

文章编号:1001-9081(2013)10-2854-04

doi:10.11772/j.issn.1001-9081.2013.10.2854

# 基于双线性对签密的安全高效远程证明协议

何 龙, 彭新光\*

(太原理工大学 计算机科学与技术学院, 太原 030024)

(\*通信作者电子邮箱 sxgrant@126.com)

**摘要:**为了解决当前远程证明方案中安全性差、效率较低的问题,提出了一种安全高效的模块级远程证明协议。该协议在构建模块属性签名时采用了签密方案,减少了属性证书的生成时间;而且采用椭圆曲线上基于双线性对的签密方案,同时也大大提高了属性证书的安全性。通过实验验证了协议的可行性。实验结果表明,该方案可以快速生成可信平台中各模块的属性签名,提高了远程证明的效率。

**关键词:**可信计算;远程证明;模块;双线性对;签密

中图分类号: TP309.7 文献标志码:A

## Safe and efficient remote attestation protocol based on bilinear pairings signcryption

HE Long, PENG Xinguang\*

(College of Computer Science and Technology, Taiyuan University of Technology, Taiyuan Shanxi 030024, China)

**Abstract:** In order to deal with the poor security and low efficiency in remote attestation, a module-level safe and efficient property attestation protocol was proposed. In the protocol, the signcryption was used to build the module property signature, which could reduce the time of building property certificate. And the signcryption scheme based on the bilinear pairings over elliptic curves also enhanced the security of property certificate. Finally, a model instance was presented to verify the feasibility of the protocol. The experiments show that the program can quickly generate the module property signature and improves the efficiency of the remote attestation.

**Key words:** trusted computing; remote attestation; module; bilinear pairing; signcryption

## 0 引言

作为可信计算的重要功能之一,远程证明以证明计算平台可信为目标,目前已成为可信计算的研究热点之一。自可信计算组织(Trusted Computing Group, TCG)提出远程证明<sup>[1-3]</sup>以来,很多工作<sup>[4-10]</sup>在此基础上实现了Linux系统中的远程证明机制。其中基于属性的远程证明与其他证明方案相比,具有明显的优点,它克服了基于二进制完整性远程证明<sup>[4]</sup>中的需要证明的信息量大、容易造成平台隐私泄露等缺点。Sadeghi等<sup>[6]</sup>首先提出基于属性的远程证明的概念,认为验证者并不是为了了解平台的配置信息细节,而是希望平台能够证明它具有某些方面的属性。与此同时,Poritz等<sup>[7]</sup>也对基于属性的证明做了相关研究;Chen等<sup>[8-9]</sup>提出了基于属性的远程证明协议(Property-Based Attestation, PBA),之后秦宇等<sup>[10]</sup>提出了基于组件属性的远程证明(Component Property-Based Attestation, CPBA),这些研究不断地推动着基于属性远程证明的快速发展。

现有的基于属性的远程证明具有以下缺点:证书发布机构为组件颁布属性证书后,证书完全暴露在不安全的网络环境中,其安全性难以得到保证;并且对于证书的签名和加密分步进行,效率较低。

针对以上缺点,本文在原有属性远程证明协议的基础上,提出了一种新的安全高效的模块级的属性远程证明方案BP-CPBA(Bilinear Pairing signcryption-Component Property-Vased

Attestation)。该方案有以下特点:引入签密,在对属性证书的安全性进行保护的同时,使得签名与加密在一步中同时完成,大大提高了效率;并且签密使用了基于椭圆曲线上双线性对<sup>[11-12]</sup>的方案,相对于安全性建立在基于大整数因数分解难题和一般离散对数问题的其他方案而言,本方案具有更高的安全性。

## 1 模块属性证明体系

### 1.1 BP-CPBA 体系结构

在本方案的证明体系中,包括五个部分,如图1所示。

1) 证书权威发布机构(Certificate Authorization, CA):作为可信第三方,负责生成模块生产商和验证中心的私钥,同时选定CA的主密钥和公钥。

2) 模块生产商(Module Factory, MF):在由权威机构CA建立模块生产商与验证中心的信任后,模块生产商MF负责生成签密证书。

3) 用户平台(User Platform, User):配置有可信平台模块(Trusted Platform Module, TPM),接受并且使用配有属性证书的各个模块,并且可以向服务提供商提出服务请求。

4) 服务提供商(Service Provider, SP):为用户平台提供各种服务,并且验证经由用户平台发送来的存储度量日志(Storage Measurement Log, SML)和平台配置寄存器(Platform Configuration Register, PCR)中的内容是否一致,但不具备针对签密证书的解签密能力。

收稿日期:2013-04-22;修回日期:2013-06-03。

基金项目:山西省自然科学基金资助项目(2009011022-2);山西省留学基金资助项目(2009-28)。

作者简介:何龙(1988-),男,陕西宝鸡人,硕士研究生,主要研究方向:网络安全、可信计算;彭新光(1955-),男,山西太原人,教授,博士生导师,CCF会员,主要研究方向:计算机网络安全。

5) 验证中心(Verification Center, VC): 负责验证属性签密证书的正确性, 并且具有验证属性与度量值对应关系的能力。

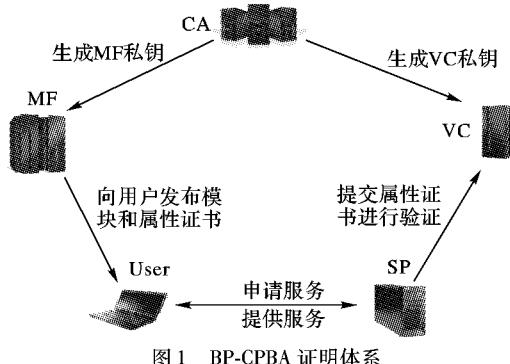


图 1 BP-CPBA 证明体系

## 1.2 证明流程

1) CA 发布模块生产商和验证中心的私钥。模块生产商和验证中心的公钥由它们的身份可以各自得出。同时 CA 选定自己的主密钥和公钥, 后者在 MF 签密时需用到。

2) 模块生产商生成模块, 并且生成属性签密证书。

3) 用户获得模块及相关证书, 并且可以向服务提供商提出服务请求。

4) 服务提供商要求验证模块可信与否, 并获得相关寄存器度量值和日志值以及模块的签密证书。

5) 服务提供商验证寄存器度量值与日志值是否一致, 并将签密证书和日志值的信息提交给验证中心。

6) 验证中心验证模块签密证书是否正确, 然后再验证证书中值与日志值的关系, 并将验证结果返回给服务提供商, 供服务提供商参考。

7) 服务提供商根据验证中心提供的验证结果, 决定是否与用户进行交互。

## 2 BP-CPBA 具体方案

### 2.1 方案中模块配置基本定义

根据 TCG 规范, 每个生产商的软件产品都被定义了一个 ID, 长度为 32 位。前 24 位代表生产商的 ID, 是生产商向 TCG 申请得到的, 后 8 位表示生产的具体软件产品的子信息。模块属性证书中的 ID 采用 TCG 的模块 ID。在经过模块生产商的 TPM 度量后, 会生成度量值(measure\_value)  $\zeta$ , 长度为 160 位; 最后是与该度量值安全等级相对应的属性值  $P$ , 长度为 160 位。

所以对于模块  $K_i$  其配置为  $(ID_i, \zeta_i, P_i)$ 。

### 2.2 BP-CPBA 详细步骤

本文提出了一种新的模块级的远程证明协议, 采用了一种基于椭圆曲线上双线性对的签密算法<sup>[12]</sup>来保证认证证书的安全性和高效性。BP-CPBA 分为四大步:

#### 2.2.1 模块属性证书的生成

1) CA 系统的初始化阶段。

(a) 系统建立(Setup)。

给定一个安全参数  $k$ , CA 选择两个阶均为素数  $q$  的循环群  $G_1$  和  $G_2$  ( $G_1$  为循环加法群,  $G_2$  为循环乘法群),  $P$  为  $G_1$  的生成元, 双线性映射  $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 。定义哈希函数  $H_1: \{0,1\}^* \rightarrow G_1$ ,  $H_2: G_2 \rightarrow \{0,1\}^n$ ,  $H_3: \{0,1\}^* \times G_2 \rightarrow \mathbb{Z}_q$ ,  $n$  为明文长度。CA 选择主密钥  $s \in \mathbb{Z}_q^*$ , 并计算  $P_{\text{pub}} = sP$ 。选择安全对称加解密算法  $E, D$ (本文选为 DES 算法)。CA 公开系统参

数  $\{G_1, G_2, n, \hat{e}, P, P_{\text{pub}}, H_1, H_2, H_3, E, D\}$ 。

(b) 密钥提取(Keygen)。

给定一个用户身份  $ID_u$  (如 MF 和 VC), CA 计算  $Q_u = H_1(ID_u)$  和私钥  $S_u = sQ_u$ 。

2) MF 产生签密文阶段(Signcrypt)。

MF 针对明文  $M = (ID \parallel \zeta \parallel P)$  产生签密文  $(c, r, S)$ 。

(a) MF 首先根据 VC 的身份标识计算 VC 的公钥  $Q_v = H_1(ID_v)$ ;

(b) MF 随机选取  $x \in \mathbb{Z}_q^*$ , 并计算  $k_1 = \hat{e}(P, P_{\text{pub}})^x$  和  $k_2 = H_2(\hat{e}(P_{\text{pub}}, Q_v)^x)$ ;

(c) 计算  $c = E_{k_2}(M)$ ,  $r = H_3(c, k_1)$  和  $S = xP_{\text{pub}} - rS_v$  ( $S_v$  为 CA 中算得的 MF 的私钥);

(d) 签密文为  $(c, r, S)$ 。

最后将签密文  $(c, r, S)$  作为签密后的模块属性证书发给用户 User。

#### 2.2.2 SP 与 User 之间的远程证明交互

用户平台向服务提供商发出服务请求, 服务提供商商会发回一个随机数  $Nonce$  和用户平台需要达到的安全等级。

用户平台的可信平台模块(TPM)对与安全等级相对应的模块进行度量。度量出模块  $mod_1$  到  $mod_n$  的度量值  $\zeta_1$  到  $\zeta_n$  (同时产生 SML 日志), 并用这些度量值形成摘要:

$$\sigma = \text{Hash}(ID_1 \parallel \zeta_1 \parallel \dots \parallel ID_n \parallel \zeta_n)$$

然后 TPM 利用  $sk_{\text{TPM}}$  进行签名( $sk_{\text{TPM}}$  为 TPM 中的身份证明密钥(Attestation Identity Key, AIK)):

$$\sigma_{\text{sign}} = \text{Sign}_{sk_{\text{TPM}}}(\sigma \parallel Nonce)$$

最终用户 User 向服务提供商 SP 提交的属性签名为:

$$\sigma_{\text{property}} = (\sigma_{\text{sign}}, \sigma, Nonce, SML, (c, r, S)_{mod_1}, \dots, (c, r, S)_{mod_n})$$

#### 2.2.3 服务提供商的验证

服务提供商在收到用户平台提供的  $\sigma_{\text{property}}$  后, 首先会验证 TPM 的身份证明密钥(AIK)证书的正确性, 然后将 SML 日志值与度量值进行比较, 查看两者是否匹配, 最后将  $\sigma_{\text{property}}$  交由验证中心 VC 进行解签密的验证。

#### 2.2.4 VC 中心的验证

1) VC 验证中心对需要验证的证书进行解签密。

对于每个签密文  $(c, r, S)$ , VC 将:

(a) VC 计算根据 MF 的身份标识计算 MF 公钥  $Q_s = H_1(ID_{\text{MF}})$ ;

(b) 计算  $k_1 = \hat{e}(P, S)\hat{e}(P_{\text{pub}}, Q_s)^r$ ;

(c) 计算  $k_2 = H_2(\hat{e}(S, Q_s)\hat{e}(Q_s, S_r)^r)$  ( $S_r$  为 CA 中算得的 VC 的私钥);

(d) 恢复消息  $M = D_{k_2}(c)$ ;

(e) 判断  $r = H_3(c, k_1)$  是否成立, 当且仅当等式成立时接受密文  $(c, r, S)$ ; 否则拒绝接受。

2) 在解签密成功后, VC 还要对日志中的度量记录和解签密后的结果进行对比, 这样可以保证 MF 在签密时所用到的 160 位的度量值与用户 User 处所获得的度量值确实一致。所以 VC 既保证了签密证书的真实性, 也保证了签密证书中值的正确性。最后 VC 将验证结果返回给 SP, 供服务提供商做出正确决策。

#### 2.3 BP-CPBA 协议安全性分析

本文中提出的远程证明方案满足以下安全要求:

1) 机密性。

在本方案中,由于密文  $c$  是由  $E$  加密而得,所以如果攻击者想从  $c$  中进行破解攻击,所面临的困难和破解对称式加密技术中的  $k_2$  一样。

$$k_2 = H_2(\hat{e}(P_{\text{pub}}, Q_r)^x) \quad (1)$$

$$k_2' = H_2(\hat{e}(S, Q_r)\hat{e}(Q_s, S_r)^r) \quad (2)$$

由于随机数  $x$  只有 MF 知道,所以也只有 MF 可以用  $x$  经过式(1)得到  $k_2$ ,而 VC 则可使用它的私钥  $S_r$  经过式(2)计算得到  $k_2'$ ,若 VC 的私钥正确,则所得的  $k_2'$  才会等于式(1)中的  $k_2$ ,也就是说,只有真实的通信双方才能得到相同的  $k_2$  和  $k_2'$ ,也才可以从  $c$  中解密得到  $M$ ,所以该方案满足机密性。

此外,如果 MF 或 VC 将其私钥泄露,则攻击者无法通过该私钥破解其他用户的私钥,由于私钥  $S_u = sQ_u$ ,即使攻击者拥有某用户(如 MF)的公钥和私钥,但攻击者无法解得 CA 的主密钥  $s$ ,若攻击者试图通过  $S_u = sQ_u$  而破解  $s$ ,则攻击者所面临的困难就等同于椭圆曲线上解离散对数难题(Elliptic Curve Discrete Logarithm Problem, ECDLP)。

## 2) 不可伪造性。

如果攻击者试图伪造  $(c', r', S')$ ,则在解签密时将无法获得通过。因为私钥  $S_s$  只有 MF 知道,这将进而导致  $S$  无法伪造,并且在解签密中计算  $k_1, k_2$  时,都用到了与该私钥对应的 MF 公钥  $Q_s$ ,所以如果攻击者有伪造,则式(3)和式(4)的推导过程将无法完成,即最终的解签密时算出的  $k_1'$  和  $k_2'$  都无法成为正确的  $k_1$  和  $k_2$ ,也就是说,在 VC 解签密时算得的  $k_1'$ 、 $k_2'$  与 MF 签密时的  $k_1, k_2$  将无法相等,最终解签密的结果将被拒绝。

$$\begin{aligned} k_2' &= H_2(\hat{e}(S, Q_r)\hat{e}(Q_s, S_r)^r) = \\ &H_2(\hat{e}(xP_{\text{pub}} - rS_s, Q_r)\hat{e}(Q_s, sQ_r)^r) = \\ &H_2\left(\frac{\hat{e}(xP_{\text{pub}}, Q_r)}{\hat{e}(rS_s, Q_r)}\hat{e}(Q_s, Q_r)^{sr}\right) = \\ &H_2\left(\frac{\hat{e}(P_{\text{pub}}, Q_r)^x}{\hat{e}(rsQ_s, Q_r)}\hat{e}(Q_s, Q_r)^{sr}\right) = \\ &H_2\left(\frac{\hat{e}(P_{\text{pub}}, Q_r)^x}{\hat{e}(Q_s, Q_r)^{sr}}\hat{e}(Q_s, Q_r)^{sr}\right) = H_2(\hat{e}(P_{\text{pub}}, Q_r)^x) = k_2 \end{aligned} \quad (3)$$

式(3)中的  $k_2'$  为解签密时得出的值,  $k_2$  为签密时产生的

值。

$$\begin{aligned} k_1' &= \hat{e}(P, S)\hat{e}(P_{\text{pub}}, Q_s)^r = \\ &\hat{e}(P, xP_{\text{pub}} - rS_s)\hat{e}(P_{\text{pub}}, Q_s)^r = \\ &\frac{\hat{e}(P, xP_{\text{pub}})}{\hat{e}(P, rS_s)}\hat{e}(P_{\text{pub}}, Q_s)^r = \frac{\hat{e}(P, P_{\text{pub}})^x}{\hat{e}(P, srQ_s)}\hat{e}(sP, Q_s)^r = \\ &\frac{\hat{e}(P, P_{\text{pub}})^x}{\hat{e}(P, Q_s)^{sr}}\hat{e}(P, Q_s)^{sr} = \hat{e}(P, P_{\text{pub}})^x = k_1 \end{aligned} \quad (4)$$

式(4)中的  $k_1'$  为解签密时得出的值,  $k_1$  为签密时产生的值。

所以该方案满足不可伪造性。

## 3 BP-CPBA 协议原型实验验证

为了验证协议方案的可行性,本文在 Ubuntu11.10 系统下,底层采用 TPM\_emulator,可信软件栈采用 jTSS(Java Trusted Software Stack),编程环境为 Eclipse,编程语言为 Java 语言,使用 jPBC(Java Pairing Based Cryptography) Library 实现本文的方案。

每个模块都有其属性证书  $(c, r, S)$ ,其中密文  $c$  来源于明文  $M, M$  的各字段如表 1 所示。

表 1 352 位明文  $M$  各字段说明

名称	类型	长度/b	说明
ID	BigInteger	32	模块 ID 值
measure_value	BigInteger	160	模块度量值
property_value	BigInteger	160	模块属性值

其中身份 ID 应向 TCG 申请,属性值由 CA 颁发获得。在本模拟实验中,身份 ID 和属性值由随机函数产生固定位的随机数,度量值由 TPM\_emulator 的 SHA-1 函数产生。

实验时序图如图 2,其中一些主要的函数有如 initialize\_CA(), signcryption(), verify\_M() 等。其中 initialize\_CA() 主要负责系统初始化的工作,各种系统参数的初始化,包括 CA 中对于私钥的生成等。而 signcryption() 则为签密的核心部分,负责签密并生成模块属性签密证书,verify\_M() 则负责相应的解签密工作。

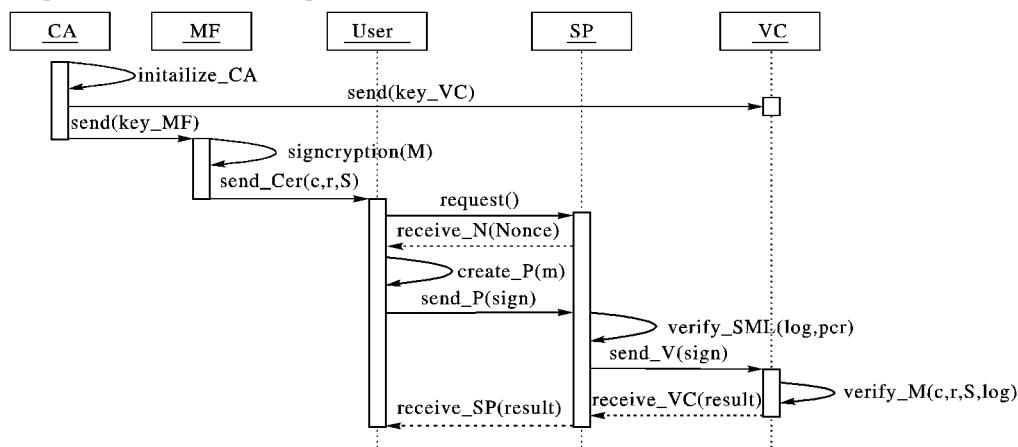


图 2 实验原型时序图

在实验中,分别针对 3、10、30 个模块的签密时间进行了统计,结果如图 3 所示。

从图 3 可以看出,当模块数增加到 30 时,签密所用的时间仍然在 1 s 以内,未达到秒级别,所以签密部分的用时是完全可以接受的。

同理,在解签密部分也分别针对 3、10 和 30 个模块三种情况进行了实验测试,解签密的情况如图 4 所示。从图 4 可以看出,解密时间也同样合理。

为了更方便而直观地体现该方案中签密和解签密部分的过程,图 5 中选取了某一单一模块的签解密过程。

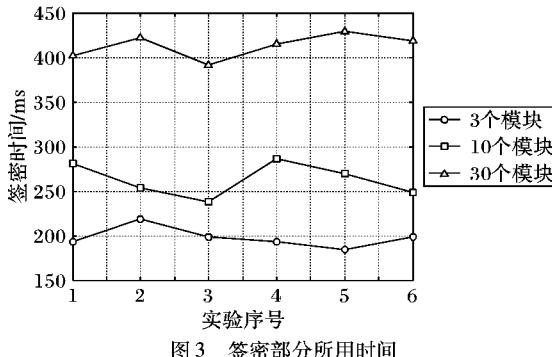


图3 签密部分所用时间

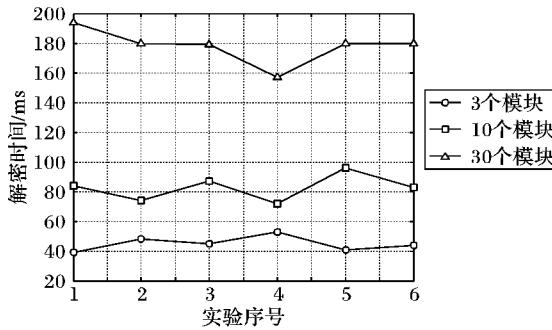


图 4 解签密部分所用时间



图5 单一模块的签解密

4 结语

本文提出了一种安全高效的基于模块属性的远程证明方案。基于椭圆曲线上双线性对的签密提高了属性证书的安全性，同时签名与加密同步完成提高了本方案的效率。该方案具备机密性、不可伪造性等安全特征，并且该方案采取的基于模块属性证明的特点避免了由于基于二进制完整性证明中所带来的验证信息量大、隐私易泄露等缺点，是一个安全高效的具备可行性的方案。

(上接第 2853 页)

- [5] WANG P, SPARKS S, ZOU C C. An advanced hybrid peer-to-peer Botnet[C]// Proceedings of the 1st Workshop on Hot Topics in Understanding Botnets. Berkeley: USENIX Association, 2007:2.
  - [6] 李鹤帅,朱俊虎,周天阳,等.基于Kademlia的新型半分布式僵尸网络[J].计算机工程,2012,38(8):92–94.
  - [7] WANG P, TYRA J, CHAN E, et al. Attacking the kad network [C]// Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks. New York: ACM, 2008: 23.
  - [8] DOUCEUR J. The Sybil attack [C]// Proceedings of the 1st International Workshop on Peer-to-Peer Systems. London: Springer-Verlag, 2002:251 – 260.
  - [9] WANG P, WU L, ASLAM B, et al. A systematic study on peer-to-

## 参考文献：

- [1] Trusted Computing Group. TPM specification version 1.2 revision 103: Part 1 – Design principles[ S/OL]. [ 2013-04-17 ]. [http://www.trustedcomputinggroup.org/files/resource\\_files/646BE624-1D09-3519-ADDA61BE37A21A74/mainP1DPrev103.pdf](http://www.trustedcomputinggroup.org/files/resource_files/646BE624-1D09-3519-ADDA61BE37A21A74/mainP1DPrev103.pdf).
  - [2] Trusted Computing Group. TPM Specification Version 1.2 Revision 103: Part 2 – Structures [ S/OL]. [ 2013-04-17 ]. [http://www.trustedcomputinggroup.org/files/resource\\_files/E14876A3-1A4B-B294-D086297A1ED38F96/mainP2Structrev103.pdf](http://www.trustedcomputinggroup.org/files/resource_files/E14876A3-1A4B-B294-D086297A1ED38F96/mainP2Structrev103.pdf).
  - [3] Trusted Computing Group. TPM Specification Version 1.2 Revision 103: Part 3 – Commands [ S/OL]. [ 2013-04-17 ]. [http://www.trustedcomputinggroup.org/files/resource\\_files/E14A09AD-1A4B-B294-D049ACC1A1A138ED/mainP3Commandsrev103.pdf](http://www.trustedcomputinggroup.org/files/resource_files/E14A09AD-1A4B-B294-D049ACC1A1A138ED/mainP3Commandsrev103.pdf).
  - [4] SAILER R, ZHANG X L, JAEGER T, *et al.* Design and implementation of a TCG-based integrity measurement architecture[ C ]// Proceedings of the 13th Usenix Security Symposium. Berkeley: USENIX, 2004: 223 – 238.
  - [5] JAEGER T, SAILER R, SHANKAR U. PRIMA: policy-reduced integrity measurement architecture[ C ]// Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. New York: ACM, 2006: 19 – 28.
  - [6] SADEGHI A, STLIBLE C. Property-based attestation for computing platforms: Caring about properties, not mechanisms[ C ]// Proceedings of the 2004 New Security Paradigms Workshop. New York: ACM, 2004: 67 – 77.
  - [7] PORITZ J, SCHUNTER M, HERREWEGHEN E V, *et al.* Property attestation-scalable and privacy-friendly security assessment of peer computers, RZ3548[ R ]. Zurich, Switzerland: IBM Zurich Research Laboratory, 2004.
  - [8] CHEN L Q, LANDFERMANN R, LOHR H, *et al.* A protocol for property-based attestation[ C ]// Proceedings of the 1st ACM workshop on Scalable Trusted Computing. New York: ACM, 2006: 7 – 16.
  - [9] CHEN L Q, LOHR H, MANULIS M, *et al.* Property-based attestation without a trusted third party[ C ]// Proceedings of the 11th International Conference on Information Security, LNCS 5222. Berlin: Springer 2008: 31 – 46.
  - [10] 秦宇, 冯登国. 基于组件属性的远程证明[ J ]. 软件学报, 2009, 20(6): 1621 – 1641.
  - [11] LEE M J. Identity-based signcryption[ EB/OL ]. [ 2013-04-17 ]. <http://eprint.iacr.org/2002/098.pdf>.
  - [12] LIBERT B, QUISQUATER J. A new identity based signcryption schemes from pairings[ C ]// Proceedings of the 2003 IEEE Information Theory Workshop. Piscataway: IEEE, 2003: 155 – 158.

peer Botnets [ C ]// Proceedings of International Conference on Computer Communications and Networks. Washington, DC: IEEE Computer Society, 2009: 1–8.

- [10] STARNBERGER G, KRUEGEL C, KIRDA E. Overbot - a botnet protocol based on Kademlia [C]// Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. New York: ACM, 2008:13.
  - [11] 朱俊虎,李鹤帅,王清贤,等.基于Kademlia协议的高生存性P2P僵尸网络[J].计算机应用,2013,33(5):1362-1377.
  - [12] DAGON D, ZOU C, LEE W. Modeling botnet propagation using time zones [C]// Proceedings of the 13rd Annual Network and Distributed System Security Symposium. Piscataway:IEEE, 2006: 235-249.