

基于身份标识加密的身份认证方案

黄仁季, 吴晓平, 李洪成

(海军工程大学信息安全系, 湖北 武汉 430033)

摘要: 在大规模通信节点的网络中, 网络节点数量大、设备种类多, 传统的 PKI 密码体系存在证书管理困难与资源浪费的问题。设计了基于身份标识加密的节点双向认证方案。利用基于身份的密码加密对通信节点进行双向的身份认证, 解决了 PKI 体系中的数字证书管理问题; 采用密钥分割的方法解决了基于身份密码体制所存在的密钥托管问题。同时, 在认证协议中引入随机因子、时间戳、散列运算等防范各种网络攻击。最后, 对加密算法的安全性和效率以及认证协议的安全性进行了分析, 证明了认证方案是安全可靠的。

关键词: 节点身份认证; 基于身份的密码体制; 密钥托管; 加密

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00047

Identity authentication scheme based on identity-based encryption

HUANG Ren-ji, WU Xiao-ping, LI Hong-cheng

(Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: In large-scale communication nodes network, there are a large number of network nodes and so many types of equipment. So there are problems of certificate management difficulties and resource waste in the traditional PKI cryptosystem. A mutual node authentication scheme based on identity-based encryption, which solved the problem of the digital certificate management in the PKI system by the identity-based encryption and the key escrow problem in identity based cryptograph by splitting the key as well, was designed. At the same time, the introduction of random factor, timestamp and hash algorithm in the authentication protocol prevented various network attacks. Finally, the security and efficiency of the encryption algorithm and the security of the authentication protocol were analyzed, which proved the security and reliability of the authentication scheme.

Key words: node identity authentication, identity based cryptograph, key escrow, encryption

1 引言

身份认证又称为实体认证, 是网络接入控制的中心环节。网络节点身份认证是指网络中的一方根据某种协议规范确认另一方身份并允许其做与身份对应的相关操作的过程。它为网络提供

了安全准入机制, 是网络安全的第一道屏障^[1]。

网络节点身份认证协议主要分为基于对称密码体制的认证协议、基于非对称密码体制的认证协议以及基于单向散列函数的认证协议等。传统的基于对称密码的认证方案, 即预共享密钥配置方案^[2], 包括矩阵密钥预分配方案^[3]与基于多

收稿日期: 2016-04-07; 修回日期: 2016-05-06。通信作者: 黄仁季, wuyingjituan@163.com

基金项目: 国家自然科学基金资助项目 (No.61100042); 湖北省自然科学基金资助项目 (No.2015CFC867); 国家社会科学基金军事学资助项目 (No.15GJ003-201)

Foundation Items: The National Natural Science Foundation of China (No.61100042), The Natural Science Foundation of Hubei Province (No.2015CFC867), The National Social Science Found Project in Military Science (No.15GJ003-201)

项式的密钥预分配方案等^[4]。由于2个节点之间需要预共享密钥，在大规模通信节点网络中所需的共享密钥数量较大，管理困难。传统的非对称密码一般采用PKI实现，需要数字证书绑定节点的身份与公钥，需要密管中心对数字证书进行管理，而PKI证书管理复杂，需要建造复杂的CA，证书发布、吊销、验证和保存需要占用较多的资源。为简化公钥证书的管理，1984年，Shamir引入了基于身份的密码学（IBC, identity based cryptograph）。在IBC中，公钥是代表用户身份的任意字符串，比如用户的名字、E-mail地址、手机号码等；存在一个可信任的机构——私钥生成器（PKG, private key generator）根据用户的身份生成相应的私钥：由于公钥直接从身份信息中提取，证书和公钥目录是不必要的，因此，简化了公钥的管理，并由此带来了不需要密钥信道的非交互式通信以及不需要证书校验，节约了计算和通信成本^[5]。然而，基于身份加密体制因为可信任机构产生并分发用户私钥，存在密钥托管的问题，另一方面，基于身份的加密算法基于双线性对的运算，提高了运算的复杂度，目前的加密算法还存在不够高效的问题^[6]。

在大规模通信网络中，通信设备之间相互通信之前首先要进行节点身份认证，确保通信双方的安全可靠。网络上通信设备数量大、种类多、通信实时性要求高，因此，通信节点之间的认证协议需要具有通用性与高效性，目前的许多认证方案不能满足其要求^[7]。针对大量通信设备之间通信情况下数字证书管理困难以及两节点之间需要进行双向认证的问题，本文设计了基于身份标识加密的网络通信节点双向认证方案。

2 相关理论

2.1 双线性 Diffie-Hellman (BDH, bilinear diffie-hellman) 问题

1) 双线性映射和双线性群

双线性映射定义：假设① G 和 G_T 是素数 p 阶乘法群，② g 是 G 的生成元，③ $e: G \times G \rightarrow G_T$ 是双线性映射，可容许双线性映射 $e: G \times G \rightarrow G_T$ 具有以下属性的映射。

①双线性：

$$e(aP, bQ) = e(P, Q)^{ab}, \forall P, Q \in G, \forall a, b \in Z_p^*$$

②非退化性： $\exists P, Q \in G, s.t. e(P, Q) \neq 1$

③可计算性：存在有效计算法计算 $e(P, Q), \forall P, Q \in G$

则说 G 是双线性群，如 G 中的群运算是有效可计算的，而且存在有效可计算的 G_T 和可容许双线性映射 $e: G \times G \rightarrow G_T$ 。

2) 双线性 Diffie-Hellman 假设

计算性 BDH 问题定义：设 G_1 和 G_2 为2个 q 阶点群，映射 $e: G_1 \times G_1 \rightarrow G_2$ 为双线性映射， P 为 G_1 的生成元，对于任意给定的 $\langle P, aP, bP, cP \rangle$ ，其中 $a, b, c \in Z_q^*$ ，计算 $e(P, P)^{abc} \in G_2$ 的问题，称为计算性 BDH 问题。算法A解决计算性 BDH 问题的优势 ϵ 为 $\Pr[A(P, aP, bP, cP) = e(P, P)^{abc}]$ 。如果不存在 t 时间的攻击者至少以优势 ϵ 解决计算性 BDH 问题，则计算性 BDH 假设成立。

判定性 BDH 问题定义：输入 $(P, aP, bP, cP, abcP)$ 和 $(P, aP, bP, cP, \mu P)$ ，其中 a, b, c, μ, P 均为随机的，输出 YES。如果 $(P, aP, bP, cP, abcP)$ 和 $(P, aP, bP, cP, \mu P)$ 是多项式时间可区分的，则判定性 BDH 问题的优势 ϵ 为 $|\Pr[A(P, aP, bP, cP, abcP) = 1] - \Pr[A(P, aP, bP, cP, \mu P) = 1]|$ ，如果不存在 t 时间的攻击者至少以优势 ϵ 解决判定性 BDH 问题，则判定性 (t, ϵ) -BDH 假设成立。

3) BDH 问题安全性结论^[8]

①如果双线性映射 e 是有效可计算的，则 G 中判定性 Diffie-Hellman (DDH, decisional diffie-hellman) 问题是容易的。

②计算性 BDH 问题能以多项式时间归约为 G 或 G_T 中的判定性 Diffie-Hellman (CDH, computational diffie-hellman) 问题。

③对于 $P \in G_T^*$ 定义一个 G 到 G_T 的同构映射 $f_P: Q \mapsto e(P, Q)$ 。如果 f_P 的逆映射存在，则计算性 BDH 问题是容易的；如果 f_P 的逆映射存在，DDH 问题在 G_T 中是容易的；从 G 到 G_T 的双线性映射 e 是一个单向函数。

2.2 基于身份加密的安全模型

在选定一个身份攻击挑战下，如果在多项式时间内敌手没有一个不可忽略的优势赢得如下游戏挑战，基于身份标识的加密 (IBE, identity-based encryption) 系统具有选择密文安全性^[8]。

系统建立：挑战者运行系统建立过程算法，将 $params$ 发送给敌手。

阶段1 敌手自适应地发出查询 i 次，每次可能为：1) 密钥生成查询，挑战者在 ID_i 上运行 **KeyGen** 算法，并将产生的私钥发给敌手；2) 解密查询，挑战者在身份 ID_i 上运行 **KeyGen** 算法，利用生成的私钥解密 c_1 ，并将结果发给敌手。

挑战阶段：敌手提交2个明文 m_1, m_2 和一个身份 ID 。ID 必须在阶段1的密钥生成查询中没有出现过。挑战者选择一个随机比特 b ，令

$$c = \text{Encrypt}(params, ID, m_b)$$

将 c 发送给敌手作为其挑战密文。

阶段2 除敌手不可以请求ID的私钥和解密查询 (ID, C) 外，同阶段1。

猜测阶段：敌手提交一个猜测的 b' ，如果与 b 相等，则敌手成功，称敌手在上述挑战过程中为一个 IND-ID-CCA（选择密文安全性）敌手。

3 基于身份标识加密的节点双向认证方案

3.1 加密算法的构造

基于 Waters IBE 方案^[8]，利用密钥产生中心 (KGC, key generate center) 的分割，设计加密算法解决密钥托管问题。密钥分割方案如图1所示。

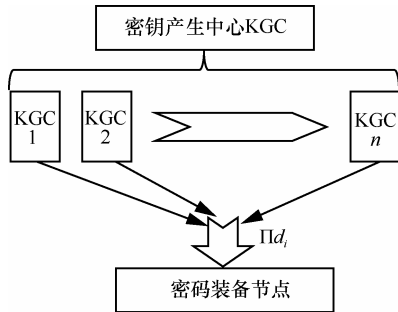


图1 密钥托管问题解决方案

k 是安全参数， G 是素数 p 阶循环群， g 是 G 的生成元， $e: G \times G \rightarrow G_T$ 是有效可计算的双线性映射。身份 ID 为 $v \in \{0,1\}^n$ （对于任意 ID ： $v \in \{0,1\}^*$ ，使用 Hash 函数 H 映射 $\{0,1\}^* \rightarrow \{0,1\}^n$ ）， $m \in G_T$ ，具体算法如下。

1) Setup(1^k)

共设置 n 个 KGC，每个 KGC 分别随机选择 $\alpha_i \in Z_p^*$ 并设置 $g_1 = g^{\alpha_i}$ ，随机选择 $g_2 \in G$ ，随机选择 $u' \in G$ 和 n 维向量 $U = (u_1, u_2, \dots, u_n)$ ， $u_i \in G$ ，

计算双线性映射 $e(g_1, g_2)$ ，每个 KGC 的系统参数和主密钥分别是 $params = (g, g_1, g_2, u', U, e(g_1, g_2))$ ， $msk = g_2^{\alpha_i}$ ，其中，每个 KGC 取相同的 g_2 ， u' 和 U 。

2) Extract(msk, v)

身份 ID 经 H 散列运算后为 n 比特的字符串，其中， v_i 表示第 i 比特， $V \subseteq \{1, \dots, n\}$ 为所有 $v_i = 1$ 的 i 的集合。随机选择 $r \in Z_p^*$ ，则可计算得到私钥

$$d_v = \{d_1, d_2\}, \text{ 其中, } d_1 = g_2^{\alpha_i} \left(u' \prod_{i \in V} u_i \right)^{r_i}, d_2 = g^{r_i}.$$

通信节点收到每个 KGC 发送来的私钥 d_v 后，

$$\text{合成自己真正的私钥 } d_v = \left\{ g_2^A \left(u' \prod_{i \in V} u_i \right)^R, g^R \right\},$$

其中， $A = \sum \alpha_i, R = \sum r_i$ 。

3) Encrypt(ID, m)

随机选择 $t \in Z_p^*$ ，计算密文 $c: c = \{c_1, c_2, c_3\}$ ，

$$\text{其中, } c_1 = e(g^A, g_2)^t m, c_2 = g^t, c_3 = \left(u' \prod_{i \in V} u_i \right)^t.$$

4) Decrypt(d_v, c)

解析密文 c ，用户私钥为 d_v ，计算明文

$$m = c_1 \frac{e(c_3, d_2)}{e(c_2, d_1)}$$

加解密一致性检验为

$$\begin{aligned} \frac{e(c_3, d_2)}{e(c_2, d_1)} &= \frac{e\left(u' \prod_{i \in V} u_i, g^R\right)}{e\left(g^t, g_2^A \left(u' \prod_{i \in V} u_i\right)^R\right)} \\ &= \frac{e\left(u' \prod_{i \in V} u_i, g^R\right)}{e\left(g^t, g_2^A\right) e\left(g^t, \left(u' \prod_{i \in V} u_i\right)^R\right)} \\ &= \frac{e\left(u' \prod_{i \in V} u_i, g\right)^{tR}}{e\left(g, g_2\right)^{tA} e\left(g, \left(u' \prod_{i \in V} u_i\right)^{tR}\right)} \\ &= \frac{1}{e\left(g^A, g_2\right)^t} \\ &= \frac{1}{e\left(g_1, g_2\right)^t} \end{aligned}$$

所以

$$\begin{aligned} Decrypt(Encrypt(m)) &= c_1 \frac{e(c_3, d_2)}{e(c_2, d_1)} \\ &= e(g^A, g_2)^t m \frac{1}{e(g_1, g_2)^t} = m \end{aligned}$$

3.2 基于身份加密的节点双向认证协议

认证协议在第 3.1 节加密算法的保护下完成节点认证, 整体认证方案如图 2 所示。

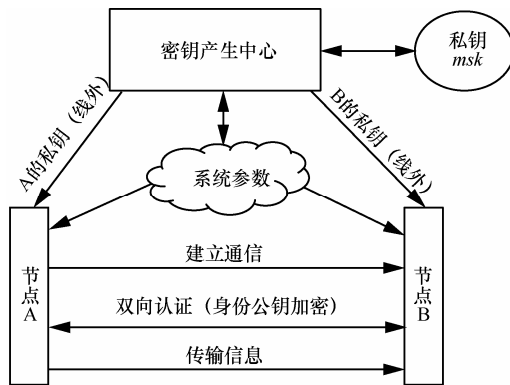


图2 节点安全认证实施过程

假设两通信设备节点 A、B 之间建立通信进行认证, 使用 3.1 节中的加密算法 E, 具体步骤如下。

1) B 向 A 发送指令, 进行认证请求。即 B 向 A 发送信息 $Request||IDB||time$, 其中, $Request$ 为建立认证请求, IDB 为 B 的身份信息, $time$ 为时间戳。

2) A 接收到 B 的认证请求后向 B 发送认证回复并对自己的身份进行认证。A 向 B 发送信息 $E(Reply||IDA||N1||time||HASH, IDB)$, 其中, $Reply$ 为对请求的回复, IDA 为 A 的身份标识, $N1$ 为由 A 产生的随机数, $time$ 为时间戳, $HASH$ 为对上述信息的散列值以进行完整性校验, 返回信息使用 B 的身份信息进行加密。

3) B 接收到 A 的返回信息, 利用自己的身份和自己的私钥对消息解密, 得到 A 的身份标识, 对随机数 $N1$ 按照双方事先约定的变换 f 进行变换返回给 B, 具体消息内容为 $E(f(N1)||N2||time||HASH, IDA)$, 其中, $f(N1)$ 为对随机数 $N1$ 的变换用以对方进行验证, $N2$ 为由 B 生成的随机数, $time$ 为时间戳, 整个消息散列运算附后并由 A 的身份信息 IDA 进行加密。

4) A 收到 B 的信息, 利用自己的身份 IDA 以及自己的私钥进行解密, 得到 $f(N1)$, 并用自己刚才生成的 $N1$ 计算 $f(N1)$ 检查是否一致, 如果

一致则通过了对 B 的身份认证, 承认 B 的合法身份, 同时对收到的 $N2$ 进行 f 变换, 用以 B 对自己的认证具体消息内容为 $E(confirm||f(N2)||time||HASH, IDB)$, 其中, $confirm$ 为认证通过确认, $time$ 为时间戳, 对消息散列运算连在后面并用 IDB 进行加密。

5) B 收到 A 的认证确认信息后, 利用自己的身份和私钥进行解密, 用生成的 $N2$ 计算 $f(N2)$ 与收到的 $f(N2)$ 比较是否一致, 通过对 A 的身份认证, 向 A 发送确认信息以及通信内容 $E(confirm||m||time||HASH, IDA)$, 其中, $confirm$ 为对 A 的身份认证结果, $time$ 为时间戳, $HASH$ 为整个消息散列值, 消息与其散列值通过 A 的身份进行加密。

6) A 与 B 完成双向身份认证, 建立正常通信。

4 安全性及效率分析

4.1 加密算法的安全性对比分析

对于用户私钥 d , 要取得或生成私钥须计算出主私钥 g_2^α , g_2 为公开参数, 但 α 为秘密参数, 所以, 计算 α 可表示为: 已知 g 和 $g_1 = g^\alpha$, 求解 α , 即离散对数问题, 具有计算复杂性。

当攻击者不知道用户私钥 d , 要对密文 c 进行破解时, 因为 $c = \left\{ e(g_1, g_2)^t m, g^t, \left(u \prod_{i \in V} u_i \right)^t \right\}$,

所以, 要得到 m 即为计算 $e(g_1, g_2)^t$, 其中生成元为 g 为公共参数, $g_1 = g^A = g^{\sum \alpha_i}$ 为公共参数, $g_2 \in G$ 为公共参数, 令 $g_2 = g^\beta$, $e(g_1, g_2)^t = e(g^A, g^\beta)^t = e(g, g)^{A\beta t}$, g^t 在密文 c 中给出, 则计算 m 可归约为已知 g, g^A, g^β, g^t 求解 $e(g, g)^{A\beta t}$ 的问题, 即计算性双线性 Diffie-Hellman 问题, 与 CDH 问题等价, 具有计算安全性。

选择明文安全 (IND-ID-CPA), 即密文不会向任何计算能力为多项式界的攻击者泄露有关明文任何有用信息。如果对任何 t 时间的 IND-ID-CPA 攻击者 A, 做至多 q_E 次私钥提取查询, 有 $Adv_A^{IBE} < \epsilon$, 则 IBE 方案是 (t, q_E, ϵ) -IND-ID-CPA 安全的。

本方案的加密过程基于 Waters 体制, 所以, 如果判定性 BDH 假设成立, 则 (t, q_E, ϵ)

-IND-ID-CPA 是安全的^[8]: $\epsilon' = \frac{\epsilon}{32(n+1)q}$, $t' = t +$

$o(\varepsilon^{-2} \ln(\varepsilon^{-1}) \lambda^{-1} \ln(\lambda^{-1}))$, $\lambda = \frac{1}{8(n+1)q_E}$, 其中, q_E

是私钥提取查询的最大次数。

在 Waters 的 IBE 体制下, 其安全性不依赖随机预言机, 是标准模型下的 IBE 方案。如表 1 所示, 与 BasicIdent 体制和 FullIdent 体制^[9]等基于随机预言的 IBE 方案相比, 具有更高的安全性。与原始的 Waters 方案相比, 本方案解决了密钥托管问题, 降低了由于 KGC 受到攻击或破坏而给整个网络带来的威胁。

表 1 加密算法安全性对比

加密方案	安全性
BasicIdent 和 FullIdent 体制	随机预言机模型 选择密文安全 要求完全信任 KGC
Waters 体制	标准模型 选择明文安全 要求完全信任 KGC
本文方案	标准模型 系统的安全不完全依赖一个 KGC

4.2 加密算法的性能对比分析

$e(g_1, g_2)$ 可以预先计算得到包含在 $params$ 之中, 所以, 加密过程不需要进行双线性映射的计算。加密过程平均 $\frac{n}{2}$ 个 G 中的群运算、2 个 G 中的幂运算及 1 个 G_r 中的幂运算。解密过程中有 2 个双线性映射的计算、1 个 G_r 中的乘法运算和 1 个 G_r 中的求逆运算。

如表 2 所示, 与 BasicIdent 体制和 FullIdent 体制相比^[10], 加密方案在系统建立阶段成本较高, 多出一个数量级; 但是在密钥提取阶段和加密阶段具有相似的时间成本, 只需要 20 ms 左右; 在解密阶段, 计算成本比 BasicIdent 体制和 FullIdent 体制多出 10 ms, 为 30 ms。基于以上分析, 本方案的加解密过程在保证安全性的前提下效率没有明显下降, 只在系统建立过程中较为耗时, 但在实际应用中系统建立对时间成本要求不高, 本方案仍具有较好的效率。

表 2 加密算法性能对比

加密方案	系统建立及密钥分配阶段	加密阶段	解密阶段
BasicIdent 体制和 FullIdent 体制	10 ms 量级	20 ms	20 ms
Waters 体制	100 ms 量级	30 ms	30 ms
本文方案	100 ms 量级	30 ms	30 ms

4.3 节点双向认证协议的安全性对比分析

认证协议主要通过双方的随机数 $N1$ 和 $N2$ 以及对双方身份加密后信息的正确解密进行节点之间的身份认证, 4.1 节证明了加密算法的安全性, 在加密算法安全时, 节点之间的认证具有有效性。同时, 本协议还具有以下抵御攻击的能力。

1) 重放攻击^[11,12]: 方案通过设置挑战随机数和时间戳来防止重放攻击, 每次认证过程由双方产生随机数进行身份确认, 每条消息均附有时间戳, 使每一次在信道中传输的消息都不相同, 攻击者不能通过截获历史消息进行重放实现非法认证。

2) 拒绝服务攻击: 攻击者为了破坏网络的服务, 可以选择对认证服务器或者认证者发动拒绝服务攻击, 耗费网络资源。如果发生对认证者的拒绝服务攻击, 认证者在收到申请者发送的消息时, 首先会检查消息中认证者的随机数与自己之前发送的是否一致, 若不一致, 则丢弃该分组, 这在一定程度上可以抵抗对认证节点的拒绝服务攻击。

3) 双向身份认证: 双向身份认证可以有效防范中间人攻击。认证过程通过对双方产生的随机数的识别与利用双方身份标识进行加密的技术结合, 实现相互间身份的认证, 可防范会话劫持。

4) 消息完整性鉴别: 通过对消息内容进行散列运算生成校验码, 对消息内容的完整性进行鉴别, 可以有效鉴别消息是否受到破坏、篡改或失真。对散列值利用基于身份密码进行加密, 保护完整性校验信息的安全性, 提高可靠度。

5) 完善的加密机制: 认证过程消息由基于身份的加密机制进行加密保护, 有效保护了传输信息的安全性, 防止受到劫获与窃听。同时, 基于节点身份的加密与解密过程也具有对节点身份的认证作用, 与认证内容相互补充。

如表 3 所示, 与现在网络上广泛使用的 Kerberos、SSL 等认证协议相比^[13], 方案中的认证协议采用了基于身份的密码体制, 不需要用数字证书绑定节点的身份与公钥, 节省了证书的生产、存储、使用成本; 在大规模的网络中不需要建立复杂的 CA 认证体系, 节约了系统的构建成本, 减少了系统的复杂度。与单纯的基于身份密码体制的认证相比, 方案中加入了随机因子、认证码等因素, 提高了认证的安全可靠性。

表3 认证协议对比

认证方案	特点
网络上常用方案	需要数字证书绑定身份与公钥，需要建立 CA 认证体系
普通基于身份的密码方案	不需数字证书与 CA，存在密钥托管问题，认证形式单一
本文方案	不需数字证书与 CA，需建立多个 KGC，多因素进行认证

5 结束语

本文对 Waters 的基于身份加密算法进行了改进，解决了基于身份密码的密钥托管问题，并利用改进的 IBE 算法设计了网络通信设备节点的双向认证方案。认证方案以加密为基础实现节点的身份认证，实现了通信设备节点间的双向认证，利用随机因子与散列值防范各种网络攻击。与传统节点认证方案相比，本文方案免去了数字证书的管理，直接以节点身份作为公钥，节约了管理成本，提高了使用效率。同时，本文方案将 IBE 体制融合入认证协议中，从算法和协议两方面保证了认证的安全性，与其他基于身份的密码相比，在保证安全性的同时最大限度地保证认证的效率与通信流量的控制。在下一步工作中，还需要进一步改进加密方案，提高解密的效率；对认证协议优化，不断提高方案的运行效率。

参考文献：

- [1] 黎妹红, 韩磊. 身份认证技术及应用[M]. 北京: 北京邮电大学出版社, 2012.
LI M H, HAN L. Identity authentication technology and application[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2012.
- [2] ESCHENAUER L, GLIGOR V. A key-management scheme for distributed sensor networks[C]//The 9th ACM Conference on Computer and Communications Security. c2002: 41-47.
- [3] DU W, DENG J, HAN Y S, et al. A pairwise key pre-distribution scheme for wireless sensor networks [J]. ACM Transaction on Information and System Security, 2005, 8(2): 228-258.
- [4] LIU D, NING P. Establishing pairwise keys in distributed sensor networks[C]//The 10th ACM Conference on Computer and Communications Security. c2003: 52-61.
- [5] 杨浩淼, 邱乐德. 基于身份的公钥密码体制的研究[M]. 成都: 电子科技大学出版社, 2012.
YANG H M, QIU L D. Research on identity-based public key cryptosystem [M]. Chengdu: University of Electronic Science and Technology Press, 2012.
- [6] 邓伦治, 王祥斌, 瞿云云. 高效的基于身份的签密方案[J]. 计算机工程与科学, 2014, 36(3): 441-445.
DENG L Z, WANG X B, QU Y Y. High-efficient signcryption scheme based on identity[J]. Computer Engineering & Science,

2014, 36(3):441-445.

- [7] 马陵勇, 卓泽朋, 廉玉忠. 新的无证书签密方案[J]. 吉林师范大学学报, 2014, 3: 93-95.
MA L Y, ZHUO Z P, LIAN Y Z. New certificateless signcryption scheme[J]. Journal of Jilin Normal University, 2014, 3:93-95
- [8] 胡亮, 赵阔, 袁巍, 等. 基于身份的密码学[M]. 北京: 高等教育出版社, 2011.
HU L, ZHAO K, YUAN W, et al. The cryptography based on identity[M]. Beijing: Higher Education Press, 2011.
- [9] BONEC D, FRANKLIN M. Identity-based encryption from the weil pairing[J]. Siam Journal on Computing, 2003, 32(3): 213-229.
- [10] 李发根, 吴威峰. 基于配对的密码学[M]. 北京: 科学出版社, 2014.
LI F G, WU W F. Based on the matching of cryptography [M]. Beijing: Science Press, 2014.
- [11] 张丽, 郝身刚, 岳贤锋. 基于双线性映射的匿名跨域认证方案[J]. 河南师范大学学报, 2013, 41(1): 155-158.
ZHANG L, HAO S G, QIU X F. An anonymous authentication for multi-domain based on the bilinear map[J]. Journal of Henan Normal University, 2013, 41(1):155-158.
- [12] 刘团奇, 张浩军, 赵志鹏. 一种云环境下基于身份的统一身份认证方案研究[J]. 中原工学院学报, 2015: 26(4): 55-58.
LIU T Q, ZHANG H J, ZHAO Z P. A unified identity authentication scheme research in cloud with ID-based[J]. Journal of Zhongyuan Institute of Technology, 2015, 26 (4): 55-58.
- [13] 叶清. 网络安全原理[M]. 武汉: 武汉大学出版社, 2014.
YE Q. Network security principle[M]. Wuhan: Wuhan University Press, 2014.

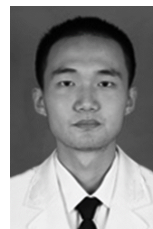
作者简介：



黄仁季 (1994-), 男, 山东青岛人, 海军工程大学硕士生, 主要研究方向为信息网络安全。



吴晓平 (1961-), 男, 山西新绛人, 博士, 海军工程大学教授、博士生导师, 主要研究方向为信息安全、密码学。



李洪成 (1991-), 男, 河南商丘人, 海军工程大学博士生, 主要研究方向为信息安全、数据挖掘。