P,V)=e(Q, \sum_{i=1}^{k}U_i)e(P_{pub}, \sum_{i=1}^{k}hQ_{ID_i})$ 可知，只需要计算 $V=\sum_{i=1}^{k}V_i, U=\sum_{i=1}^{k}U_i$，而不需要单独验证各个签名 (U_i, V_i)。签名长度的压缩率为 $1/k$，即同单个签名的长度相当，同时，整个签名验证过程只需要 3 个双线性对计算，因此具有很高的效率。

结束语 本文利用双线性对提出了一个基于身份的聚合签名方案。方案中聚合签名的长度仅和单个签名的长度相当，而签名的验证仅需要 3 个双线性对和 k 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 Diffie-Hellman 问题的困难性证明了方案在随机预言模型下的安全性及不可伪造性。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// G. Blakley and David Chaum, eds. Proceedings of Crypto 1984, volume 196 of LNCS. 1981: 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 and 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] Jae Choon Cha, Jung Hee Cheon. An identity-based signature from Gap Diffie-Hellman groups [C] // Proceedings of PKC 2003, 2567 of LNCS. 2003: 18-30

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

[7] Boneh D, Lynn B, Shacham H. Short signatures from the Weil Pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319

[8] Lysyanskaya A, Micali S, Reyzin L, et al. Sequential aggregate signatures from trapdoor permutations[C]// Advances in Cryptography-Eurocrypt 2004, 3027 of LNCS. 2004: 74-90

[9] Lu S, Ostrovsky R, Sahai A, et al. Sequential aggregate signatures and multisignatures without random oracles [C] // Advances in Cryptography-Eurocrypt 2006, 4004 of LNCS. 2006: 465-485

[10] Jung Hee Cheon, Yongdae Kim, Hyo Jin Yoon. 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] Gentry C, Ramzan Z. Identity-based aggregate signatures[C]// Proceedings of PKC 2006, 3958 of LNCS. 2006: 257-273

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