一类可证安全的基于身份代理签名体制*

顾纯祥，李景峰，祝跃飞
(信息工程大学 信息工程学院 计算机与网络工程系，河南 郑州 450002)

摘 要：当前，基于身份的数字签名体制研究取得丰硕的成果，利用双线性映射的 GDH(Gap Diffie-Hellman) 问题，人们提出了许多可证安全的基于身份密码体制。提供了一种直接利用现有的基于身份的数字签名体制，构造基于身份代理签名体制的途径，并利用可证安全理论，在标准计算模型下给出了严格的安全性证明。

关键词：基于身份签名体制；基于身份代理签名体制；可证安全；存在性伪造
中图法分类号：TP309.2 **文献标识码**：A **文章编号**：1001-3695(2005)10-0096-03

A Class of Provable Secure ID-based Proxy Signature Schemes

GU Chun-xiang, LI Jing-feng, ZHU Yue-fei
(Dept. of Computer & Network Engineering, College of Information Engineering, Information Engineering University, Zhengzhou Henan 450002, China)

Abstract: In the last couple of years, ID-based cryptosystems have got fruitful achievements. Using the bilinear pairings, people proposed many new ID-based crypto schemes with provable-security. In this paper, we first describe how to construct a secure ID-based proxy signature schemes from any secure ID-based signature scheme. Then, with the theory of provable-security, we prove that the construction is secure in the standard computational model.

Key words: ID-based Signature; ID-based Proxy Signature; Provable Security; Existential Forgery

1 引言

自 M Mambo 等人[1] 在 1996 年首先提出代理签名体制以来，人们对如何构造安全有效的代理签名体制的研究产生了极大的兴趣[1,2,4]。由于应用环境的复杂性，代理签名体制的安全问题一直是人们关注的焦点之一。文献[1,2]对代理签名体制的安全特性进行了一定的研究，提出安全代理签名体制应具有以下性质：①可验证性；②强不可伪造性；③强身份确认性；④强不可否认性；⑤禁止错误使用。

这些非形式的要求为代理签名体制的安全性分析提供了启发式的安全目标，对代理签名体制研究具有重要意义，但是，它们的具体含义是不够清晰的。以此为依据进行安全性分析，由于缺乏严密的理论证明，其结论往往是不可靠的。现实情况是：现有的许多代理签名体制都存在安全问题，伴随着新的代理签名体制的提出，旧的体制不断被攻破。读者可以在文献[3]中看到翔实的例子。近年来，基于计算复杂度的“可证安全”理论[5,6] 成为定义密码体制安全和获得安全性证据的较为实用的方法。最近，文献[4]对以基于证书的 PKI 类代理签名的可证安全性进行了一定的研究，并建立了相应的安全模型。

基于身份的代理签名是一种特殊的基于身份公钥密码体制(ID_PKC)。早在 1984 年，A Shamir[7] 就提出基于身份密码体制的思想：将公开的身份信息(如 E-mail 地址、IP 地址，名字等)作为用户公钥/私钥对的公钥部分，用户私钥由一个称为私钥生成者(PKG)的可信第三方生成。相对 PKI/CA 技术，基于身份的密码体制无须公钥证书的管理与鉴别，在应用中带来极大的便利。近年来，随着双线性映射及相关计算问题的提出和椭圆曲线上 Weil 对和 Tate 对的成功应用[8,9]，基于身份的密码体制获得了长足的发展，一方面，基于身份的加密、签名新体制[8,9] 被不断提出；另一方面，其安全性理论也日趋成熟。但是，基于身份的代理签名体制方面的进展则不够理想。F Zhang 等人[10] 提出了一个基于身份的代理签名体制，但由于缺乏相应的安全模型，文中只能对该体制进行简单的非形式化分析。

收稿日期：2004-10-05；修返日期：2004-11-08
基金项目：国家“973”计划资助项目(G1999035804)；国家自然科学基金资助项目(9020415, 60473021)；河南省杰出青年基金资助项目(0212001400)

2 双线性映射及基于身份的数字签名体制

设 q 为大素数，G_1 和 G_2 分别为 q 阶的加法循环群和乘法循环群。映射 $\hat{e}: G_1 \times G_2 \to G_2$ 具有如下性质：

(1) 映射 $\hat{e}$ 具有双线性，对所有 $P, Q \in G_1$，$\alpha, \beta \in Z_q$，有 $\hat{e}(\alpha P, \beta Q) = \hat{e}(P, Q)^{\alpha\beta}$；

(2) 对 G_1 的生成元 P，$\hat{e}(P, P)$ 是 G_2 的生成元；

(3) 对任意的 $P, Q \in G_1$，存在有效算法计算 $\hat{e}(P, Q)$。

实际中，利用椭圆曲线上的 Weil 对或 Tate 对可构造有效的具有上面性质的双线性映射。

称 G_1 满足 GDH 假设，若 G_1 的 DDH(判定性 Diffie-Hellman) 问题是容易的，而 CDH(计算性 Diffie-Hellman) 问题是困难的。在本文的描述中，默认系统参数 G_1 满足 GDH 假设，并且 G_1 上离散对数问题(DLP)也是困难的。

一般而言，基于身份数字签名体制是由四个多项式时间算法组成的算法组[9]：

(1) *Setup*。参数生成算法，由可信中心 PKG 完成，输入安

全参数 $1^k(k\in N)$,输出系统主密钥 s 和系统参数 $para$, PKG 公开发布 $para$,保密主密钥 s。

(2) *Extract*。私钥解析算法,输入用户身份 $ID_U\in\{0,1\}^*$, PKG 利用掌握的主密钥 s 和系统参数,解析出秘密私钥 d_U,把 d_U 通过安全信道传送给用户作为私钥,身份 ID_U 作为相应公钥。

(3) *Sign*。签名算法,输入用户私钥 d_U 和消息 $m\in\{0,1\}^*$,返回相应签名(m,σ)。

(4) *Verify*。签名的验证算法,输入用户身份 ID_U 和签名(m,σ),验证该签名是否为身份 ID_U 的用户的合法签名。

在可计算理论中,函数 $f: N\to R$ 称为可忽略的,如果对的多项式 $p(\cdot)$ 存在 $n_p\in N$,使得当 $n>n_p$ 时,$f(n)\leq 1/p(n)$。

文献[9]提出了基于身份的数字签名体制的安全性定义——适应性选择消息和身份下存在性不可伪造的(EUF-ACMIA)。

定义 1　安全的基于身份数字签名体制: *ID_Sign* 为基于身份数字签名体制,$S(\cdot)$ 表示以签名谕示,$E(\cdot)$ 表示私钥解析谕示,*ID_Sign* 称为适应性选择消息和身份下存在性不可伪造的(EUF-ACMIA),如果对任意的概率多项式时间的谕示图灵机 A,概率

$$Succ(A)=Pr\left[\begin{array}{l}para\leftarrow Setup(1^n),(ID,m,\delta)\leftarrow A^{S(\cdot)E(\cdot)}(para):\\ Verify((m,\delta,ID)=1,(ID,m,)\notin S_{list},(ID,.)\notin E_{list}\end{array}\right]$$

是可以忽略的。其中 S_{list} 和 E_{list} 分别表示 A 对谕示 $S(\cdot)$ 和 $E(\cdot)$ 的所有访问及相应应答所构成的序列。

3　一类基于身份代理签名体制的构造

当前,基于身份的数字签名体制研究取得丰硕的成果,基于双线性映射的 GDH 问题,文献[9]皆提出了可证安全的基于身份签名体制。但是,基于身份的代理签名研究则相对薄弱, F Zhang 等人[10]提出了一个基于身份的代理签名体制。据我们所知,这是目前唯一的基于身份的代理签名体制,但由于缺乏相应的安全模型, F Zhang 等人没有证明该体制是“可证安全”的。

本文利用基于身份的密码体制存在可信的 PKG 为用户生成私钥的特点,提供了一种直接利用现有的基于身份的数字签名体制,构造基于身份代理签名体制的途径,并在标准模型下给出了安全性证明。首先我们对该体制进行形式化定义。

3.1　基于身份代理签名体制的形式化定义

定义 2　基于身份代理签名体制:一个基于身份代理签名体制是由一组多项式时间算法组成的算法组(令 A 为授权者,身份为 ID_A; B 为代理者,身份为 ID_B)。

(1) *Setup*:参数生成算法,由可信中心 PKG 完成,输入安全参数 $1^\lambda(\lambda\in N)$,输出系统主密钥 s 和系统参数 $para$, PKG 保密 s, 公开 $para$。

(2) *Extract*:私钥生成算法,输入 $ID_U\in\{0,1\}^*$, PKG 计算用户私钥 d_U 并通过安全信道传送给身份为 ID_U 的用户。

(3) *PD*:授权算法,输入 A 的私钥 d_A 和授权信息 m_ω(包含 ID_A, ID_B 及授权限制 R 等),输出为对 B 的授权证书 $proxy_{A\to B}$。

(4) *PV*:授权验证算法,输入为 ID_A 和授权证书 $proxy_{A\to B}$,验证 $proxy_{A\to B}$ 是否为 A 对 B 的合法代理授权。

(5) *PSKG*:代理密钥对生成算法,输入代理者私钥 d_B 和授权证书 $proxy_{A\to B}$,生成用于代理签名的私钥 d_p。

(6) *Sgn*:代理签名算法,输入代理私钥 d_p,消息 $m\in\{0,1\}^*$,输出代理签名(m,σ)。

(7) *Ver*:代理签名的验证算法,输入 ID_A 和对 m 的代理签名(m,σ),验证该签名是否为 A 的有效代理签名。

(8) *ID*:输入一个合法代理签名(m,σ),输出代理者身份 ID_B。

3.2　一种基于身份代理签名体制的构造方法

设 $ID\_Sign=\{Setup, Extract, Sgn', Ver'\}$ 为基于身份的数字签名体制,以 *ID_Sign* 可构造代理签名体制 $ID\_PSign=\{Setup, Extract, PD, PV, PSKG, Sgn, Ver, ID\}$,其中记授权者为 A,身份为 ID_A;代理者为 B,身份为 ID_B。

(1) *PD*, A 对授权信息 m_ω 产生数字签名,输出授权证书 $proxy_{A\to B}=(m_\omega, Sgn'(m_\omega, d_A))$。

(2) *PV*,如果 $Ver'(proxy_{A\to B}, ID_A)\neq 1$, B 拒绝接受代理;否则接受代理。

(3) *PSKG*,如果 B 接受代理, B 将 $proxy_{A\to B}$ 发送给 PKG, PKG 首先验证 A 的签名,若 $Ver'(proxy_{A\to B}, ID_A)=1$,则对 m_ω 解析出私钥 d_P,通过安全信道将 d_P 传送给 B,作为 B 对 A 的代理签名私钥。

(4) *Sgn*,设代理签名私钥为 d_P,对消息 m, B 计算签名 $\tau=Sgn'(m_\omega||m, d_P)$,以$(m_\omega,\sigma)$ 作为对消息 m 的代理签名。

(5) *Ver*,验证者收到代理签名$(m,(m_\omega,\sigma))$后,如果 $Ver'((m_\omega||m,\sigma,m_\omega)=1$ 且签名满足 m_ω 的代理限制,签名认证成功,否则失败。

(6) *ID*, m_ω 中包含 B 的身份标识 ID_B。

此时,我们称 *ID_PSign* 为由 *ID_Sign* 演化而来的基于身份的代理签名体制。

4　安全性证明

在基于计算复杂度的“可证安全”理论中,要证明一个体制是安全的,首先要建立一个安全模型,形式化的严格刻画攻击者的能力和要达到的安全目标,安全性证明就是要在某计算复杂度假设下(如 DLP, GDH 等),证明该体制确实达到定义的安全目标。

4.1　基于身份代理签名体制的安全模型

就基于身份代理签名体制而言,攻击者的最终目的是伪造代理签名或授权证书,根据攻击的结果可以分为如下几类:

(1) 完全摧毁。攻击者可以获得系统主密钥或与某个身份相对应的用户私钥或与某个授权证书向对应的代理签名私钥。

(2) 一般性授权伪造。攻击者获得一个有效的对任意授权信息生成合法授权证书的算法。

(3) 一般性代理签名伪造。攻击者有一个有效的对任意消息和授权证书,产生有效基于身份代理签名的算法。

(4) 存在性授权伪造。攻击者可以对某个新的授权信息生成合法授权证书。

(5) 存在性代理签名伪造。攻击者可以伪造对某个新的消息和授权证书,提供有效的基于身份代理签名。

基于身份代理签名体制工作在复杂的网络环境下,对于攻击者的能力,有著名的 Dolev-Yao 模型:攻击者的知识和能力不能够低估,可以控制整个通信网络,进行适应性主动攻击。就代理签名而言,最强的适应性主动攻击者应具有以下能力:

(1) 可以控制整个通信网络,具有监听、截获、伪造和窜改通信信息的能力;

(2) 具有控制一定数量的用户并获取其私钥的能力;

(3) 可以对选择的授权信息生成授权证书的能力;

(4) 可以对选取的授权证书和消息生成代理签名的能力;

(5) 可以控制一定数量的用户并获取其代理私钥的能力。

以形式化的语言描述,即攻击者除可以控制网络通信外,还具有访问以下谕示的能力:

(1) *Extract(.)*。私钥解析谕示,输入身份 ID_i,得到相应私钥 d_i。

(2) *PD(.)*。授权谕示,输入授权者身份 *ID* 和授权信息 m_ω,输出授权 *proxy*。

(3) *PSKG(.)*。代理私钥生成谕示,输入代理者身份 *ID* 和授权 *proxy*,输出代理私钥 d_p。

(4) *Sgn(.)*。代理签名谕示,输入授权 *proxy* 和消息 $m\in\{0,1\}^*$,输出代理签名(m, ϑ)。

一个基于身份代理签名体制是安全的,应该达到以下安全目标:

(1) 在适应性主动攻击下,存在性授权伪造成功的概率是可忽略的;

(2) 在适应性主动攻击下,存在性基于身份代理签名伪造成功的概率是可忽略的。

以形式化语言描述,称基于身份的代理签名体制是适应性选择消息和身份的攻击下存在性不可伪造的(D&S-EUF-ACMIA),如果对任意的概率多项式时间的攻击者 A(即谕示图灵机),在下面的试验中获得非零返回值的概率是可以忽略的。

定义 3 试验 $Exp_A(k)$: $ID\_PS=(Setup, Extract, PD, PV, PSKG, Sgn, Ver, ID)$ 是基于身份的代理签名体制,攻击者为 *A*,安全参数 *k*,定义试验 $Exp_A(k)$:

(1) 运行 Setup,把生成的系统参数 *para* 给 A。

(2) 令 $C_{list}\leftarrow\Phi$; $D_{list}\leftarrow\Phi$; $G_{list}\leftarrow\Phi$; $S_{list}\leftarrow\Phi$。

(3) *A* 的输入为 *para*, *A* 可以任意的次序做任意次以下操作或询问:

①询问 *Extract(.)* 谕示,输入身份 ID_i,得到相应私钥 d_i,令 $C_{list}=C_{list}\cup\{(ID_i, d_i)\}$;

②询问 *PD(.)* 谕示,若 *A* 得到 $proxy\leftarrow PD(ID_i, m_\omega)$,令 $D_{list}=D_{list}\cup\{(ID_i, m_\omega, proxy)\}$;

③询问 *PSKG(.)* 谕示,若 *A* 得到 $d_P\leftarrow PSKG(ID_j, proxy)$,令 $G_{list}=G_{list}\cup\{(ID_j, proxy, d_P)\}$;

④询问 *Sgn(.)* 谕示,若 *A* 得到 $(m, \vartheta\leftarrow Sgn(proxy, m))$,令 $S_{list}=S_{list}\cup\{(proxy, m, \vartheta\}$。

(4) *A* 输出 $(ID_i, m_\omega, proxy)$ 或 $(proxy, m, \vartheta)$。

(5) 若 *A* 的输出结果满足下面条件之一,则攻击成功:

①输出为 $(ID_i, m_\omega, proxy)$,满足 $PV(proxy, ID_i)=1$, $(ID_i,.)\mid C_{list}$, 且 $(ID_i, m_\omega, proxy)\mid D_{list}$, $Exp_A(k)$ 返回值为 1;

②输出为 $(proxy, m, \vartheta)$,设授权者和代理者身份分别为 ID_i 和 ID_j,满足 $Ver((m, \vartheta, ID_i)=1$, $(proxy, m,.)\notin S_{list}$, 且 $(ID_j,.)\notin C_{list}$, $(ID_j, proxy,.)\notin G_{list}$, $Exp_A(k)$ 返回值为 2;否则 $Exp_A(k)$ 返回值为 0。

定义 4 安全的基于身份代理签名体制:基于身份的代理签名体制 *ID_PS* 是安全的,若对任意的概率多项式时间的攻击者 A,任意的多项式 $p(.)$ 和所有的充分大的 *k*,有:

$Pr[Exp_A(k)=1]<1/p(k)$ 且 $Pr[Exp_A(k)=2]<1/p(k)$,即 *ID_PS* 是适应性选择消息和身份的攻击下存在性不可伪造的(D&S-EUF-ACMIA)。

4.2 安全性证明

定理 1 设 $ID\_PSign=\{Setup, Extract, PD, PV, PSKG, Sgn, Ver, ID\}$ 为由 $ID\_Sign=\{Setup, Extract, Sgn', Ver'\}$ 演化而来的基于身份代理签名体制,若 *ID_Sign* 是 *EUF-ACMIA*,则 *ID_PSign* 是 D&S-EUF-ACMIA。

证明:假设存在概率多项式时间的攻击者 A,执行 $Exp_A(k)$,并以不可忽略的概率 ε返回值不为 0,由 A 可以构造 *ID_Sign* 的 ACMIA 攻击者 B。

(1) 运行 Setup,把生成的系统参数 *para* 作为 B 的输入。

(2) 令 $C_{list}\leftarrow\Phi$, $D_{list}\leftarrow\Phi$, $G_{list}\leftarrow\Phi$, $S_{list}\leftarrow\Phi$。

(3) 将 *para* 作为 A 的输入,运行 A 执行 $Exp_A(k)$,B 如下模拟 A 的各谕示:

①*Extract(.)* 谕示,对询问 ID_i, B 以 ID_i 访问自己的 *Extract(.)* 谕示,并把结果作为对 A 的应答,令 $C_{list}=C_{list}\cup\{(ID_i, d_i)\}$。

②*PD(.)* 谕示,对输入 ID_i 和 m_ω, B 以 ID_i 和 m_ω 访问 *Sgn'(.)* 谕示,设得到应答为 δ B 以 $proxy=(m_\omega, \delta)$ 作为对 A 的应答,令 $D_{list}=D_{list}\cup\{(ID_i, m_\omega, proxy)\}$。

③*PSKG(.)* 谕示,对输入 ID_j 和 *proxy*,设 $proxy=(m_\omega, \delta)$,授权者身份为 ID_i,若 $Ver'(proxy, ID_i)\neq 1$, B 应答为⊥;否则, B 以 m_ω 访问自己的 *Extract(.)* 谕示,把应答 d_P 作为对 A 的应答,令 $G_{list}=G_{list}\cup\{(proxy, d_P)\}$。

④*Sgn(.)* 谕示,对输入 *proxy* 和 *m*,设 $proxy=(m_\omega, \delta)$, B 以 m_ω 和 $m_\omega||m$ 访问 *Sgn'(.)* 谕示,设得到应答为 τ B 以 (m_ω, ϑ) 作为对 A 的应答,令 $S_{list}=S_{list}\cup\{(proxy, m, \vartheta\}$。

(4) 设 S'_{list} 和 E_{list} 分别表示攻击者 B 对签名谕示 *S'(.)* 和密钥解析谕示 *E(.)* 的所有访问及相应应答所构成的序列。若 A 输出 $(ID_i, m_\omega, proxy)$,满足 $PV(proxy, ID_i)=1$, $(ID_i,.)\mid C_{list}$, 且 $(ID_i, m_\omega, proxy)\notin D_{list}$,设 $proxy=(m_\omega, \delta)$,则 B 可输出 (ID_i, m_ω, δ) 满足 $Ver'((m_\omega, \delta), ID_i)=1$ 且 $(ID_i, m_\omega,.)\notin S'_{list}$, $(ID_i,.)\notin E_{list}$;若 A 的输出 $(proxy, m, \vartheta)$,设 $proxy=(m_\omega, \delta)$,授权者和代理者身份分别为 ID_i 和 ID_j,满足 $Ver((m, \vartheta, ID_i)=1$, $(proxy, m,.)\notin S_{list}$, $(ID_j,.)\notin C_{list}$, $(proxy,.)\notin G_{list}$,则 B 可输出 $(m_\omega, m_\omega||m, \vartheta)$ 满足 $Ver'((m_\omega||m, \vartheta, m_\omega)=1$ 且 $(m_\omega||m, m_\omega,.)\notin S'_{list}$, $(m_\omega,.)\notin E_{list}$。

可见,若 A 执行 $Exp_A(k)$ 以不可忽略的概率 ε返回值不为 0,则概率

$$Succ(B)=\Pr\left[\begin{array}{l}Para\leftarrow Setup(1^n), (ID, m, \delta)\leftarrow B^{S(.),E(.)}(para):\\ Ver'((m, \delta), ID)=1\&(ID, m,.)\notin S'_{list}\&(ID,.)\notin E_{list}\end{array}\right]\geq\varepsilon$$

即 *ID_Sign* 存在概率多项式时间的 ACMIA 攻击者以不低于 ε的概率存在性伪造成功。因此,若 *ID_Sign* 是 EUF-ACMIA,则 *ID_PSign* 一定是 D&S-EUF-ACMIA。

(下转第 133 页)

返回地址。

(5) 一般方法(General) 。除没有参数和返回值外, 与 C 过程相同。

(6) 一般 C 方法(general C) 。同 C 过程。

3 例子

FreeLove(也称 3544 幽灵, one-half) 病毒是一种变形混合病毒[6]。它有若干组加密指令, 每组有十条指令。每次传染这十条指令都被插入原文件的十个不固定的位置。每条指令占十个字节, 这十个字节除包含指令字节外, 是一些无意义的"填充"字节, 指令字节在其中位置不定。

下面是 VDL 语言对 FreeLove 病毒的描述:

```
virusdescription {
virusinfo
virusname: " FreeLove" ;
viruslength: 3544;
virustype: mixed;
sideeffect: " destroy file" ;
filedata
long sig; // FreeLove 病毒的特征码包含在位置 sig 处, sig 在某个方法中被赋值
include { 0x2e, 0x89, 0x87, 0xa0, 0x02, 0x2e, 0x8c, 0x9f,
0xa2, 0x02, 0x2e, 0xc6, 0x87, 0xa9, 0x02, 0x23} at sig;
include orgfile[ . . ] with rest; // 使用方法 Rest 恢复原文件
com: { // com 文件的头三个字节包含在病毒体偏移 0x10 处
include orgfile[ 0. . 3] at virusbody + 0x10;
} ;
exe: { // exe 文件的文件头包含在病毒体偏移 0x10 处
include orgfile[ 0. . 0x1a] at virusbody + 0x10
}
bootdata // 在主引导记录 MBR 包含特征码
include { 0x8e, 0xd3, 0xfb, 0x8e, 0xdb, 0x83, 0x2e, 0x13,
0x04, 0x04, 0xb1, 0x06, 0xcd, 0x12, 0xd3, 0xd0} at MBR;
method
int key1, key2, key3;
general Init
{ //查找加密密钥, 略
} ;
// 查询方法 sch 定义
search sch( p)
{ // 略
} ; // 加密方法 Encry 定义
encrypt encry( p)
{
// 略
} ; // 恢复方法 Rest 定义
restore rest( p)
{ // 略
} ; }
```

4 结束语

VDL 针对病毒的检测和清除而设计, 对绝大多数病毒, 描述程序不超过 20 行。使用 LEX 和 YACC 编写 VDL 的编译程序, 将 VDL 的描述程序翻译成 C 程序, 然后再编译生成可执行程序。对于病毒的检测, 没有采用通常病毒检测程序使用的 Aho-Corasick 算法[7~9], 而是采用定位查找算法, 即在指定位置查找相应的特征串, 极大地减少误报率; 清除子程序根据病毒描述中被感染程序的数据进行恢复。通过试验表明, 自动产生的病毒检测和清除程序执行效率和准确率都相当高。

参考文献:

[1] evin, R B. The Computer Virus Handbook[C] . Osborne McGraw-Hill, 1990.

[2] Hoffman L J. Rogue Programs[C] . Van Nostrand Reinhold, 1990.

[3] Perriot F. Striking Similarities: Win32 / Simile and Metamorphic Virus Code Symentec[EB/OL] . http: / / securityresponse. symantec. com/ avcenter/ reference / striking. similarities. pdf, 2002.

[4] 祝恩, 等. 计算机病毒自动变形机理的分析[J] . 计算机工程与科学, 2002, 24(6) : 14-17.

[5] David M Chess. Virus Verification and Removal Tools and Techniques [EB/OL] . http: / / www. research. ibm. com / antivirus/ SciPapers/ Chess / CHESS3 / chess3. html, 1991.

[6] 张红瑞. 幽灵病毒的特征与清除[J] . 计算机世界, 1996, 2: 88-91.

[7] Aho A V, *et al.* Efficient String Matching: An Aid to Bibliographic Search[J] . Communications of the ACM, 1975, 18: 333-340.

[8] Aho A V. Algorithms for Finding Patterns in Strings[C] . Jvan Leeuwen. Handbook of Theoretical Computer Science: Algorithms and Complexity, volume A, MIT Press, 1990. 255-300.

[9] Kumar S, *et al.* Generic Virus Scanner in C + + [C] . Proceedings of the 8th Computer Security Application Conference, 1992. 210-219.

作者简介:

左志宏(1966-) , 男, 副教授, 主要研究方向为计算机网络与信息安全; 周明天(1939-) , 男, 教授, 博士生导师, 主要研究方向为计算机网络与网络安全。

(上接第 98 页)

参考文献:

[1] Mambo, K Usuda, E Okamoto. Proxy Signatures for Delegating Signing Operation[C] . 3rd ACM Conference on Computer and Communications Security (CCS '96) , New York: ACM Press, 1996. 48-57.

[2] B Lee, H Kim, K Kim. Strong Proxy Signature and Its Applications [C] . Proc. of the 2001 Symposium on Cryptography and Information Security (SCIS '01) , vol 2 / 2, Oiso, Japan, 2001. 603-608.

[3] Guilin Wang, *et al.* Security Analysis of Some Proxy Signatures[EB/OL] . Information Security and Cryptology-ICISC 2003, Primary version Available, http: / / eprint. iacr. org / 2003 / 196 / .

[4] A Boldyreva, *et al.* Secure Proxy Signature Schemes for Delegation of Signing Rights[EB/OL] . http: / / eprint. iacr. org / 2003 / 096.

[5] S Goldwasser, S Micali, R Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks[J] . SIAM Journal of Computing, 1988, 17(2) : 281-308.

[6] D Pointcheval, J Stern. Security Arguments for Digital Signatures and Blind Signatures[J] . Journal of Cryptology, 2000, 13(3) : 361-369.

[7] A Shamir. Identity-based Cryptosystems and Signature Schemes[C] . Advances in Cryptology-CRYPTO '84, volume 196 of LNCS, Springer-Verlag, 1984. 47-53.

[8] D Boneh, M Franklin. Identity-based Encryption from the Weil Pairing[C] . J Kilian. Advances in Cryptology- CRYPTO 2001, volume 2139 of LNCS, Springer-Verlag, 2001. 213-229.

[9] J C Cha, J H Cheon. An Identity-based Signature from Gap Diffie-Hellman Groups[C] . Y Desmedt. Public Key Cryptography-PKC 2003, volume 2567 of LNCS, Springer-Verlag, 2002. 18-30.

[10] F Zhang, K Kim. Efficient ID-based Blind Signature and Proxy Signature from Bilinear Pairings[C] . ACISP 03, LNCS 2727, Springer-Verlag, 2003. 312-323.

作者简介:

顾纯祥(1976-) , 男, 安徽霍山人, 教员, 博士研究生, 主要研究方向为网络安全; 李景峰(1977-) , 男, 江苏南京人, 博士研究生, 主要研究方向为网络安全; 祝跃飞(1962-) , 男, 浙江杭州人, 教授, 博士生导师, 主要研究方向为网络安全。