

基于无证书签名的抗 DNS 中间人攻击方案

胡杨^{1,2}, 韩增杰^{1,2}, 叶帼华^{1,2}, 姚志强^{1,2,3}

1. 福建师范大学计算机与网络空间安全学院, 福建 福州 350117;
2. 福建省公共服务大数据挖掘与应用工程技术研究中心, 福建 福州 350108;
3. 非遗数字化与多源信息融合福建省高校工程研究中心, 福建 福清 350300

摘要: 为应对域名系统协议中存在的中间人攻击问题, 提出一种轻量化的解决方案。该方案在 DNSSEC 的基础上引入无证书签名技术构建新的签名算法, 去除难以部署的信任链以提高消息认证的效率和安全性; 同时通过使用对称加密技术确保消息的机密性, 加大敌手的攻击难度。理论分析证明了所提方案能够抵抗常见的中间人攻击类型, 实验对比结果显示所提方案较同类方案具有更好的性能表现。

关键词: 域名系统; 中间人攻击; 无证书签名

中图分类号: TP393

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021093

Preventing man-in-the-middle attacks in DNS through certificate less signature

HU Yang^{1,2}, HAN Zengjie^{1,2}, YE Guohua^{1,2}, YAO Zhiqiang^{1,2,3}

1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
2. Fujian Engineering Research Center of Public Service Big Data Mining and Application, Fuzhou 350108, China
3. Engineering Research Center for ICH Digitalization and Multi-Source Information Fusion, Fuqing 350300, China

Abstract: Aiming at resisting the man-in-the-middle attacks in the domain name system protocol, a lightweight solution was proposed. The scheme introduced certificate less signature algorithm, removed the difficult-to-deploy trust chain to improve the efficiency and security of authentication. By using symmetric encryption technology, the proposed solution ensured the confidentiality of the message and increase the attack difficulty. The theoretical analysis proved the proposed scheme can resist common man-in-the-middle attacks. Experimental comparison results show the scheme has better performance than similar schemes.

Keywords: domain name system, man-in-the-middle attacks, certificate less signature

收稿日期: 2021-07-14; 修回日期: 2021-10-12

通信作者: 叶帼华, yegh2002@139.com

基金项目: 国家自然科学基金(61872090, 61972096); 福建省引导性科技项目计划(2019H0010); 非遗数字化与多源信息融合福建省高校工程研究中心开放课题(FJ-ICH 201901)

Foundation Items: The National Natural Science Foundation of China (61872090, 61972096), The Guiding Science and Technology Planning Project of Fujian (2019H0010), The Foundation of Engineering Research Center for ICH Digitalization and Multi-Source Information Fusion (FJ-ICH 201901)

论文引用格式: 胡杨, 韩增杰, 叶帼华, 等. 基于无证书签名的抗 DNS 中间人攻击方案[J]. 网络与信息安全学报, 2021, 7(6): 167-177.

HU Y, HAN Z J, YE G H, et al. Preventing man-in-the-middle attacks in DNS through certificate less signature[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 167-177.

1 引言

域名系统 (DNS, domain name system) 作为互联网基础设施, 能够将域名和 IP 地址互相映射, 从而保证其他网络应用的正常运行。DNS 协议在设计之初对安全问题考虑不够充分: 由于缺乏必要的认证机制, 用户无法确认信息自身的正确性以及来源的真实性^[1]。随着互联网的快速发展, DNS 需要设计与其相匹配的安全协议来保障数据传输, 其中抵御中间人攻击成为 DNS 安全保障体系中最重要的问题。中间人攻击是一种恶意第三方秘密控制两个或多个端点之间的通信通道攻击^[2], 攻击者利用欺骗、冒充等手段拦截或篡改通信双方的交互信息, 破坏数据的机密性、完整性以及可用性。在域名解析过程中, DNS 协议使用缓存机制提高解析效率, 但这也为中间人攻击提供了可能性。在 DNS 缓存中毒攻击中, 攻击者利用恶意数据覆盖本地 DNS 的缓存条目, 导致流量定向到恶意服务器。为解决上述问题, 许多学者提出了解决方案。Herzberg 等^[3]对 DNS 中间人的防御机制进行研究并分类: DNS 伪造检测、熵增加机制、基于密码学的解决方案以及 DNS 体系结构变化。在 DNS 伪造检测中, 一类是使用机器学习进行流量鉴别, 如 Thomas 等^[4]使用机器学习技术进行实时检测恶意软件域并将其准确聚类到特定变体, 无须获取恶意软件样本, 但该类方案的效果依赖于机器学习的方法以及样本的选取; 另一类方案是询问对等节点统计得出结果, 如 Zhao 等^[5]提出的 DCG 系统可以将同一份查询复制到多个 DNS 服务器, 使用投票机制将出现次数最多的查询作为最后结果, 但投票机制存在开销处理问题, 所以此类方案解析效率低。在熵增加机制中, 文献[6]增加了 DNS 数据包的随机性以增加敌手的攻击难度, 然而不能抵御对短域名的攻击。在基于密码学的解决方案中, IETF 提出 DNS 安全扩展 (DNSSEC, DNS security extensions) 确保数据的完整性以及对源身份的认证, 但该方案部署困难、引入额外的开销、增加服务响应时间^[7]; Herrmann 等^[8]在 DNSCurve^[9]的基础上提出 EncDNS, 该方案对 DNS 查询内容进行加密, 但需要修改原有 DNS 的协议规范, 广泛部署

较为困难。在体系结构变化中, 一类方案是更换 DNS 传输协议, 如 Zhu 等^[10]提出的 T-DNS 使用 TCP 和 TLS 代替 UDP 传输 DNS 消息, 但 TCP 在建立连接时会增加时间开销且与现有的 DNS 基础设施不兼容; 另一类方案是利用区块链的特性设计去中心化的 DNS, 如 Blockstack 建立分散的网络基础设施, 提供不被劫持和篡改的域名服务, 但存在域名注册较慢、与现有的 DNS 基础设施不兼容以及 51% 攻击问题^[11]。

近年来, 无证书技术签名引起学术界极大的关注, 为了更好地应对 DNS 解析过程出现的中间人攻击以及恶意密钥生成中心 (KGC, key generate center) 攻击, 本文在 DNSSEC 的基础上引入无证书签名技术提出一种轻量化解决方案。该方案可以有效抵抗常见的中间人攻击类型, 能够在原有基础设施上部署和运行, 并在安全性的前提下优化协议的运行效率, 以达到轻量化的目的。

2 相关工作

DNSSEC 作为 IETF 提出的首个完善的 DNS 安全机制, 其体系结构如图 1 所示。该方案虽然在一定限度上解决了 DNS 中间人攻击问题, 但是通信双方都必须使用 DNSSEC 协议才能维护数据来源的真实性和完整性; DNSSEC 没有针对恶意 KGC 攻击、缓冲区溢出, 拒绝服务攻击提供保护, 也不能提供机密性; DNSSEC 在短时间内不可能全部部署。Bernstein 等^[9]提出 DNSCurve 作为 DNSSEC 的替代方案, 该方案采用椭圆曲线加密体制简化了密钥管理问题, 并为所有 DNS 查询实现逐个数据包加密。但是 DNSCurve 只改进了 DNSSEC 签名算法, 并没有解决 DNSSEC 固有的问题 (恶意 KGC 攻击等)。Chetioui 等^[12]提出 E-DNSSEC 加强 DNSSEC 的安全性, 该方案是在 DNSSEC 的基础上对 DNS 中传输的数据使用对称密钥进行加密与哈希处理再发送出去。该方案使用对称加密有效地解决了 DNSSEC 本身不能提供机密性的问题, 但依然无法抵御恶意 KGC 攻击。

数字签名作为公钥密码体制的重要组成部分, 能够确保消息在传送过程中的完整性以及消

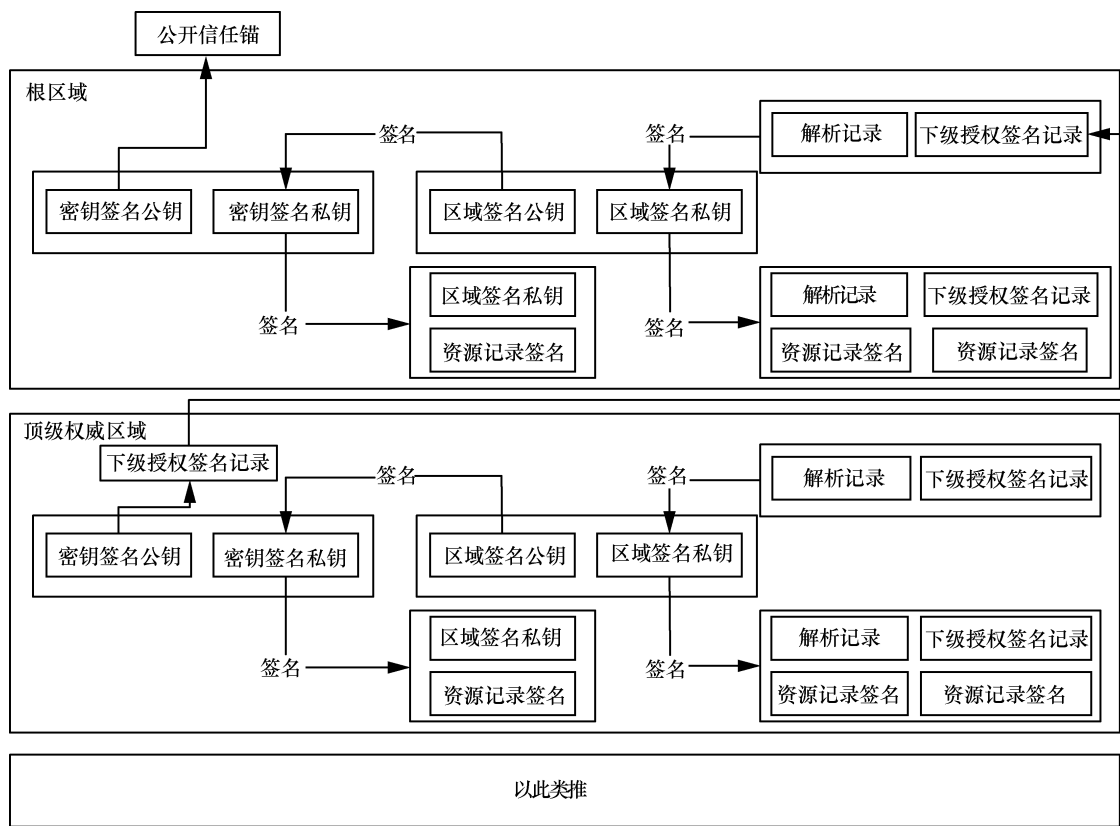


图1 DNSSEC安全体系结构
Figure 1 DNSSEC security architecture

息源身份的真实性。基于公钥基础设施 (PKI, public key infrastructure)^[13]的数字签名是一种常用的签名方式,如在电子政务^[14]等领域均会使用该密码体制。这种密码体制需要证书管理机构验证用户身份、分发证书、存储和更新证书等,因此会产生额外的开销。为了解决基于传统公钥签名体制所存在证书管理问题,Shamir^[15]提出了基于身份密码机制的数字签名,该签名体制将用户公开且唯一确定的身份信息作为公钥,私钥是由系统主密钥生成的。由于私钥生成中心知道任何用户的私钥,故存在密钥托管问题。为了解决基于身份密码机制数字签名中的密钥托管问题,Al-Riyami 和 Paterson^[16]共同提出基于无证书密码体制的数字签名概念。在无证书密码体制中,用户的私钥由 KGC 产生的部分私钥和用户的秘密值共同计算得出,解决了基于身份的数字签名体制中的密钥托管问题。Liu 等^[17]基于文献[18]提出了首个在标准模型下的无证书签名方案,并给出了详细的安全性证明过程。Xiong 等^[19]指出文献[17]中的无证书签名方案无法抵抗第二类攻

击者。由于双线性配对的计算开销比乘法运算和指数运算要高,因此,为了提高计算效率,He 等^[20]首次提出不使用双线性配对的无证书签名方案,并证明了该方案可以同时抵抗两类攻击者。随后 Tsai 等^[21]指出文献[20]无法抵抗第二类攻击者。

与此同时,Islam 等^[22]设计出一种不使用双线性配对的无证书签名方案并证明了该方案的安全性,后来 Tiwari 等^[23]发现并证明文献[22]不能抵抗第二类攻击者。Yeh 等^[24]提出了一种适用于物联网环境下移动设备的无证书签名方案,其方案的安全性依赖于椭圆曲线离散对数问题的不可解,并证明了该方案可以同时抵御上述两类攻击者。文献[25]提出一种适用于在无线传感网下多方通信的无证书签名方案,该方案通过形式化的安全模型证明其安全性。Wang 等^[26]分析指出 Wu 等和其他签名方案的不足之处并提出了一系列的评价标准。Saeed 等^[27]提出了一种新型的无证书签名,该方案利用轻量级签名使得无线体域网用户能够基于物联网匿名享受医疗服务。

综上所述,由于 DNSSEC 部署困难、运行效

率较低,并且只能抵抗部分中间人攻击,本文拟在 DNSSEC 的基础上引入无证书签名技术并结合文献[28]中的 3 个基本原则提出一种安全且轻量的抗 DNS 中间人解决方案。主要贡献如下。

1)提出一种抗 DNS 中间人攻击的解决方案,相较于之前的 DNSSEC 去掉了原有的信任链、DS 记录并引入了无证书签名技术,使得方案在确保安全性的前提下具有良好的前向保密性,更易于部署。

2)在签名算法和验证签名算法中,本方案在保证安全性的前提下未使用双线性配对运算。经过安全分析,该签名方案具有不可伪造性,并有更高的运行效率。

3 无证书签名方案的安全性模型

密码学方案的安全性通常规约为数学困难问题,利用困难问题的不可解来证明方案的安全性,本文所涉及的数学困难问题是椭圆曲线下的离散对数问题(ECDLP, elliptic curve discrete logarithm problem)。

无证书签名的安全模型中有两类攻击者:第一类攻击者 A_I 充当恶意用户替换其他用户的公钥但不能获取系统主密钥;第二类攻击者 A_{II} 充当恶意 KGC 获取系统主密钥但不能替换用户的公钥^[29]。无证书签名方案的安全模型用以下两个游戏进行刻画。

(1) 游戏一(适用于第一类攻击者)

阶段一:系统参数设置。挑战者 B 运行系统参数生成算法,输入参数 λ ,输出系统主密钥以及安全参数 $params$ 。挑战者将参数发送给 A_I 并保存主密钥。

阶段二:自适应询问。攻击者 A_I 在多项式时间内自适应地向挑战者 B 进行公钥询问、部分私钥询问、公钥替换询问、秘密值询问以及签名询问,利用返回信息来伪造签名。挑战者 B 按照签名方案模拟并回答。

阶段三:签名伪造。 A_I 输出一个 $(M^*, \sigma^*, ID^*, P^*)$, A_I 在游戏中获胜,当且仅当:

- 1) 伪造签名 σ^* 验证有效;
- 2) A_I 在询问过程中没有询问过 ID^* 对应的部分私钥;

3) A_I 在询问过程中没有询问过 ID^* 对应公钥 P^* 对消息 M^* 的签名。

A_I 在此游戏获胜的概率为 $\text{succ}_{I}(k)$ 。

(2) 游戏二(适用于第二类攻击者)

阶段一:系统参数设置。系统参数生成过程同游戏一一致,挑战者将主密钥和 $params$ 发送给 A_{II} 。

阶段二:自适应询问。同游戏一一致,但攻击者不能进行公钥替换询问。

阶段三:签名伪造。 A_{II} 输出 $(M^*, \sigma^*, ID^*, P^*)$, A_{II} 在游戏中获胜条件与游戏一一致,但攻击者不能替换 ID^* 的公钥。

A_{II} 在此游戏获胜的概率为 $\text{succ}_{II}(k)$ 。

4 方案提出

由于 IETF 所提出的 DNSSEC 易受到恶意 KGC 等其他中间人攻击,本文在 DNSSEC 的基础上引入无证书签名与对称加密技术提出新的签名认证方案抵抗 DNS 中间人攻击。

4.1 方案安全体系结构

DNS 无证书的抗中间人攻击安全体系结构如图 2 所示。本文提出的无证书签名方案主要由 3 部分组成:KGC、服务器(根域名服务器、顶级域名服务器、权威域名服务器)和递归解析器。方案的主要步骤如下。

1)可信中心初始化系统参数,服务器与递归解析器向可信中心进行注册,获取部分公私钥及参数。

2)服务器与递归解析器获取部分公私钥后,结合秘密值生成完整的公私钥以及对应的会话密钥,并将公钥公开。

3)递归解析器收到查询内容后,使用自身与根域名解析器之间的会话密钥将查询内容加密后,将密文发给根域名解析器。

4)根域名解析器收到密文后,使用会话密钥解密后进行域名解析。

5)递归解析器与顶级域名服务器、权威域名服务器之间的交互过程同上述过程一致。

6)解析后的结果,使用私钥进行签名,发给递归解析器;递归解析器使用对应的公钥进行验证,若验证成功,则接受该消息并返回给本地用户,否则丢弃。

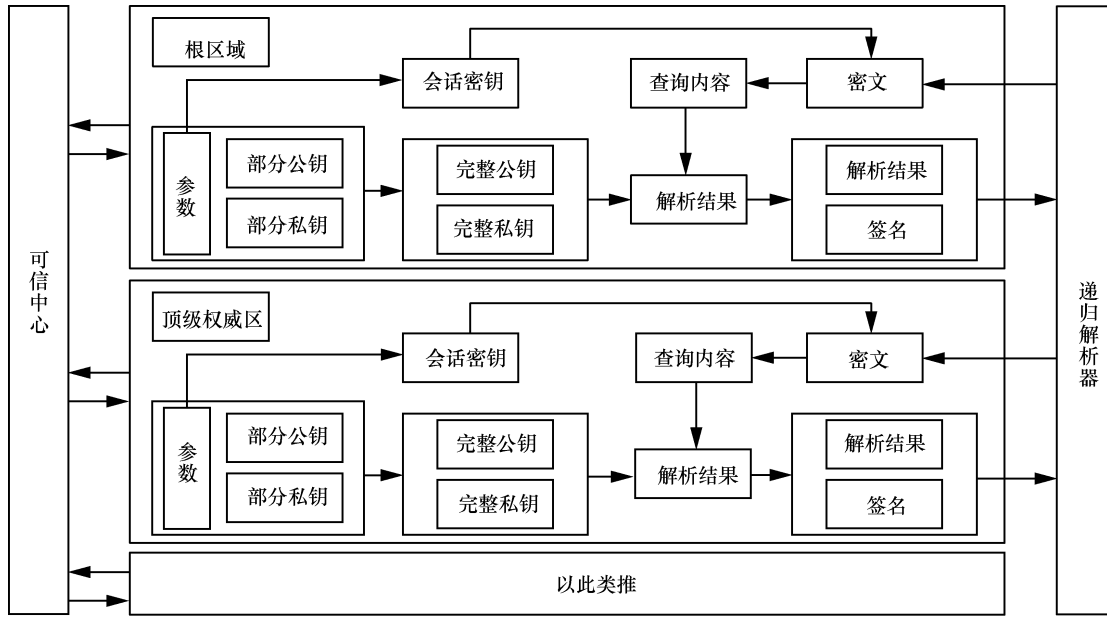


图 2 DNS 无证书的抗中间人攻击安全体系结构

Figure 2 DNS certificateless security architecture against man-in-the-middle attack

4.2 方案的具体设计

本文所提出的方案主要分为 4 个阶段：系统初始化阶段、实体注册及密钥生成阶段、消息签名阶段、认证阶段。本文所使用的重要符号以及相关含义如表 1 所示。

表 1 符号说明
Table 1 Notions and their meanings

符号	含义
G	q 阶椭圆曲线的循环群
P	群 G 生成元
s	主密钥
P_{pub}	系统公钥
IP_i	实体 i 的 IP 地址
t_i	时间戳
H_0	$\{0, 1\}^* \rightarrow Z_q^*$
H_1	$G \times G \rightarrow Z_q^*$
H_2	$G \times \{0, 1\}^* \rightarrow Z_q^*$
H_3	$\{0, 1\}^* \times G \times G \times \{0, 1\}^* \rightarrow Z_q^*$
K_i	会话密钥
σ_i	实体 i 的签名
$\oplus$	异或运算

4.2.1 系统初始化阶段

本阶段，KGC 生成系统参数并公开公共参

数，然后根服务器、顶级域名服务器以及权威域名服务器向 KGC 注册获取部分公私钥。

首先，系统给定安全参数 λ 。KGC 选择两个素数 p 、 q ，并生成在有限域 F_p 上阶数为 q 的椭圆曲线群 G 。 P 是群 G 的生成元，KGC 随机选择 $s \in Z_q^*$ 作为主密钥然后计算系统公钥 $P_{\text{pub}} = sP$ 。

接着，KGC 选取 4 个哈希函数， $H_0: \{0, 1\}^* \rightarrow Z_q^*$ ， $H_1: G \times G \rightarrow Z_q^*$ ， $H_2: G \times \{0, 1\}^* \rightarrow Z_q^*$ ， $H_3: \{0, 1\}^* \times G \times G \times \{0, 1\}^* \rightarrow Z_q^*$ 。

最后，KGC 公开系统参数 $\text{params} = \{p, q, G, F_p, F_q, P, P_{\text{pub}}, H_0, H_1, H_2, H_3\}$ ，并将主密钥秘密保管。

4.2.2 实体注册及密钥生成阶段

(1) 服务器

服务器先秘密产生两个随机数 x_i ， $a_i \in Z_q^*$ 。计算部分公钥 $X_i = x_iP$ ， $A_i = a_iP$ 。然后服务器将 $\{IP_i, X_i, A_i\}$ 发给 KGC 进行注册。

KGC 验证 IP_i 的正确性。验证通过后，计算 $B_i = IP_i \oplus H_2(D_i, T_i)$ ， $D_i = sA_i$ 。然后 KGC 随机选取秘密值 $d_i, w_i \in Z_q^*$ ，计算 $Y_i = w_iP$ ， $\alpha_i = H_1(A_i, X_i)$ ， $C_i = (A_i, B_i)$ ， $y_i = w_i + s\alpha_i \bmod q$ ， $j_i = d_i + sH_0(IP_i)$ ， $J_i = d_iP$ 。KGC 将 $\{C_i, d_i, y_i, Y_i, j_i, J_i\}$ 通

过安全信道发回给服务器。

服务器将 (x_i, y_i) 作为私钥秘密保存。 (X_i, Y_i) 则作为公钥并与 J_i 公开。

根域名服务器、顶级域名服务器以及权威域名服务器根据上述方法注册后分别得到自己的公私钥对 $(x_R, y_R), (X_R, Y_R); (x_T, y_T), (X_T, Y_T); (x_A, y_A), (X_A, Y_A)$ 。

(2) 递归解析器

递归解析器向 KGC 进行注册。KGC 随机选择 $z_r \in Z_q^*$ ，计算 $Z_r = z_r P$ 。KGC 将 (z_r, Z_r) 通过安全信道发回给递归解析器作为公私钥。

递归解析器将私钥 z_r 秘密保存，将公钥 Z_r 公开。

4.2.3 消息签名阶段

所有实体在注册完成后，用户通过递归解析器进行交互。交互过程如下。

1) 用户使用浏览器访问某个网站，按域名解析过程将查询消息发送给递归解析器。

2) 递归解析器计算与根域名服务器之间的会话密钥 $K_R = z_r (J_R + H_0(IP_R)P_{pub})$ 。该解析器使用会话密钥对查询的内容进行加密，得出查询密文 β 。递归解析器将密文 β 发送给根域名服务器。

3) 根域名服务器收到密文 β 并计算对称密钥：

$$\begin{aligned} j_R Z_r &= (d_R + sH_0(IP_R))z_r P = \\ z_r (d_R P + H_0(IP_R)sP) &= K_R \end{aligned}$$

4) 根域名服务器使用 K_R 对 β 进行解密之后，通过查询获取所要查询网站对应的顶级域名服务器的 IP_T ，该查询结果定义为 M_R 。根服务器计算签名 $\sigma_R = x_R + y_R + d_R \cdot \mu_R \bmod q$ ， $\mu_R = H_3(M_R, C_R, J_R, t_R)$ ，将 $\{M_R, \sigma_R, C_R, t_R\}$ 发给递归解析器。

4.2.4 认证阶段

递归解析器收到根域名解析器的消息后，首先验证 t_R 是否在规定时间范围内。假如超出规定范围，直接丢弃；否则计算 $\alpha_R = H_1(A_R, X_R)$ ， $\mu_R = H_3(M_R, C_R, J_R, t_R)$ 。接着递归解析器验证等式 $\sigma_R P = X_R + Y_R + \alpha_R P_{pub} + J_R \mu_R$ 是否成立，如果等式不成立，直接丢弃该响应；否则，接收该消息。通过计算可以得出以上等式均成立。

按照 DNS 解析的顺序，递归解析器继续向顶级域名服务器、权威域名服务器进行递归查询，

最后将得到的 IP 地址发回给本地用户。

5 安全性与效率分析

5.1 会话密钥安全性

本方案提出递归解析器发送的内容是使用对称密钥 K_i 对查询内容进行加密得出的 β_i ，会话密钥为： $K_i = z_r (J_i + sH_0(IP_i)P_{pub}) = j_i Z_r$ ， $J_i = d_i P$ ， $j_i = d_i + sH_0(IP_i)$ ， $Z_r = z_r P$ ， $P_{pub} = sP$ 。攻击者要计算出会话密钥 K_i 就要计算 $z_r d_i P + z_r sPH_0(IP_i)$ ，而攻击者仅知道 $J_i = d_i P$ ， $Z_r = z_r P$ 以及 $P_{pub} = sP$ ，所以攻击者必须要解决 ECDLP 才能计算出会话密钥 K_i 。由于 ECDLP 是困难的，因此本方案通过会话密钥确保查询内容不会在传输过程中被恶意篡改。

5.2 互相认证

一方面，根据 5.1 分析可以得知，只有通信双方才能计算出会话密钥 K_i ；另一方面，递归解析器通过签名来验证消息的来源。攻击者在计算具体消息的签名 $\sigma_i = x_i + y_i + d_i \cdot \mu_i \bmod q$ ， $\mu_i = H_3(M_i, C_i, J_i, t_i)$ 过程中，需要知道 x_i 、 y_i 以及 d_i 具体数值。而 (x_i, y_i) 是服务器的私钥， d_i 则是服务器在注册阶段 KGC 随机选择的数值，因此攻击者无法伪造正确的签名。

5.3 前向保密性

递归解析器与服务器的会话密钥具有前向保密性。根据公式 $K_i = z_r (J_i + sH_0(IP_i)P_{pub})$ 看出，即便在查询过程中某个阶段会话密钥被攻击者获取，由于包含 J_i 与 IP_i 会随着查询过程发生变化，其他阶段的会话密钥也会随之更换。

5.4 抵抗攻击

本文提出的方案可以抵抗恶意 KGC 攻击、重放攻击以及中间人攻击。

恶意 KGC 攻击：本文提出的方案基于无证书签名方案，根域名服务器、顶级域名服务器以及权威域名服务器的公私钥是由服务器与 KGC 共同生成的，因此可以有效抵抗密钥托管造成的恶意 KGC 攻击。

重放攻击：如果攻击者截获从服务器发回的信息 $\{M_R, \sigma_R, C_R, t_R\}$ 并重新发给递归解析器。根据上述过程可知，递归解析器在收到来自服务器的

消息后首先检验消息中的时间戳 t_i 是否在规定的时间内, 如果不在, 递归解析器会直接丢弃该消息。因此递归解析器能够判断并抵抗来自攻击者的重放攻击。

中间人攻击: 根据以上对互相认证安全的分析可知该方案可以抵抗中间人攻击。

5.5 安全性证明

本文在随机预言机模型下证明了所提方案的安全性。具体过程如下。

5.5.1 第一类攻击者的安全性分析

定理 1 假设游戏一中的哈希函数 H_0, H_1, H_2, H_3 均为随机预言机, 若攻击者 A_1 能够在多项式时间内获胜的优势为 ε (假设进行 q_i 次 H_i 询问, $i=0, 1, 2, 3$), 则挑战者 B 能够以 $\text{Adv}(A_1) \geq \frac{\varepsilon}{q_1 q_3}$ 的优势解决 ECDLP。

证明 假设挑战者 B 能解决 ECDLP, 其困难问题嵌入循环群 (G, p, g) 上的问题实例 (P, sP) , 攻击成功的条件是求出 $s \in Z_q^*$ 。挑战者 B 进行如下模拟。

阶段一: 初始化

挑战者 B 按照方案要求进行系统初始化。挑战者随机选择一个数 $s \in Z_q^*$ 作为系统主密钥, 则系统公钥为 $P_{\text{pub}} = sP$ 。挑战者 B 将该公钥以及系统参数 $\text{params} = \{p, q, F_p, G, P, P_{\text{pub}}, H_0, H_1, H_2, H_3\}$ 发送给攻击者 A_1 , 将主密钥秘密保存。

阶段二: 自适应性询问

H_0 询问: 攻击者对 H_0 进行哈希询问。挑战者 B 需要准备一张空白的哈希表 L_0 用来记录攻击者的询问以及对应的回答。攻击者 A_1 输入 IP_i , $IP_i \in \{0, 1\}^*$, 哈希表 L_0 中数组格式为 (IP_i, h_{0i}) , $h_{0i} \in Z_q^*$, 挑战者会按照如下返回结果: 如果攻击者查询的 IP_i 已在列表的数组 (IP_i, h_{0i}) 中, 则直接返回对应的 h_{0i} ; 否则挑战者随机选择一个数 $h_{0i} \in Z_q^*$, 将这个数返回给攻击者, 并将新的数组 (IP_i, h_{0i}) 写入哈希表 L_0 中。

H_1 询问: 攻击者对 H_1 进行哈希询问。挑战者 B 需要准备一张空白的哈希表 L_1 用来记录攻击者的询问以及对应的回答。攻击者 A_1 输入 (A_i, X_i) , $A_i, X_i \in Z_q^*$, 哈希表 L_1 中数组格式为 (A_i, X_i, h_{1i}) ,

$h_{1i} \in Z_q^*$, 挑战者会按照如下返回结果: 如果攻击者查询的内容已在列表的数组 (A_i, X_i, h_{1i}) 中, 则直接返回对应的 h_{1i} ; 否则挑战者随机选择一个数 $h_{1i} \in Z_q^*$, 将这个数返回给攻击者, 并将新的数组 (A_i, X_i, h_{1i}) 写入表 L_1 中。

H_2 询问: 攻击者对 H_2 进行哈希询问。挑战者 B 需要准备一张空白的哈希表 L_2 用来记录攻击者的询问以及对应的回答。攻击者 A_1 输入 (D_i, T_i) , $D_i \in Z_q^*$, $T_i \in \{0, 1\}^*$, 哈希表 L_2 中数组格式为 (D_i, T_i, h_{2i}) , $h_{2i} \in Z_q^*$, 挑战者会按照如下返回结果: 如果攻击者查询的内容已在列表的数组 (D_i, T_i, h_{2i}) 中, 则直接返回对应的 h_{2i} ; 否则挑战者随机选择一个数 $h_{2i} \in Z_q^*$, 将这个数返回给攻击者, 并将新的数组 (D_i, T_i, h_{2i}) 写入哈希表 L_2 中。

H_3 询问: 攻击者对 H_3 进行哈希询问。挑战者 B 需要准备一张空白的哈希表 L_3 用来记录攻击者的询问以及对应的回答。攻击者 A_1 输入 (M_i, C_i, J_i, t_i) , $C_i, J_i \in Z_q^*$, $M_i, t_i \in \{0, 1\}^*$, 哈希表 L_3 中数组格式为 (M_i, C_i, J_i, t_i) , $h_{3i} \in Z_q^*$, 挑战者会按照如下返回结果: 如果攻击者查询的内容已在列表的数组 (M_i, C_i, J_i, t_i) 中, 则直接返回对应的 h_{3i} ; 否则挑战者随机选择一个数 $h_{3i} \in Z_q^*$, 将这个数返回给攻击者, 并将新的数组 (M_i, C_i, J_i, t_i) 写入哈希表 L_3 中。

用户秘密值询问: 挑战者 B 创建一张空哈希表 L_4 记录攻击者查询用户 IP_i 所对应的秘密值与部分公钥。如果攻击者要查询的 IP_i 在列表中存在, 直接返回该 IP_i 所对应的秘密值 x_i 与部分公钥 X_i ; 否则挑战者随机选择 $x_i \in Z_q^*$, 计算 $X_i = x_i P$, 将 x_i, X_i 作为用户部分公私钥, 并记录到哈希表 L_4 中。

部分私钥查询: 挑战者 B 在哈希表 L_4 中记录查询用户 IP_i 所对应的部分公私钥。如果攻击者要查询的 IP_i 在列表中存在, 直接返回该 IP_i 所对应的部分私钥 y_i 与部分公钥 Y_i ; 否则挑战者随机选择 $w_i, a_i \in Z_q^*$, 计算 $Y_i = w_i P$, $A_i = a_i P$, $y_i = w_i + s \cdot H_1(A_i, X_i) \bmod q$ 。将 y_i, Y_i 作为用户部分公私钥输出, 并按照对应应用户 IP_i 记录到哈希表 L_4 中。

公钥查询: 挑战者 B 在哈希表 L_4 中记录查询用户 IP_i 所对应的公钥。如果攻击者要查询的 IP_i 在列表中存在, 直接返回该 IP_i 所对应的公钥(X_i, Y_i); 如果挑战者发现存在 X_i , 则继续筛选对应的 Y_i , 否则返回至用户秘密值查询生成 IP_i 对应的 X_i ; 如果挑战者发现存在 X_i , 但其对应的 Y_i 不存在, 那么返回至部分私钥查询生成 X_i 对应的 Y_i 。最后将(X_i, Y_i)作为用户公钥输出, 并按照对应用户 IP_i 记录到哈希表 L_4 中。

公钥替换: 攻击者可以替换用户公钥中的某个部分公钥或全部公钥。如果在询问之前, 攻击者试图替换部分公钥或全部公钥, 则模拟中止; 否则, 攻击者将数组 (IP_i, x_i, X_i) 或 (IP_i, y_i, Y_i) 发送给挑战者。挑战者运行部分密钥检查, 如果测试成功, 更新哈希表 L_4 。

签名查询: 攻击者 A_I 向挑战者发送 (IP_i, M_i) 进行签名询问。挑战者 B 接收到询问之后会对上述所创建的 4 个哈希表进行综合查询, 并且随机选取一个数 $d_i \in Z_q^*$, 计算 $J_i = d_i P$ 以及签名 $\sigma_i = x_i + y_i + d_i \cdot \mu_i \bmod q$, $\mu_i = H_3(M_i, C_i, J_i, t_i)$ 。输出 (IP_i, J_i, σ_i) 给攻击者 A_I 。

阶段三: 攻击者挑战

攻击者 A_I 停止询问, 输出任意消息 m^* , 身份为 IP^* 的签名 σ' 。根据分叉引理可知, 攻击者可以获得消息 m^* 的另一个有效签名 σ'' , 由此可得:

$$\sigma' = X_{IP^*} + Y_{IP^*} + sa'P + J'h'_{i3} \quad (1)$$

$$\sigma'' = X_{IP^*} + Y_{IP^*} + sa''P + J''h''_{i3} \quad (2)$$

根据式 (1)、式 (2) 中可以计算出 $s = (h'_{i1} - h''_{i1})^{-1}[(\sigma' - \sigma'')P - (J'h'_{i3} + J''h''_{i3})]$ 作为困难问题的解; 否则挑战者没有解决椭圆曲线的离散对数问题。若攻击者 A_I 之前询问过 H_1 , 则攻击失败, 没有询问的概率至少为 $\frac{1}{q_1}$; 若攻击者 A_I 之前询问过 H_3 , 则攻击失败, 没有询问的概率至少为 $\frac{1}{q_3}$ 。因此模拟成功的概率至少为 $\frac{1}{q_1 q_3}$ 。

因此, 若挑战者模拟成功, 并且攻击者 A_I 以不可忽略的概率 ε 破坏该签名方案的不可伪造性。那么, 挑战者能够在多项式时间内以 $\text{Adv}(A_I) \geq \frac{\varepsilon}{q_1 q_3}$ 优势解决 ECDLP。

5.5.2 第二类攻击者的安全性分析

定理 2 假设游戏二中哈希函数 H_0, H_1, H_2, H_3 均为随机预言机, 若攻击者 A_{II} 能够在多项式时间内获胜的优势为 ε (假设进行 q_i 次 H_i 询问, $i=0, 1, 2, 3$), 则挑战者 B 能够以 $\text{Adv}(A_{II}) \geq \frac{\varepsilon}{q_1 q_3}$ 的优势解决 ECDLP。

证明 假设挑战者 B 能解决 ECDLP, 其困难问题嵌入循环群 (G, p, g) 上的问题实例 (P, sP) , 攻击成功的条件是求出 $s \in Z_q^*$ 。攻击者 A_{II} 能够获取系统主密钥但是不能更换用户公钥。挑战者 B 进行如下模拟:

阶段一: 初始化

挑战者 B 进行系统初始化, 将系统参数 $\text{params} = \{p, q, F_p, G, P, P_{\text{pub}}, H_0, H_1, H_2, H_3\}$ 和系统密钥 $s \in Z_q^*$ 发送给攻击者 A_{II} 。

阶段二: 自适应性询问

攻击者 A_{II} 在多项式时间内自适应地向挑战者 B 进行有限次询问, 步骤与定理 1 中的证明一致。

阶段三: 攻击者挑战

攻击者 A_{II} 停止询问, 输出身份为 IP^* , 任意消息 m^* 的有效签名 σ' , 根据分叉引理可知, 攻击者可以获得消息 m^* 的另一个有效签名 σ'' , 由此可得:

$$\sigma' = X_{IP^*} + Y_{IP^*} + sa'P + J'h'_{i3} \quad (3)$$

$$\sigma'' = X_{IP^*} + Y_{IP^*} + sa''P + J''h''_{i3} \quad (4)$$

根据式 (3)、式 (4) 可以计算出 $x_{IP^*} = \frac{1}{2} P^{-1}[(\sigma' + \sigma'')P - 2Y_{IP^*} - (a' + a'')P_{\text{pub}} - (J'h'_{i3} + J''h''_{i3})]$ 作为困难问题的解; 否则挑战者没有解决椭圆曲线的离散对数问题。若攻击者 A_{II} 之前询问过 H_1 , 则攻击失败, 没有询问的概率至少为 $\frac{1}{q_1}$; 若攻击者 A_{II} 之前询问过 H_3 , 则攻击失败, 没有询问的概率至少为 $\frac{1}{q_3}$ 。因此模拟成功的概率至少为 $\frac{1}{q_1 q_3}$ 。

因此, 若挑战者模拟成功, 并且攻击者 A_{II}

以不可忽略的概率 ε 破坏该签名方案的不可伪造性。那么, 挑战者能够在多项式时间内以 $\text{Adv}(A_1) \geq \frac{\varepsilon}{q_1 q_3}$ 优势解决 ECDLP。

5.6 效率与安全性分析

下面计算效率 and 安全性这两方面分别对文献[30-32]提出的方案以及文献[7, 9, 12]提出的方案与本文方案进行分析比较, 对比结果如表 2 与表 3 所示。

(1) 计算效率

文献[30]的签名算法和验证算法由模的取逆运算、椭圆曲线的标量乘法运算构成, 算法开销为 $T_{\text{sm}} + T_{\text{inv}}$ 和 $6T_{\text{sm}}$ 。文献[31]的签名算法和验证算法由取逆运算、椭圆曲线的标量乘法运算构成, 算法开销分别为 $T_{\text{sm}} + T_{\text{inv}}$ 和 $6T_{\text{sm}}$ 。文献[32]的签名算法和验证算法由模的取逆运算、椭圆曲线的标量乘法运算以及双线性配对运算构成, 算法开销为 $T_{\text{sm}} + T_{\text{inv}}$ 和 $2T_{\text{sm}} + T_{\text{par}}$ 。经综合得到表 2, 其中本方案的签名算法和验证算法由模的取逆运算、哈希运算以及椭圆曲线的标量乘法运算构成, 开销分别为 $T_{\text{sm}} + T_h$ 和 $2T_{\text{sm}} + T_h$ 。

仿真实验中采用密码库 MIRACL 做加密操作, 模的取逆运算等操作在 I7-4700 处理器、4 GB 内存和 Windows7 操作系统下的执行时间分别是: $T_{\text{inv}} \approx 11.62T_m$, $T_{\text{sm}} \approx 29.00T_m$, $T_h \approx 29.00T_m$, $T_{\text{par}} \approx 87.00T_m$ (T_m 表示循环群 G 上的模乘运算所需的计算开销)。由此得出的总开销如表 2 所示, 可以看出文献[30-31]中的无证书签名方案所使用到的椭圆曲线标量乘运算次数较多, 计算开销较本文方案高; 文献[32]使用的椭圆曲线标量乘运算次数较少, 所以这种方案的效率较本文方案高。

表 2 无证书方案计算效率比较
Table 2 Comparison of computing efficiency of certificate less schemes

方案	签名算法	验证算法	总开销 (T_m)	第一类攻击者	第二类攻击者
文献[30]	$T_{\text{sm}} + T_{\text{inv}}$	$6T_{\text{sm}}$	≈ 214.60	不安全	不安全
文献[31]	$T_{\text{sm}} + T_{\text{inv}}$	$6T_{\text{sm}}$	≈ 214.60	不安全	不安全
文献[32]	$T_{\text{sm}} + T_{\text{inv}}$	$2T_{\text{sm}} + T_{\text{par}}$	≈ 185.60	安全	不安全
本文方案	$T_{\text{sm}} + T_h$	$2T_{\text{sm}} + T_h$	≈ 203.00	安全	安全

由表 2 看出, 相较文献[30-31]而言, 本文方案的计算效率更高。另外, 因为文献[30-32]的签名方案可以被轻松绕过部分私钥或秘密值从而构造一个任意消息的有效签名, 故均不能同时抵抗两类攻击者。

(2) 安全性

本文通过虚拟机对文献[7,9,12]方案进行实验分析, 然后利用本地服务器充当恶意 KGC 发送恶意消息进行仿真攻击; 而本文方案用 Python 语言实现无证书签名算法, 其中引入对称加密算法增加了保密性, 并通过手动生成恶意的签名进行仿真攻击。由表 3 可知, 在源身份认证方面, 各个方案均能够都对消息的源身份进行签名认证。在传输过程的保密性方面, DNSSEC 没有提供保密性; DNSCurve 为每个 DNS 数据包计算不同的密钥流并对其进行加密, 可以保护消息的内容免受中间人攻击; E-DNSSEC 和本文方案使用对称加密的方法对传输消息进行加密。在抵抗恶意 KGC 攻击方面, 除了本文方案的其他方案, 均不能抵抗恶意 KGC 攻击, 因为其他方案均是基于传统公钥体制进行签名的。在效率方面, 其他方案在 DNSSEC 的基础上进行签名算法改进, 并没有对其结构改动, 而本文方案去掉了其难以部署的信任链以及 DS 记录等, 计算效率相比于其他方案更高。

表 3 不同 DNSSEC 方案的安全性比较
Table 3 Safety comparison of different DNSSEC schemes

方案	源身份认证	保密性	恶意 KGC 攻击
DNSSEC ^[7]	是	否	不安全
DNSCurve ^[9]	是	是	不安全
E-DNSSEC ^[12]	是	是	不安全
本文方案	是	是	安全

6 结束语

为了解决现有 DNSSEC 存在的恶意 KGC 以及难部署等问题, 本文在 DNSSEC 基础上引入无证书技术, 对原有方案签名过程进行改进与精简, 进而提出一种更高效、更易于部署的签名认证方案。与此同时, 该方案具有前向保密性, 能够抵抗密钥冒充泄露与抵抗中间人攻击, 并在随机预

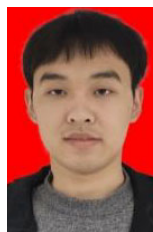
言模型下证明了方案的安全性。下一步的工作是研究对 DNS 缓冲区投毒攻击的群认证, 进一步提高域名解析过程的安全性。

参考文献:

- [1] 王文通, 胡宁, 刘波, 等. DNS 安全防护技术研究综述[J]. 软件学报, 2020, 31(7): 2205-2220.
WANG W T, HU N, LIU B, et al. Survey on technology of security enhancement for DNS[J]. Journal of Software, 2020, 31(7): 2205-2220.
- [2] CONTI M, DRAGONI N, LESYK V. A survey of man in the middle attacks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2027-2051.
- [3] HERZBERG A, SHULMAN H. Antidotes for DNS poisoning by off-path adversaries[C]//Proceedings of 2012 Seventh International Conference on Availability, Reliability and Security. Piscataway: IEEE Press, 2012: 262-267.
- [4] THOMAS M, MOHAISEN A. Kindred domains: detecting and clustering botnet domains using DNS traffic[C]//Proceedings of the 23rd International Conference on World Wide Web. 2014: 707-712.
- [5] ZHAO Y, HU N, ZHANG C, et al. DCG: a client-side protection method for DNS cache[J]. Journal of Internet Services and Information Security, 2020, 10(2): 103-121.
- [6] EASTLAKE D, ANDREWS M. Domain name system (DNS) cookies[R]. RFC Editor, 2016.
- [7] EASTLAKE D, KAUFMAN C. Domain name system security extensions[R]. RFC Editor, 1997.
- [8] HERRMANN D, FUCHS K P, LINDEMANN J, et al. EncDNS: A lightweight privacy-preserving name resolution service[M]//Computer Security-ESORICS 2014. 2014: 37-55.
- [9] BERNSTEIN D J. DNSCurve: usable security for DNS[EB]. 2009.
- [10] ZHU L, HU Z, HEIDEMANN J, et al. Connection-oriented DNS to improve privacy and security[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. 2015: 171-186.
- [11] ALI M, NELSON J, SHEA R, et al. Blockstack: a global naming and storage system secured by blockchains[C]//Proceedings of 25th Usenix Security Symposium. 2016: 181-194.
- [12] CHETIOUI K, ORHANOUC, HAJJI S E. New protocol E-DNSSEC to enhance DNSSEC security[J]. International Journal of Network Security, 2018, 20(1): 19-24.
- [13] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [14] 宋潇潇. PKI 技术在电子政务中的研究与应用[J]. 电子元器件与信息技术, 2019, 3(3): 19-21, 25.
SONG X X. Research and application of PKI technology in E-government[J]. Electronic Component and Information Technology, 2019, 3(3): 19-21, 25.
- [15] SHAMIR A. Identity-based cryptosystems and signature schemes[M]//Advances in Cryptology. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984: 47-53.
- [16] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Proceedings of 1st International Conference on Applied Cryptography and Network Security. 2003: 452-473.
- [17] LIU J K, AU M H, SUSILO W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model: extended abstract[C]//Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. 2007: 273-283.
- [18] CHOI K Y, PARK J H, HWANG J Y, et al. Efficient certificateless signature schemes[M]//Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2007: 443-458.
- [19] XIONG H, QIN Z, LI F. An improved certificateless signature scheme secure in the standard model[J]. Fundamental Informaticae, 2008, 88(1): 193-206.
- [20] HE D, CHEN J, ZHANG R. An efficient and provably-secure certificateless signature scheme without bilinear pairings[J]. International Journal of Communication Systems, 2012, 25(11): 1432-1442.
- [21] TSAI J L, LO N W, WU T C. Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings[J]. International Journal of Communication Systems, 2014, 27(7): 1083-1090.
- [22] ISLAM S H, BISWAS G P. Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography[J]. International Journal of Computer Mathematics, 2013, 90(11): 2244-2258.
- [23] TIWARI N. On the security of pairing-free certificateless digital signature schemes using ECC[J]. ICT Express, 2015, 1(2): 94-95.
- [24] YEH K H, SU C H, CHOO K K Raymond, et al. A novel certificateless signature scheme for smart objects in the Internet of things[J]. Sensors (Basel, Switzerland), 2017, 17(5): 1001.
- [25] WU F, XU L L, KUMARI S, et al. A new and secure authentication scheme for wireless sensor networks with formal proof[J]. Peer-to-Peer Networking and Applications, 2017, 10(1): 16-30.
- [26] WANG D, LI W T, WANG P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(9): 4081-4092.
- [27] SAEED M E S, LIU Q Y, TIAN G Y, et al. Remote authentication schemes for wireless body area networks based on the internet of things[J]. IEEE Internet of Things Journal, 2018, 5(6): 4926-4944.
- [28] 汪定, 李文婷, 王平. 对三个多服务器环境下匿名认证协议的分析[J]. 软件学报, 2018, 29(7): 1937-1952.
WANG D, LI W T, WANG P. Cryptanalysis of three anonymous authentication schemes for multi-server environment[J]. Journal of

Software, 2018, 29(7): 1937-1952

- [29] HUANG X Y, MU Y, SUSILO W, et al. Certificateless signatures: new schemes and security models[J]. The Computer Journal, 2011, 55(4): 457-474.
- [30] KARATI A, HAFIZUL ISLAM S, BISWAS G P. A pairing-free and provably secure certificateless signature scheme[J]. Information Sciences, 2018, 450: 378-391.
- [31] PAKNIAT N, VANDA B A. Cryptanalysis and improvement of a pairing-free certificateless signature scheme[C]//Proceedings of 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC). Piscataway: IEEE Press, 2018: 1-5.
- [32] DENG L Z, YANG Y X, GAO R H, et al. Certificateless short signature scheme from pairing in the standard model[J]. International Journal of Communication Systems, 2018, 31(17): e3796.

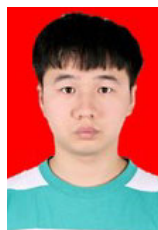


韩增杰（1997- ），男，山西洪洞人，福建师范大学硕士生，主要研究方向为大数据安全与隐私保护。



叶幅华（1976- ），女，福建霞浦人，福建师范大学副教授，主要研究方向为大数据安全与隐私保护、信息安全。

[作者简介]



胡杨（1996- ），男，河南鹤壁人，福建师范大学硕士生，主要研究方向为大数据安全与隐私保护。



姚志强（1967- ），男，福建莆田人，博士，福建师范大学教授、博士生导师，主要研究方向为大数据安全与隐私保护、多媒体安全、应用安全。

网络与信息安全学报

2021年(第7卷)总目次

综 述

	期	页码
人工智能模型数据泄露的攻击与防御研究综述.....		
.....任 奎, 孟泉润, 闫守琨, 秦 湛	1	[2021001](1)
社交网络中的社团隐私研究综述.....		
.....蒋忠元, 陈贤宇, 马建峰	2	[2021021](10)
边缘计算开源平台综述.....		
.....顾笛儿, 卢 华, 谢人超, 黄 韬	2	[2021020](22)
基于编码的数字签名综述.....		
.....宋永成, 黄欣沂, 伍 玮, 陈海霞	4	[2021079](1)
算力网络研究进展综述.....		
.....贾庆民, 丁 瑞, 刘 辉, 张 晨, 谢人超	5	[2021034](1)
图像非加性隐写综述.....		
.....王垚飞, 张卫明, 陈可江, 周文柏, 俞能海	6	[2021102](1)

专 栏

基于仿生机理的内生安全防御体系研究.....		
.....胡爱群, 方兰婷, 李 涛	1	[2021002](11)
跨域访问控制技术研究.....		
.....诸天逸, 李凤华, 成 林, 郭云川	1	[2021003](20)
6G 网络安全场景分析及安全模型研究.....		
.....张成磊, 付玉龙, 李 晖, 曹 进	1	[2021004](28)
基于免疫算法的网络功能异构冗余部署方法.....		
.....张青青, 汤红波, 游 伟, 李英乐	1	[2021005](46)
快速响应的高效多值拜占庭共识方案.....		
.....周 旺, 胡红钢, 俞能海	1	[2021006](57)
Hyperledger Fabric 平台的国密算法嵌入研究.....		
.....曹 琪, 阮树骅, 陈兴蜀, 兰 晓, 张红霞, 金泓键	1	[2021007](65)
比特币区块链的数据压缩.....		
.....陈晓姣, 林宪正, 俞能海	1	[2021008](76)
基于比特币区块链的隐蔽信息传输研究.....		
.....张 涛, 伍前红, 唐宗勋	1	[2021009](84)
基于可满足性无关项的轻量级高隐蔽性木马设计与检测.....		
.....武玲娟, 朱嘉诚, 唐时博, 谭 静, 胡 伟	2	[2021025](35)

用于硬件木马检测的电磁辐射分析方法研究		
.....唐永康, 胡 星, 苏 颢, 李少青	2	[2021030](43)
基于模型检测的硬件木马检测技术研究		
.....张启智, 赵毅强, 高 雅, 马浩诚	2	[2021029](57)
紧凑的 Aigis-sig 数字签名方案软硬件协同实现方法		
.....周 朕, 何德彪, 罗 敏, 李 莉	2	[2021026](64)
准静态场景下基于智能超表面的密钥生成方法		
.....郝一诺, 金 梁, 黄开枝, 肖帅芳	2	[2021027](77)
基于电平转换器的物理不可克隆函数电路设计		
.....韩丽娟, 钱 蕾, 姚恩义, 娄 鑫, 曹 元, 刘宴华	2	[2021024](86)
基于 FPGA 的新型强弱混合型 PUF 电路设计		
.....连佳娜, 汪鹏君, 李 刚, 马雪娇, 翟官宝	2	[2021028](94)
面向图神经网络的对抗攻击与防御综述		
.....陈晋音, 张敦杰, 黄国瀚, 林 翔, 鲍 亮	3	[2021051](1)
基于软件定义的可重构卷积神经网络架构设计		
.....李沛杰, 张 丽, 夏云飞, 许立明	3	[2021043](29)
基于图神经网络的代码漏洞检测方法	陈 皓, 易 平	3 [2021039](37)
神经网络后门攻击研究	谭清尹, 曾颖明, 韩 叶, 刘一静, 刘哲理	3 [2021053](46)
面向 SDN/NFV 环境的网络功能策略验证	陈浩宇, 邹德清, 金 海	3 [2021035](59)
考虑拜占庭属性的 SDN 安全控制器多目标优化部署方案	王 涛, 陈鸿昶	3 [2021060](72)
基于 Renyi 熵的 SDN 自主防护系统	赵 普, 赵文涛, 付章杰, 刘 强	3 [2021049](85)
容器云中基于 Stackelberg 博弈的动态异构调度方法		
.....曾 威, 扈红超, 李凌书, 霍树民	3	[2021063](95)
基于主机系统调用频率的容器入侵检测方法		
.....季一木, 杨卫东, 李 奎, 刘尚东, 刘 强, 邵思思, 尤 帅, 黄乃娇	4	[2021073](18)

基于智能合约的高对抗性僵尸网络研究	赵 昊, 舒 辉, 康 绯, 邢 颖	4	[2021070](30)
基于网络特征混淆的欺骗防御技术研究	赵金龙, 张国敏, 邢长友	4	[2021045](42)
基于侧信道与量化推理缺陷的模型逆向攻击	李景海, 唐 明, 黄诚轩	4	[2021038](53)
生成对抗网络研究综述	王正龙, 张保稳	4	[2021080](68)
面向对手建模的意图识别方法综述	高 巍, 罗俊仁, 袁唯淋, 张万鹏	4	[2021052](86)
隐私保护的加密流量检测研究	张心语, 张秉晟, 孟泉润, 任 奎	4	[2021057](101)
网络加密流量侧信道攻击研究综述	李 玎, 祝跃飞, 芦 斌, 林 伟	4	[2021050](114)
PRINCE 密码算法的差分-线性分析	刘正斌	4	[2021072](131)
基于智能电网的安全密钥共享算法	顾 伟, 沈 剑, 任勇军	4	[2021081](141)
基于 SM9 算法的部分盲签名方案			
..... 吕 尧, 侯金鹏, 聂 冲, 苏 锐, 王 彬, 蒋鸿玲		4	[2021037](147)
基于深度学习的数字图像取证技术研究进展			
..... 乔 通, 姚宏伟, 潘彬民, 徐 明, 陈艳利		5	[2021047](13)
基于访问控制安全高效的多用户外包图像检索方案			
..... 宋甫元, 秦 拯, 张吉昕, 刘 羽		5	[2021076](29)
基于 RSA 的图像可识别对抗攻击方法	张 宇, 李海良	5	[2021065](40)
基于分层嵌入的二值图像隐写方法	程宇翔, 张卫明, 李伟祥, 俞能海	5	[2021074](49)
计算机扑克智能博弈研究综述			
..... 袁唯淋, 廖志勇, 高 巍, 魏婷婷, 罗俊仁, 张万鹏, 陈 璟		5	[2021087](57)
联邦学习研究综述	周传鑫, 孙 奕, 汪德刚, 葛桦玮	5	[2021056](77)
模型学习与符号执行结合的安全协议代码分析技术			
..... 张协力, 祝跃飞, 顾纯祥, 陈 熹		5	[2021067](93)
基于改进的 Transformer 编码器的中文命名实体识别			
..... 郑洪浩, 于洪涛, 李邵梅		5	[2021041](105)
面向时间敏感网络的控制管理机制研究综述			
..... 汪 硕, 尹淑文, 卢 华, 张继栋		6	[2021105](11)

航空自组网节点失效分析方法·····	谢丽霞, 严莉萍, 杨宏宇	6	[2021084](21)
面向大规模工控网络的关键路径分析方法·····			
·····	张耀方, 张哲宇, 曲海阔, 张 格, 王子博, 王佰玲	6	[2021069](31)
面向网络层的动态跳变技术研究进展·····			
·····	何威振, 陈福才, 牛 杰, 谭晶磊, 霍树民, 程国振	6	[2021104](44)
网络空间公共基础设施体系及安全策略研究·····			
·····	邱 洁, 韩 瑞, 魏志丰, 王志洋	6	[2021106](56)
基于区块链的访问控制技术研究进展·····	高振升, 曹利峰, 杜学绘	6	[2021044](68)
基于区块链的电网可信分布式身份认证系统·····			
·····	杨冠群, 刘 荫, 徐 浩, 邢宏伟, 张建辉, 李恩堂	6	[2021054](88)
基于信誉评估机制和区块链的移动网络联邦学习方案·····			
·····	杨 明, 胡学先, 张启慧, 魏江宏, 刘文芬	6	[2021083](99)
基于区块链的数据完整性多方高效审计机制·····	周家顺, 王 娜, 杜学绘	6	[2021107](113)

学术论文

面向边缘计算的隐私保护密钥分配协议·····	沈 剑, 周天祺, 王 晨, 杨惠杰	1	[2021010](93)
面向云应用的拟态云服务架构·····	普黎明, 卫红权, 李 星, 江逸茗	1	[2021011](101)
面向对抗样本攻击的移动目标防御·····			
·····	王 滨, 陈 靓, 钱亚冠, 郭艳凯, 邵琦琦, 王佳敏	1	[2021012](113)
基于移动 Sink 的 WSN 安全数据收集方法·····			
·····	苗春雨, 范 渊, 李 晖, 葛凯强, 张小孟	1	[2021013](121)
移动边缘计算安全防御研究·····	陈 璐, 汤红波, 游 伟, 柏 溢	1	[2021014](130)
融合宏观与微观的双层威胁分析模型·····	孙 澄, 胡 浩, 杨英杰, 张红旗	1	[2021015](143)
移动边缘群智感知动态隐私度量模型与评价机制·····			
·····	赵明烽, Lei Chen, 钟 洋, 熊金波	1	[2021016](157)
LiCi 密码的差分故障攻击·····	陈伟建, 罗皓翔	2	[2021033](104)

基于候选函数组的固件间函数对应关系构建方法		
..... 肖睿卿, 祝跃飞, 刘胜利, 芦 斌	2	[2021018](110)
基于超高频 RFID 的被动生物识别电子锁		
..... 邹 祥, 韩劲松, 曲宇航, 肖 剑, 许 贤	2	[2021022](126)
基于在线计数的改进快速泄露评估		
..... 时争光, 郑梦策, 胡红钢, 俞能海	2	[2021017](141)
基于双层注意力的 Deepfake 换脸检测		
..... 龚晓娟, 黄添强, 翁 彬, 叶 锋, 徐 超, 游立军	2	[2021032](151)
基于多因素聚类选择的 Android 应用程序分类风险评估方法		
..... 超 凡, 杨 智, 杜学绘, 韩 冰	2	[2021023](161)
基于区块链的智能服务交易跨链服务框架与通信机制		
..... 康博涵, 章 宁, 朱建明	3	[2021062](105)
基于对抗学习的强 PUF 安全结构研究		
..... 李 艳, 刘 威, 孙远路	3	[2021019](115)
资源公钥基础设施数据同步的改进方法研究		
..... 冷 峰, 赵 琦, 延志伟, 曾 宇	3	[2021064](123)
Fabric 中的匿名身份认证技术研究		
..... 叶岳洋, 张兴兰	3	[2021036](134)
基于多视图半监督集成学习的人体动作识别算法		
..... 陈圣楠, 范新民	3	[2021061](141)
LowMC 实例的差分枚举攻击效果分析		
..... 葛欣欣, 李智虎, 王美琴, 胡 凯	3	[2021046](149)
在 DNSSEC 下保障顶级域名解析托管服务稳定迁移的操作机制		
..... 何 峥, 冷 峰, 张翠玲	3	[2021059](156)
基于 TensorFlow 的恶意代码片段自动取证检测算法		
..... 李炳龙, 佟金龙, 张 宇, 孙怡峰, 王清贤, 常朝稳	4	[2021048](154)
基于 TPCM 的容器云可信环境研究		
..... 刘国杰, 张建标, 杨 萍, 李 铮	4	[2021068](164)
基于权限聚类的属性值优化		
..... 毋文超, 任志宇, 杜学绘	4	[2021077](175)
基于图结构源代码切片的智能化漏洞检测系统		
..... 邹德清, 李 响, 黄敏桓, 宋 翔, 李 浩, 李伟明	5	[2021088](113)

在线社交网络中延伸访问控制机制研究		
..... 谢绒娜, 范晓楠, 袁琳, 郭子晨, 朱家玉, 史国振	5	[2021075](123)
基于规则关联的安全数据采集策略生成		
..... 陈佩, 李凤华, 李子孚, 郭云川, 成林	5	[2021085](132)
基于图卷积网络的多源本体相似度计算方法	孙留倩, 魏玉良, 王佰玲	5 [2021071](149)
基于通信顺序进程的 Android 程序复杂信息流分析方法		
..... 袁占慧, 杨智, 张红旗, 金舒原, 杜学绘	5	[2021086](156)
面向服务监管的信息服务标识生成与管理方案		
..... 李响, 王浩, 刘千歌, 王超, 毛剑, 刘建伟	5	[2021055](169)
基于时间压缩的流量加速回放方法		
..... 王硕, 柏军, 王佰玲, 张旭, 刘红日	5	[2021082](178)
SGX 在可信计算中的应用分析	赵波, 袁安琪, 安杨	6 [2021066](126)
基于多特征融合的 Webshell 恶意流量检测方法		
..... 李源, 王运鹏, 李涛, 马宝强	6	[2021103](143)
基于结构熵约束的图聚类方法	张志颖, 田有亮	6 [2021098](155)
基于无证书签名的抗 DNS 中间人攻击方案		
..... 胡杨, 韩增杰, 叶帼华, 姚志强	6	[2021093](167)

教育与教学

双一流视域下网络安全人才培养研究——以江苏省为例		
..... 肖甫, 黄海平, 胡素君, 孙力娟	2	[2021031](1)
信息安全专业课程思政的逆向教学设计——以西安电子科技大学“无线通信网络安全” 课程为例	李瑾, 曹进, 张跃宇, 张美茹, 李晖	3 [2021058](166)
面向网络空间安全人才培养的 PRIDE 教学模式探索与实践		
..... 刘建伟, 李大伟, 高莹, 孙钰, 郭华	4	[2021078](183)

Chinese Journal of Network and Information Security

Contents List Vol.7 (2021)

Comprehensive Reviews

	No.	Page
Survey of artificial intelligence data security and privacy protection		
.....REN Kui, MENG Quanrun, YAN Shoukun, QIN Zhan	1	[2021001](1)
Survey of community privacy in social network		
.....JIANG Zhongyuan, CHEN Xianyu, MA Jianfeng	2	[2021021](10)
Survey on open source edge computing platforms		
.....GU Dier, LU Hua, XIE Renchao, HUANG Tao	2	[2021020](22)
Survey of code-based digital signatures		
.....SONG Yongcheng, HUANG Xinyi, WU Wei, CHEN Haixia	4	[2021079](1)
Survey on research progress for compute first networking		
.....JIA Qingmin, DING Rui, LIU Hui, ZHANG Chen, XIE Renchao	5	[2021034](1)
Survey on image non-additive steganography		
.....WANG Yaoifei, ZHANG Weiming, CHEN Kejiang, ZHOU Wenbo, YU Nenghai	6	[2021102](1)

Special Topics

Research on bionic mechanism based endogenous security defense system		
.....HU Aiqun, FANG Lanting, LI Tao	1	[2021002](11)
Research on cross-domain access control technology		
.....ZHU Tianyi, LI Fenghua, CHENG Lin, GUO Yunchuan	1	[2021003](20)
Research on security scenarios and security models for 6G networking		
.....ZHANG Chenglei, FU Yulong, LI Hui, CAO Jin	1	[2021004](28)
Network function heterogeneous redundancy deployment method based on immune algorithm		
.....ZHANG Qingqing, TANG Hongbo, YOU Wei, LI Yingle	1	[2021005](46)
Rapid responsive and efficient multi-valued Byzantine consensus scheme		
.....ZHOU Wang, HU Honggang, YU Nenghai	1	[2021006](57)
Embedding of national cryptographic algorithm in Hyperledger Fabric		
.....CAO Qi, RUAN Shuhua, CHEN Xingshu, LAN Xiao, ZHANG Hongxia, JIN Hongjian	1	[2021007](65)
Compression of bitcoin blockchain		
.....CHEN Xiaojiao, LIN Xianzheng, YU Nenghai	1	[2021008](76)
Bitcoin blockchain based information convert transmission		
.....ZHANG Tao, WU Qianhong, TANG Zongxun	1	[2021009](84)

Design and detection of hardware Trojans design based on satisfiability don't cares·····		
····· <i>WU Lingjuan, ZHU Jiacheng, TANG Shibo, TAN Jing, HU Wei</i>	2	[2021025](35)
Research on electromagnetic radiation based side-channel analysis method for hardware		
Trojan detection····· <i>TANG Yongkang, HU Xing, SU Ting, LI Shaoqing</i>	2	[2021030](43)
Survey on model checking based hardware Trojan detection technology·····		
····· <i>ZHANG Qizhi, ZHAO Yiqiang, GAO Ya, MA Haocheng</i>	2	[2021029](57)
Compact software/hardware co-design and implementation method of Aegis-sig digital		
signature scheme····· <i>ZHOU Zhen, HE Debiao, LUO Min, LI Li</i>	2	[2021026](64)
Key generation method based on reconfigurable intelligent surface in quasi-static scene		
····· <i>HAO Yinuo, JIN Liang, HUANG Kaizhi, XIAO Shuaifang</i>	2	[2021027](77)
Novel level shifter based physical unclonable function circuit design ·····		
····· <i>HAN Lijuan, QIAN Lei, YAO Enyi, LOU Xin, CAO Yuan, LIU Yanhua</i>	2	[2021024](86)
Novel hybrid strong and weak PUF design based on FPGA·····		
····· <i>LIAN Jiana, WANG Pengjun, LI Gang, MA Xuejiao, ZHAI Guanbao</i>	2	[2021028](94)
Adversarial attack and defense on graph neural networks: a survey·····		
····· <i>CHEN Jinyin, ZHANG Dunjie, HUANG Guohan, LIN Xiang, BAO Liang</i>	3	[2021051](1)
Architecture design of re-configurable convolutional neural network on software definition		
····· <i>LI Peijie, ZHANG Li, XIA Yunfei, XU Liming</i>	3	[2021043](29)
Code vulnerability detection method based on graph neural network ·····		
····· <i>CHEN Hao, YI Ping</i>	3	[2021039](37)
Survey on backdoor attacks targeted on neural network·····		
····· <i>TAN Qingyin, ZENG Yingming, HAN Ye, LIU Yijing, LIU Zheli</i>	3	[2021053](46)
Verification on policies for network functions in SDN/NFV-based environment·····		
····· <i>CHEN Haoyu, ZOU Deqing, JIN Hai</i>	3	[2021035](59)
Multi-objective optimization placement strategy for SDN security controller considering		
Byzantine attributes····· <i>WANG Tao, CHEN Hongchang</i>	3	[2021060](72)
SDN self-protection system based on Renyi entropy·····		
····· <i>ZHAO Pu, ZHAO Wentao, FU Zhangjie, LIU Qiang</i>	3	[2021049](85)
Dynamic heterogeneous scheduling method based on Stackelberg game model in container		
cloud····· <i>ZENG Wei, HU Hongchao, LI Lingshu, HUO Shumin</i>	3	[2021063](95)
Container intrusion detection method based on host system call frequency·····		
····· <i>JI Yimu, YANG Weidong, LI Kui, LIU Shangdong, LIU Qiang, SHAO Sisi,</i>		
<i>YOU Shuai, HUANG Naijiao</i>	4	[2021073](18)

High resistance botnet based on smart contract			
..... ZHAO Hao, SHU Hui, KANG Fei, XING Ying	4	[2021070](30)	
Research on deception defense techniques based on network characteristics obfuscation			
..... ZHAO Jinlong, ZHANG Guomin, XING Changyou	4	[2021045](42)	
Using side-channel and quantization vulnerability to recover DNN weights			
..... LI Jinghai, TANG Ming, HUANG Chengxuan	4	[2021038](53)	
Survey of generative adversarial network			
..... WANG Zhenglong, ZHANG Baowen	4	[2021080](68)	
Survey of intention recognition for opponent modeling			
..... GAO Wei, LUO Junren, YUAN Weilin, ZHANG Wanpeng	4	[2021052](86)	
Study on privacy preserving encrypted traffic detection			
..... ZHANG Xinyu, ZHANG Bingsheng, MENG Quanrun, REN Kui	4	[2021057](101)	
Survey of side channel attack on encrypted network traffic			
..... LI Ding, ZHU Yuefei, LU Bin, LIN Wei	4	[2021050](114)	
Differential-linear cryptanalysis of PRINCE cipher			
..... LIU Zhengbin	4	[2021072](131)	
Secure key-sharing algorithm based on smart grid			
..... GU Wei, SHEN Jian, REN Yongjun	4	[2021081](141)	
Partial blind signature scheme based on SM9 algorithm			
..... LYU Yao, HOU Jinpeng, NIE Chong, SU Mang, WANG Bin, JIANG Hongling	4	[2021037](147)	
Research progress of digital image forensic techniques based on deep learning			
..... QIAO Tong, YAO Hongwei, PAN Binmin, XU Ming, CHEN Yanli	5	[2021047](13)	
Efficient and secure multi-user outsourced image retrieval scheme with access control			
..... SONG Fuyuan, QIN Zheng, ZHANG Jixin, LIU Yu	5	[2021076](29)	
RSA-based image recognizable adversarial attack method			
..... ZHANG Yu, LI Hailiang	5	[2021065](40)	
Binary image steganography method based on layered embedding			
..... CHENG Yuxiang, ZHANG Weiming, LI Weixiang, YU Nenghai	5	[2021074](49)	
Survey on intelligent game of computer poker			
..... YUAN Weilin, LIAO Zhiyong, GAO Wei, WEI Tingting, LUO Junren,			
..... ZHANG Wanpeng, CHEN Jing	5	[2021087](57)	
Survey of federated learning research			
..... ZHOU Chuanxin, SUN Yi, WANG Degang, GE Huawei	5	[2021056](77)	
Security protocol code analysis method combining model learning and symbolic			
execution			
..... ZHANG Xieli, ZHU Yuefei, GU Chunxiang, CHEN Xi	5	[2021067](93)	
Chinese NER based on improved Transformer encoder			
..... ZHENG Honghao, YU Hongtao, LI Shaomei	5	[2021041](105)	

Survey of control and management mechanisms for time-sensitive network		
..... <i>WANG Shuo, YIN Shuwen, LU Hua, ZHANG Jidong</i>	6	[2021105](11)
Aeronautical Ad Hoc network node failure analysis method		
..... <i>XIE Lixia, YAN Liping, YANG Hongyu</i>	6	[2021084](21)
Key path analysis method for large-scale industrial control network		
<i>ZHANG Yaofang, ZHANG Zheyu, QU Haikuo, ZHANG Ge, WANG Zibo, WANG Bailing</i>	6	[2021069](31)
Research progress on dynamic hopping technology for network layer		
<i>· HE Weizhen, CHEN Fucui, NIU Jie, TAN Jinglei, HUO Shumin, CHENG Guozhen</i>	6	[2021104](44)
Research of public infrastructure system and security policy in cyberspace		
..... <i>QIU Jie, HAN Rui, WEI Zhifeng, WANG Zhiyang</i>	6	[2021106](56)
Research progress of access control based on blockchain		
..... <i>GAO Zhensheng, CAO Lifeng, DU Xuehui</i>	6	[2021044](68)
Credible distributed identity authentication system of microgrid based on blockchain		
..... <i>YANG Guanqun, LIU Yin, XU Hao, XING Hongwei, ZHANG Jianhui, LI Entang</i>	6	[2021054](88)
Federated learning scheme for mobile network based on reputation evaluation mechanism		
and blockchain		
<i>YANG Ming, HU Xuexian, ZHANG Qihui,</i>		
<i>WEI Jianghong, LIU Wenfen</i>	6	[2021083](99)
Multi-party efficient audit mechanism for data integrity based on blockchain		
..... <i>ZHOU Jiashun, WANG Na, DU Xuehui</i>	6	[2021107](113)

Papers

Privacy protection key distribution protocol for edge computing		
..... <i>SHEN Jian, ZHOU Tianqi, WANG Chen, YANG Huijie</i>	1	[2021010](93)
Mimic cloud service architecture for cloud applications		
..... <i>PU Liming, WEI Hongquan, LI Xing, JIANG Yiming</i>	1	[2021011](101)
Moving target defense against adversarial attacks		
<i>· WANG Bin, CHEN Liang, QIAN Yaguan, GUO Yankai, SHAO Qiqi, WANG Jiamin</i>	1	[2021012](113)
Secure data collection method of WSN based on mobile Sink		
..... <i>MIAO Chunyu, FAN Yuan, LI Hui, GE Kaiqiang, ZHANG Xiaomeng</i>	1	[2021013](121)
Research on security defense of mobile edge computing		
..... <i>CHEN Lu, TANG Hongbo, YOU Wei, BAI Yi</i>	1	[2021014](130)
Two-layer threat analysis model integrating macro and micro		
..... <i>SUN Cheng, HU Hao, YANG Yingjie, ZHANG Hongqi</i>	1	[2021015](143)

Dynamic privacy measurement model and evaluation system for mobile edge crowdsensing	<i>ZHAO Mingfeng, LEI Chen, ZHONG Yang, XIONG Jinbo</i>	1	[2021016](157)
Differential fault attack on LiCi cipher	<i>CHEN Weijian, LUO Haoxiang</i>	2	[2021033](104)
Method for constructing function correspondence between firmware based on candidate function group	<i>XIAO Ruiqing, ZHU Yuefei, LIU Shengli, LU Bin</i>	2	[2021018](110)
Passive biometric electronic lock via UHF RFID	<i>ZOU Xiang, HAN Jinsong, QU Yuhang, XIAO Jian, XU Xian</i>	2	[2021022](126)
Improved fast leakage assessment based on online counting	<i>SHI Zhengguang, ZHENG Mengce, HU Honggang, YU Nenghai</i>	2	[2021017](141)
Deepfake swapped face detection based on double attention	<i>GONG Xiaojuan, HUANG Tianqiang, WENG Bin, YE Feng, XU Chao, YOU Lijun</i>	2	[2021032](151)
Classified risk assessment method of Android application based on multi-factor clustering selection	<i>CHAO Fan, YANG Zhi, DU Xuehui, HAN Bing</i>	2	[2021023](161)
Research on inter-blockchain service framework and communication mechanism based on smart service transaction	<i>KANG Bohan, ZHANG Ning, ZHU Jianming</i>	3	[2021062](105)
Research on security architecture of strong PUF by adversarial learning	<i>LI Yan, LIU Wei, SUN Yuanlu</i>	3	[2021019](115)
Research on improved scheme of resource public key infrastructure data synchronization	<i>LENG Feng, ZHAO Qi, YAN Zhiwei, ZENG Yu</i>	3	[2021064](123)
Research on anonymous identity authentication technology in Fabric	<i>YE Yueyang, ZHANG Xinglan</i>	3	[2021036](134)
Human action recognition method based on multi-view semi-supervised ensemble learning	<i>CHEN Shengnan, FAN Xinmin</i>	3	[2021061](141)
Effect of the difference enumeration attack on LowMC instances	<i>GE Xinxin, LI Zhihu, WANG Meiqin, HU Kai</i>	3	[2021046](149)
Operation mechanism for ensuring the stable migration of top-level domain name resolution hosting services with DNSSEC	<i>HE Zheng, LENG Feng, ZHANG Cuiling</i>	3	[2021059](156)
Auto forensic detecting algorithms of malicious code fragment based on TensorFlow	<i>LI Binglong, TONG Jinlong, ZHANG Yu, SUN Yifeng, WANG Qingxian, CHANG Chaowen</i>	4	[2021048](154)
Research on the trusted environment of container cloud based on the TPCM	<i>LIU Guojie, ZHANG Jianbiao, YANG Ping, LI Zheng</i>	4	[2021068](164)

Permission clustering-based attribute value optimization		
..... <i>WU Wenchao, REN Zhiyu, DU Xuehui</i>	4	[2021077](175)
Intelligent vulnerability detection system based on graph structured source code slice		
..... <i>ZOU Deqing, LI Xiang, HUANG Minhuan, SONG Xiang, LI Hao, LI Weiming</i>	5	[2021088](113)
Research on extended access control mechanism in online social network		
..... <i>XIE Rongna, FAN Xiaonan, YUAN Lin, GUO Zichen, ZHU Jiayu, SHI Guozhen</i>	5	[2021075](123)
Using rule association to generate data collection policies		
..... <i>CHEN Pei, LI Fenghua, LI Zifu, GUO Yunchuan, CHENG Lin</i>	5	[2021085](132)
Novel similarity calculation method of multisource ontology based on graph convolution network		
..... <i>SUN Liuqian, WEI Yuliang, WANG Bailing</i>	5	[2021071](149)
Android complex information flow analysis method based on communicating sequential process		
..... <i>YUAN Zhanhui, YANG Zhi, ZHANG Hongqi, JIN Shuyuan, DU Xuehui</i>	5	[2021086](156)
Information service identity generation and management scheme for service supervision		
..... <i>LI Xiang, WANG Hao, LIU Qiange, WANG Chao, MAO Jian, LIU Jianwei</i>	5	[2021055](169)
Accelerated traffic replay method based on time compression		
..... <i>WANG Shuo, BAI Jun, WANG Bailing, ZHANG Xu, LIU Hongri</i>	5	[2021082](178)
Application progress of SGX in trusted computing area		
..... <i>ZHAO Bo, YUAN Anqi, AN Yang</i>	6	[2021066](126)
Webshell malicious traffic detection method based on multi-feature fusion		
..... <i>LI Yuan, WANG Yunpeng, LI Tao, MA Baoqiang</i>	6	[2021103](143)
Graph clustering method based on structure entropy constraints		
..... <i>ZHANG Zhiying, TIAN Youliang</i>	6	[2021098](155)
Preventing man-in-the-middle attacks in DNS through certificate less signature		
..... <i>HU Yang, HAN Zengjie, YE Guohua, YAO Zhiqiang</i>	6	[2021093](167)

Education and teaching

Research on the cultivation of cyber security talents under the perspective of double tops based on Jiangsu province		
..... <i>XIAO Fu, HUANG Haiping, HU Sujun, SUN Lijuan</i>	2	[2021031](1)
Reverse teaching design of curriculum ideological and political in information security major —Take the wireless communication network security course of Xidian University as an example		
..... <i>LI Jin, CAO Jin, ZHANG Yueyu, ZHANG Meiru, LI Hui</i>	3	[2021058](166)
Exploration and practice of PRIDE teaching mode oriented to cybersecurity talent cultivation		
..... <i>LIU Jianwei, LI Dawei, GAO Ying, SUN Yu, GUO Hua</i>	4	[2021078](183)

《网络与信息安全学报》

第二届编辑委员会

主 任 委 员：方滨兴

常务副主任委员：李风华

副 主 任 委 员：李 晖 俞能海 Kui Ren[USA] 刘建伟

邹德清 杜学绘 刘华鲁

委 员：（按姓氏笔画排序）

丁 勇	马建峰	王 标	王 滨	王布宏
王连海	王良民	王国胤	王明生	王美琴
牛 犇	仇洪冰	田有亮	田俊峰	史国振
付章杰	冯 涛	朱建明	延志伟	仲 盛
向 涛	刘 哲	刘 渊	刘西蒙	刘哲理
闫 峥	孙东红	杨宏宇	肖 甫	肖 亮
吴 铤	吴晓平	邱卫东	何道敬	沈 剑
沈 超	张小松	张云勇	张红旗	张宏莉
张建标	张振江	陆月明	陈立全	陈兴蜀
陈性元	陈雷霆	苗春雨	林 鹏	易东山
赵 波	赵琉涛	咸鹤群	禹 勇	姚志强
秦 拯	贾 焰	殷丽华	翁 健	黄欣沂
曹春杰	彭国军	蒋文保	韩伟力	韩劲松
程 光	阚海斌			

David Naccache [FRA] Gang Qu [USA] Jinjun Chen [AUS]

Willy Susilo [AUS] Yier Jin [USA]