一个新的基于身份的聚合签名方案

文毅玲 马建峰 王 超
(西安电子科技大学计算机与网络安全教育部重点实验室 西安 710071)

摘 要 聚合签名由Boneh等人提出,主要是通过聚合多个签名为一个签名,来提高签名与验证的效率。提出一个新的基于身份的聚合签名方案。与Xu等人的同类方案相比,新方案在签名和验证时各少一次对运算,显著提高了计算效率。在Computational Diffie-Hellman(CDH)问题困难性假设下,提出的聚合签名在随机预言机模型下能抵抗存在性伪造攻击。此外,针对最近由Chen等人提出的聚合签名方案给出一种攻击方法,指出其不能抵抗存在性伪造攻击。

关键词 基于身份的签名,聚合签名,可证明安全
中图法分类号 TP309 **文献标识码** A

New ID-based Aggregate Signature Scheme

WEN Yi-ling MA Jian-feng WANG Chao
(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

Abstract An aggregate signature scheme was proposed by Boneh et al. in which multiple signatures can be compressed into a short signature. So it is more efficiency than others. We presented a new ID-based aggregate signature scheme. Compared with the scheme proposed by Xu et al., our scheme requires less one pairing operation in the signing and verification, respectively. So it is more efficiency than the former. The proposed scheme is secure against existential forgery in the random oracle model by assuming the intractability of the computational Diffie-Hellman (CDH) problem. Otherwise, we analysed the scheme proposed by Chen et al, and fould the scheme cannot against existential forgery.

Keywords ID-based signature, Aggregate signature, Provable security

2003年欧密会上,Boneh等人首次提出聚合签名。目前,聚合签名已成为一个研究热点。它是一种具有附加性质的签名:n个用户对n个消息分别签署的n个签名,能够合成一个短的签名,而验证者只需对聚合后的短的签名进行验证,便可以确信n个消息是否被n个用户分别进行了签名。聚合签名的研究具有广泛的应用前景。例如:在深度为n的公钥基础设施(PKI)环境下,每一个用户的公钥证书都由一个长为n的证书链组成,这个链包含着n个不同级别的CA对n个不同级别的证书的签名(处于第i层的CA认证第$i+1$层的CA)。类似地,在安全边界网关协议(SBGP)中,一个路由器收到n个签名的列表后,签名自己的部分,再将其一起提交给下一个路由器,产生一个长为$n+1$的签名列表。这些情形都包含着多个用户对多个消息分别签名,使得验证者的工作量极大。聚合签名正是通过聚合来提高验证效率。此外,聚合签名在设计可验证加密签名和环签名中都有很好的应用。文献[1-4]分别给出聚合签名在合约签订、级联认证和密钥协商以及无线路由等方面的应用。

1 相关工作

Boneh等人最初提出的聚合签名限制于不同用户签名不同的消息。当消息内容相同时,他们建议签名者将各自的公钥附加到消息中。这种修改的缺陷是:仍然要求附加公钥后的"加强的消息"互相不同。Bellare等人详细研究了这一问题,指出可以取消这种限制而得到一种新的无限制聚合签名方案,从而较好地解决了聚合签名中消息互异性问题。Shao在文献[5]中对文献[6]的安全模型进行分析,指出其与标准的数字签名安全模型相比,攻击者的能力受到了限制,并提出一个新的安全模型,对文献[6]中的方案进行了轻微的修改。Lysyanskaya等人基于陷门单向函数提出有序聚合签名,在他们设计的方案中,签名者依次将自己的签名聚合到由它前面的签名者产生的聚合签名中,产生自己的聚合签名。文献[7-9]各自提出了基于身份的聚合签名。其中,文献[7]的聚合签名是基于文献[8]中的签名方案设计的,其优点在于将安全性紧密归约到Computational Diffie-Hellman(CDH)问题的困难性。文献[8]中的方案不能抵抗存在性伪造攻击,因而是不安全的。文献[11]中的方案首先要广播并聚合随机数,这就要求聚合之前就必须确定参与聚合的签名用户,若不满足文献[6]给出的聚合签名的递增性(incrementally),用户可以随时将自己的签名聚合到已有的聚合签名中。这使得验证方必须收到全部单个签名后,才能聚合完成验证,因此,它不是严格意义上的聚合签名(另见文献[9]的分析)。文献[9]通过共享第一个用户选定的随机数,使得验证算法所需的运算个

到稿日期:2010-07-28 返修日期:2010-11-14 本文受863项目(2007AA01Z429,2007AA01Z405),国家自然科学基金重点项目(60633020)资助。

文毅玲(1971—),男,博士生,讲师,主要研究方向为密码学与信息安全,E-mail:ylwen@mailbox.gxnu.edu.cn。

数与参与聚合的签名个数无关，验证效率大大提高，但其安全性基于第一个签名者的诚实性和时钟同步，实现难度较大。针对特殊的安全需求和应用环境，文献[12]提出一个通用的指定接收者的聚合签名方案。文献[13]给出两个无公钥证书的聚合签名方案。文献[14]将聚合签名与代理签名相结合，提出一个聚合代理签名方案。文献[15]将基于RSA问题(单向陷门置换)的有序聚合签名进一步压缩为固定规模，类似于基于身份体制下的文献[9]，使得聚合签名的规模与参与聚合的签名数无关。文献[16]对基于(Public Key Infrastructure) PKI的应用环境，提出一个具有常数个对运算的聚合签名方案，以提高聚合签名的效率。

我们设计出一个新的基于身份的聚合签名方案，其效率在同类方案中具有明显的优势，并且是可证明安全的。本文第2节介绍一些预备知识；第3节介绍对最近由程相国等人提出的聚合签名方案的攻击；第4节描述我们设计的聚合签名方案；第5节给出安全性证明和效率分析；最后是结论。

2 一些预备知识

2.1 可接受的双线性映射

定义 1 设 G 和 T 是 q 阶循环群，q 为一大素数，P 为 G 的生成元，G 中的运算为加法，T 中的运算为乘法。设群 G 和 T 中的离散对数问题是困难的，可接受的双线性映射 $\hat{e}:G\times G\to T$ 是满足以下条件的映射：

1)双线性性：$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$，$\forall a,b\in Z_q^*$，$\forall Q\in G$；

2)非退化性：$\exists P,Q\in G$，满足 $\hat{e}(P,Q)\neq 1_T$；

3)可计算性：$\forall P,Q\in G$，存在有效算法计算 $\hat{e}(P,Q)$。

2.2 困难问题与符号

设 G 是由 P 生成的一个阶为大素数 q 的循环群。并假设 G 中的乘法和求逆运算可以在一个单位时间内完成。设 G 的运算为加法。$\forall a,b,c\in Z_q^*$：

定义 2(Computation Diffie-Hellman Problem, CDHP) 给定 (P,aP,bP)，计算 abP。

定义 3(Decisional Diffie-Hellman Problem, DDHP) 给定 (P,aP,bP,cP)，判定 $c=ab$ 是否成立。如果成立，则称 (P,aP,bP,cP) 为一个 DH 组。

定义 4 称一个群 G 为一个 GDH 群，假如 G 上的 DDHP 是多项式时间可解的，而没有概率多项式时间算法以不可忽略的优势解决 G 中的 CDHP。

定义 5(Gap Diffie-Hellman Groups, GDHG) 设 (G,T) 是两个阶为大素数 q 的群，且 G 和 T 中的 CDHP 是困难的。若存在一个可接受的双线性映射 $\hat{e}:(G\times G)\to T$，则称 (G,T) 为 GDH 群组。

可接受的双线性映射 $\hat{e}$ 的引入，使得 G 中的 DDHP 是容易解决的：因为对任意的 $\forall a,b,c\in Z_q^*$，$\hat{e}(aP,bP)=\hat{e}(P,P)^{ab}$，$\hat{e}(P,cP)=\hat{e}(P,P)^{c}$，所以 $c=ab \bmod Z_q^* \Leftrightarrow \hat{e}(P,P)^{ab}=\hat{e}(P,P)^{c}\Leftrightarrow \hat{e}(aP,bP)=\hat{e}(P,cP)$。

3 对程-刘方案的安全分析

程-刘等的方案描述详见文献[8]，下面给出对程-刘等的方案的攻击：

设 $ID_1,ID_2,\cdots,ID_{n-1}$ 是 $n-1$ 个签名者的身份，ID_n 是伪造者 A 的身份。在基于身份的环境中，A 有权访问 H_2，获得签名者的身份对应公钥 $Q_{ID_1},Q_{ID_2},\cdots,Q_{ID_n}$。攻击者 A 选择 n 个随机数 $r_1,r_2,\cdots,r_n'$ 和 n 条消息 $M_1,M_2,\cdots,M_n$。对于 $i=1,2,\cdots,n-1$，计算：$U_i=r_iQ_{ID_i}$，$h_i=H_1(M_i,U_i)$。然后计算 $U_n=r_n'Q_{ID_n}-\sum_{i=1}^{n-1}h_iQ_{ID_i}-\sum_{i=1}^{n-1}U_i$，$h_n=H_1(M_n,U_n)$，$V=(r_n'+h_n)D_{ID_n}$。那么 $\sigma=(U=\sum_{i=1}^{n}(U_i+h_iQ_{ID_i}),V)$ 就是 A 伪造的 $ID_1,ID_2,\cdots,ID_n$ 对消息 $M_1,M_2,\cdots,M_n$ 的有效聚合签名，因为它能通过验证算法：

$$\begin{aligned}\hat{e}(P,V)&=\hat{e}(P,(r_n'+h_n)D_{ID_n})\\&=\hat{e}(P_{Pub},(r_n'+h_n)Q_{ID_n})\\&=\hat{e}(P_{Pub},r_n'Q_{ID_n}+h_nQ_{ID_n})\\&=\hat{e}(P_{Pub},U_n+\sum_{i=1}^{n-1}h_iQ_{ID_i}+\sum_{i=1}^{n-1}U_i+h_nQ_{ID_n})\\&=\hat{e}(P_{Pub},\sum_{i=1}^{n}(U_i+h_iQ_{ID_i})\\&=\hat{e}(P_{Pub},U)\end{aligned}$$

4 新的聚合签名方案

新的聚合签名方案由6个算法组成，详述如下。

(1) 系统建立：设 (G,T) 是一个 GDH 群组，$\hat{e}:(G\times G)\to T$ 是可计算的双线性映射。$H_1:\{0,1\}^*\times G\to Z_q^*$ 和 $H_2:\{0,1\}^*\to G^*$ 是两个安全 Hash 函数。私钥产生中心(PKG)随机选取 $s\in Z_q^*$，计算 $P_{Pub}=sP$。系统的公开参数是 (G,P,P_{Pub},H_1,H_2)，s 是系统的主密钥。

(2)密钥提取：每个用户把自己的身份 ID_i 发送给 PKG 索取自己的签名密钥。PKG 确认 ID_i 的身份后，计算 $Q_{ID_i}=H_2(ID_i)$，$D_{ID_i}=sQ_{ID_i}$。其中 D_{ID_i} 为第 i 个用户的签名密钥。

(3) 单个签名算法：设 ID_i 要签名的消息为 M_i。ID_i 随机选取 $r_i\in Z_q^*$，计算 $U_i=r_iP_{Pub}$，$h_i=H_1(M_i,U_i)$ 和 $V_i=(r_i,h_i)D_{ID_i}$。ID_i 输出消息 M_i 的签名是 $\sigma_i=(U_i,V_i)(i=1,2,\cdots,n)$。

(4) 单个签名验证：验证者收到签名后，计算 $h_i=H_1(M_i,U_i)$，验证 $\hat{e}(P,V_i)$ 和 $\hat{e}(U_i+h_iP_{Pub},Q_{ID_i})$ 是否相等。

(5) 签名的聚合：计算 $V=\sum_{i=1}^{n}V_i$，则 $\sigma=(U_1,U_2,\cdots,U_n,V)$ 就是 $ID_1,ID_2,\cdots,ID_n$ 对消息 $M_1,M_2,\cdots,M_n$ 的聚合签名。

(6) 聚合签名的验证：当验证者接收到消息及聚合签名时，先计算 $h_i=H_1(M_i,U_i)$，$Q_{ID_i}=H_2(ID_i)$，σ 是正确的聚合签名当且仅当 $\hat{e}(P,V)=\prod_{i=1}^{n}\hat{e}(U_i+h_iP_{pub},Q_{ID_i})$，因为 $\hat{e}(P,V)=\hat{e}(P,\sum_{i=1}^{n}V_i)=\hat{e}(P,\sum_{i=1}^{n}(r_i+h_i)D_{ID_i})=\prod_{i=1}^{n}\hat{e}(P,(r_i+h_i)D_{ID_i})=\prod_{i=1}^{n}\hat{e}(U_i+h_iP_{pub},Q_{ID_i})$

5 安全性和效率

5.1 安全性分析

文献[1]中提出的聚合签名安全模型是基于公钥证书体制下的，不适合基于身份的情形。文献[7-9]各自提出了基于

身份聚合签名的安全模型。这里参考文献[7]中的安全模型。

选定身份聚合签名攻击游戏：

(1) 建立：攻击者 A 被随机地提供一个用户身份的 ID_1。

(2) 询问：

(a)Hash 函数值询问：A 适应性地询问聚合签名算法中的 Hash 函数获得相应的函数值(此处，Hash 函数的行为被视为随机预言机)。

(b)私钥提取询问：A 适应性地询问他选择身份 $ID_i(i\neq 1)$对应的私钥。

(c)签名询问：A 适应性地询问他选择的消息在 ID_1 下的签名。

(3) 回答：A 输出 $k-1$ 附加的身份 $ID_2, ID_3, \cdots, ID_k$。这里 $k\leqslant N$。这些身份将与 ID_1 一起被包含在 A 伪造的聚合签名中。同时，A 输出消息 $M_1, M_2, \cdots, M_k$ 和对应于这些消息的 k 个用户的聚合签名。

如果身份 $ID_1, ID_2, \cdots, ID_k$ 对消息 $M_1, M_2, \cdots, M_k$ 的聚合签名是有效的且是非平凡的(即 A 没有查询身份 ID_1 对消息 M_1 的签名)，那么称 A 伪造成功，并称成功的概率为 A 的优势。其中，概率是遍取所有密钥生成算法和 A 的所有可能性。

定义 6 如果一个聚合签名伪造者 A 运行至多项式时间 t；对 Hash 函数 H_1, H_2 分别做至多 q_{H_1}, q_{H_2} 次询问；对私钥提取做至多 q_E 次询问；对签名预言机做至多 q_S 次询问；且在上述选定身份聚合签名攻击游戏中以至少优势 ε 伪造不超过 N 个用户的聚合签名，则称伪造者 A 在选定身份聚合签名模型中$(t,\varepsilon,q_{H_1},q_{H_2},q_E,q_s,N)$－攻破聚合签名方案。如果没有一个伪造者$(t,\varepsilon,q_{H_1},q_{H_2},q_E,q_s,N)$－攻破它，就称该聚合签名方案在选定身份模型下是抗存在性伪造攻击$(t,\varepsilon,q_{H_1},q_{H_2},q_E,q_s,N)$－安全的。

定理 1 假设群 G 上的 CDHP 是困难的，则提出的基于身份的聚合签名方案，对任意满足下列不等式的 t 和 ε，在选定身份聚合签名模型下是$(t,\varepsilon,q_{H_1},q_{H_2},q_E,q_s,N)$－抗存在性伪造攻击安全的。

$$\varepsilon\geqslant\left(\frac{q}{q-q_{H_1}}\right)^{q_S}\varepsilon'$$

$$t\leqslant\frac{1}{2}(t'-c_G 2(N-1)-c_G(q_{H_1}+q_{H_2}+q_S+q_E))$$

式中，c_G 是 G 中一个标量乘法和加法的时间常量。

证明：假设存在攻击者 A 能够$(t,\varepsilon,q_{H_1},q_{H_2},q_E,q_s,N)$－攻破聚合签名方案，我们将构造一个 t' 时间算法 B 以至少 ε' 的优势解决 G 中的 CDH 问题。这与 G 是一个(t',ε')-GDH 群相矛盾。

给予算法 B：$X=xP\in G$ 和 $Y=yP\in G$。B 的目标是输出 $xY=xyP\in G$。B 在攻击游戏中模拟挑战者与攻击者 A 的交互如下：

(1) 建立：B 将 $P_{Pub}=X$ 发送给 A 作为系统公钥，并提供给 A 一个随机生成的身份 ID_1。

(2) 询问：

1. Hash 函数模拟

H_1 的询问：为回答 A 对 H_1 的询问，B 维护一张由一系列三元组(M_i,U_i,h_i)组成的可扩展的表 L_1。L_1 初始为空。当 A 向 H_1 询问(M_j,U_j)时，B 做如下处理：

(a) 若(M_j,U_j)已在 L_1 的某个组(M_i,U_i,h_i)中，B 就回答 $H_1(M_j,U_j)=h_j$；

(b) 否则，B 随机选取 $h_j\in Z_q^*$，将(M_j,U_j,h_j)增加到 L_1 中，并回答 $H_1(M_j,U_j)=h_j$。

H_2 的询问：为保持一致性，B 需要维护一张由二元组(ID_i,x_i)组成的可扩展的表 L_2。L_2 开始时为空。当攻击者 A 提交身份 ID_j 给 H_2 时，B 做如下处理：

(a) 若 $ID_j=ID_1$，B 回答$(H_2(ID_j)=yP)$；

(b) 若 $ID_j\neq ID_1$ 且已在 L_2 的某个二元组(ID_i,x_i)中，则 B 以 $H_2(ID_j)=x_jP$ 回答；

(c) 若 $ID_j\neq ID_1$ 且不在 L_2 中，B 随机选取 $x_j\in Z_q^*$，将(ID_j,x_j)添加到 L_2 中，并以 $H_2(ID_j)=x_jP$ 回答。

2. 私钥提取模拟

对 A 要询问私钥的身份，总假设 A 已经进行过 H_2 查询。当 A 请求询问身份 ID_j 的私钥时，B 从搜索表 L_2 找到(ID_j,x_j)。若 $ID_j=ID_1$，B 输出拒绝。否则，B 以 $D_{ID_j}=x_j$ 回答，即将 x_j 作为 ID_j 的私钥。

3. 签名模拟

A 询问消息 M 在身份 ID_1 下的签名。B 随机选取 $r_t\in Z_q^*$，$h_t\in Z_q^*$，计算 $U_t=r_tP-h_tP_{Pub}$。搜索 L_1，也分 3 种情况处理：

(a)若有(M_j,U_j,h_j)在 L_1 中使得 $M_j=M$ 且 $U_j=U_t$，但 $h_j\neq h_t$，B 输出失败并停止模拟；

(b)若有(M_j,U_j,h_j)在 L_1 中使得 $M_j=M,U_j=U_t$ 且 $h_j=h_t$，计算 $V_t=r_t$yP；

(c)若没有(M_j,U_j,h_j)在 L_1 中使得 $M_j=M,U_j=U_t$，添加(M_j,U_t,h_t)到 L_1 中，计算 $V_t=r_tyP$。

除(a)外，签名单个签名(U_t,V_t)能通过验证算法，因为 $\hat{e}(P,V_t)=\hat{e}(P,r_tyP)=\hat{e}(r_tP,yP)=\hat{e}(U_t+h_tP_{Pub},Q_{ID_1})$。

(3) 输出：如果上述模拟没有因失败而停止，A 将在 t 时间表内，以至少优势 ε 伪造出一个 $k(k\leqslant N)$个用户的非平凡的有效聚合签名。不妨设 $\sigma=(U_1,U_2,\cdots U_k,V)$是伪造的 $ID_1, ID_2, \cdots, ID_k$ 对消息 $M_1, M_2, \cdots, M_k$ 的聚合签名，且 A 没有查询身份 ID_1 对消息 M_1 的签名。

那么 B 每重放一次预言机，就会获得另一个非平凡的有效聚合签名。假设对聚合签名中的数据进行适当调整，就会有 $\sigma'=(U_1',U_2',\cdots,U'_{k'},V')$是 $ID_1, ID_2', \cdots, ID'_{k'}$ 对消息 $M_1, M_2'\cdots M'_{k'}$的有效而非平凡的聚合签名 $k'(k'\leqslant N)$。由分叉引理[20]，$h'_1\neq h_1$，B 搜索表 L_1 和 L_2，找到(M_i,U_i,h_i)和(ID_i,x_i)以及(M_i',U_i',h_i')和(ID_i',x_i')，分别计算出 $V_i=x_iU_i+h_ix_iX(i=1,2,\cdots,k)$和 $V'_i=x_i'U_i'+h'_ix_i'X(i=1,2,\cdots,k)$，则$(U_i,V_i)$和$(U_i',V_i')$分别是 ID_i 对 M_i 和 ID_i'对 M_i'的有效签名，因为它们能通过验证算法：

$$\begin{aligned}\hat{e}(P,V_i)&=\hat{e}(P,x_iU_i+h_ix_iX)=\hat{e}(x_iP,U_i+h_iX)\\&=\hat{e}(Q_{ID_i},U_i+h_iP_{Pub})\\\hat{e}(P,V_i')&=\hat{e}(P,x_i'U_i'+h_i'x_i'X)\\&=\hat{e}(x_i'P,U_i'+h_i'X)\\&=\hat{e}(Q_{ID'_i},U_i'+h_i'P_{Pub})\end{aligned}$$

又由于

$$V=\sum_{i=1}^{k}V_i=(r_1+h_1)D_{ID_1}+\sum_{i=2}^{k}V_i$$

$V'=\sum_{i=1}^{k'}V_i'=(r_1+h_1')D_{ID_1}+\sum_{i=2}^{k'}V_i'$

得到：

$V_1=(r_1+h_1)D_{ID_1}=-V-\sum_{i=2}^{k}V_i$

$V_1'=(r_1+h'_1)D_{ID_1}=V'-\sum_{i=2}^{k'}V_i'$

从而有 $V_1-V_1'=-(h_1D_{ID_1}-h_1'D_{ID_1})$，$xyP=D_{ID_1}=(h_1-h_1')^{-1}(V_1-V_1')$为算法 B 的最终输出。

下面计算求解 CDHP 的时间和概率。

算法 B 求解 CDHP 的成功概率取决于 B 模拟挑战者成功的概率和攻击者 A 成功的概率 ε。即取决于如下几个事件：

E_1：B 不放弃 A 的单个签名询问。

E_2：当 E_1 发生时，A 伪造出一个有效的非平凡的聚合签名。

E_3：当 E_2 发生时，B 重放预言机过程中不放弃签名询问。

算法 B 成功的概率为 $\Pr[E_1\wedge E_2\wedge E_3]=\Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_1\wedge E_2]$。

对于 A 的签名询问，为了简化，不直接求 L_1 中的(M_j,U_j,h_j)使得 $M_j=M$ 且 $U_j=U_t$，但 $h_j\neq h_t$ 的概率，而放大到考虑 L_1 中没有(M_j,U_j,h_j)使得 $M_j=M,U_j=U_t$ 的概率。由于 L_1 中只有 q_{H_1} 个元是在对 H_1 询问时产生的，由签名询问产生的不在 L_1 中的元都能成功模拟签名。因此，每次签名询问 L_1 中有(M_j,U_j,h_j)使得 $M_j=M,U_j=U_t$ 的概率至多是$\frac{q_{H_1}}{q}$，那么每次签名询问，B 不放弃的概率至少是 $1-\frac{q_{H_1}}{q}$，从而 q_S 次询问不放弃的概率为 $\Pr[E_1]\geqslant(1-\frac{q_{H_1}}{q})^{q_S}$；由于 B 对 Hash 和私钥提取询问的回答都是均匀随机的，因此在 E_1 发生的条件下，A 认为是在真实环境中进行的，从而有 $\Pr[E_2|E_1]\geqslant\varepsilon$，于是有$\Pr[E_1\wedge E_2\wedge E_3]\geqslant\Pr[E_3|E_1\wedge E_2](1-\frac{q_{H_1}}{q})^{q_S}\varepsilon$。重放预言机，概率不变。因此，$\Pr[E_1\wedge E_2\wedge E_3]\geqslant(1-\frac{q_{H_1}}{q})^{q_S}\varepsilon\geqslant\varepsilon'$为所求。$B$ 算法运行的时间是 A 运行的时间 t 加上运行 Hash 和签名查询 $q_{H_1}+q_{H_2}+q_S+q_E$ 的时间，B 求解 CDHP 的时间以及重放预言机的时间。于是，$2t+c_G2(N-1)+c_G(q_{H_1}+q_{H_2}+q_S+q_E)\leqslant t'$正为所求。

5.2 效率

从计算和通信开销两方面进行分析。考虑同类的基于身份的无序聚合签名，对于 n 个签名的聚合：新方案的聚合签名是$(U_1,U_2,\cdots,U_n,V)$，与文献[7]的通信规模一样大，比文献[9]的(ω,S,T)通信量要大。但与不聚合相比，通信节约了$(n-1)|G|$(其中$|G|$表示群 G 中元素的通信规模)。在计算量上，新方案与文献[7]所需要的对运算随参与聚合的签名数量线性增长。但新方案比文献[7]在签名和验证时各少一次对运算，并使用两个普通的密码 Hash 函数，而文献[7]是基于文献[10]提出的签名方案，两个 Hash 函数之一是 MapToPoint 的 Hash 函数，文献[6]指出这类函数可以由普通的密码 Hash 函数来构造，但构造一个安全的 MapToPoint 的 Hash 函数比较复杂且运算效率低。文献[17]进一步指出：考虑域 $F_{3^{163}}$ 上由方程 $y^2=x^3-x+1$ 定义的椭圆曲线，此曲线上导出的 GDH 群提供 1551-比特离散对数安全性，求 MapToPoint 的 Hash 函数值需要解至少一个二次或三次方程，比 Z_q^* 上的求逆需要更多开销。此外，目前最好的算法，一个是对运算的开销大约为 11110 个域 $F_{3^{163}}$ 上的乘法，一个是点乘的开销大约为几百个域 $F_{3^{163}}$ 上的乘法。因此，我们的方案要优于文献[7]中的方案。尽管文献[9]使用了 MapToPoint 的 Hash 函数，但聚合验证时只要 3 个对运算，与参与聚合的签名数量无关，因此新方案计算效率比文献[9]低。不过，文献[9]中方案的安全性是基于第一个签名者的诚实性和时钟同步基础之上，实现难度较大。表 1 给出同类方案的计算效率比较。

表 1　同类方案的计算效率比较

	密钥生成	签名	验证	聚合	聚合验证
[6]	1Pm	2Pm+1MTP+1Ad	3Pa+1Mu+1MTP	(n−1)Ad	(n+2)Pa+nMTP+nMu+(n−1)Ad
[9]	2Pm	4Pm+1MTP	3Pa+1Pm+1Ad	2(n−1)Ad	3Pa+(n−1)Pm+(2n−1)Ad
[Ours]	1Pm	2Pm	2Pa+1Pm+1Ad	(n−1)Ad	(n+1)Pa+nPm+nAd

其中，Pa 表示对运算，Pm 表示群 G 上的点乘，Ad 表示群 G 上的加法，MTP 表示映射到 G 中的点的 MapToPoint 的 Hash 函数，Mu 表示群 T 中的乘法。

结束语　设计出一个新的基于身份的聚合签名，该方案在 CDH 困难性假设下，在随机预言机模型下证明是抗存在性伪造攻击安全的。其计算开销在同类方案中有较大的优势。基于身份的签名，以签名人员的身份作为验证公钥，解决了公钥管理问题，但基于身份的密码体制中私钥托管问题仍需解决，下一步将致力于这一问题。

参 考 文 献

[1] Wang Chi-hung, Kuo Yan-sheng. An Efficient Contract Signing Protocol Using the Aggregate Signature Scheme to Protect Signers' Privacy and Promote Reliability[C]// Proc. of ACM SIGOPS Operating Systems Review 2005. Brighton, United Kingdom, 2005, 39: 66-79

[2] Yao Dan-feng, Tamassia R. Cascaded Authorization with Anonymous-signer Aggregate Signatures[C]// Proc. of the 2006 IEEE Workshop on Information Assurance. West Point, New York, 2006: 84-91

[3] Wang Sheng-bao, Cao Zhen-fu, Wang Qin, et al. Authenticated Key Agreement Protocol Using Bilinear Aggregate Signatures[C]// Proc. of Global Mobile Congress 2005. Delson Group Inc, 2005: 328-332

[4] Zhu Hua-fei, Bao Feng, Li Tie-yan, et al. Sequential Aggregate Signatures for Wireless Routing Protocols[C]// Proc. of IEEE Wireless Communications and Networking Conference 2005. New Orleans, LA USA, 2005: 2436-2439

[5] Shao Zu-hua. Enhanced Aggregate Signatures from Pairings[C]// Proc. of State Key Laboratory of Information Security Conference on Information Security and Cryptology 2005. Berlin: Springer-Verlag, 2005: 140-149

(下转第 80 页)

组(4)中式(4.3)和式(4.4)的验证,但 B 要找到$\langle T_{1_i}, t_i\rangle_k$,并通过式(4.2)的验证则是困难的,因为根据式(4.2),有

$$\prod_{i=1}^{k} T_{1_i}^{t_i} = T_1'(Z^k)^c (R_0^{s_0} R_1^{s_1} S^{s_v} h^{-s_{ew}})^{-1} \pmod n$$

根据哈希函数的抗碰撞性,c 对应唯一的 T_1',而 c, s_0, s_1, s_v, s_{ew} 均已给定,故 $d = T_1'(Z^k)^c (R_0^{s_0} R_1^{s_1} S^{s_v} h^{-s_{ew}})^{-1} \pmod n$ 为给定值。因此如果 B 可找到$\langle T_{1_i}, t_i\rangle_k$,使得 $\prod_{i=1}^{k} T_{1_i}^{t_i} = d \pmod n$,则与引理 1 相矛盾。

综上,除非签名者的密钥和 DAA 证书同时泄漏,否则改进方案中多重签名不可伪造。证毕。

计算开销方面,基于离散对数的多重签名主要开销在于签名过程中的指数运算次数。假设共有 k 个签名者,则在原方案中共需进行 $16k+11$ 次指数运算,而在改进方案中需 $15k+10$次,因此性能也得以提高。特别是改进方案显著削减了签名收集者的运算开销(由原 $6k$ 次缩减为 0 次)。收集者通常会成为多重签名方案中的性能瓶颈,这一点对提高方案的效率有着实际意义。通信开销方面,改进方案较原方案增加了一轮签名者之间的交互,因此开销有所增加,之后的工作将就此方面做进一步优化。

结束语 本文对一种基于可信计算技术的多重签名方案进行了安全分析,表明其不能抵抗签名伪造攻击。分析了该安全缺陷产生的原因,并给出一种可证安全的改进方案。研究结果表明,对多重签名方案,对手的攻击手段往往更为多样,因此仅仅考虑部分签名的安全性是不够的,对于部分签名合成过程中可能存在的安全隐患也必须加以重视。

参 考 文 献

[1] Lu R B, He Dake, Wang C J. Security analysis and improvement of a new threshold multi-proxy multi-signature scheme [J]. Journal of Electronics, 2008, 25(3): 372-377

[2] Meng Tao, Zhang Xiao-ping, Yu Long-jiang, et al. An ID-Based Blind Multisignature Scheme [A]// Proc of the 3rd International Conference on Innovative Computing Information and Control [C]. Washington, USA: IEEE Computer Society, 2008: 556-568

[3] 王晓峰,张璟,王尚平. 多重数字签名及其安全性证明[J]. 计算机学报,2008,31(1):176-183

[4] Alexandra B, Craig D, O'Neil A. Ordered multisignatures and identity-based sequential aggregate signatures with applications to secure routing [A]// Proc of the 14th ACM Conference on Computer and Communications Security [C]. Alexandria, USA: ACM Press, 2007: 276-285

[5] Bellare M, Neven G. Multi-Signatures in the plain public key model and a general forking lemma [A]// Proc of the 13th ACM Conference on Computer and Communication Security [C]. Alexandria, USA: ACM Press, 2006: 390-399

[6] Hao Li-ming, Yang Shu-tang, Lu Song-nian, et al. Efficient and secure multiSignature scheme based on trusted computing [J]. Wuhan University Journal of Natural Sciences, 2008, 13(2): 180-184

[7] 张焕国,罗捷,金刚,等. 可信计算研究进展[J]. 武汉大学学报:理学版,2006,52(5):513-518

[8] Brickell E, Camenisch J, Chen Liqun. Direct anonymous attestation [A]// Proc of the 11th ACM Conference on Computer and Communication Security [C]. Washington, USA: ACM Press, 2004: 132-145

[9] Cramer R, Shoup V. Signature schemes based on the strong RSA assumption [J]. ACM Transactions on Information and System Security (ACM TISSEC), 2000, 3(3): 161-185

[10] Trusted Computing Group. TCG Specification Architecture Overview[EB/OL]. http://www.trustedcomputinggroup.org, 2009

[11] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols[J]. LNCS, 2003, 2576: 268-289

(上接第 57 页)

[6] Boneh D, Gentry C, Lynn B, et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps[C]// Proc. of the 22th Annual International Conference on the Theory and Applications of Cryptographic Techniques 2003. Berlin: Springer-Verlag, 2003: 416-432

[7] Xu Jing, Zhang Zhen-feng, Feng Deng-guo. ID-Based Aggregate Signatures from Bilinear Pairings[C]// Proc. of the Chinese-American Networking Symposium 2005. Berlin: Springer-Verlag, 2005: 110-119

[8] 程相国,刘景美,王新梅. m_挠群上一种基于身份的聚合签名方案[J]. 西安电子科技大学学报,2005,32(3):427-431

[9] Gentry C, Ramzan Z. Identity-based Aggregate Signatures[C]// Proc. of the 9th International Conference on Practice and Theory in Public Key Cryptography 2006. Berlin: Springer-Verlag, 2006: 257-273

[10] Sakai R, Ohgish K, Kasahara M. Cryptosystems Based on Pairing[C] //Proc. of 2000 Symposium on Cryptography and Information Security. Okinawa, Japan, 2000: 26-28

[11] Cheng Xiang-guo, Liu Jing-mei, Wang Xin-mei. Identity-Based Aggregate and Verifiably Encrypted Signatures from Bilinear Pairing[C] // Proc. of The 2005 International Conference on Computational Science and Applications. Berlin: Springer-Verlag, 2005: 1046-1054

[12] Mihara A, Tanaka K. Universal Designated-verifier Signature with Aggregation[C] // Proc. of the 2th International Conference In IT & Application 2005. Sydney, Australia, 2005, II: 514-519

[13] Gong Zheng, Long Yu, Hong Xuan, et al. Two Certificateless Aggregate Signatures From Bilinear Maps[C]// Proc. of the International Association for Computer and Information Science 2007. Toowoomba, Australia, 2007: 188-193

[14] Li Jin, Kim K, Zhang Fang-guo, et al. Aggregate Proxy Signature and Verifiably Encrypted Proxy Signature[C]// Proc. of International Conference on Provable Security 2007. Berlin: Springer-Veralg, 2007: 208-217

[15] Mu Yi, Susilo W, Zhu Hua-fei. Compact Sequential Aggregate Signatures[C]// Proc. of the 22th Annual ACM Symposium on Applied Computing. Seoul, Korea, 2007: 249-253

[16] Wen Yiling, Ma Jian-feng. An Aggregate Signature Scheme with Constant Pairing Operations[C]// Proc. of the 2008 International Conference on Computer Science and Software Engineering. 2008, 3: 830-833

[17] Zhang Fang-guo, Safavi-Naini R, Susilo W. An Efficient Signature Scheme from Bbilinear Pairings and Its Applications[C]// Proc. of the 7th International Conference on Practice and Theory in Public Key Cryptography 2004. Berlin: Springer-Veralg, 2004: 277-290