标准模型下高效的基于身份可净化签名方案

明 洋 李 瑞
(长安大学信息工程学院 西安 710064)

摘 要 可净化签名方案中,净化者能够修改原消息的特定部分,不必与签名者交互就能生成修改消息的有效签名。利用双线性对,基于Waters技术和Li技术,提出一个标准模型下安全的基于身份可净化签名方案。安全性分析表明,所提方案能够满足不可伪造性、不可区分性和不可变性。和现有标准模型下安全方案相比,该方案计算效率高、通信代价小。

关键词 基于身份,可净化签名,标准模型,双线性对
中图法分类号 TN918.1 **文献标识码** A

Efficient Identity-based Sanitizable Signature Scheme in Standard Model

MING Yang LI Rui
(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract Sanitizable signature scheme allows stanitizer to modify the specific part of the original message without interacting with the signer to generate a valid signature to modify the message. This paper came up with an identity-based sanitizable signature scheme design based on Waters technology and Li technology under the standard model with the application of bilinear pairings. The safty analysis shows that the proposed scheme is able to satisfy the characteristics of unforgeability, indistinguishability and immutability. Compared with the the existing safty scheme under the standard model, this design has higher computational efficiency and smaller communication cost.

Keywords Identity-based, Sanitizable signature scheme, Standard model, Bilinear pairings

1 引言

1984年,Shamir首次提出基于身份公钥密码体制[1],目的是简化传统基于证书公钥密码体制的密钥管理过程。该体制中用户使用自己的身份(如名字、电子邮箱等)作为自己的公钥,从而减轻了用户对公钥证书的需求。2001年,Boneh和Franklin[2]首次提出一个实用的基于身份加密方案。之后,大量基于身份的加密和签名方案[3-6]被提出。

数字签名是提供认证性、完整性和不可否认性的重要技术,是信息安全的核心技术之一。然而,像多媒体办公、多媒体教育以及网上医疗系统这些应用程序为了隐藏高度机密信息,需要适当地改变一部分签署的文件,而不是保留完整的文件。例如,当官方文件经过净化后,在公民的要求下非机密信息可以是公开的,而官方披露的信息中秘密信息实则都是加密的。如果披露的信息是被传统的数字签名方案加密过的,公民无法核实披露信息的正确性。2005年,Ateniese等人首次提出了可净化数字签名[9]的概念。可净化数字签名中允许签名者在对消息进行签名的同时指定一个净化者,并允许该净化者在签名者不在场的情况下对消息签名对进行签名者许可的修改。Miyazaki等人[7]和Steinfeld等人[8]提出了相似的概念。在文献[9]中,Ateniese等人讨论了可净化数字签名的广泛用途,并列举了许多实际应用,如医疗数据匿名化发布和安全路由等。但是,文中可净化签名的定义并不完善,且对基本安全需求缺乏形式化定义。之后,Klonowski等人[10]和Canard等人[11]陆续提出了可净化数字签名的扩展和变型,在一定程度上提高了可净化数字签名的实用性。2009年,Brzuska等人[12]完善了可净化数字签名的定义,并对Ateniese等人[9]提出的安全需求进行了形式化定义。同年,Brzuska等人[13]提出了一个基于传统数字签名的可净化数字签名方案。该方案虽然具有较短的签名长度和较高的计算效率,但是不满足透明性。因此,Brzuska等人[14]引入了一个新的可净化数字签名的安全性需求——不可连接性(unlinkability),并构造了一个基于群签名方案的可净化签名方案。

目前,大部分可净化签名方案都是基于公钥基础设施构建的。2010年,明洋等人首次提出一个标准模型下可证安全的基于身份的可净化签名方案[15],但效率不高。本文利用Water签名[16]和Li签名[17]的技术,提出了一个高效的基于身份可净化签名方案(IDSS),并在标准模型中证明了该方案是安全的,能够满足不可伪造性、不可区分性和不可变性。

到稿日期:2012-10-26 返修日期:2013-01-28 本文受国家自然科学基金项目(61202438),中国博士后科学基金项目(2011M501427),西安市科技计划项目(CX1258③),中央高校基础研究支持计划资助项目(CHD2012JC047)资助。

明 洋(1979—),男,博士,副教授,主要研究方向为公钥密码学、可证明安全理论、无线网络安全,E-mail:yangming@chd.edu.cn;李 瑞(1987—),女,硕士,主要研究方向为密码学、数字签名。

2 预备知识

2.1 双线性对

令 G_1,G_2 是两个 q 阶循环群,其中 q 为素数,g 是 G_1 的生成元。定义两个群上的双线性映射为 $e:G_1\times G_1=G_2$,且满足以下性质:

(1)双线性:$e(g^a,g^b)=e(g,g)^{ab}$,对所有的 $a,b\in Z_q^*$ 均成立。

(2)非退化性:$e(g,g)\neq 1$。

(3)可计算性:存在有效算法计算 e。

2.2 困难问题假设

计算性 Diffie-Hellman 问题(CDH):给定 $g^a,g^b\in G$,对任意的 $a,b\in z_q$,计算 g^{ab}。

(ε,t)计算性 Diffie-Hellman 假设:如果不存在任何一种概率多项式算法在时间 t 内以至少 ε 的概率解决群 G 上 CDH-问题,则称群 G 上的(ε,t)-CDH 假设成立。

3 基于身份可净化签名

3.1 基于身份可净化签名形式化定义

基于身份的可净化签名[15]由以下 5 个多项式时间算法组成。

(1)系统建立:输入一个安全参数 k,PKG 生成系统参数 *params* 和主密钥 *msk*,其中 *params* 公开,主密钥 *msk* 保密。

(2)密钥生成:给定 *params*、*msk* 和用户身份 *ID*,PKG 产生密钥 d_{ID},且 PKG 能够为所有用户产生密钥,并通过安全信道发送给用户。

(3)签名:给定 *params*、签名者身份 ID_s、消息 M 和签名者私钥 d_{ID_s},签名者输出签名 σ 和秘密信息 ψ。

(4)净化:给定 *params*、签名者身份 ID_s、消息的签名 σ 和秘密信息 ψ,净化者输出消息 $\overline{M}$ 和 $\overline{M}$ 的净化签名 $\bar{\sigma}$。

(5)验证:给定 *params*、签名者身份 ID_s、原始消息签名对(M,σ)或净化消息签名对$(\overline{M},\bar{\sigma})$,如果签名有效,输出“接受”,否则输出“拒绝”。

3.2 可净化签名的安全模型

可净化签名必须满足不可伪造性、不可区分性和不可变性[11]。

不可伪造性:不可伪造性指任何人都不能伪造签名者或净化者的签名(外部攻击)。

不可区分性:任何人都不能区分消息是否净化。

不可变性:净化者不能随意改变消息的有效签名,除了被允许净化的部分(内部攻击)。

不可伪造性通过挑战者 C 与攻击者 A 之间的交互游戏来定义,具体如下:

1. 系统建立:C 运行系统建立算法,生成系统参数 *params* 和主密钥 *msk*。C 返回系统参数 *params* 给 A 并保密主密钥。

2. 询问:攻击者 A 适应性进行以下询问:

密钥询问:当攻击者 A 询问身份 *ID* 的密钥时,C 运行密钥生成算法生成 d_{ID},并返回给 A。

签名询问:当 A 询问任意身份 *ID* 对消息的签名时,C 运行密钥生成算法和签名算法得到签名 σ,并返回给 A。

3. 伪造:攻击者 A 输出消息 m^*、身份 ID^* 下的签名 σ^*。

如果满足下面 3 个条件,则攻击成功:

(1)攻击者不能对身份 ID^* 做密钥询问。

(2)攻击者不能对(ID^*,m^*)进行签名询问。

(3)σ^* 是身份 ID^*、消息 m^* 的有效签名。

定义 1 如果攻击者 A 最多运行 t 时间内,最多进行 q_e 次密钥询问和 q_s 次签名询问,以不小于 ε 的概率赢得上述游戏,则称攻击者 A 是基于身份可净化签名(ε,t,q_e,q_s)-伪造者。如果基于身份可净化签名中不存在(ε,t,q_e,q_s)-伪造者,则称方案是(ε,t,q_e,q_s)-安全的。

不可区分性通过挑战者 C 与区分者 D 之间的交互游戏来定义,具体如下:

1. 系统建立:C 运行系统建立算法和安全参数 k,生成系统参数 *params* 和主密钥 *msk*。C 返回系统参数 *params* 给 D 并保密主密钥。

2. 第 1 步:同不可伪造性游戏一样,D 运行密钥询问和签名询问的多项式算法。

不可挑战性:第 1 步运行完毕,D 在身份 ID^* 上输出两个签名对(M_0^*,σ_0^*),(M_1^*,σ_1^*),并且设置净化者允许改变的指数 K^*,提交这些参数给 C。C 随机选取 $b\in\{0,1\}$,如果 $b=0$,C 运行可净化算法,返回$(\overline{M}_0^*,\bar{\sigma}_0^*)$给 D;否则,如果 $b=1$,C 运行可净化算法,返回$(\overline{M}_1^*,\bar{\sigma}_1^*)$给 D。

3. 第 2 步:同第 1 步,D 再次询问多项式有限数集。

推测:最后,如果 $b'=bD$,输出 b'赢得游戏。

D 的概率定义为 $Adv(D)=|\Pr[b'=b]-1/2|$,$\Pr[b'=b]$指 $b'=b$ 的概率。

定义 2 如果区分者最多运行 t 时间内,最多进行 q_s 次密钥询问和 q_e 次签名询问,以不小于 ε 的优势赢得不可区分性游戏,则基于身份可净化签名方案是(ε,t,q_e,q_s)无条件不可区分的。

不可变性要求净化者除了允许净化的部分以外,不能产生消息的有效签名。通过挑战者 C 与攻击者 A 之间的交互游戏定义,具体如下:

1. 初始化:敌手 A 发送 K_s 给 C,K_s 是净化者允许改变的指数。

2. 系统建立:C 运行系统建立算法和安全参数 k,生成系统参数 *params* 和主密钥 *msk*。C 返回系统参数 *params* 给 A 并保密主密钥。

3. 询问:同不可伪造性游戏一样,A 运行密钥询问和签名询问的多项式算法。

注意,在签名询问中,C 也能发送秘密信息 ψ 给 A。

4. 伪造:最后,A 在身份 ID^* 上输出消息 $M^*=(m_1^*,\cdots,m_n^*)$的签名 σ^*,即对任何 $j\in\{1,\cdots,q_s\}$,存在 $i\notin K_s:m_{j,i}\neq m_i^*$,$\sigma^*$ 是一个有效签名。

A 的概率被定义为赢得上述游戏的成功概率。

定义 3 如果攻击者最多运行 t 时间内,最多进行 q_s 次密钥询问和 q_e 次签名询问,以不小于 ε 的优势赢得不可变性游戏,则基于身份可净化签名方案的(ε,t,q_e,q_s)是不可变的的。

4 所提方案

1. 系统建立:给定安全参数 k,选取素数 q 阶循环群 G_1,G_2,$g\in G_1$,双线性映射为 $e:G_1\times G_1\rightarrow G_2$,$H_u:\{0,1\}^*\rightarrow\{0,$

$1\}^n, H_m:\{0,1\}^* \to \{0,1\}^n$。PKG 随机选取 $a\in Z_q^*$，$g_2\in G_1$，计算 $g_1=g^a\in G_1$。随机选择 $u'\in Z_q$，$v'\in G_1$，n 维的向量$(u_1, u_2,\cdots,u_n)\in z_q^n$，$(v_1,v_2,\cdots,v_n)\in G_1^n$。计算 $z_1=e(g_1,g_2)$，$z_2=e(g,g_2)$。则系统的公开参数为 $params=(q,g,g_1,g_2,u'v',u_1,u_2,\cdots,u_n,v_1,v_2,\cdots,v_n,z_1,z_2)$，主密钥为 a。

2. 密钥生成：假定用户身份 ID 为长度为 n 的比特串 $ID_1,\cdots,ID_n$。$U\subseteq\{1,2,\cdots,n\}$为 $ID[i]=1$ 的序号 i 的集合。PKG 随机选取 $r_{ID}\in Z_q^*$，并计算：

$$d_{ID}=(d_1,d_2)=(g_2^{a+r_{ID}(u'+\sum_{i=1}^{n}u_i^{ID_i})}, z_2^{r_{ID}})$$

3. 签名：签名者首先验证：$e(g,d_1)=z_1\cdot d_2^{(u'+\sum_{i=1}^{n}u_i^{ID_i})}$ 是否成立，如果等式成立，则 d_{ID} 存在，否则重新生成密钥。假定消息 m 为长度 n 的比特串 $v_1,v_2,\cdots,v_n$，$K_s\subseteq\{1,\cdots,n\}$是净化者允许修改的指数，签名者随机选取 $r\in Z_q^*$，计算：

$$\sigma=d_1\cdot(v'\prod_{j=1}^{n}v_j^{m_j})^r, d_2, g^r)=(\sigma_1,\sigma_2,\sigma_3)$$

则签名为 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，同时签名者把秘密信息$(v_j)^r(j\in K_s)$安全地发送给净化者。

4. 净化：设消息 $\bar{M}=(\bar{m}_1,\cdots,\bar{m}_n)$的签名不同于 $M=(m_1,\cdots,m_n)$。令 $K'=\{j\in K: m_j=0,\bar{m}_j=1\}$，$K''=\{i\in K: m_j=1,\bar{m}_j=0\}$，满足 $K'\cup K''=K$，$K'\cap K''=\phi$。当收到 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，$(m_j)^r(j\in K_s)$后，净化者进行：

(1)验证签名 σ 的有效性。

(2)随机选择 $\bar{r}_{ID},\bar{r}\in Z_q^*$，计算：

$$\bar{\sigma}_1=\sigma_1\cdot g_2^{\bar{r}_{ID}(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot\frac{\prod_{i\in K'}m_j^r}{\prod_{i\in K''}m_j^r}\cdot(v'\prod_{j=1}^{n}v_j^{\bar{m}_j})^{\bar{r}}$$

$$\bar{\sigma}_2=\sigma_2\cdot g^{\bar{r}_{ID}},\bar{\sigma}_3=\sigma_3\cdot g^{\bar{r}}$$

则净化签名为 $\bar{\sigma}=(\bar{\sigma}_1,\bar{\sigma}_2,\bar{\sigma}_3)$。

5. 验证：收到 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$后，验证方程 $e(g,\sigma_1)=z_1\cdot\sigma_2^{(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot e(v'\prod_{j=1}^{n}v_j^{m_j},\sigma_3)$的有效性。如果有效，则输出“接受”，否则“拒绝”。

正确性：

$$\begin{aligned}e(\sigma_1,g)&=e(g,g_2^{a+r_{ID}(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot(v'\prod_{j=1}^{n}v_j^{m_j})^r)\\&=e(g^a,g_2)e(g^{r_{ID}},g_2^{(u'+\sum_{i=1}^{n}u_i^{ID_i})})e(g^r,(v'\prod_{j=1}^{n}v_j^{m_j}))\\&=e(g_1,g_2)\sigma_2^{(u'+\sum_{i=1}^{n}u_i^{ID_i})}e(\sigma_3,(v'\prod_{j=1}^{n}v_j^{m_j}))\\&=z_1\sigma_2^{(u'+\sum_{i=1}^{n}u_i^{ID_i})}e(\sigma_3,(v'\prod_{j=1}^{n}v_j^{m_j}))\end{aligned}$$

由 $K'=\{j\in K: m_j=0,\bar{m}_j=1\}$和 $K''=\{j\in K: m_j=1,\bar{m}_j=0\}$，可知：

$$\bar{m}_j-m_j=\begin{cases}1, & j\in K'\\0, & j\in K''\end{cases}$$

$$\begin{aligned}\bar{\sigma}_1&=\sigma_1\cdot g_2^{\bar{r}_{ID}(u'+\sum_{i=1}^{n}u_i^{ID_i})}\frac{\prod_{j\in K'}m_j^r}{\prod_{j\in K''}m_j^r}\cdot(v'\prod_{j=1}^{n}v_j^{\bar{m}_j})^{\bar{r}}\\&=g_2^{a+r_{ID}(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot(v'\prod_{j=1}^{n}v_j^{m_j})^r\cdot g_2^{\bar{r}_{ID}(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot\\&\quad\prod_{j=1}^{n}v_j^{r(\bar{m}_j-m_j)}\cdot(v'\prod_{j=1}^{n}v_j^{\bar{m}_j})^{\bar{r}}\\&=g_2^{a+(u'+\sum_{i=1}^{n}u_i^{ID_i})(r_{ID}+\bar{r}_{ID})}(v')^r(v')^{\bar{r}}(\prod_{j=1}^{n}v_j^{m_j})^r(\prod_{j=1}^{n}v_j^{\bar{m}_j})^{\bar{r}}\cdot\\&\quad\prod_{j=1}^{n}v_j^{r(\bar{m}_j-m_j)}\\&=g_2^{a+(u'+\sum_{i=1}^{n}u_i^{ID_i})(r_{ID}+\bar{r}_{ID})}(v'\prod_{j=1}^{n}v_j^{\bar{m}_j})^{(r+\bar{r})}\end{aligned}$$

5 安全性证明

定理 1(不可伪造性) 若(ε',t')-CDH 假设成立，所提方案是(ε,t,q_e,q_s)-存在性不可伪造的，其中 $\varepsilon'=\frac{\varepsilon}{16(q_e+q_s)q_s(n+1)^2}$，$t'=t+(2q_e+(n+1)q_s)t_e$，$q_e$ 为密钥询问次数，q_s 为签名询问次数，t 为群 G_1 中指数运算时间，n 为消息的比特串长度。

证明：假定(ε,t,q_e,q_s)-攻击者 A 存在，构造一个算法 B，在 t'时间内，以 ε'的概率解决 CDH 问题。即给定 g,g^a,g^b，计算 g^{ab}。算法 B 模拟游戏中挑战者 C 与攻击者 A 进行交互。具体如下：

系统建立：B 随机选取整数 $0\leqslant l_u\leqslant q$，$0\leqslant l_m\leqslant q$，且 $0\leqslant k_u\leqslant n$，$0\leqslant k_m\leqslant n$，$(l_u(n+1)<q, l_m(n+1)<q)$。随机选取 $x'\in Z_{l_u}$，n 维向量 $X=(x_i)$，且 $x_i\in Z_{l_u}$；随机选取 $y'\in Z_{l_m}$，n 维向量 $Y=(y_j)$，且 $y_j\in Z_{l_m}$。为了便于分析，定义如下 3 个函数，其中身份 $ID=(ID_1,\cdots,ID_n)$，消息 $M=(m_1,\cdots,m_n)$，且 $(ID_i,m_j)\in\{0,1\}(1\leqslant i\leqslant n, 1\leqslant j\leqslant n)$：

$$F(ID)=x'+\sum_{i=1}^{n}x_iID_i-l_uk_u$$

$$K(M)=y'+\sum_{j=1}^{n}y_jm_j-l_mk_m$$

$$L(M)=w'+\sum_{j=1}^{n}w_jm_j$$

计算：

(1)$g_1=g^a$，$g_2=g^b$。

(2)$u'=-l_uk_u+x'$，$u_i=x_i$，$1\leqslant i\leqslant n$，即对任何身份 ID，满足 $u'+\sum_{i=1}^{n}u_i^{ID_i}=F(ID)$。

(3)$v'=g_2^{-l_m\cdot k_m+z'}g^{w'}$，$v_j=g_2^{z_j}g^{w_j}$，$1\leqslant j\leqslant n$，即对任何 M，满足 $v'\prod_{j=1}^{n}v_j^{m_j}=g_2^{K(M)}g^{L(M)}$。最后，$B$ 返回所有参数给 A。

询问：B 回答攻击者 A 的询问。

1. 密钥询问：当 A 对身份 ID 进行密钥询问时，如果 $F(ID)=0 \bmod q$，B 终止模拟；$F(ID)\neq 0 \bmod q$ 时，B 随机选取 $r_{ID}\in Z_q^*$，计算：

$$\begin{aligned}d_{ID}&=(d_1,d_2)\\&=(g_1^{-1}(gg_2)^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}, e(gg_2, g^rg_1^{-\frac{1}{(u'+\sum_{i=1}^{n}u_i^{ID_i})}}))\end{aligned}$$

正确性：

$$\begin{aligned}e(d_1,g)&=e(g_1^{-1}(gg_2)^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})},g)\\&=e(g_1^{-1}(gg_2)^{rF(ID)},g)\\&=e(g_2^a((gg_2)^{F(ID)})^{r-\frac{a}{F(u)}},g)\\&=e(g_2^a,g)\cdot e(((gg_2)^{F(ID)})^{r-\frac{a}{F(u)}},g)\\&=e(g_1,g_2)\cdot e((gg_2)^{F(ID)},g^{r-\frac{a}{F(ID)}})\\&=e(g_1,g_2)\cdot e(gg_2,g^rg_1^{-\frac{1}{F(ID)}})^{F(ID)}\\&=z_1\cdot d_1^{(u'+\sum_{i=1}^{n}u_i^{ID_i})}\end{aligned}$$

2. 签名询问：当 A 对(ID,M)进行签名询问时，如果 $K(M)=0 \bmod q$，B 终止模拟；如果 $K(m)\neq 0 \bmod l_m$，首先进

行密钥询问，得到密钥询问后进行签名生成算法得到签名；如果 $F(ID)=0 \bmod q$ 且 $K(m)\neq 0 \bmod q$，B 随机选择 $s\in Z_q$，$r\in Z_q$，其中 $s'=s-\frac{a}{K(M)}$，计算：

$$\begin{aligned}\sigma&=(\sigma_1,\sigma_2,\sigma_3)\\&=(g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}g_1^{-\frac{L(M)}{K(M)}}(v'\prod_{j=1}^{n}v_j^{m_j})^s,z_2^r,g^sg_1^{-\frac{1}{K(M)}})\\&=(g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}g_2^a(v'\prod_{j=1}^{n}v_j^{m_j})^{s'},z_2^r,g^{s'})\end{aligned}$$

正确性：

$$\begin{aligned}\sigma_1&=g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}g_1^{-\frac{L(M)}{K(M)}}(v'\prod_{j=1}^{n}v_j^{m_j})^s\\&=g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}g_1^{\frac{L(M)}{K(M)}}(g_2^{K(M)}g^{L(M)})^s\\&=g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}g^{a\cdot\frac{L(M)}{K(M)}}g_2^{K(M)s}g^{L(M)s}\\&=g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}g^{a\cdot\frac{L(M)}{K(M)}}g_2^{K(M)s}g^{L(M)s}\\&=g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}((v'\prod_{j=1}^{n}v_j^{m_j})g_2^{-K(M)})^{s'}g_2^{K(M)s'}g_2^a\\&=g_2^{r(u'+\sum_{i=1}^{n}u_i^{ID_i})}(v'\prod_{j=1}^{n}v_j^{m_j})^{s'}g_2^a\\&=g_2^{a+r(u'+\sum_{i=1}^{n}u_i^{ID_i})}(v'\prod_{j=1}^{n}v_j^{m_j})^{s'}\\&=d_1(v'\prod_{j=1}^{n}v_j^{m_j})^{s'}\end{aligned}$$

$\sigma_2=z_2^r=d_2$，$\sigma_3=g^sg_1^{\frac{1}{K(m)}}=g^{s+\frac{a}{K(m)}}=g^{s'}$。

如果 $F(ID)=0 \bmod q$ 且 $K(m)=0 \bmod q$，则 B 放弃。

伪造：攻击者 A 输出身份 ID^* 对消息 M^* 的有效签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$。如果 $K(M^*)\neq 0 \bmod q$ 且 $F(ID^*)\neq 0 \bmod q$，则算法 B 放弃；如果 $K(M^*)=0 \bmod q$ 且 $F(ID^*)=0 \bmod q$，则算法 B 计算：

$$\frac{\sigma_1^*}{(\sigma_3^*)^{L(M^*)}}=\frac{g_2^{a+r^*(u'+\sum_{i=1}^{n}u_i)}\cdot[v'\prod_{j=1}^{n}v_j^{m_j}]^{s^*}}{g^{L(M^*)\cdot s^*}}=g_2^a=g^{ab}$$

将其作为 CDH 问题的解。

正确性：

$$\begin{aligned}\frac{\sigma_1^*}{(\sigma_3^*)^{L(M^*)}}&=\frac{g_2^{a+r^*(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot[v'\prod_{j=1}^{n}v_j^{m_j}]^{s^*}}{g^{L(M^*)\cdot s^*}}\\&=\frac{g_2^{a+r^*(u'+\sum_{i=1}^{n}u_i^{ID_i})}\cdot(g_2^{K(M^*)}g^{L(M^*)})^{s^*}}{g^{L(M^*)\cdot s^*}}\\&=g_2^a=g^{ab}\end{aligned}$$

下面分析 B 成功的概率，B 不放弃满足以下条件：

(1) $F(ID_i)\neq 0 \bmod l_u$；

(2) $K(M_j)\neq 0 \bmod l_m$；

(3) $K(M^*)=0 \bmod q$，$F(ID^*)=0 \bmod q$。

假定 $q_I\leqslant q_e+q_s$，为了方便计算，作如下定义：

A_i：$F(ID_i)\neq 0 \bmod l_u$，$i=1,\cdots,q_I$

B_i：$K(M_j)\neq 0 \bmod l_m$，$j=1,\cdots,q_s$

C：$F(ID^*)=0 \bmod q$

D：$K(M^*)=0 \bmod q$

算法 B 模拟成功的概率为 $P_i[\neg abort]=\Pr[\bigwedge_{i=1}^{q_I}A_i\ \bigwedge_{i=1}^{q_s}B_i\wedge C\wedge D]$。

函数 F 和 K 是相互的，即事件 $(\bigwedge_{i=1}^{q_I}A_i\wedge C)(\bigwedge_{i=1}^{q_s}B_i\wedge D)$ 是相互独立的。由 $l_u(n+1)<q$，得到 $F(ID_i)=0 \bmod q\Rightarrow F(ID_i)=0 \bmod l_u$。即如果 $F(ID_i)=0 \bmod l_u$ 存在唯一的 k_u $(0\leqslant k_u\leqslant n)$，满足 $F(ID)=0 \bmod q$，已知 $k_u,x',x_1,\cdots,x_n$ 随机选取，所以：

$$\begin{aligned}\Pr[A^*]&=\Pr[F(ID^*)=0 \bmod q\wedge F(ID^*)=0 \bmod l_u]\\&=\Pr[F(ID^*)=0 \bmod l_u]\cdot\Pr[F(ID^*)=0 \bmod q/F(ID^*)=0 \bmod l_u]\\&=\frac{1}{l_u}\frac{1}{n+1}\end{aligned}$$

因为事件 A_i 和 C 是相互独立的，则：

$$\begin{aligned}\Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C]&=\Pr[C]\Pr[\bigwedge_{I=1}^{q_I}A_i/C]\\&=\Pr[C](1-\Pr[\bigvee_{i=1}^{q_I}\neg A_i/C])\\&=\Pr[C](1-\sum_{i=1}^{q_I}\Pr[\neg A_i/C])\\&=\frac{1}{l_u(n+1)}(1-\frac{q_I}{l_u})\\&\geqslant\frac{1}{l_u(n+1)}(1-\frac{q_e+q_s}{l_u})\end{aligned}$$

类似处理，求得：

$$\begin{aligned}\Pr[\bigwedge_{i=1}^{q_s}B_i\wedge D]&=\Pr[D]\Pr[\bigwedge_{I=1}^{q_S}B_i/D]\\&=\frac{1}{l_m(n+1)}(1-\frac{q_s}{l_m})\end{aligned}$$

令 $l_u=2(q_e+q_s)$，$l_m=2q_s$，则：

$$\begin{aligned}\Pr[\neg abort]&=\Pr[\bigwedge_{i=1}^{q_I}A_i\ \bigwedge_{i=1}^{q_s}B_i\wedge C\wedge D]\\&=\frac{1}{l_u(n+1)}(1-\frac{q_e+q_s}{l_u})\cdot\frac{1}{l_m(n+1)}(1-\frac{q_s}{l_m})\\&=\frac{1}{16(q_e+q_s)q_s(n+1)^2}\end{aligned}$$

若 B 没有放弃，则 A 成功的概率为 ε，因此 B 能够以 $\varepsilon'=\frac{\varepsilon}{16(q_e+q_s)q_s(n+1)^2}$ 的概率解决 CDH 问题。

B 运行的时间等于 A 进行 q_e 次密钥询问和 q_s 次签名询问。每个密钥询问中需要 2 个群 G_1 中的指数运算。每个签名询问中需要 $(n+1)$ 个群 G_1 的指数运算。假设 G_1 中指数运算时间为 t_e。因此，总的运行时间至少为：

$$t'=t+(2q_e+(n+1)q_s)t_e$$

则上述算法 B 在不多于 t' 的时间内，以概率 ε' 成功解决了 CDH 困难问题，这与 (ε',t')-CDH 假定相矛盾，所以本文是安全的。

定理 2(不可区分性) 所提方案是 (ε,t,q_e,q_s) 无条件不可区分的。

证明：挑战者 C 与区分者 D 的交互如下：

系统参数设置：C 选取系统参数如下：

随机选取 $u',u_1,\cdots,u_n\in G_1$，$s_1,\cdots,s_n\in Z_q^*$ 并且计算 $m_j=g^{s_j}$ $(j=1,\cdots,n)$。C 将系统参数 $(G_1,G_2,e,q,g,g_1,g_2,u',m',u_1,\cdots,u_n,m_1,\cdots,m_n)$ 发送给 D。C 已知主密钥，运行参数私钥提取算法和签名算法，回答询问。

挑战：D 输出身份 ID^* 上消息 $M_0^*=(m_{0,1}^*,\cdots,m_{0,n}^*)$ 和 $M_1^*=(m_{1,1}^*,\cdots,m_{1,n}^*)$ 的签名 $\sigma_0^*=(\sigma_{0,1}^*,\sigma_{0,2}^*,\sigma_{0,3}^*)$ 和 $\sigma_1^*=(\sigma_{1,1}^*,\sigma_{1,2}^*,\sigma_{1,3}^*)$。$D$ 选择可修改的指数集合 K^*。假设 $K^*=(n-l+1,\cdots,n)$，则 $|K^*|=l$。

令 $K_1^*=\{i\in K^*,j\in\{0,1\}:m_{j,i}^*=0,m_i^*=0\}$，则 $K_1^*\cup$

$K_2^* = K^*$，$K_1^* \cap K_2^* = \phi$。C 随意选取 $r \in \{0,1\}$：

如果 $r=0$，C 随机选取 $\bar{r}_0^*, \hat{r}_0^* \in Z_q^*$，计算：

$$\bar{\sigma}_{0,1}^* = \sigma_{0,1}^* g_2^{\bar{r}_0^*(u'+\sum_{i=1}^{n} u_i^{ID_i})} \frac{\prod_{i\in k_1^*}(\sigma_{0,3}^*)^{s_i}}{\prod_{i\in k_2^*}(\sigma_{0,3}^*)^{s_i}} (v' \prod_{j=1}^{n} v_j^{m_{0,i}^*})^{\hat{r}_0^*}$$

$$\bar{\sigma}_{0,2}^* = \sigma_{0,2}^* g^{\bar{r}_0^*}, \bar{\sigma}_{0,3}^* = \sigma_{0,3}^* g^{\hat{r}_0^*}$$

令 $\bar{\sigma}^* = \bar{\sigma}_0^* = (\bar{\sigma}_1^* = \bar{\sigma}_{0,1}^*, \bar{\sigma}_2^* = \bar{\sigma}_{0,2}^*, \bar{\sigma}_3^* = \bar{\sigma}_{0,3}^*)$

如果 $r=1$，C 随机选取 $\bar{r}_1^*, \hat{r}_1^* \in Z_q^*$，计算：

$$\bar{\sigma}_{1,1}^* = \sigma_{1,1}^* g_2^{\bar{r}_1^*(u'+\sum_{i=1}^{n} u_i^{ID_i})} \frac{\prod_{i\in k_1^*}(\sigma_{1,3}^*)^{s_i}}{\prod_{i\in k_2^*}(\sigma_{1,3}^*)^{s_i}} (v' \prod_{j=1}^{n} v_j^{m_{1,i}^*})^{\hat{r}_1^*}$$

$$\bar{\sigma}_{1,2}^* = \sigma_{1,2}^* g^{\bar{r}_1^*}, \bar{\sigma}_{1,3}^* = \sigma_{1,3}^* g^{\hat{r}_1^*}$$

令 $\bar{\sigma}^* = \bar{\sigma}_1^* = (\bar{\sigma}_1^* = \bar{\sigma}_{1,1}^*, \bar{\sigma}_2^* = \bar{\sigma}_{1,2}^*, \bar{\sigma}_3^* = \bar{\sigma}_{1,3}^*)$

C 返回 $\bar{\sigma}^* = (\bar{\sigma}_1^*, \bar{\sigma}_2^*, \bar{\sigma}_3^*)$ 给 D。

当 C 得到签名后，D 继续进行私钥询问和签名询问。

$$\Pr[\bar{\sigma}_0^* = \bar{\sigma}^*] = \Pr\begin{bmatrix}\bar{\sigma}_{0,1}^* = \bar{\sigma}_1^* \\ \bar{\sigma}_{0,2}^* = \bar{\sigma}_2^* \\ \bar{\sigma}_{0,3}^* = \bar{\sigma}_3^*\end{bmatrix} = \Pr\begin{bmatrix}\bar{r}_0^* = \bar{r}^* \\ \hat{r}_0^* = \hat{r}^*\end{bmatrix} = \frac{1}{q^2}$$

$$\Pr[\bar{\sigma}_1^* = \bar{\sigma}^*] = \Pr\begin{bmatrix}\bar{\sigma}_{1,1}^* = \bar{\sigma}_1^* \\ \bar{\sigma}_{1,2}^* = \bar{\sigma}_2^* \\ \bar{\sigma}_{1,3}^* = \bar{\sigma}_3^*\end{bmatrix} = \Pr\begin{bmatrix}\bar{r}_1^* = \bar{r}^* \\ \hat{r}_1^* = \hat{r}^*\end{bmatrix} = \frac{1}{q^2}$$

由此可见，概率分布相同，区分者 D 的优势可以忽略。

因此，本方案满足不可区分性。

定理 3(不可变性) 若攻击者在 t 时间内，q_e 次私钥提取询问和 q_s 次签名询问后以优势 ε 攻破不可变性，则存在算法 B 以 $\varepsilon' = \varepsilon$，时间 $t' = t + (lq_e + 2lq_s)t_e$ 生成一个有效签名。其中，t_e 表示 G_1 中指数运算时间，l 表示允许改变的位数。

证明：假设存在攻击者 A 攻破方案的不可变性，则存在一个算法 B 以不可忽略的优势生成一个有效签名。B 运行 A 作为一个子程序在不可变性游戏里模拟挑战者与 A 进行交互。

初始化：假设 $k_s \subseteq \{1,\cdots,n\}$ 是净化者能够改变的指数集合。发送 $K \subseteq K_s$ ($K=\{n-l+1,\cdots,n\}$, ($|K|=l$)) 给 A。

系统建立：B 向挑战者 C 询问，得到 $(G_1, G_2, e, q, g, g_1, g_2, u', m', u_1, \cdots, u_{n-l}, m_1, \cdots, m_{n-l})$，进行：

(1) 随机选取 $t_i \in Z_q^*$ ($i=n-l+1,\cdots,n$)，计算 $u_i = g^{t_i}$ ($i=n-l+1,\cdots,n$)。

(2) 随机选取 $s_i \in Z_q^*$ ($i=n-l+1,\cdots,n$)，计算 $v_i = g^{s_i}$ ($i=n-l+1,\cdots,n$)。

B 返回系统参数 $(G_1, G_2, e, q, g, g_1, g_2, u', m', u_1, \cdots, u_{n-l}, m_1, \cdots, m_{n-l})$ 给 A。

询问：B 进行私钥提取询问和签名询问。

私钥提取询问：当 A 对身份 $ID=(ID_1,\cdots,ID_n)$ 进行私钥提取询问时，B 进行：

(1)对身份 $(ID_1,\cdots,ID_n)$ 进行私钥提取询问，得到 (d_1, d_2)。

(2)计算 $\bar{d}_1 = d_1 \cdot \prod_{i=n-l+1}^{n} d_2^{ID_i t_i}$，$\bar{d}_2 = d_2$。

B 返回 $(\bar{d}_1, \bar{d}_2)$ 给 A。

签名询问：A 对身份 $ID=(ID_1,\cdots,ID_n)$ 下的消息 $M=(m_1,\cdots,m_n)$ 进行签名询问，B 进行：

(1)询问 $(ID_1,\cdots,ID_n)$ 下的消息 $(m_1,\cdots,m_{n-l})$ 上的签名得到 $(\sigma_1,\sigma_2,\sigma_3)$。

(2)计算 $\bar{\sigma}_1 = \sigma_1 \cdot \prod_{i=n-l+1}^{n} \sigma_2^{ID_i t_i} \cdot \prod_{i=n-l+1}^{n} \sigma_3^{m_i s_i}$，$\bar{\sigma}_2 = \sigma_2$，$\bar{\sigma}_3 = \sigma_3$。

B 返回 $(\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3)$ 和 $\sigma_3^{m_i s_i}$ ($i=n-l+1,\cdots,n$) 给 A。

伪造：A 输出身份 $\overline{ID}^* = (\overline{ID}_1^*,\cdots,\overline{ID}_n^*)$ 的消息 $\overline{M}^* = (\overline{m}_1^*,\cdots,\overline{m}_n^*)$ 的签名 $\bar{\sigma}^* = (\bar{\sigma}_1^*, \bar{\sigma}_2^*, \bar{\sigma}_3^*)$。

(1)A 发送签名 $\bar{\sigma}^* = (\bar{\sigma}_1^*, \bar{\sigma}_2^*, \bar{\sigma}_3^*)$ 给 B。对任何 $j \in \{1,\cdots,q_s\}$，存在 $i \notin \{n-l+1,\cdots,n\}$ 且 $m_{j,i} \neq m_i^*$。

(2) B 设置 $(ID_1^*,\cdots,ID_{n-l}^*)$ 和消息 $M^* = (m_1^*,\cdots,m_{n-l}^*)$，$m_i^* = \overline{m}_i^*$，$i=1,\cdots,n-l$。对任何 $j \in \{1,\cdots,q_s\}$，存在 $i \notin \{1,\cdots,n-l\}$，$m_{j,i} \neq m_i^*$。$B$ 计算

$$\sigma_1^* = \frac{\bar{\sigma}_1^*}{\prod_{i=n-l+1}^{n} (\bar{\sigma}_2^*)^{ID_i^* i_i^*} \cdot \prod_{i=n-l+1}^{n} (\bar{\sigma}_3^*)^{\overline{m}_i^* s_i^*}}$$

$$\sigma_2^* = \bar{\sigma}_2^*, \sigma_3^* = \bar{\sigma}_3^*$$

因此，$\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ 是身份 $ID^* = (ID_1^*,\cdots,ID_{n-l}^*)$ 下的消息 $M^* = (m_1^*,\cdots,m_{n-l}^*)$ 的有效签名。由定义 1 可知，可以解决 CDH 问题。

当 A 成功时，B 以 ε 的概率即可成功。由定理 1 分析方法可知，$t' = t + (lq_e + 2lq_s)t_e$

6 效率分析

表 1 给出明洋方案[15]和所提方案的比较。由于 $e(g_1, g_2)$ 可以进行预计算，因此在计算验证计算量时，略去这个部分的计算量。表 1 中 $|G|$ 表示 G 中元素的长度，$|G_2|$ 表示 G_2 中元素的长度，Exp 表示指数运算的运算量，E 表示对运算的运算量。

表 1 计算量与通信量比较

方案	签名长度	签名计算量	验证计算量
明洋方案	3|G|	5Exp	3E
本文方案	2|G|+G2	2Exp	Exp+2E

由表 1 可以看出，所提方案的签名计算量减少 3 个指数运算、1 个 e 运算。另外，在该方案的签名中，$\sigma_2 = d_2 = e(g, g_2)^{r_{ID}}$ 由于可以进行预计算而作为系统公开参数的一部分，即签名 $\sigma = (\sigma_1, \sigma_3)$，因此减少了运算量，降低了通信代价。

结束语 作为一种特殊的签名，基于身份可净化签名有着广泛的应用，特别适合净化者为了隐藏敏感信息而改变签名文件的情况。本文利用 Waters 方法，结合基于身份的加密和净化签名提出了一种高效的基于身份可净化签名方案。分析表明所提方案在标准模型下可证安全，与文献[15]的标准模型下安全的方案相比，该方案进一步缩短了系统参数的长度，减小了验证算法的计算量。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto 1984. New York: Springer-Verlag, 1984: 47-53

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

[3] Paterson K G. ID-based signatures from pairings on elliptic curves[J]. IEEE Comunication Letter, 2002, 38(18)

[4] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups [C] // Proceeding of LNCS. Heidelberg: Springer-Verlag, 2003: 18-30

[5] Hess F. Efficient identity based signature schemes based on pairings[C] // Proceeding of LNCS. Heidelberg: Springer-Verlag, 2003: 310-324

[6] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C] // Proceedings of the 11th Australasian Conferece on Information Security and Privacy. Berlin/Heidelberg: Springer-Velag, 2006: 207-222

[7] Miyazaki K, Susaki S, Iwamura M, et al. Digital documents sanitizing problem[J]. IEICE Technical Report, 2003, 103: 61-67

[8] Steinfeld R, Bull L, Zheng Y. Content extraction signatures[C] // Proceeding of Information Security and Cryptology-ICISC. Berlin: Springer-Verlag, 2001: 285-304

[9] Ateniese G, Chou D H, de Medeiros B, et al. Sanitizable signatures[C] // Proceeding of Computer Security-ESORICS. Berlin: Springer-Verlag, 2005: 159-177

[10] Lonowskim M, Lauks A. Extended sanitizable signatures[C] // Proceeding of Information Security and Cryptology-ICISC. Berlin: Springer-Verlag, 2006: 343-355

[11] Canard S, Laguillaumie F, Milhau M. Trapdoor sanitizable signatures and their application to content protection[C] // Proceedings of Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2008: 258-276

[12] Brzuska C, Fischlin M, Freudenreich T, et al. Security of sanitizable signatures revisited[C] // Proceedings of Public Key Cryptography-PKC. Berlin: Springer-Verlag, 2009: 317-336

[13] Brzuskac, Fischlinm, Lehmanna, et al. Sanitizable signatures: how to partially delegate control for authenticated data[C] // Proceedings of Special Interest Group on Biometrics and Electronic Signatures. Bonn: GI, 2009: 117-128

[14] Brzuskac, Fischlinm, Lehmanna, et al. Unlinkability of sanitizable signatures[C] // Proceedings of Public-Key Cryptography-PKC. Berlin: Springer-Verlag, 2010: 444-461

[15] Ming Yang, Shen Xiao-qin, Peng Ya-mian. Identity- Based Sanitizable Signature Scheme in the Standard Model[C] // Proceedings of International Conference on Intormation Computing and Application. Berlin/Heidelberg: Springer-Verlag 2010: 9-16

[16] Waters B. Efficient identity-based encryption without random oracles [C] // Proceedings of Eurocrypt. Berlin/Heidelberg: Springer-Verlag, 2005: 114-127

[17] 李继国，姜平进. 标准模型下可证安全的基于身份的高效签名方案[J]. 计算机学报，2009(11)：2130-2136

(上接第 149 页)

由图 3 可见，在整个过程中，线性网络编码中间节点的处理过程保持不变；并且，网络编码是作用在已产生的密文上的。所以尽管产生混沌序列的初值是在实数域中进行选择，但它并未影响到进行网络编码的有限域，整个安全网络编码的有限域没有任何改变。所以，基于混沌序列的安全网络编码具有普遍通用性。

结束语 本文提出了一种基于混沌序列的低开销的安全网络编码方案，其利用混沌序列和“一次一密”加密体制的特性，结合线性随机网络编码，对原始信源消息向量进行了改变。该安全网络编码方案不需要知道网络拓扑，内部节点不需要任何新的功能且对有线和无线网络均适用。

经理论特性分析和安全性定理的证明表明，改进的安全网络编码方案在攻击者有有限计算能力和窃听能力的情况下，能够达到信息论安全的要求，有效地减小了开销，并且适用于所有线性网络编码。

参 考 文 献

[1] Ahlswede R, Cai Ning, Li S Y R, et al. Network Information Flow [J]. IEEE Transactions on Information Theory, 2000, 46 (4): 1204-1216

[2] Yeung R W. Distributed source coding for satellite communications [J]. IEEE Transactions on Information Theory, 1999, 45 (4): 1111-1120

[3] Cai N, Yeung R. Secure network coding [C]// IEEE International Symposium Information Theory. 2002, 2: 323

[4] Feldman J, Malkin T, Servedio R A. On the capacity of secure network coding [C] // 42nd Annual Allerton Conf. Commun. 2004

[5] Feldman J, Malkin T, Servedio R A. Secure network coding via filtered secret sharing [C] // 42nd Annual Allerton Conf. Commun. 2004

[6] Zhang Yan, Xu Cheng-qi, Wang Feng. A novel scheme for secure network coding using one-time pad [C] // International Conference on Networks Security, Wireless Communications and Trusted Computing. vol. 1, 2009: 92-98

[7] Maximilian R, Sagduyu Y E, Honig M L, et al. Training overhead for decoding random linear network codes in wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2009, 27(5): 729-737

[8] 徐光宪，付晓. 基于稀疏矩阵的低复杂度安全网络编码算法[J]. 计算机工程，2012，38(9)：55-57

[9] Adeli M, Liu Hua-ping. Secure Network Coding with Minimum Overhead Based on Hash Functions [J]. IEEE Communications Letters, 2009, 13(12): 956-958

[10] 李克荣. 基于网络编码和 Hash 函数的一个保密通信方案 [D]. 扬州：扬州大学，2010

[11] Jain K. Security based on network topology against the wiretapping attacking[J]. IEEE Wireless Communication, 2004(2): 68-71

[12] Bhattad K, Narayanan K R. Weakly Secure Network Coding [EB/OL]. http://netcod.org/papers/06Bhattad N-final.pdf, 2007-05-22

[13] 赵慧，卓新建，陆传赉. 一种基于网络拓扑的安全网络编码算法分析 [C]//通信理论与技术新进展—第十三届全国青少年通信学术会议. 2008: 844-846

[14] 徐光宪，付晓. 抗万能攻击的安全网络编码[J]. 计算机科学，2012，39(8)：88-91

[15] 徐光宪，吴巍. 基于伪随机序列的 Arnold 加密算法[J]. 计算机科学，2012，39(12)：79-82

[15] 李菲菲. 混沌扩频序列的研究 [D]. 葫芦岛：辽宁工程技术大学，2011

[16] Jaggi S, Sanders P, Chou P A, et al. Polynomial time algorithms for multicast network code construction [J]. IEEE Transactions on Information Theory, 2005, 51(6): 1973-1982

[17] 王汝言，楼芃雯，樊思龙，等. 容迟网络编码节点状态感知的数据转发策略[J]. 重庆邮电大学学报：自然科学版，2013，25(2)：215-220