一个可证安全和前向安全的群盲签名方案

张硕英[1] 刘 锋[2]

[1](山东工商学院计算机科学与技术学院 山东 烟台 246005)

[2](山东工商学院数学与信息科学学院 山东 烟台 246005)

摘 要 在公共资源的管理、重要情报的签发和电子现金系统中,群签名都发挥着重要作用。但是群签名效率不高,且无法保证信息的匿名性。为此,通过盲化信息和简化签名过程,提出一种基于中国剩余定理的、高效的、具有前向安全性的群盲签名方案,并在随机预言机模型下证明其安全性。该方案可以动态地增加或删除群成员而不需要频繁地改变其余群成员的密钥信息,仅需通过计算改变群公开信息。通过群成员私钥随时间更新,使方案具有前向安全性。对该方案进行效率分析,方案系统开销较小,签名长度较短,更适用于公开且低带宽的通信环境。

关键词 群签名 盲签名 短签名 前向安全性 可证安全 动态性

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.03.047

A PROVABLY SECURE AND FORWARD SECURE GROUP SIGNATURE SCHEME

Zhang Shuoying[1] Liu Feng[2]

[1](*School of Computer Science and Technology, Shandong Technology and Business University, Yantai 246005, Shandong, China*)

[2](*School of Mathematics and Information Science, Shandong Technology and Business University, Yantai 246005, Shandong, China*)

Abstract Group signature scheme plays an important role in the management of public resources, the issuance of important information, and electronic cash systems. However, group signature scheme is inefficient, and it cannot guarantee the anonymity of information. To address the problem, an efficient and forward-secure blind group signature scheme based on the Chinese remainder theorem is proposed. The scheme simplified the signing process and blinds information. Its security was proved under the random oracle model. The scheme could dynamically add or delete group members without frequently changing the key information of the remaining group members. And the scheme only needed to change the group public information through calculation. Meanwhile, the private keys of group members were updated over time, so that the scheme had forward security. The efficiency of the scheme was analyzed. The scheme had a small system overhead and a short signature length. And the scheme was more suitable for open and low-bandwidth communication environments.

Keywords Group signature Blind signature Short signature Forward security Provably secure Dynamics

0 引 言

随着互联网的快速发展,电子现金系统成为人们生活中极其重要的支付方式。其中使用最广泛的技术,便是数字签名。随着数字签名的研究和发展,使数字签名方案具有了各种特殊的性质,例如盲性。1983 年,Chaum[1] 提出盲签名方案。这种方案下,签名者无法得知所签消息的具体内容,也无法在对消息签名之后得知何时签署的这条消息。1991 年,群签名(即群数字签名)[2] 是由 Chaum 等提出的一个签名概念。这种机制中,一个群组中的任一成员可通过匿名的方式代表整个群组对消息进行签名。与其他签名方案相同,群签名可以公开验证。同时群中有一个群管理员

收稿日期:2020 - 10 - 29。国家自然科学基金面上项目(61771294,61972235)。**张硕英**,硕士生,主研领域:密码学。**刘锋**,教授。

可以通过打开签名的方式,追踪到具体的签名者。1998 年,Lysyanskaya 等[3]在国际金融密码会议上,将群签名技术和盲签名技术相结合,提出了群盲签名方案,以实现一个在线的多银行电子先进系统。2004 年,文献[4]提出一个基于中国剩余理论的群签名方案。该方案在添加或删除群成员时,不改变其他合法群成员的密钥。之后又有不少方案在文献[4]的基础上进行改进,使方案具有防联合攻击性。2015 年,文献[5]也利用中国剩余定理设计了一个群签名方案。以上群签名方案均对消息没有保护措施。盲签名可以对用户需要签名的信息提供有效的保护。许多盲签名方案也被相继提出。但是群盲签名方案的效率低下,这样的方案离实际应用于电子现金系统还有一段距离。

短签名方案[6]被提出后,很多相关方案都是在文献[6]方案基础上进行了改进,或者在某种特定环境下在文献方案的基础上设计特定方案[7-8]。另外,数字签名技术中,存在一不可忽视的问题—密钥泄漏。密钥泄漏会引起之前合法签名的失效。为解决这一问题,Anderson[9]提出了前向安全性的概念。前向安全性是指通过密钥的定期更新,使其对之前密钥进行保护,某一时刻的密钥泄漏不会影响之前密钥对信息的签名。文献[10]提出了一个前向安全的代理签名方案。文献[11]将前向安全技术应用到群签名方案中。文献[12]利用中国剩余定理提出的群签名方案具有前向安全性,并实现了抗共模攻击功能。文献[13]通过 BLS 短签名方案中涉及的办法设计了签名方案,并通过密钥更新使方案具有前向安全性,但是该方案密钥更新无限制,时间长会加重系统负担。文献[14]提出一个前向安全群签名方案。该方案可以对密钥进行更新,并对更新次数进行限制,但签名过程计算量大,系统开销较大。

本文基于中国剩余定理提出一个可证安全的具有前向安全性的群盲签名,方案可以动态高效地添加或删除群成员,同时盲化签名消息和简化签名过程,减少系统计算量,签名长度较短;证明其正确性、匿名性、动态性、可追踪性、前向安全性,并在随机预言机模型下证明其不可伪造性。

1　基础知识

定义 1　双线性对。在双线性映射中,设 l 是一个安全参数,q 是一个 l-bit 的素数。G_1、G_2是分别由 P、Q 生成的阶为 q 的循环加法群和循环乘法群。设群 G_1、G_2中的离散问题都是困难问题。称映射 $e:G_1\times G_1\rightarrow G_2$为双线性对,其中 Z_q^* 为循环群,如果映射 e 满足以下性质:

1) 双线性性:对于任意的 $a,b\in Z_q^*$,$e(aP,bQ)=e(P,Q)^{ab}$总是成立。

2) 非退化性:$e(P,Q)\neq 1$。

3) 易计算性:存在与给定的安全参数相关的有效算法计算:$e(P,Q)$。

定义 2　计算性 Diffie-Hellman 问题(CDH 问题)。给定 $P,aP,bP\in G_1$($a,b\in Z_q^*$ 是未知的随机数),计算 $abP\in G_1$是困难的。

2　具有前向安全性的群盲签名

本文根据中国剩余定理(孙子定理)设计一个签名长度较短、满足盲性且具有前向安全性的群签名方案。方案由以下部分构成。

2.1　系统建立

1) 系统参数。选择 2 个阶为 l-bit 的素数的群 G_1(由 g 生成)、G_2(其中 l 为选定的安全参数),定义双线性映射:$e:G_1\times G_1\rightarrow G_2$,另外选取一个安全的哈希函数 $H:\{0,1\}^*\rightarrow\{0,1\}^l$,公布系统参数$\{l,G_1,G_2,g,H\}$。

2) 假设 GM 为群管理员,有 k 个拥有 I_{D_i}的群成员 $P_i(i=1,2,\cdots,k)$。群管理员为每个群成员 P_i随机选取一个大素数 p_i,且这些大素数互不相同,保证在p_i-1中包含 2 个大素数,同时保证乘法群 $Z_{p_i}^*$ 的生成元为 g。每一位群成员 P_i随机选择所属的初始私钥 $x_{i,0}\in Z_{p_i}^*$,并且计算其公钥 $y_i=x_{i,0}g(\mathrm{mod}\ p_i)$。将计算出的公钥 y_i发送给群管理员,群管理员规定群成员公钥生存时间为 T 个时间段,当公钥生存时间用尽时,群成员需要重新选择私钥,并计算公钥。在这 T 个时间段内,群成员的私钥 $x_{i,0}$随时间更新,但公钥 y_i不变。

群管理员利用群成员的公钥 y_i和之前选择的 p_i,构造如下的同余方程组:

$$\begin{cases} c\equiv y_1(\mathrm{mod}\ p_1)\\ c\equiv y_2(\mathrm{mod}\ p_2)\\ \quad\vdots\\ c\equiv y_k(\mathrm{mod}\ p_k)\end{cases}$$

解为:$c=P'_1P_1p_1+P'_2P_2p_2+\cdots+P'_kP_kp_k(\mathrm{mod}\ P)$。其中:$P=p_1p_2\cdots p_k$,$P_i=P/p_i$,$P'_iP_i=1(\mathrm{mod}\ p_i)$,$i=1,2,\cdots,k$。

最后,群管理员将(g,c)作为公开参数,并将(I_{D_i},y_i)保存,以便用来之后打开签名追踪签名者。

2.2 群成员的加入

假设现有安全用户 P_{k+1} 请求加入群组(或者 GM 需要添加用户 P_{k+1} 为群成员),首先 GM 选择一个大素数 p_{k+1} 发送给用户 P_{k+1},其中 $p_{k+1}\neq p_i(i=1,2,\cdots,k)$。用户 P_{k+1} 随机选取 $x_{k+1,0}\in Z^*_{p_{k+1}}$ 作为初始私钥,并计算相应的公钥 $y_{k+1}=x_{k+1,0}g(\bmod p_{k+1})$ 发送给 GM,GM 收到用户 P_{k+1} 的公钥 y_{k+1} 之后,根据中国剩余定理重新计算 c 并公开,同时保存 $(I_{D_{k+1}},y_{k+1})$。完成以上操作,用户 P_{k+1} 便成为群中的成员了。

根据上述过程,可以得到如下结论:增加群成员这一过程不会令其他合法群成员密钥对发生改变,需要改变的是群组系统公开参数 c 和群管理员维护的 (I_{D_i},y_i) 列表。

2.3 群成员的删除

假设 GM 要删除某群成员 P_j,GM 只需要将 P_j 的公钥 y_j 改为 y'_j,确保 $y'_j\neq y_j$,而后利用中国剩余定理重新计算新的同余方程组的解 c 并公布,同时删除 GM 维护的 (I_{D_i},y_i) 列表中的 (I_{D_j},y_j)。通过上述过程,群成员 P_j 就被 GM 删除了,其密钥也不再能生成有效的群签名。

通过上述过程,可以得到如下结论:新成员的加入不会令其他合法群成员密钥对发生改变,需要改变的是群组系统公开参数 c 和群管理员维护的 (I_{D_i},y_i) 列表。

2.4 密钥更新

设群成员 P_i 的初始私钥为 $x_{i,0}$。在第 1 个时间段内,通过密钥更新算法计算用户私钥,为 $x_{i,1}=x^2_{i,0}(\bmod p_i-1)$。以此类推,在第 $j+1$ 个时间段内,通过密钥更新算法计算用户私钥,为 $x_{i,j+1}=x^2_{i,j}(\bmod p_i-1)$。当第 $j+1$ 个时间段的私钥产生后,立即抹除第 j 个时间段的私钥记录。当 $j=T$ 时,第 $j+1$ 个时间段内的用户私钥为空串。

当公钥生存时间用尽后,群成员需要重新选取私钥,计算公钥并发送给群管理员。群管理员更新用户信息。

2.5 群签名的生成

在第 t 时间段内,消息持有者向群组申请对消息 m 进行签名。

① 消息盲化。消息持有者计算 $h=(I_{D_i},y_i,m)$,随机选取 2 个秘密值 $u,v\in Z^*_q$,计算 $V=vg,\lambda=uh+V$,将 λ 发送给群成员 P_i。

② 签名。群成员 P_i 计算 $S_1=x_{i,t}\lambda$,将 (t,S_1) 发送给消息持有者。

③ 脱盲。消息持有者计算 $S_2=S_1-vy_j^{2^t},S=u^{-1}S_2$,则 S 为群成员 P_i 对消息 m 的签名。

④ 最终签名对为 (t,m,p_i,S)。

2.6 群签名验证

验证者接受到 (t,m,p_i,S) 后,想要对群成员部署的签名进行验证,需要如下操作。

1) 利用群公开参数 c,通过对 $y_i\equiv c(\bmod p_i)$ 的计算,得到 y_i。

2) 其次判断 $e(S,g)=e(h,y_i^{2^t})$,等式成立则说明签名合法。

2.7 签名打开

当发生争议需要打开签名时,群管理员可以通过计算 $y_i\equiv c(\bmod p_i)$ 得到 y_i,再通过查询 (I_{D_i},y_i) 列表,查出用户的 I_D,从而就能确定签名者的具体身份。

3 安全性分析

3.1 正确性分析

定理 若签名 (t,m,p_i,S) 是合法的群签名,则能通过签名验证。

证明 验证者利用群公开信息 (g,c) 和签名 (t,m,p_i,S),通过 $y_i\equiv c(\bmod p_i)$ 计算出签名者的公钥 y_i,而后验证 $e(S,g)=e(h,y_i^{2^t})$ 等式是否成立。验证过程如下:

$$\begin{aligned}
&e(S,g)=e(u^{-1}S_2,g)=\\
&\quad e(u^{-1}(S_1-vy_i^{2^t}),g)=\\
&\quad e(u^{-1}((x_{i,t}\lambda)-vy_i^{2^t}),g)=\\
&\quad e(u^{-1}((x_{i,t}(uh+vg))-vy_i^{2^t}),g)=\\
&\quad e(u^{-1}((x_{i,t}(uh+vg))-v(x_{i,0}^{2^t}g)),g)=\\
&\quad e(u^{-1}(x_{i,t}uh),g)=e(x_{i,t}h,g)=e(h,x_{i,t}g)=\\
&\quad e(h,y_i^{2^t})
\end{aligned}$$

3.2 盲性证明

对于任意给定的合法签名 (t,m,p_i,S) 及任意中间值 (λ,V,h,S_1,S_2),只存在唯一盲化因子 $u,v\in Z^*_q$。因为对 $u,v\in Z^*_q$ 选择具有随机性,所以签名方案的盲性是显然的。

现在,证明给定的合法签名 (t,m,p_i,S) 及任意中间值 (λ,V,h,S_1,S_2),对任意的 $u,v\in Z^*_q$ 均满足式(1)-式(3)。

$$\lambda=uh+V \tag{1}$$

$$S_1=x_{i,t}\lambda,S_2=S_1-vy_j^{2^t},S=u^{-1}S_2 \tag{2}$$

$$V=vg \tag{3}$$

由式(1)－式(3)可得到 $u=\log_g(\lambda-V)\in Z_q^*$, $v=\log_g V\in Z_q^*$。通过函数性质可得盲化因子的唯一性。

下面证明 $u,v\in Z_q^*$ 满足式(2)。由双线性对的基本性质,可得:

$$S_2=S_1-vy_i^{2^t}\Leftrightarrow e(S_2,y_i^{2^t})=e(S_1-vy_i^{2^t},y_i^{2^t})$$

因此,只需要证明 $u,v\in Z_q^*$ 满足等式 $e(S_2,y_i^{2^t})=e(S_1-vy_i^{2^t},y_i^{2^t})$。由于$(t,m,p_i,S)$是合法签名,即 $e(S,g)=e(h,y_i^{2^t})$。则:

$$\begin{aligned}e(S_1-vy_i^{2^t},y_i^{2^t})&=e(x_{i,t}\lambda-vx_{i,t}g,y_i^{2^t})=\\&e(x_{i,t}(uh+vg)-vx_{i,t}g,y_i^{2^t})=\\&e(x_{i,t}uh,y_i^{2^t})=e(S_2,y_i^{2^t})\end{aligned}$$

因此,盲化因子 $u,v\in Z_q^*$ 总是存在,盲化因子参与的运算过程与最终合法签名无任何关联。盲性得证。

3.3　存在不可伪造性

本节将在安全模型[15]下对方案进行安全性分析。

定理　存在一个适应性选择消息和身份的攻击者 F,以(t,ε)攻破本文方案,记 F 访问 H 预言机、签名预言机的次数分别为 q_H、q_S,则存在一个(t',ε')算法 C 在时间 $t'<t+(q_St_S+2q_Ht_H)$内以 $\varepsilon'\geqslant\left(\varepsilon-\frac{1}{2^l}\right)\left(1-\frac{1}{q_H}\right)^{q_S}\frac{1}{q_H}$的优势解决 CDH 困难性问题。其中 t_H、t_S表示询问 H 预言机和签名预言机一次所花费的时间。

证明　假定给 C 一个挑战:给定 $ag\in G$ 和 $bg\in G$, C 的目标是调用 F 为子程序,最终输出 CDH 困难性问题的一个解 abg。

C 在系统建立初始化后,挑选身份 I_D 作为挑战身份,挑战身份 I_D 的公钥为 $y=ag$,发送系统参数和 y 给 F。

1) H 询问:C 维护一个含数组(m_i,d_i,h_i)的列表 H^{List}。当 F 对(I_D,y,m)进行 H 询问,如果该询问值已在列表中,C 返回以前定义的值;否则,C 操作如下:

(1) 如果 $m\neq m^*$,则随机选择一个 $d\in Z_q^*$,计算 $h=dg$,C 再将其作为 $H(I_D,y,m)$的值返回给 F。C 记录(I_D,y,m)到 H^{List}。

(2) 如果 $m=m^*$,则 C 返回给 F 一个值为 bg 的数据(bg 作为 $H(I_D,y,m)$的输出值),并且在 H^{List}中记录$(m,\perp,bg)$(其中"⊥"为空)。

2) 签名询问:当 F 对 C 进行一个关于 m 的签名询问时:

(1) 如果 $m=m^*$,C 返回"⊥"。(该事件用 E_2表示)。

(2) 如果 $m\neq m^*$ 时,C 从 H^{List}中恢复数组列表(m,d,h),随机选择 $u,v\in Z_q^*$,计算 $V=vg$,$\lambda=uh+V$, $S_1=du\lambda+vy$,$S_2=S_1-vy_j^{2^t}$,$S=u^{-1}S_2$返回给 F,容易验证 S 满足签名验证 $e(S,g)=e(h,y_i^{2^t})$。

之后 F 不再进行询问,并输出一个关于身份 I_D 的签名消息对$(\overline{m},S^*)$,且该签名满足验证签名等式 $e(S,g)=e(h,y_i^{2^t})$。如果 $\overline{m}\neq m$,伪造失败。(该事件用 E_2表示)。否则,$\overline{m}=m$,C 从 H^{List}中恢复数组列表$(m^*,\perp,bg)$,因为签名验证等式 $e(S^*,g)=e(h^*,y_i^{2^t})$成立,所以等式 $e(S^*,g)=e(bg,ag)^{2^t}=e(abg,g)^{2^t}$成立(其中 t 是时间常数)。

所以 C 可以通过 $ag\in G$ 和 $bg\in G$,成功计算出 abg 作为 CDH 问题的一个实例的解答。

下面分析 C 在这个过程中的优势:

1) 首先对 H 询问的回答与现实世界一样是不可区分的,在 Z_q^* 中的每一个回答是均匀独立分布的,且 H 询问的应答是有效的。

2) 对签名预言机的回答是有效的,除非事件 E_1或 E_2发生。

3) 如果 F 伪造了一个有效的签名,同时事件 E_1 和 E_2都不发生,则 C 就能够解决 CDH 问题的一个实例。

现计算这些事件发生的概率,显然下式成立:

$$P(\neg E_1\wedge\neg E_2)=\left(1-\frac{1}{q_H}\right)^{q_S}\cdot\frac{1}{q_H}$$

然而,这种模拟并不完美,当 F 没有进行询问就伪造出了合法的签名,这种事件发生的概率不超过$\frac{1}{2^l}$(其中 l 为安全参数),所以 C 在该过程中的优势为:

$$\varepsilon'\geqslant\left(\varepsilon-\frac{1}{2^l}\right)\left(1-\frac{1}{q_H}\right)^{q_S}\frac{1}{q_H}$$

而 C 运行的时间 $t'<t+(q_St_S+2q_Ht_H)$。

3.4　匿名性

群成员的身份信息由群管理员统一管理维护,除群管理员之外的用户均无法从合法的群签名中,计算出签名者的具体身份信息。即只确定签名由群组签署,无法得到签名者的具体身份,从而实现了匿名性。

3.5　可追踪性

如果对签名来源产生争议,群管理员通过群公开信息计算出用户公钥 y_i,而后根据系统建立之初所建立的群成员信息列表(I_{D_i},y_i),就可以追踪到签名者的具体身份。

3.6　动态性

群管理员可以动态地添加或删除群成员。当添加某成员时,仅需要利用用户提供的公钥和为用户选择

的大素数,构建新的同余方程组,根据中国剩余定理重新计算群公开信息并公开即可;当删除某群成员时,仅需要将其公钥改为不同的随机数,重新根据中国剩余定理计算公开信息 c 并公开即可。无论添加群成员还是删除群成员的过程,其他群成员的用户信息并没有受到影响。这种方式简单而高效,对其他用户也无影响。

3.7 前向安全性

群成员的私钥 $x_{i,t}$ 与时间段 $j(1\leqslant j\leqslant T)$ 建立联系,私钥随时间而变化。公钥 y_i 在生存时间内有效且保持不变。因为 $x_{i,j+1}=x_{i,j}^2(\bmod p_i-1)$ 是基于求解模平方根问题的困难性问题的单向函数。求解模平方根问题的困难性问题基于大素数的分解,所以在不知道大素数的分解情况下,通过 $x_{i,j+1}=x_{i,j}^2(\bmod p_i-1)$ 求解出第 j 个时间段之前的私钥是不可能的,因此群成员的私钥 $x_{i,t}$ 是前向安全的。

假设群成员第 j 个时间段的私钥 $x_{i,j}$ 泄漏后,攻击者想伪造 j 时间段之前的签名,必须求解出 j 时间段之前的私钥。如果攻击者能够求解出 j 时间段之前的私钥,说明攻击者能够解决模平方根问题的困难性问题。所以 j 时间段之前的签名是前向安全的。

综上所述,本文方案具有前向安全性。

4 效率分析

本文利用中国剩余定理设计一个具有前向安全性的短群盲签名方案,通过消息盲化过程,保证信息安全性,简化签名过程,减少系统计算开销。本文方案主要运算为模幂(运算量为 E)、模乘运算(运算量为 M)、模平方运算(运算量为 S)、双线性对运算(运算量为 e)、求逆运算(运算量为 I)、散列运算(运算量为 H)。将本文方案与相关经典签名方案进行计算量上的对比,如表 1 所示。

表 1 与其他方案的运算量比较

方案	密钥更新	成员增加	成员删除	签名算法	验证算法
文献[6]	无	无	无	E	$e+E$
文献[15]	无	无	无	E	$H+2e$
文献[12]	$2S$	$I(S+M)$	$E+IM$	$2E+M$	$2E+M$
文献[13]	$I(2E+4M)$	IE	IE	$E+4M+e$	e
文献[14]	S	IM	$E+IM$	$E+M$	$2E+M$
本文方案	S	IM	$E+IM$	E	$H+2e$

由表 1 中各个方案的计算量的比较,可以得到结论:本文方案在签名算法和验证算法上的效率与 BLS 短签名方案基本相同。在签名长度方面,选择阶为 160 bit 的椭圆曲线上的群和双线性对映射,安全强度相当于 1 024 bit 的 RSA 密码体制算法,本文方案的签名长度为 160 bit,与 BLS 短签名方案[6]基本相同。签名长度较短利于在公开且低带宽的通信环境进行传输。在密钥更新和成员更换过程中,与文献[16]和文献[19]相比,本文系统开销更少。与文献[14]方案相比较,在签名和验证签名的总效率上,本文计算量较少、效率较高。

5 结 语

本文方案利用中国剩余定理高效动态地添加删除群成员,通过密钥更新算法实现前向安全性,并限制密钥的生存时间,进一步提高安全性;通过盲化消息保护待签名消息的安全性;简化签名过程,减少系统计算量。通过对本文方案进行安全性分析,实现了不可伪造性、前向安全性等特性。进行效率分析,发现与同类典型方案相比,本文方案签名长度较短,盲化和签名过程简单,适用于传输受限的应用场所。但当群成员数量较多时,要求群管理员系统有较强的计算能力。下一步将研究在群成员数量较多时,减少群组系统的系统开销。

参 考 文 献

[1] Chaum D. Blind signatures for untraceable payments[C]// Advances in Cryptology,1983:199 - 203.

[2] Chaum D, Heyst E. Group signatures[C]//Workshop on the Theory and Application of Cryptographic Techniques, 1991:257 - 265.

[3] Lysyanskaya A, Ramzan Z. Group blind digital signatures: A scalable solution to electronic cash[C]//International Conference on Financial Cryptography,1998:184 - 197.

[4] 陈泽文,张龙军,王育民,等.一种基于中国剩余定理的群签名方案[J].电子学报,2004(7):1062 - 1065.

[5] 党佳莉,俞惠芳.使用中国剩余定理的群签名方案[J].计算机工程,2015,41(2):113 - 116.

[6] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[C]//International Conference on the Theory and Application of Cryptology and Information Security, 2001:514 - 532.

[7] Karati A, Biswas G. Cryptanalysis and improvement of a certificateless short signature scheme using bilinear pairing [C]//International Conference on Advances in Information Communication Technology and Computing,2016:1 - 6.

(下转第 320 页)

编文件的标准化规则进行钻研,将复杂的数据格式精细化,进一步加快模型的执行速度。

参 考 文 献

[1] 范宇杰,陈黎飞,郭躬德. 软件代码的恶意行为学习与分类[J]. 数据采集与处理,2017,32(3):612 - 620.

[2] 吴丽娟,李阳,梁京章. 一种基于明可夫斯基距离的加壳 PE 文件识别方法[J]. 现代电子技术,2016,39(19):80 - 81.

[3] 杨燕,蒋国平. 基于 N-Gram 的计算机病毒特征码自动提取的改进方法[J]. 计算机科学,2017,44(S2):338 - 341,361.

[4] Lee T H, Kwang-Ho K. A study on detection of small size malicious code using data mining method[J]. Convergence Security Journal,2019,19(1):11 - 17.

[5] Naeem H, Guo B, Naeem M, et al. Identification of malicious code variants based on image visualization[J]. Computer & Electrical Engineering,2019,76:225 - 237.

[6] Webster G, Kolosnjali B, Zarras A, et al. Deep learning for classification of malware system call sequences[C]//29th Australasian Joint Conference,2016:137 - 149.

[7] Fan Y J, Hou S F, Zhang Y M, et al. Gotcha-sky malware Scorpion: A metagraph2vec based malware detection system [C]//24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining,2018:253 - 262.

[8] Ntantogian C, Poulios G, Karopoulos G, et al. Transforming malicious code to ROP gadgets for antivirus evasion[J]. IET Information Security,2019,13(6):570 - 578.

[9] 李翼宏,刘方正,杜震宇. 一种改进主动学习的恶意代码检测算法[J]. 计算机科学,2019,46(5):92 - 99.

[10] 刘亚姝,王志海,侯跃然,等. 一种基于概率主题模型的恶意代码特征提取方法[J]. 计算机研究与发展,2019,56(11):2339 - 2348.

[11] 陈博,马秀峰. 国内 LDA 模型研究现状可视化分析[J]. 情报探索,2020(11):128 - 134.

[12] Benmalek M, Challal Y, Derhab A. An improved key graph based key management scheme for smart grid AMI systems [C]//IEEE Wireless Communications and Networking Conference,2019:15 - 18.

[13] Sun J C, Yao Y, Xia Y, et al. Exploring the characteristics of acupoints in the treatment of stroke with complex network and point mutual information method[J]. TMR Non-Drug Therapy,2019,2(3):95 - 102.

[14] 张梦琇,周菊玲. 几何分布的参数估计及 EM 算法[J]. 数学的实践与认识,2018,48(20):125 - 128.

[15] Mora D, Rivera G, Velasquez I, et al. A virtual element method for the vibration problem of Kirchhoff plates[J]. ESAIM: Mathematical Modelling and Numerical Analysis, 2018,52(4):1437 - 1456.

[16] 李建伏,巴建军. 基于 MCMC 的 DBSCAN 改进算法[J]. 计算机工程与设计,2020,41(1):122 - 126.

[17] He S M, Shin H S, Tsourdos A. Distributed multiple model joint probabilistic data association with Gibbs sampling-aided implementation[J]. Information Fusion,2020,64:20 - 31.

[18] 胥小波,张文博,何超,等. 一种基于行为集成学习的恶意代码检测方法[J]. 北京邮电大学学报,2019,42(4):89 - 95.

[19] 强晗,郭亚兰,田礼明. 基于深度置信网络的恶意代码检测方法研究[J]. 计算机技术与发展,2019,29(7):93 - 97.

[20] 咎家玮,杨勇. 基于 DOM 树的跨站脚本攻击防御技术研究[J]. 通信与信息技术,2018(3):62 - 67.

[21] 李江华,邱晨. 一种基于元信息的 Android 恶意软件检测方法[J]. 计算机应用研究,2019,36(10):3058 - 3062.

(上接第 312 页)

[8] Lin C, Shen Z, Chen Q, et al. A data integrity verification scheme in mobile cloud computing[J]. Journal of Network and Computer Applications,2017,77:146 - 151.

[9] Anderson R. Two remarks on public key cryptography[C]// ACM Conference on Computer and Communications Security, 1997:135 - 147.

[10] 赵雪娇. 一种具有前向安全的无证书数字签名方案[J]. 信息通信,2019(2):109 - 110.

[11] Song D. Practical forward secure group signature schemes [C]//8th ACM Conference on Computer and Communications Security,2001:225 - 234.

[12] 欧海文,张沙蚌. 基于中国剩余定理的前向安全群签名[J]. 计算机应用,2011,31(S1):98 - 100.

[13] 王硕,程相国,陈亚萌,等. 前向安全的群签名方案[J]. 青岛大学学报(自然科学版),2017(3):38 - 42,47.

[14] 洪璇,张绪霞. 基于中国剩余定理的前向安全群签名方案[J]. 计算机应用研究,2020,37(9):2806 - 2810.

[15] 左黎明,夏萍萍,陈祚松. 一种可证安全的短盲签名方案[J]. 计算机工程,2019,45(12):114 - 118.

[16] 欧海文,雷亚超,王湘南. 一种安全高效的群签名方案[J]. 计算机应用与软件,2020,37(7):309 - 312,328.

[17] 岳笑含,惠明亨,王溪波. 基于群签名的前向安全 VANET 匿名认证协议[J]. 计算机科学,2018,45(S2):382 - 388.

[18] 徐潜,谭成翔,冯俊,等. 基于格的前向安全无证书数字签名方案[J]. 计算机研究与发展,2017,54(7):1510 - 1524.

[19] 王硕,程相国,陈亚萌,等. 基于身份的密钥隔离群签名方案[J]. 计算机工程与应用,2018,54(16):76 - 80.

[20] 王勇兵. 基于离散对数的双向安全签名方案[J]. 青海师范大学学报(自然科学版),2016,32(2):6 - 10.