

一种基于身份的无线传感器网络广播方法

曹晓梅, 吴 亮, 杨 庚

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要: 从基于身份密钥体系出发, 提出了一种适用于无线传感器网络的轻量级广播方法——IBESB (Identity-Based Encryption Scheme For Broadcasting). 首先简要介绍了安全证明基础, 然后给出广播算法, 并在随机预言模型中就选择密文安全性和完整性给出了基于 BDH 假设的证明, 与经典算法在计算复杂性、内存需求等方面进行的分析比较表明, IBESB 在这些方面都有一定的优势, 最后讨论了可进一步研究的内容。

关键词: 基于身份标识密钥系统; 无线传感器网络; 广播加密

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)08-0009-05

An Identity-Based Encryption Scheme for Broadcasting

CAO Xiao-mei, WU Liang, YANG Geng

(College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: This paper proposes a broacasting algorithm based on identity encrpytion scheme named as IBESB. Firstly, we introduce the preconditions of the algorithm proof, then IBESB is described in details. The security and integrity on choosing ciphertext in random oracle model are proved based on BDH assumption. Compared with traditional broacasting algorithms, IBESB outstands them both in computing complexity and memory cost.

Key words: identity-based cryptography; wireless sensor network; broadcast encryption

1 引言

无线传感器网络 (Wireless Sensor Network, WSN)^[1]具有广泛的应用前景, 但传感器节点在能源、计算能力、存储量等方面存在较大局限, 使 WSN 的研究面临众多挑战。

广播是 WSN 数据传输的主要方式之一, 寻找一种高效、安全的广播加密方案对安全敏感的 WSN 应用场景 (如小区安保、战地侦测等) 尤为重要。针对广播加密的研究引起了广泛关注, 较为典型的的就是 TESLA、 μ TESLA 及其扩展和推广^[2]。

基于身份标识的加密算法 (Identity-Based Encryption, IBE) 由 Shamir 于 1984 年首先提出^[3]。但直到 2001 年 Boneh 和 Franklin^[3]才给出了一个可实际应用的实现方法, 随后, 文献[4]中提出了一种

适用于 WSN 的既可用于分配密钥, 同时又可发送广播消息的加密机制, 本文对该方案进行了完善, 提出一种基于身份的 WSN 广播方法——IBESB (Identity-Based Encryption Scheme For Broadcasting)。相比于文献[5], IBESB 充分考虑广播组的动态性, 网络中任意节点都可以成为广播源, 但只有添加到广播组中节点才能解密广播包, 同时通过有效的加密和认证机制确保广播安全性, 文中对方案的完整性和选择密文攻击安全性进行了基于 BDH 假设和随机预言模型的证明。

2 背景介绍

当前针对基于身份密钥体系安全性的研究主要采用随机预言模型 (Random Oracle Model) 或选择 ID (Select ID), 证明基础都建立在 BDH (Bilinear-

收稿日期: 2010-05-13; 修回日期: 2010-06-13

基金项目: 国家自然科学基金项目 (60873231); 江苏省高校自然科学基金项目 (08KJB520006); 江苏省“六大人才高峰”基金项目 (06-E-044)

Diffie-Hellman)之上,本节简要介绍证明中用到的相关概念.

2.1 BDH(Bilinear-Diffie-Hellman)问题

IBE 的核心是使用了超奇异椭圆曲线上的一个双线性映射(Weil pairing). BDH 问题是 IBE 加密方案的安全性基础,本文第 4 节的安全性证明建立在 BDH 假设之上. BDH 问题是 CDH(Computational Diffie-Hellman)困难问题的一个变形.

我们记 Z_q 为素数阶 q 的加法群, $Z_q = \{0, \dots, q-1\}$, Z^+ 为正整数.

(1) 设 p 是一个大的素数, $p \equiv 2 \pmod{3}$, 并且存在大素数 q 使得 $p = 6q - 1$;

(2) $E/GF(p)$ 是在 $GF(p)$ 上构造的椭圆曲线: $y^2 = x^3 + 1$, P 是该曲线上阶为 q 的一个点, 由 P 生成的循环群记为 G ;

(3) BDH 问题: 对随机 $a, b, c \in Z_p^*$, 已知 (P, aP, bP, cP) 来计算 $\hat{e}(P, P)^{abc} \in GF(p^2)$. 其中 $\hat{e}: G \times G \rightarrow GF(p^2)^*$ 是一具有下列性质的映射:

① 双线性性: 如果对所有的 $x, y \in G, a, b \in Z$, 都有 $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$, 则映射 $\hat{e}$ 称为一个双线性映射.

② 非退化性: 存在 $P, Q \in G$, 使得 $\hat{e}(P, Q) \neq 1$.

③ 可计算性: 有一个多项式时间算法来计算 $\hat{e}(P, Q)$.

2.2 安全模型

随机预言机模型是一种探索性分析一个密码学原型和协议的方法, 它为密码学理论和实践提供了一座桥梁^[6]. 在这种方法中, 与原型或协议有关的算法(包括敌手的算法) 可以向一个或多个函数的预言机进行询问, 而这些函数是对某一特殊的 n 和 k 的, 从 $\{0, 1\}^n$ 至 $\{0, 1\}^k$ 的一个映射.

组合安全性目标和攻击模型可以获得不同的安全性, 对公钥加密最强的安全性是 IND-CCA2, 通常称为选择密文安全性.

不可区分性(IND)指攻击者选择两个明文, 加密者随机选一个, 返回其密文, 则攻击者不能以明显大于 $1/2$ 的概率正确猜测选择的是哪一个明文. 非适应性选择密文攻击(CCA1)指攻击者在得到目标密文 y^* 之前可询问解密预言机(以下简称解密机), 但在得到 y^* 之后不可以. 适应性选择密文攻击(CCA2)指攻击者在得到 y 后还可询问解密机, 但不可询问 y^* .

3 基于身份的广播加密方法

文中提出算法主要由四个函数组成: Setup, Extract, Encrypt 和 Decrypt, 分别完成系统参数建立、密钥提取、加密和解密的功能.

算法 1: 基于身份的广播算法(以全网广播为例)

(1) Setup: 随机选择 $x \in Z_q^*$, $\text{Params} = \{q, p, \hat{e}, n, P, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$, 其中哈希函数 $H_1: \{0, 1\}^* \rightarrow G_1^*$, $H_2: Z_q^* \times G_2 \rightarrow \{0, 1\}^n$, $H_3: \{0, 1\}^n \times \{0, 1\}^n \rightarrow Z_q^*$ 和 $H_4: \{0, 1\}^n \rightarrow \{0, 1\}^n$.

(2) Extract: 对给定的节点 $\text{Id} \in \{0, 1\}^*$, 设 id 是源节点.

计算 $Q_i = H_1(\text{Id}) \in E/GF(p)$, 每个节点密钥对 (S_i, Q_i) , 其中 $S_i = xQ_i$, 取主密钥为 $S_{\text{id}} = S_1 = xQ_1$,

$$L = (Q_1 + Q_2 + \dots + Q_n)P$$

$Q_{v1} = Q_1 + Q_2 + \dots + Q_n$, $Q_{vi} = Q_1 + Q_i, 2 \leq i \leq n$

$$U_i = vQ_{vi}, U_1 = vQ_{v1}$$

$v \in Z_q^*$ 由广播源节点随机选择

(3) Encrypt: 对原文 $m \in M$ 和公钥 Id , 加密步骤如下:

Step 1: 计算 $R = vL, vP$

Step 2: 随机取 $\sigma \in \{0, 1\}^n, r = H_3(\sigma, M), g = \hat{e}(S_{\text{id}}, L)$

Step 3: 密文 $C = (r, \sigma \oplus H_2(r, g^v), H_{4(\sigma)}(M))$

Step 4: 广播包 $(C, R, G), G = \{U_1, U_2, \dots, U_n\}$

(4) Decrypt: 设 $C = (U, V, W)$ 为密文, 解密步骤如下:

Step 1: 首先计算 $g^v = \hat{e}(S_{\text{id}}, vL)$;

Step 2: 然后计算 $\sigma = V \oplus H_2(U, g^v)$;

Step 3: 解密出消息 $M = D_{4(\sigma)}(W)$;

Step 4: 最后计算 $r = H_3(\sigma, M)$, 如果 $U \neq r$, 则认证失败.

在实际的广播过程中, 广播源节点根据需求选取目标节点群, 在 Extract 过程中, L 为目标节点群 Q_i 之和与 P 的乘积, 同时在广播包中包含目标节点群的 U_i 值, 节点在本地通过 Params 和自己的私钥 S_i 解密出广播包内容, 未加入广播组内节点无法计算出 g^v .

4 分析和比较

4.1 正确性分析

正确性在于要保证广播组内节点在本地内通过 Params 和自己的私钥 S_i 解密出广播包内容,由第3节可知:

$$\begin{aligned}
 Q_{vi} &= Q_1 + Q_i, Q_{v1} = Q_1 + Q_2 + \dots + Q_n, U_i \\
 &= vQ_{vi} \\
 g^v &= \hat{e}(vL, S_{id}) \\
 &= \hat{e}[(Q_1 + Q_2 + \dots + Q_n)Pv, xQ_1] \\
 &= \hat{e}\{[(n-2)Q_i + (Q_1 + Q_2) + (Q_1 + Q_3) + \dots + \\
 &\quad (Q_1 + Q_{i-1}) + (3-n)(Q_1 + Q_i) \dots + (Q_1 + \\
 &\quad Q_n)]Pv, xQ_1\} \\
 &= \hat{e}\{[(n-2)Q_i]Pv, xQ_1\} \times \hat{e}\{[(Q_1 + Q_2) + (Q_1 \\
 &\quad + Q_3) + \dots + (Q_1 + Q_{i-1}) + (3-n)(Q_1 + Q_i) \dots \\
 &\quad + (Q_1 + Q_n)]Pv, xQ_1\} \\
 &= \hat{e}\{[(n-2)xQ_i]Pv, Q_1\} \times \hat{e}\{[v(Q_1 + Q_2) + \\
 &\quad v(Q_1 + Q_3) + \dots + v(Q_1 + Q_{i-1}) + v(3-n)(Q_1 \\
 &\quad + Q_i) \dots + v(Q_1 + Q_n)]xP, Q_1\} \\
 &= \hat{e}\{[(n-2)S_i]Pv, Q_1\} \times \hat{e}\{[U_2 + U_3 + \dots + \\
 &\quad U_{i-1} + (3-n)U_i + \dots + U_n]P_{pub}, Q_1\}
 \end{aligned}$$

这样节点在本地就可以解密出广播包内容,这样机制有效保证了广播过程的正确性。

4.2 安全性分析

通过上面分析可知,本文广播方法能有效排除合谋攻击,下面就基于身份密钥体系安全性的几个方面给出相关证明。

(1) 语义安全性:因为未添加广播组内节点即使获得了这些公开参数也无法构造解密式,在实际的广播过程中,广播源节点根据需求选取目标节点群,在 Extract 过程中, L 为目标节点群 Q_i 之和与 P 的乘积,同时在广播包中包含目标节点群的 U_i 值,节点在本地通过 Params 和自己的私钥 S_i 解密出广播包内容,未加入广播组内节点无法计算出 g^v 。所以这种机制有效地排除了合谋攻击和伪造广播消息的可能性,从而保证了广播过程中的安全性。

(2) 基于椭圆曲线双线性映射安全性(语法安全性):下面分别就算法的完整性、选择密文攻击、向前向后保密性三个方面的安全性给出相关证明,主要采用针对 CCA2 的不可区分性(IND-CCA2)证明方法,设计一个挑战者/应答游戏,通过概率的推导证明其安全性。

① 完整性

广播包在加密过程中经过了 Hash 运算,其内容安全性有一定保证,我们仅考察密文不可伪造性。假设攻击者 π 是一个具有二项式时间概率的图灵机 (polynomial time probabilistic Turing machine),其目标是使用任意的 Id 给用户发送一个合法的广播包。在第3节中,广播包通过源节点私钥构造,假定攻击者 π 不可获取源节点私钥。攻击者可以对以下四种预言机发起询问:

身份哈希预言机 (Identity hash oracle):对任意给定的 Id 生成对应的哈希值 $H_1(\text{Id})$ 。

加密预言机 (Encryption oracle):攻击者提供任意明文,获取加密后的密文。

密钥生成预言机 (Key generation oracle):攻击者提交任意 Id,获取对应私钥。

解密预言机 (Decryption oracle):攻击者提供任意密文,获取对应的明文。

唯一的限制是,攻击者 π 不能将密钥生成和密文预言机给出的信息用来询问。

性质1 假设 π 是一个二项式受限的攻击者,可以以 ϵ 的优势伪造密文,并且至多可以发起 n_1 个对身份的 H_1 询问和 n_d 个解密询问,则存在受二项式时间限制的算法 B 以至少 $\epsilon/n_1^2 n_d$ 的优势解决 BDH 问题。

证明:

假设算法 B 的输入为 P, xP, yP 和 zP ,为在 π 的帮助下输出 $\hat{e}(P, P)^{xyz}$, B 可以运行哈希运算 H_1 和 H_2 , π 在给出猜测的密文前可对其提出解密询问。显然,如果 π 在一次解密问答后获取的是合法的明文, π 伪造成功。作为对询问的响应, B 将对 H_1, H_2 的询问信息保存在链表 $H_1^{\text{list}}, H_2^{\text{list}}$ 中,同时将可能的答案保存在 H^{ans} 中。

- 当 π 对 H_1 预言机发起询问时, B 随机选取 $\alpha \in \{1, n_1\}$ 。对 Id_π 的询问处理如下:如果这是第 α 次询问, B 给出 yP , 我们称 Id_π 为一个已猜测过的 Id (以下简称 GID)。否则, B 随机选取 $\ell \in Z_q^*$, 将 $\langle \text{Id}_\pi, \ell \rangle$ 加入 H_1^{list} 。

- 当 π 对 H_2 的询问为 $\langle r, h \rangle \in Z_q^* * G_2$ 时, B 随机给出 $t \in \{0, 1\}^n$, 并将 $\langle r, h, t \rangle$ 加入 H_2^{list} 中。

- 当 π 对 Id_π 发起私钥询问时,如果 Id_π 是 GID, 算法 B 失败。否则, H_1^{list} 必然包含 $\langle \text{Id}_\pi, \ell \rangle$, B 给出 ℓxP 。

- 当 π 对明文 M 发起加密询问时,如果 Id_π 是

GID, B 随机选择 $r \in Z_q^*$, $t \in \{0, 1\}^n$, 然后 B 给出密文 $C = \langle r, t, E_k(M) \rangle$. 否则, 根据假设, H_1^{lis} 必然包含 $\langle \text{Id}_\pi, \mathcal{E} \rangle$, 则, π 的私钥为 $\mathcal{E} xP$, 密文由对应的加密算法生成, (例如, $l = \hat{e}(zP, \mathcal{E} xP)$).

- 当 π 对密文 $C = \langle U, V, W \rangle$ 发起解密询问时, 如果 Id_π 是 GID, B 在 H_2^{list} 中查找 $\langle U, l, t \rangle$, 如果查找到相应条目, l 被加入 H^{ans} 中. π 被告知 C 是无效的 (即使 C 是合法的). 否则, 不失一般性, 假设 π 不是 GID, 密文由解密算法解密, 如果是合法的, 把明文传给 π , π 获胜.

π 最后将终止, 如果 H^{ans} 为空, B 失败, 否则 B 随机给出 H^{ans} 中一个元素. π 从不对 GID 发起密钥生成询问的概率至少为 $1/n_1$, 如果 π 提交了一个合法的密文, 那么 π 以至少 $1/n_1$ 的概率伪造了一个密文. 在此情形下, 如果 $l = \hat{e}(P, P)^{xyz}$ 不在 H^{ans} 中, 则 π 无法伪造密文, 因为 H_2 是一个随机预言模型. 那么 π 询问 $H_2(l)$ 的概率至少为 ϑ , 在此种情形下 B 不会失败, 因为 H^{ans} 必不为空, 并以至少 $1/n_d$ 的概率给出正确的 l , 所以有 $\text{Adv}(B) \geq \vartheta/n_1^2 n_d$.

性质 2 记事件 π 在上述模拟过程中询问 $H_2(U, l)$ 为 P , 那么在模拟过程中的 $\Pr[P]$ 和现实攻击一致.

证明:

采用归纳法来证明, 设 P_k 为 π 在前 k 次模拟过程中询问 $H_2(U, l)$ 的概率, 显然在模拟和现实两种情况下 $\Pr[P_0] = 0$, 假设对 $k > 0$ 有在两种情况下 $\Pr[P_{k-1}]$ 相同, 那么对 P_k 也同样成立

$$\begin{aligned}\Pr[P_k] &= \Pr[P_k | P_{k-1}] \Pr[P_{k-1}] + \\ &\quad \Pr[P_k | \neg P_{k-1}] \Pr[\neg P_{k-1}] \\ &= \Pr[P_{k-1}] + \Pr[P_k | \neg P_{k-1}] \\ &\quad \Pr[\neg P_{k-1}]\end{aligned}$$

$\neg P$ 表示 P 的否定. 可以观察到, 只要 π 没有询问 $H_2(U, l)$, 它在模拟和现实攻击中的视角是一致的, 所以 $\Pr[P_k | \neg P_{k-1}]$ 在两种情形下相等, 即得证.

② 选择密文攻击

性质 3 π 是一个受二项式时间限制的攻击者, 其优势为 ϑ , 并且至多可以发起 n_1 个对身份的 H_1 询问和 n_2 个对 H_2 的询问, 同时, 假设方案是抗密文伪造攻击的, 那么存在二项式受限的算法 B 以至少 $\vartheta/n_1^2 n_2$ 的优势解决 BDH 问题.

证明:

与对性质 1 的证明相比, 除解密询问有区别外

其他步骤基本相似. 无论何时, π 提出解密询问时都会被告知提交的密文是非法的. B 对 H_1 和 H_1 的处理机制与性质 1 中相同. 在一定数量的询问后, π 抛出两个明文 M_0, M_1 和一个它希望挑战的 Id_j . 如果 Id_j 不是已猜测过的 Id , 则 B 失败. 否则, B 随机选择 $U \in Z_q^*$, $V \in \{0, 1\}^n$ 和 $\sigma \in \{0, 1\}^n$, 然后 B 计算 $W = E_\sigma(M_b)$ ($b \in \{0, 1\}$), 以挑战密文 $C = \langle U, V, W \rangle$ 做为给 π 的应答. π 继续发起更多的生成密钥、加密、解密询问, B 以与定理 1 中相同的方式应答 (除解密询问外), 唯一的限制是不能发起对 Id_j 的询问. 最后, π 给出它猜测的 $\neg b \in \{0, 1\}$, 如果 $\neg b = b$, 则胜出.

π 从不对已猜测过的 Id 发起密钥生成询问的概率至少为 $1/n_1$, 同时 π 对已猜测过的 Id 发起密钥生成询问的概率也至少为 $1/n_1$. 如果 π 从不对 $l = \hat{e}(P, P)^{xyz}$ 发起 $H_2(U, l)$ 的询问, 因为 H_2, H_4 是随机预言机, 所以 π 无法获知 M . 在这种情形下, π 无法区分它是在模拟还是现实情形下, 所以没有优势. 因此, π 询问 $H_2(l)$ 的概率至少为 ϑ . 如果 π 发起 $H_2(U, l)$ 的询问, 倘若 B 从 H_2^{list} 中猜出正确的对应元素, 则胜出. 所以, 我们有 $\text{Adv}(B) \geq \vartheta/n_1^2 n_2$.

③ 向前向后保密性

性质 4 本加密方法提供了向前向后保密性.

证明:

如第 3 节所述, 每个节点通过本地的私钥和参数 Params 解密广播包, 如果节点未被添加入广播组, 则节点无法解密广播包内容. 当节点退出广播组后, 下次广播的时候节点 U_i 就不会被添加到广播包附带消息, 这样, 节点在本地无法生成最终的两次双线性运算的解密算法式, 从而保证了向后保密性. 当节点加入时, 同样类似, 之前的广播组中未添加新加入节点 U_j 值, 节点同样无法解密出消息内容, 从而保证了向前保密性.

4.3 性能分析

由于本文给出的基于 IBE 算法的 WSN 广播加密方法中与节点有关的仅有加密过程和解密过程, 且仅依赖于 IBE 算法中的 Encrypt 和 Decrypt 函数. 因此, 只需要分析这两个函数来研究我们提出的方法的安全性、复杂性及性能等.

(1) 算法复杂性

IBE 算法的核心是使用了超奇异椭圆曲线上的一个双线性映射, 双线性映射由椭圆曲线上的 Weil pairing 派生得到. $\hat{e}$ 可以表示成如下形式^[7]: $\hat{e}(P,$

$Q) = f_A(B)/f_B(A)$, $f_A(B)$ 与 $f_B(A)$ 具有相同的复杂度. 因此只要计算 $f_A(B)$ 的复杂度. 根据已有研究可知 $f_A(B)$ 的运算量是 $(4I + 25M)\log_2 r$, 其中 $0 < r < q$. 所以, 计算 $\hat{e}(P, Q)$ 的复杂度为 $2 \times (4I + 25M)\log_2 r$, 即为 $O(\log_2 q)$. 算法中应用到四个哈希函数, 使用的 Hash 是安全散列算法 (Secure Hash Algorithm), 算法的复杂性为 $O(n)$. 所以基于 IBE 算法的主要计算复杂性为 $O(n) + O(\log_2 q)$. 表 1 给出了本文算法的计算复杂度, N 为广播组节点数.

表 1 计算复杂性表

	IBESB 算法	
	加密过程	解密过程
$\hat{e}$ 运算	1	2
哈希运算	3	3
XOR 运算	1	1
乘法运算	$N + 1$	3
加法运算	$2N - 2$	$N - 1$

(2) 存储需求

在基于 IBE 的方法中, 每个无线节点仅需要存储公共参数 π 、自己的身份标识 Id 和自己的密钥 K_{Id} . 而且存储量与网络的规模无关, 并能保证与任何节点都有密钥对进行通信. 而不是以一种概率的形式保证节点之间的共享密钥对. 在这一点上, 也显示了基于 IBE 的密钥方法的优越性. 尽管基于 IBE 的加密方法也是非对称加密方法, 但它可以用椭圆曲线算法进行实现, 正是这一点, 使得它既具有了非对称密钥系统的灵活性, 又显示了与对称密钥系统相当的简单性.

5 结束语

本文是将非对称加密算法应用到 WSN 广播的一次探索, IBESB 充分考虑广播组的动态性, 网络中任意节点都可以成为广播源, 但只有添加到广播组中节点才能解密广播包, 同时通过有效的加密和认

证机制确保广播安全性. 已有的研究结果和我们的分析表明, 与目前的随机类型算法相比, 在内存需求、健壮性和安全性方面都有改进, 在计算复杂性方面也是可接受的. 因此, 下一步的工作将应用无线传感器网络测试平台 TinyOS 和 TingPK^[8], 对 IBESB 进行更深入的算法复杂性研究, 从理论和应用角度得到更详细的结果.

参考文献:

- [1] Akyildiz I F. Wireless sensor networks: a survey [J]. Computer Networks, 2002, 38(4):393-422.
- [2] Perrig A. SPINS: security protocols for sensor networks [J]. Wireless Networks, 2002, 8(7):521-534.
- [3] Shamir A. Identity - based cryptography and signature schemes [C]// Advances in Cryptology, CRYPTO' 84, Lecture Notes in Computer Science. Berlin: Springer - Verlag, 1985(196):47-53.
- [4] Wander A S. Energy analysis of public - key cryptography for wireless sensor networks[C]// Proceedings of the 3rd Int'l Conf. on Pervasive Computing and Communications. New York: IEEE Publishing, 2005:324-328.
- [5] Yang G, Wang J T. An identity - based encryption scheme for broadcasting[C]// IFIP International Conference on. New York, 2007(9):123-126.
- [6] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols[C]// Proceedings of the First Annual Conference on Computer and Communications Security. New York: ACM, 1993:62-73.
- [7] Wang L, Wu C K. Efficient identity - based multicast scheme from bilinear pairing[J]. Communications, 2005, 152(6):877-882.
- [8] Watro R. TinyPK: securing sensor networks with public key technology[C]// Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN'04. New York: ACM Press, 2004:59-64.

作者简介:

曹晓梅 女, (1974-), 博士, 副教授. 研究方向为网络信息安全.