高效的基于身份在线/离线签密方案

于 刚 韩文报
(信息工程大学信息工程学院 郑州 450002)

摘 要 基于身份密码体制提出一个在线/离线签密方案。相比已有的方案,该方案在线、离线计算效率高、离线存储量小、在线密文长度短。并且,在 l-BDHI 难题和 l-SDH 难题假设下,该方案是随机预言模型下可证安全的。

关键词 在线/离线签密,基于身份密码体制,随机预言模型,双线性对
中图法分类号 TP309 **文献标识码** A

Efficient Identity Based Online/Offline Signcryption Scheme

YU Gang HAN Wen-bao
(School of Information Engineering, Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, China)

Abstract We proposed an efficient identity based online/offline signcryption scheme with shorter ciphertext. Under the l-BDHI assumption and l-SDH assumption, the scheme can be proved secure in the random oracle model.

Keywords Online/offline signcryption, Identity based cryptography, Random oracle model, Bilinear pairing

1 引言

保证消息的机密性、提供消息的认证性和不可否认性是信息安全的两个主要目标。通常,数字加密能实现消息的秘密传输和数据的秘密储存,电子签名能提供消息的完整性、认证性和不可否认性。传统的"先签名后加密"能保证消息在复杂、开放的网络信道上既保密又认证地传输,它消耗的代价是单纯电子签名和数字加密所需代价的总和,代价较高。为了提高效率、节省带宽,Zheng[1]提出"签密"的概念。签密可以在一个合理的逻辑步骤内同时完成签名和加密两项功能,代价要远远低于传统的"先签名后加密",是实现既保密又认证传输消息的理想方法。

基于身份的密码体制由 Shamir[2]在 1984 年提出。在基于身份的密码体制中,任意给定的字符串都可以作为用户的公钥,例如用户的身份(ID)可以包括身份证号、家庭住址、电子邮箱、社会保证金号等任何可以唯一确定用户身份的字符串或其组合。这样用户的公钥即是他们的身份或由身份简单变换而来,不需要公钥目录、公钥证书。

在线/离线的思想最先由 Even 等[3]在电子签名中引入。Even 等[3]将签名过程分为两个阶段:离线阶段(给定消息之前)和在线阶段(给定消息之后)。在线/离线签名方案非常实用,特别是当签名者拥有较强的计算能力但是给定消息后反应时间很少时,在线/离线签名方案可以使签名者从容应对连续密集的签名请求。在线/离线签名方案尤其适用于无限传感网络和智能卡应用系统,计算量较大的离线阶段可以在无限传感网络的基站(或者智能卡应用系统的智能卡)上运行,在线阶段可以在一个计算能力较弱的处理器上运行(无限传感网络的结点)。

在线/离线的思想同样适用于签密,最早由 An 等[4]引入。同在线/离线签名类似,计算难度大的运算,例如指数运算、双线性对运算等,都应该在离线阶段完成,在线阶段运算要求简单快速。此外,离线阶段的运算应该与签密的消息独立,因为离线阶段的运算在给定消息之前进行。An 等在文献[4]中并没有给出具体的在线/离线签密方案。Zhang 等[5]利用对称加密方案给出第一个具体的在线/离线签密方案。此后,Xu 等[6]也给出一个在线/离线签密方案。第一个基于身份的在线/离线签密方案由 Sun 等[7]给出。上述的在线/离线签密方案存在一个很大的缺陷:离线阶段需要给定接收者的信息(公钥、身份等)。此缺陷很大程度上阻碍了在线/离线签密方案在实际中的应用。Liu 等[8]针对此缺陷提出一个实用的在线/离线签密方案,该方案在离线阶段与接收者的信息独立。

本文基于 Liu 等[8]的方案,提出一个更高效的方案。本文方案具有更高的计算效率、更小离线存储需求和更短的在线密文长度。并且,在 l-BDHI 难题和 l-SDH 难题假设下,本文方案是随机预言模型下可证安全的。

2 双线性对及其相关困难假设

2.1 双线性对

设$(G_1,+)$、$(G_2,\cdot)$为 q 阶循环群。一个双线性映射$\hat{e}$:$G_1\times G_1\rightarrow G_2$ 称作双线性对[9],若满足以下性质:

双线性性:对于任意的 $P,Q\in G_1$ 和任意的 $a,b\in Z_q^*$,有$\hat{e}$

到稿日期:2011-09-08 返修日期:2012-01-18 本文受国家自然科学基金项目(61003291),国家"863"计划基金项目(2009AA01Z417)资助。
于 刚(1984—),男,博士生,主要研究方向为信息安全和网络密码,E-mail:gyu1010@126.com;韩文报(1963—),男,教授,博士生导师,主要研究方向为信息安全和网络密码。

$(aP,bQ)=\hat{e}(P,Q)^{ab}$。

非退化性：存在 $P,Q\in G_1$，满足 $\hat{e}(P,Q)\neq 1$。

可计算性：对所有的 $P,Q\in G_1$，$\hat{e}(P,Q)$ 可以在多项式时间内有效计算出来。

2.2 相关困难假设

本文的方案基于以下两个难题。目前为止，这两个问题都没有多项式时间的算法可以解决。

设 $(G_1,G_2,q,\hat{e})$ 是一个双线性对系统，$\hat{P}$ 是群 $(G_1,+)$ 的一个生成元。

定义 1 l-SDH 问题（l-Strong Diffie-Hellman problem）[10]

给定 $(\hat{P},a\hat{P},a^2\hat{P},\cdots,a^{l-1}\hat{P},a^l\hat{P})$，其中 $a,l\in Z_q^*$，群 G_1 中的 l-SDH 问题是输出 $(b,\frac{1}{b+a}\hat{P})$，$b\in_R Z_q^*$。

定义 2 l-BDHI 问题（l-Bilinear Diffie- Hellman Inversion problem）[11]

给定 $(\hat{P},a\hat{P},a^2\hat{P},\cdots,a^{l-1}\hat{P},a^l\hat{P})$，其中 $a,l\in Z_q^*$，群 G_1 中的 l-BDHI 问题是输出 $(\hat{P},\hat{P})^{\frac{1}{a}}$。

3 基于身份在线/离线签密算法构成及安全模型

3.1 算法构成

基于身份在线/离线签密由 5 个算法组成：系统初始化算法（Setup）、密钥提取算法（Extract）、离线签密算法（Offline-Signcrypt）、在线签密算法（Online-Signcrypt）和解签密算法（Unsigncrypt）。

Setup.：此算法由 PKG 完成。输入安全参数 1^k，输出系统主密钥 s 和系统参数 $Params$。PKG 保密 s，公开系统参数 $Params$。

Extract：给定身份信息 ID_U，PKG 利用系统主密钥 s 和系统参数 $Params$ 输出私钥 D_{ID_U}，并将私钥 D_{ID_U} 秘密交给用户 ID_U。

Offline-Signcrypt：给定发送者 ID_S 的私钥 D_{ID_S}，输出离线密文 δ_{off}。

Online-Signcrypt：给定明文消息 m、接收者的身份 ID_R 以及离线密文 δ_{off}，输出在线密文 δ_{on}。

Unsigncrypt：给定在线密文 δ_{on}、接收者的私钥 D_{ID_R} 和发送者的身份 ID_S，输出明文消息 m 或者输出表示解签密失败的符号 $\perp$。

3.2 安全模型

定义 3 如果没有任何多项式有界时间的敌手以不可忽略的优势赢得以下游戏，则称一个基于身份的在线/离线签密方案在适应性选择密文攻击下不可区分（IND -CCA2）。

Setup. 输入安全参数 1^k，然后挑战者 C 运行算法 Setup(1^k)，最后将系统参数 $Params$ 发送给敌手 A。

Phase 1. 在此阶段，敌手 A 执行多项式有界次如下询问：

Extract 询问：A 给定一个身份 ID_U，C 返回私钥 D_{ID_U} 给 A。

Signcrypt 询问：A 给定两个身份 ID_S、ID_R 和一个明文消息 m。C 返回在线密文 δ_{on}。

Unsigncrypt 询问：A 给定两个身份 ID_S、ID_R 和在线密文 δ_{on}。C 利用接收者的私钥 D_{ID_R} 返回明文 m 或解签密失败符号 $\perp$。

Challenge. A 生成两个相同长度的明文 m_0、m_1 和希望挑战的两个身份 ID_S^*、ID_R^*。ID_R^* 不能是已经执行过 Extract 询问的身份。C 随机选择 $b\in\{0,1\}$，对明文 m_b 签密并将在线密文 δ_{on}^* 发送给 A。

Phase 2. 在此阶段，A 继续执行多项式有界次询问。但是不能对 ID_R^* 执行 Extract 询问，也不能对密文 δ_{on}^* 执行 Unsigncrypt 询问。

Guess. 最后，A 输出一个值 b' 作为对 b 的猜测。如果 $b'=b$，A 赢得游戏。A 的优势定义为：$Adv(A)=|2P[b'=b]-1|$。

定义 4 如果没有任何多项式有界时间的敌手以不可忽略的优势赢得以下游戏，则称一个基于身份在线/离线签密方案在适应性选择消息攻击下抗存在性伪造（EUF -CMA）。

Setup. 输入安全参数 1^k，挑战者 C 运行算法 Setup(1^k)，将系统参数 $Params$ 发送给 A。

Probe. 此阶段，敌手 A 执行多项式有界次 Extract 询问、Signcrypt 询问、Unsigncrypt 询问。

Forge. 最后，A 输出两个身份 ID_S^*、ID_R^* 以及一个在线密文 δ_{on}^*。其中 $(\delta_{on}^*,ID_S^*,ID_R^*)$ 不是 A 由 Signcrypt 询问得到，并且 A 没有对 ID_S^* 执行过 Extract 询问。如果对 $(\delta_{on}^*,ID_S^*,ID_R^*)$ 解签密，结果不是符号 $\perp$，则 A 赢得游戏。A 的优势在于他胜利的概率。

4 具体方案

具体方案算法描述如下：

Setup：输入安全参数 1^k，PKG 选取阶数为大素数 q 的两个循环群 $(G_1,+)$ 和 $(G_2,\cdot)$，群 G_1 的生成元为 P，双线性对为 $\hat{e}:G_1\times G_1\to G_2$；随机选择主密钥 $s\in Z_q^*$，计算系统公钥 $P_{Pub}=sP$；定义密码意义上安全的 3 个 Hash 函数：

$H_0:\{0,1\}^{n_1}\to Z_q^*$

$H_1:\{0,1\}^{n_2}\times G_1^*\times G_1^*\times G_1^*\times Z_q^*\to Z_q^*$

$H_2:G_2^*\times G_1^*\times G_1^*\times G_1^*\to\{0,1\}^{n_2}\times Z_q^*\times\{0,1\}^{n_1}$

其中，n_1，n_2 分别代表身份及消息的比特长度；最后 PKG 保密主密钥 s，公开系统参数。

Extract：用户将其身份信息 ID_U 提交给 PKG，PKG 计算 $D_{ID_U}=\frac{1}{s+Q_U}P$，其中 $Q_U=H_0(ID_U)$ 为用户公钥，最后将私钥 D_{ID_U} 秘密交给用户 ID_U。用户 ID_U 可以计算并存储 $P_{ID_U}=H_0(ID_U)P+P_{Pub}$，以备后用。

Offline-Signcrypt：此阶段，发送者 ID_S 利用其私钥 D_{ID_S} 执行以下步骤：

随机选择 $x,u,\alpha,\beta\in Z_q^*$。

计算 $X=\hat{e}(P,P)^x$、$T_0=x(\alpha\cdot P+P_{Pub})$。

计算 $T_1=x\beta\cdot P$、$V=D_{ID_S}-u\cdot P$。

输出离线密文 $\sigma_{off}=(X,T_0,T_1,V,x,u,\alpha,\beta)$。

Online-Signcrypt：此阶段，发送者 ID_S 得到接收者的身

份 ID_R 及要发送的消息 m 后，

计算 $v=\beta^{-1}(H_0(ID_R)-\alpha) \bmod q$。

计算 $\sigma=h_1 x\beta+u \bmod q$，其中 $h_1=H_1(m,T_0,T_1,V,v)$。

计算 $\delta=m\|\sigma\|ID_S\oplus h_2$，其中 $h_2=H_2(X,T_0,T_1,V)$。

输出在线密文 $\sigma_{on}=(T_0,T_1,V,\delta,v)$。

Unsigncrypt：收到密文 $\sigma_{on}=(T_0,T_1,V,\delta,v)$ 后，接收者 ID_R 执行以下步骤：

计算 $X=\hat{e}(T_0+vT_1,D_{ID_R})$。

计算 $m\|\sigma\|ID_S=\delta\oplus h_2$，其中 $h_2=H_2(X,T_0,T_1,V)$。

验证 $\hat{e}(V+\sigma P,P_{ID_S})=\hat{e}(P,P)\hat{e}(T_1,P_{ID_S})^{h_1}$，其中 $h_1=H_1(m,T_0,T_1,V,v)$。若成立，则返回消息 m，否则返回 $\perp$。

5 性能分析

5.1 安全分析

第 3.2 节定义的安全模型是在随机预言模型下建立的，因此在下面的证明中假设方案中用到的 Hash 函数是理想的随机预言机。此外，设敌手对随机预言机 H_i 分别询问 q_i 次($i=0,1,2$)，敌手进行 q_s 次签密询问和 q_u 次解签密询问。

机密性

定理 1 在随机预言模型下，若存在一个 IND-CCA2 敌手 A 能够在多项式时间内以优势 ε 赢得游戏，则存在一个挑战者 C 能够在多项式时间内至少以下面的优势解决 l-BDHI 问题：

$$\frac{1}{q_0}\frac{1}{q_2}\left(1-\frac{q_s(q_s+q_1)}{q}\right)\left(1-\frac{q_u}{q}\right)\varepsilon$$

证明：设 $(\hat{P},a\hat{P},a^2\hat{P},\cdots,a^{l-1}\hat{P},a^l\hat{P})$(其中 $a,l\in Z_q^*$)是一个 l-BDHI 实例，C 需要输出 $\hat{e}(\hat{P},\hat{P})^{1/a}$。

Setup. 开始，C 随机选择 $\pi\in\{1,\cdots,q_0\}$，以及 $I_\pi,w_1,\cdots,w_{\pi-1},w_{\pi+1},\cdots,w_l\in Z_q^*$。对任意 $i\in\{1,\cdots,l\}\backslash\{\pi\}$，$C$ 计算 $I_i=I_\pi-w_i$。C 构造多项式 $f(z)=\prod_{i=1,i\neq\pi}^{l}(z+w_i)=\sum_{i=0}^{l-1}c_i z^i$ 得到 $c_0,\cdots,c_{l-1}\in Z_q^*$。$C$ 计算 $P=\sum_{i=0}^{l-1}c_i a^i\hat{P}=f(a)\hat{P}$ 作为选取的群 G_1 的生成元。类似地，对任意 $i\in\{1,\cdots,l\}\backslash\{\pi\}$，$C$ 构造多项式 $f_i(z)=f(z)/(z+w_i)=\sum_{j=0}^{l-2}d_{i,j}z^j$ 得到 $d_{i,1},\cdots,d_{i,l-2}\in Z_q^*$，计算 $\hat{H}_i=\sum_{j=0}^{l-2}d_{i,j}(a^j\hat{P})=\frac{f(a)}{a+w_i}\hat{P}=\frac{1}{a+w_i}P$。

最后，C 令 $P_{Pub}=-(a+I_\pi)P$，其中 $aP=af(a)\hat{P}$。此时系统主密钥为 $s=-(a+I_\pi)$，C 也不知道。简单计算可知，$-\hat{H}_i=\frac{1}{I_i+s}P$，$C$ 将 $(i,I_i,-\hat{H}_i)$ 添加到表 L_I 中。此外，C 还要维护 $L_i(i=1,2)$ 两张表，分别用于记录随机预言机 H_i 的询问/回答的条目。最后，C 将公开参数发送给 A。

Phase 1. C 如下回答敌手 A 的询问：

$H_0(ID_i)$ 询问：对于第 $i\in\{1,\cdots,q_0\}$ 次询问，C 在表 L_I 中搜寻 $(i,I_i,-\hat{H}_i)$，并返回 I_i。

$H_1(m,T_0,T_1,V,v)$ 询问：若 $((m,T_0,T_1,V,v),h_1)\in L_1$，返回 h_1；否则随机选取 $h_1\in Z_q^*$，并将 $((m,T_0,T_1,V,v),h_1)$ 添加到 L_1 中，返回 h_1。

$H_2(X,T_0,T_1,V)$ 询问：若 $((X,T_0,T_1,V),h_2)\in L_2$，返回 h_2；否则随机选取 $h_2\in\{0,1\}^{n_2}\times Z_q^*\times\{0,1\}^{n_1}$，并将 $((X,T_0,T_1,V),h_2)$ 添加到 L_2 中，返回 h_2。

Extract(ID_i) 询问：若 $ID_i=ID_\pi$，则终止模拟；否则在表 L_I 中搜寻 $(i,I_i,-\hat{H}_i)$，并返回 $-\hat{H}_i$。

Signcrypt(ID_i,ID_j,m) 询问：假设 A 在此前执行过 $H_0(ID_i)$、$H_0(ID_j)$ 询问以及 Extract(ID_i) 询问，需要考虑两种情况。

情形 1：$i\neq\pi$

C 可以得到 ID_i 的私钥，从而可以严格按照方案给出密文。

情形 2：$i=\pi$

通常，都假定发送者和接收者不同，即 $j\neq\pi$，因此 C 可以得到接收者 ID_j 的私钥 $D_{ID_j}=-\hat{H}_j$，并生成密文如下：

随机选择 $x,\alpha,\beta,\sigma\in Z_q^*$、$V\in G_1$。

计算 $T_0=x(\alpha\cdot P+P_{Pub})$、$T_1=x\beta\cdot P$。

计算 $v=\beta^{-1}(H_0(ID_R)-\alpha) \bmod q$。

计算 $X=\hat{e}(T_0+vT_1,D_{ID_j})$、$\delta=m\|\sigma\|ID_i\oplus h_2$，其中 $h_2=H_2(X,T_0,T_1,V)$。

输出在线密文 $\sigma_{on}=(T_0,T_1,V,\delta,v)$。

Unsigncrypt(ID_i,ID_j,δ_{on}) 询问：同样 C 需要考虑两种情况。

情形 1：$j\neq\pi$

C 可以得到 ID_j 的私钥，从而可以严格按照方案恢复明文。

情形 2：$j=\pi$

C 按以下步骤遍历表 L_2 中记录 (X,T_0,T_1,V,h_2)：

计算 $m\|\sigma\|ID_i=\delta\oplus h_2$。

若 $ID_i=ID_\pi$ 或者 $ID_i\notin L_I$，移到表 L_2 中下一条记录并重新开始；否则，在表 L_I 中寻找 $(i,I_i,*)$，令 $H_0(ID_i)=I_i$。

若 $((m,T_0,T_1,V,v),h_1)\in L_1$，令 $h_1=H_1(m,T_0,T_1,V,v)$；否则移到表 L_1 中下一条记录并重新开始。

若 $\hat{e}(V+\sigma P,P_{ID_i})=\hat{e}(P,P)\hat{e}(T_1,P_{ID_i})^{h_1}$，返回 m，否则移到表 L_2 中下一条记录且重新开始。

如果遍历表 L_2 中所有记录后还是没有消息返回，则返回符号 $\perp$。

Challenge. 敌手 A 输出两个挑战的身份 (ID_S^*,ID_R^*) 和两个消息 (m_0,m_1)，其中 A 不能询问 ID_R^* 的私钥。如果 $ID_R^*\neq ID_\pi$，C 终止这个模拟；否则 C 随机选取 $b\in\{0,1\}$，并生成如下对消息 m_b 的密文：

随机选择 $\alpha^*,\beta^*,v^*,\sigma^*\in Z_q^*$。

计算 $T_0=\alpha^*\cdot P$、$T_1=\beta^*\cdot P$。

计算 $v=\beta^{-1}(H_0(ID_R)-\alpha) \bmod q$。

随机选择 $V^*\in G_1$、$\delta^*\in\{0,1\}^{n_2}\times Z_q^*\times\{0,1\}^{n_1}$。

输出挑战密文 $\delta_{on}^*=(T_0^*,T_1^*,V^*,\delta^*,v^*)$。

可以验证 δ_{on}^* 是正确模拟的，首先令 $\xi=\alpha^*+v^*\beta^*$，$T=-\xi P$ 和 $\rho=\xi/a$，因为 $s=-a-I_\pi$，所以可以验证 $T=-\xi P=-a\rho P=\rho(I_\pi+s)P$。

Phase 2. 敌手 A 进行第二轮询问，其间 A 不能对 $\delta_{on}^*=(T_0^*,T_1^*,V^*,\delta^*,v^*)$ 执行解签密询问，不能对接收者 ID_R^*

执行私钥询问。

Guess. 模拟结束时，A 输出 b' 作为对 b 的猜测，如果 $b'=b$，C 将至少以 $1/q_2$ 的概率得到 $X^*=\hat{e}(P,P)^{\rho}=\hat{e}(\hat{P},\hat{P})^{f(a)^2\xi/a}$，那么待解决的 l-BDHI 难题可以得到解决：

$$\left(\frac{X^{*1/\xi}}{\hat{e}\left(\sum_{i=0}^{l-2}c_{i+1}a^i\hat{P},c_0\hat{P}\right)\hat{e}\left(\sum_{j=0}^{l-2}c_{j+1}a^j\hat{P},P\right)}\right)^{\frac{1}{c_0^2}}$$

$$=\frac{\hat{e}(\hat{P},\hat{P})^{f(a)^2/c_0^2a}}{\hat{e}(\hat{P},\hat{P})^{\frac{c_0(c_1+c_2a+c_3a^2+\cdots+c_{l-1}a^{l-2})+f(a)(c_1+c_2a+c_3a^2+\cdots+c_{l-1}a^{l-2})}{c_0^2}}}$$

$$=\hat{e}(\hat{P},\hat{P})^{\frac{f(a)^2-(c_1a+c_2a^2+c_3a^3+\cdots+c_{l-1}a^{l-1})(c_0+f(a))}{c_0^2a}}$$

$$=\hat{e}(\hat{P},\hat{P})^{\frac{f(a)^2-(f(a)-c_0)(c_0+f(a))}{c_0^2a}}=\hat{e}(\hat{P},\hat{P})^{\frac{1}{a}}$$

如果以下事件发生，游戏模拟将会终止，C 将失败。

E_1：敌手未选取 ID_π 作为接收者进行挑战，即 $ID_R^*\neq ID_\pi$。

E_2：敌手 A 对身份 ID_π 进行私钥询问。

E_3：签密询问的第二种情况下，C 未通过查表 L_1 而隐含的定义 h_1，而 h_1 已经被定义。

E_4：C 拒绝一个正确的解签密询问。

显然有，$\Pr[\neg E_1]=1/q_0$，$\neg E_2\subset\neg E_1$，$\Pr[E_3]\leqslant q_s(q_s+q_1)/q$ 以及 $\Pr[E_4]\leqslant q_u/q$。

综上所述，C 成功的概率至少为：

$$\frac{1}{q_0}\frac{1}{q_2}\left(1-\frac{q_s(q_s+q_1)}{q}\right)\left(1-\frac{q_u}{q}\right)\varepsilon$$

不可伪造性

定理 2 在随机预言模型下，若存在一个 EUF-ACMA 敌手 A 能够在多项式时间内以 ε 的优势赢得游戏，则存在一个挑战者 C 能够在多项式时间内至少以下面的优势解决 $l+1$-SDH 问题：

$$\frac{1}{q_0^2}\frac{1}{q_2^2}\left(1-\frac{q_s(q_s+q_1)}{q}\right)^2\left(1-\frac{q_u}{q}\right)^2\frac{1}{4(q_s+q_1)^2}\varepsilon^2$$

证明：设 $(\hat{P},a\hat{P},a^2\hat{P},\cdots,a^l\hat{P},a^{l+1}\hat{P})$，其中 $a,l\in Z_q^*$，是一个 $l+1$-SDH 实例，C 需要输出 $(b,(1/b+a)\hat{P})$，其中 $b\in_R Z_q^*$。

Setup. 最开始，C 随机选择 $\pi\in\{1,\cdots,q_0\}$，以及 I_π，$w_1,\cdots,w_{\pi-1},w_{\pi+1},\cdots,w_l\in Z_q^*$。构造多项式 $f(z)=\prod_{i=1,i\neq\pi}^{l}(z+w_i)=\sum_{i=0}^{l-1}c_iz^i$ 得到 $c_0,\cdots,c_{l-1}\in Z_q^*$。构造群 G_1 的一个生成元 $P=\sum_{i=0}^{l-1}c_ia^i\hat{P}=f(a)\hat{P}$。类似地，对任意 $i\in\{1,\cdots,l\}\backslash\{\pi\}$，$C$ 构造多项式 $f_i(z)=f(z)/(z+w_i)=\sum_{j=0}^{l-2}d_{i,j}z^j$ 得到 $d_{i,1},\cdots,d_{i,l-2}\in Z_q^*$，计算 $\hat{H}_i=\sum_{j=0}^{l-2}d_{i,j}(a^j\hat{P})=\frac{f(a)}{a+w_i}\hat{P}=\frac{1}{a+w_i}P$。

对任意 $i\in\{1,\cdots,l\}\backslash\{\pi\}$，$C$ 令 $I_i=w_i$。

最后，C 令 $P_{Pub}=-aP=f(a)\hat{P}$。此时系统主密钥 $s=-a$，C 也不知道。C 将 $(i,I_i,-\hat{H}_i)$ 添加到表 L_I 中。此外，C 还要维护 $L_i(i=1,2)$ 两张表。最后，C 将公开参数发送给 A。

Probe. 与定理 1 的 Phase 1 相同，A 向 C 执行多项式有界次询问。

Forge. 与定理 1 类似，C 至少以概率 $\frac{1}{q_0}\frac{1}{q_2}\left(1-\frac{q_s(q_s+q_1)}{q}\right)\left(1-\frac{q_u}{q}\right)\varepsilon$ 得到一个正确的密文 $\delta_{\sigma n}^*=(T_0^*,T_1^*,V^*,\sigma^*,v^*)$，此处唯一不同的是要求 $ID_S^*=ID_\pi$。

把生成密文 $\delta_{\sigma n}^*$ 时用到的 $H_1(m,T_0^*,T_1^*,V^*,v)$ 询问称作关键询问。游戏其间，A 一共执行 q_1+q_s 次 H_1 询问。选取 $i_b\in\{1,\cdots,q_1+q_s\}$，第 i_b 次 H_1 询问恰好是关键询问的概率为 $1/q_1+q_s$。假设 R' 记录 H_1 询问的答案，R'' 记录其它随机语言询问的答案。将 R' 划分成两个阶段，R_1' 包含 $1,\cdots,i_b-1$ 次询问答案，R_2' 包含 $i_b,\cdots,q_1+q_s$ 次询问答案。C 重新进行一次模拟，其中 R_1'、R'' 不变，R_2' 不同。应用“分叉引理”[12]，其中 $\Theta=R''\cup R_1'$，$\gamma=R_2'$，那么这两次模拟以概率 $\frac{1}{q_0^2}\frac{1}{q_2^2}\left(1-\frac{q_s(q_s+q_1)}{q}\right)^2\left(1-\frac{q_u}{q}\right)^2\frac{1}{4(q_s+q_1)^2}\varepsilon^2$ 输出两个签名 (m,σ^*) 和 $(m,\sigma^{*'})$，满足：

$$\hat{e}(V^*+\sigma^*P,P_{ID_S^*})=\hat{e}(P,P)\hat{e}(T_1,P_{ID_S^*})^{h_1}$$

$$\hat{e}(V^*+\sigma^{*'}P,P_{ID_S^*})=\hat{e}(P,P)\hat{e}(T_1,P_{ID_S^*})^{h_1'}$$

因此有：

$$\hat{e}(V^*+\sigma^*P,P_{ID_S^*})^{1/h_1}\hat{e}(P,P)^{1/h_1'}$$

$$=\hat{e}(V^*+\sigma^{*'}P,P_{ID_S^*})^{1/h_1'}\hat{e}(P,P)^{1/h_1}$$

化简得：

$$\hat{e}\left(\frac{h_1'}{h_1'-h_1}(V^*+\sigma^*P)-\frac{h_1}{h_1'-h_1}(V^*+\sigma^{*'}P),P_{ID_S^*}\right)$$

$$=\hat{e}(P,P)$$

又因为，

$$P_{ID_S^*}=P_{ID_\pi}=(I_\pi+a)P$$

所以有，

$$\frac{h_1'}{h_1'-h_1}(V^*+\sigma^*P)-\frac{h_1}{h_1'-h_1}(V^*+\sigma^{*'}P)=\frac{1}{I_\pi+a}P$$

此外，可以通过构造多项式 $f(z)/(z+I_\pi)=\frac{e_{-1}}{z+I_\pi}+\sum_{j=1}^{l-2}e_jz^j$，得到 $e_{-1},e_0,\cdots,e_{l-2}\in Z_q^*$。

从而计算，

$$\frac{1}{e_{-1}}\left(\frac{h_1'}{h_1'-h_1}(V^*+\sigma^*P)-\frac{h_1}{h_1'-h_1}(V^*+\sigma^{*'}P)-\sum_{j=0}^{l-2}e_ja^jP\right)$$

$$=\frac{1}{e_{-1}}\left(\frac{1}{I_\pi+a}P-\sum_{j=0}^{l-2}e_ja^j\hat{P}\right)=\frac{1}{e_{-1}}\left(\frac{e_{-1}}{I_\pi+a}\hat{P}\right)$$

$$=\frac{1}{I_\pi+a}\hat{P}$$

$(I_\pi,\frac{1}{I_\pi+a}\hat{P})$ 就是 $l+1$-SD 问题的一个答案。

5.2 效率分析

本节对改进方案与 Liu 等[8]的方案进行效率比较，结果如表 1 所列。在表 1 中，假设 $|G_1|=160$ 比特，$|q|=160$ 比特，$|G_2|=1024$ 比特，$|m|=160$ 比特；简写 PM，PA，E，I，M 分别表示群 G_1 中的点乘运算、群 G_1 中的点加运算、群 G_2 中的指数运算、域 Z_q^* 中的求逆运算、域 Z_q^* 中的模运算。

表1 效率比较

方案	Liu等[8]方案	改进方案
离线计算量	6PM+3PA+1E+3I	3PM+2PA+1E
在线计算量	3M	2M+1I
离线存储量	2624 比特	2144 比特
在线密文长度	1280 比特	960 比特
解签密计算量	$2\hat{e}$+4PM+4PA+1I	$2\hat{e}$+2PM+2PA+1E

结束语 本文提出一个高效的基于身份在线/离线签密方案。在保证安全的前提下，改进的方案在线及离线签密的运算量、解签密的运算量比Liu等[8]的方案有所降低，并且减少了离线存储量，缩短了在线密文长度。

参 考 文 献

[1] Zheng Y. Digital signcryption or How to Achieve Cost(Signature Encryption)≤Cost(Signature)+Cost(Encryption) [C]// Proceeding of CRYPTO'97, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]// Proceeding of CRYPTO'84, LNCS 196. Berlin: Springer-Verlag, 1984: 47-53

[3] Even S, Goldreich O, Micali S. On-line/offline digital signatures [C]// Proc. CRYPTO 89, LNCS 2442. 1989: 263-277

[4] An J, Dodis Y, Rabin T. On the Security of Joint Signature and Encryption [C]// Proc. EUROCRYPT 2002, LNCS 2332. 2002: 83-107

[5] Zhang F, Mu Y, Susilo W. Reducing security overhead for mobile networks [C]// AINA Workshop '05. 2005: 398-403

[6] Xu Z, Dai G, Yang D. An efficient online / offline signcryption scheme for MANET[C]// AINA Workshop '07. 2007: 171-176

[7] Dongdong S, Xinyi H, Yi M, et al. Identity-based on-line/off-line signcryption [C]// Network and Parallel Computing. 2008: 34-41

[8] Liu J, Baek J, Zhou J. Online/Offline Identity-Based Signcryption Re-visited [R]. Cryptology ePrint Archive. Report2010/274, 2010

[9] Boneh D, Franklin M. Identity based encryption from the Weil pairing [C]// Advances in Cryptology-Crypto'01, LNCS 2139. 2001

[10] Boneh D, Boyen X. Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles [C]// Proc. EUROCRYPT 2004, LNCS 3027. 2004: 223-238

[11] Boneh D, Boyen X. Short Signatures without Random Oracles [C]// Proc. EUROCRYPT 2004, LNCS 3027. 2004: 56-73

[12] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures [J]. Journal of Cryptology, 2000, 13(3): 361-396

(上接第 33 页)

值来计算节点之间的信任值。图1表明，节点 a 对节点 b 的信任值随着恶意节点的增多快速增大。而在本文模型中，通过综合考虑对目标节点 b 的直接信任度和交易资源的总好评度，在计算两个节点之间的信任值时利用相似度和声誉把评价节点集合进行了两次筛选，从而随着恶意节点的增多，节点 a 对节点 b 的信任值变化不大。图1表明，在本文信任模型下，网络中恶意节点的增多对信任值有较小的影响。实验说明本文信任机制可以有效抵制恶意节点。

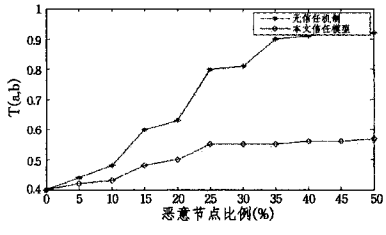

图1 信任值与恶意节点的关系

结束语 本文提出了一种基于资源评价的信任管理模型，提出了资源的总好评度的概念，在计算直接信任值时考虑了时效性和资源的重要程度两个因素，在计算节点的声誉时重点考虑了交易量因子的影响，以便很好地抑制节点通过小规模的成功交易来获取高的声誉值。引入激励机制，能有效地提高节点参与的积极性。分析及仿真表明，本文模型能较好地抵御恶意节点的攻击，提高网络交易的成功率。

参 考 文 献

[1] ORAM A. Peer-to-peer amassing the power of disruptive technology [M]. [S. l.]: O'Reilly Press, 2001

[2] Serious S, Gummadi P K, Gribble S D. A measurement study of P2P file sharing systems[C]// Kienzle M G, Shenoy P J, eds. Proc. of the Multimedia Computing and Networking 2002 (MMCN 2002). SPIE Press, 2002

[3] Blaze M, Feigenbaum J, Lacy J. Decent ralized trustmanagement [C]// Proceedingsof the 1996 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 1996: 164-173

[4] 贾兆庆，薛广涛，唐新怀，等. 非结构化 P2P 中的一种信任机制[J]. 计算机研究与发展，2010，47(4)：645-652

[5] Kamvar S D, Schollser M T, Garcia-Molainah. The eigentrust algorithm for reputation management in P2P networks[C]// Proceedings of the 12th International Conference on World Wide Web. New York: ACM, 2003: 640-651

[6] 窦文，王怀民，贾焰，等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报，2004，15(4)：571-583

[7] 贺明科，郝智勇. P2P 网络中基于网络拓扑特性的信任管理[J]. 计算机工程，2010(24)

[8] 吴鹏，吴国新，方群. 一种基于概率统计方法的 P2P 系统信任评价模型[J]. 计算机研究与发展，2008，45(3)：408-416

[9] 魏德健，贾智平，李新. 面向无线自组网的分布式信任管理模型[J]. 计算机应用，2011(1)

[10] 梁保松，曹殿立. 模糊数学及其应用[M]. 北京：科学出版社，2007：131-132

[11] 张仕斌，何大可，盛志伟. 信任管理模型的研究与发展[J]. 计算机应用研究，2006(07)：18-22