无线传感器网络中的高效签名算法

贾晨军[1]，廖永建[2]，陈抗生[1]

(1. 浙江大学信息学院　杭州　310027；2. 电子科技大学计算机科学与工程学院　成都　610054)

【摘要】无线传感器网络节点的计算、存储和通信能力都十分有限，通常被认为不适合使用公钥密码学技术。然而，近年来的许多研究成果表明，一些经过优化的公钥算法是可以为无线传感器网络提供更加有力的安全保障的。该文基于身份的密码系统进一步简化了传统公钥系统，根据无线传感器网络自身的特点，对现有的基于身份的签名算法的安全模型进行改进，并在此基础上提出了新的签名算法，同时也给出了安全证明。现有算法的存储需求与被签名信息长度成正比，而新算法存储需求为常量，因此更加适合在无线传感器网络中的使用。

关　键　词　基于身份的签名；　公钥密码学；　安全；　标准模型；　无线传感器网络

中图分类号　TN918.91　　**文献标识码**　A　　doi:10.3969/j.issn.1001-0548.2009.04.015

Efficient Signature Algorithm in Wireless Sensor Network

JIA Chen-jun[1], LIAO Yong-jian[2], and CHEN Kang-sheng[1]

(1. College of Information Science and Engnieering, Zhejiang University　Hangzhou　310027;

2. School of Computer Sinence and Technology, University of Electronic Science and Techology of China　Chengdu　610054)

Abstract　The nodes of wireless sensor network are very limited in its processing power, storage capacity and communications capability, so it is usually to be considered unsuitable for the use of public key cryptography technology. However, in recent years many research results indicated that some optimized public-key algorithm can provide much more security for wireless sensor networks (WSN). The identity-based public system simplifies the certificates management which is cumbersome in certificate based public key system. According to the features of WSN, the security model of identity-based public-key system is modified. A new identity-based signature (IBS) system is presented and proved secure in the new security model without random oracle. Storage requirement in previous IBS systems is directly related to message length, but it is constant in our new system, so the new system is more suitable for wireless sensor networks.

Key words　IBS;　public key cryptography;　random oracle;　security;　standard mode;　WSN

无线传感器网络(WSN)是由一组传感器节点以自组织方式构成的无线网络，由于无线传感器网络开放的体系结构，使得任何潜在的对手都可以很容易地截取、窃听和伪造信息，因此安全性对无线传感器网络来说是很重要的问题。因为无线传感器网络节点的计算、存储和通信能力都十分有限，使得大多数传统的安全解决方案难以直接应用到无线传感器网络上，因此设计无线传感器网络的安全机制成为一项极富挑战性的工作。在所有的安全机制中，身份认证是首先要解决的问题，在确认通信双方的身份以后才能进行相关的信息交换，否则所有信息的保密性、不可否认性、完整性等安全需求都无从谈起。

在使用基于对称密钥的方案中，认证是通过双方共享(或者通过其他节点共享)的密钥来实现的，现有的基于对称密钥的方案有如下几种：预置全局密钥、预置所有共享密钥[1]基于KDC的方案、基于多项式的方案[2]、Eschenauer-Gligor基本方案[3]、q-composite方案[4]等。

虽然公钥系统解决了密钥分发的问题，但是与对称密钥系统相比，公钥系统的计算开销要大得多。文献[5]从软硬件的性能方面分析了在传感器网络中使用公钥系统的可行性，从而为在无线传感器网络中使用公钥算法开辟了道路。

文献[6]提出了基于身份的公钥体制的概念，它不再需要证书管理，极大地简化了安全通信的实现。文献[7-8]提出了第一个高效的基于身份的加密方案，给出了一个通用的签名方案，文献[9]在文献[7]

收稿日期：2008－04－07；修回日期：2009－02－10
基金项目：国家自然科学基金(60673075)
作者简介：贾晨军(1978－)，男，博士生，主要从事无线网络安全方面的研究.

的基础上提出了在随机预言机模型下被证明是安全的密钥协商和加密方案，但是并没有明确地提出签名方案，由于网络节点计算能力有限，文献[7]中的签名方案并不可行。单纯使用基于身份的加密方案，具有部分解决身份认证的功能，因为只有拥有与加密公钥对应的解密私钥的个体才能有效地解密信息。这在点对点的认证中是可行的，但是在一对多的认证中，如广播，如果使用上述方法，认证节点就需要计算并发送多个不同的加密认证数据。对于能量、计算能力、存储能力和通信能力都非常有限的无线传感器网络节点来说，是非常奢侈的。文献[10]提出了一个高效、安全的IBE方案，并在标准模型下给出了证明(文献[7]方案在随机预言机模型下被证明是安全的)。文献[11]采用了与文献[10]类似的技巧，给出了在标准模型下可证明安全的IBS方案，但是文献[11]与文献[10]共同的缺陷是公开参数非常大。在文献[11]的方案中公开参数包含了$n_{\mathrm{u}}+n_{\mathrm{m}}+5$个群元素，其中$n_{\mathrm{u}}$代表身份信息的比特串的长度，$n_{\mathrm{m}}$代表被签名消息的比特串的长度。虽然$n_{\mathrm{u}}$、$n_{\mathrm{m}}$也可以是散列函数的输出大小，但$n_{\mathrm{u}}$、$n_{\mathrm{m}}$必须至少等于160。而且，如果使用一个在$F_p^2$上的椭圆曲线，那么一个群元素至少是1 024 bit，才能达到与1 024 bit RSA相当的安全级别。因此，每个参与者必须存储至少325 kb的公开参数，这对于现在常见的无线传感器网络节点来说是不可能的。本文提出一签名算法，并且在标准模型下给出了安全性的证明。

1 预备知识

本文为了叙述方便，对一些符号进行约定：Z_q表示所有小于q的正整数组成的集合；Z_q^*表示模q的整数乘法群；$x\in_R Z_q^*$表示从Z_q^*中随机选取任意元素x；$\{0,1\}^*$表示任意长的字符串；$\{0,1\}^l$表示长度为l的字符串。

1.1 双线性函数

设G_1、G_2是两个p阶乘法群，p是大素数。双线性映射$e:G_1\times G_1\to G_2$满足以下条件：

(1) 双线性(bilinear)，对于任意的$P,Q,R\in G_1$，$e(P,QR)=e(P,Q)e(P,R)$，且$e(PQ,R)=e(P,R)e(Q,R)$。

(2) 非退化(non-degenerate)，e不能将$G_1\times G_1$中的所有元素都映射到G_2的单位元，即存在$P,Q\in G_1$，使得$e(P,Q)$不等于G_2的单位元。

(3) 可计算性(computable)，对任意的$P,Q\in G_1$，都存在一个高效的算法来计算$e(P,Q)$。

1.2 基于身份的签名方案的定义

基于身份的签名方案包含4个算法[11]：

系统密钥生成：生成系统参数和系统的主密钥。

用户密钥生成：根据用户身份信息，生成用户的私钥。

消息签名：使用用户的私钥对消息进行签名；

签名验证：使用系统参数与签名者的身份以及被签名消息，对签名信息进行验证。

1.3 复杂性假设

定义 1 q-SDH(strong diffie-hellman assumption)问题[12]：

给定$(g',g'^{\alpha},g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in G_2^2\times G_1^{q+1}$输出$(c,g^{1/(\alpha+c)})$是困难的，其中$c\in Z_p$。如果$P_{\mathrm{r}}[A(g',g'^{\alpha},g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})=(c,g^{1/(\alpha+c)})]\geqslant\varepsilon$，则算法$A$以$\varepsilon$的优势解决q-SDH问题，其中的概率依赖于随机选取$g'\in G_2,g\in G_1$，从Z_p中随机选取α以及A选择的随机比特。如果不存在如上算法A，则称q-SDH问题是困难的。

定义 2 q-BSDH(bilinear strong diffie-hellman assumption)问题：

给定$(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in G_1^{q+1}$输出$(c,e(g,g^{1/(\alpha+c)}))$是困难的，其中$c\in Z_p$。如果$P_{\mathrm{r}}[A(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})=(c,e(g,g^{1/(\alpha+c)}))]\geqslant\varepsilon$，则算法$A$以$\varepsilon$的优势解决q-BSDH问题，其中的概率依赖于随机选取$g\in G_1$，从Z_p中随机选取α以及A选择的随机比特。如果不存在如上算法A，则称q-BSDH问题是困难的。

1.4 NAPQ-ID-EU安全

在许多无线传感器网络中，公钥签名算法主要用来进行认证，使用基于身份的公钥算法，使得节点不需要存储大量的证书数据，这对于计算能力和存储能力都很有限的无线传感器网络节点来说是非常重要的。在密钥离线分配的无线传感器网络中，攻击者能获得的私钥，只有那些被俘获节点的私钥。在这种情况下，可以对传统的安全模型进行修改，在攻击者能力被减弱的同时，可以得到效率更高的签名算法。由于在密钥离线分配的无线传感器网络中，攻击者无法发出对任意ID的私钥申请，所以这种修改是安全的。而从文献[1-4,9,14]中可知，密钥离线分配无线传感器网络的应用是非常广泛的，因此，新方案的应用范围很大。

将新的安全定义为NAPQ-ID-EU安全(非适应性私钥请求的基于ID的存在不可伪造安全)，同时本文定义挑战者与攻击者之间的交互游戏为：

请求：攻击者将它要进行私钥请求的所有 $\mathrm{ID}\in\{\mathrm{ID}_n\}$ 提交给挑战者。

响应：挑战者在得到攻击者提交的所有ID以后，将系统参数交给攻击者，并且将私钥请求ID的私钥返回给攻击者。

伪造：攻击者提交一份明文 M，一个 $\mathrm{ID}_0\notin\{\mathrm{ID}_n\}$ 和一个签名 σ。

将上述攻击者定义为NAPQ-ID-EU攻击者。假设 Adv 为攻击者获胜的优势。

定义 3　对于一个基于身份的签名系统，假设所有的NAPQ-ID-EU攻击者，在q次私钥请求后，在 t 时间内最多以 ε 的优势 Adv 赢得上述游戏，则称该签名系统是 (t,q,ε) NAPQ-ID-EU 安全的，即 $\mathrm{Adv}<\varepsilon$。

2　基于身份的签名方案

假设 G_1、G_2 是两个阶为 p 的乘法循环群；p 为一个大素数；选取双线性函数 $e:G_1\times G_1\to G_2$；用户的身份信息 $\mathrm{ID}\in Z_p$；待签名消息 $M\in\{0,1\}^*$；H 为全域Hash函数，$H:\{0,1\}^*\to Z_p$；$\alpha\in_R Z_p$ 表示 α 从 Z_p 中随机选取的。

系统密钥生成：选择 $\alpha\in_R Z_p$，随机选择 G_1 的生成元 g，计算 $g_1=g^{\alpha}$，选取 $h\in_R G_1$。系统的公开参数是 $\{g,g_1,h\}$，系统的主密钥为 α。

用户密钥生成：$\mathrm{ID}_{\mathrm{usr}}$ 为用户usr的身份信息，选取 $r\in_R Z_p$，用户usr的私钥为：

$$d_{\mathrm{usr}}=h^{1/(\alpha-\mathrm{ID}_{\mathrm{usr}})}$$

消息签名：使用usr的私钥 d_{usr} 对消息 $M\in Z_p$ 签名，选择 $t\in_R Z_p$，计算签名：

$$\sigma=(h^{tH(M)+1/(\alpha-\mathrm{ID}_{\mathrm{usr}})},g^t,g_1^t)$$

签名验证：用 $\sigma=(C_1,C_2,C_3)$ 表示用 $\mathrm{ID}_{\mathrm{usr}}$ 对 M 的签名结果。可以用 $\mathrm{ID}_{\mathrm{usr}}$ 验证：

$$e(C_2,g_1)=e(g,C_3)$$

$$e(C_1,g_1g^{-\mathrm{ID}_{\mathrm{usr}}})=e(h^{H(M)},C_2^{-\mathrm{ID}_{\mathrm{usr}}}C_3)e(h,g)$$

本文方案正确性：

$$e(C_1,g_1g^{-\mathrm{ID}_{\mathrm{usr}}})=e(h^{tH(M)+1/(\alpha-\mathrm{ID}_{\mathrm{usr}})},g^{\alpha-\mathrm{ID}_{\mathrm{usr}}})=e(h^{H(M)},C_2^{-\mathrm{ID}_{\mathrm{usr}}}C_3)\ e(h,g)$$

3　安全性证明

下面证明方案的安全性。

定理 1　当 (t',ε) q′-BSDH假设成立时，签名方案是 (t,q,ε) NAPQ-ID-EU 安全的。其中 $t'=t-O(t_{\exp}q^2)$，而 $t_{\exp}$ 是在 G_1 上进行指数运算所需的最大时间。

证明：假设存在一个 (t,q,ε) 攻击者A，则可以构造一个模拟算法B，B可以利用A解决 (t',ε') q-BSDH 问题。为了表述方便，本文定义 $g_i=g^{\alpha^i}$，$g'_i=g'^{\alpha^i}$，$g_0=g$。

假设 B 收到一个 q′-BSDH 问题的实例，$(g,g_1,\cdots,g_{q'}),q=q'+1$，可按下面的方式来构造$B$：

请求：攻击者A提交一组 q_s 个互不相同的ID，$\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_{q_s}$，其中 $q_s\leqslant q$。由于攻击者需要事先提交请求，所以可假设A一共提交了 q 个请求，即 $q_s=q$。如果A提交的请求少于 q 个，可将 q 约减。

响应：B根据A所提交的请求来生成系统参数和 q 个ID的私钥。如果 $\alpha\in\mathrm{ID}_i,i\in q_s$，则$B$可以立即解决 q-BSDH 问题，否则定义多项式 $f(X)=\prod_{i=1}^{q}(X-\mathrm{ID}_i)$，将其展开可以得到 $f(X)=\sum_{i=0}^{q}a_iX^i$。$B$ 选取 $\theta\in_R Z_p^*$，并计算 $h\leftarrow\prod_{i=0}^{q}g_i^{a_i\theta}$，$B$将系统参数 (g,g_1,h) 发送给A。可知 $h=g^{\theta f(\alpha)}$。

接下来，B需要生成每个被请求的ID的私钥。定义多项式 $f_i(X)=f(X)/(X-\mathrm{ID}_i)=\prod_{j=0,j\neq i}^{q}(X-\mathrm{ID}_j)$，将其展开 $f_i(X)=\sum_{j=0}^{q-1}b_{ij}X^i$，并计算系数 b_{ij}。计算：

$$d_i\leftarrow\prod_{j=0}^{q-1}g_j^{b_{ij}\theta}$$

得 $d_i=g^{\theta f_i(\alpha)}=g^{\theta f(\alpha)/(\alpha-\mathrm{ID}_i)}=h^{1/(\alpha-\mathrm{ID}_i)}$，所以，$d_i$ 是一个合法的私钥。可以利用该私钥生成任意消息的合法签名。

伪造：攻击者伪造用户 $\mathrm{ID}_{\mathrm{usr}},\mathrm{ID}_{\mathrm{usr}}\notin\{\mathrm{ID}_i\}$ 对消息 M 的一个合法签名 $\sigma=(C_1,C_2,C_3)$，可知 $e(C_2,g_1)=e(g,C_3)$ 和 $e(C_1,g_1g^{-\mathrm{ID}_{\mathrm{usr}}})=e(h^{H(M)},C_2^{-\mathrm{ID}_{\mathrm{usr}}}C_3)\times e(h,g)$。

由于 $\mathrm{ID}_{\mathrm{usr}}\notin\{\mathrm{ID}_i\}$，所以 $f(\mathrm{ID}_{\mathrm{usr}})\neq 0$。令 $f'(X)=f(X)-f(\mathrm{ID}_{\mathrm{usr}})$，则有 $f'(\mathrm{ID}_{\mathrm{usr}})=0$。因此 $\mathrm{ID}_{\mathrm{usr}}$ 是 $f'(X)$ 的一个根，则 $F'(X)=f'(X)/(X-\mathrm{ID}_{\mathrm{usr}})$，可以表示为 $F'(X)=\sum_{i=0}^{q-1}c_iX^i$。

由计算 $l\leftarrow\prod_{i=0}^{q}g_i^{c_i\theta}$，可知 $l=g^{\theta F'(\alpha)}=$

$g^{\theta\frac{f(\alpha)-f(\mathrm{ID_{usr}})}{\alpha-\mathrm{ID_{usr}}}}$，因此 $e(g,l)=e(g,g)^{\theta\frac{f(\alpha)-f(\mathrm{ID_{usr}})}{\alpha-\mathrm{ID_{usr}}}}$。由 $g_1g^{-\mathrm{ID_{usr}}}=g^{\alpha-\mathrm{ID_{usr}}}$ 可知 $e(C_1,g)=e(C_1,g_1g^{-\mathrm{ID_{usr}}})^{1/(\alpha-\mathrm{ID_{usr}})}$。攻击者伪造的签名可以通过验证，即：$e(C_1,g_1g^{-\mathrm{ID_{usr}}})=e(h^{H(M)},C_2^{-\mathrm{ID_{usr}}}C_3)e(h,g)$，推出 $e(C_1,g)=\{e(h^{H(M)},C_2^{-\mathrm{ID_{usr}}}C_3)e(h,g)\}^{1/(\alpha-\mathrm{ID_{usr}})}$，又由 $e(C_2,g_1)=e(g,C_3)$，可知 $C_2^{\alpha}=C_3$。

所以，$e(C_1,g)=e(h^{H(M)},C_2)e(h,g)^{1/(\alpha-\mathrm{ID_{usr}})}$ $e(C_2^{-H(M)},h)e(C_1,g)=e(h,g)^{1/(\alpha-\mathrm{ID_{usr}})}$。代入 $h=g^{\theta f(\alpha)}$ 得到 $e(C_2^{-H(M)},h)e(C_1,g)=\ e(g,g)^{\theta f(\alpha)/(\alpha-\mathrm{ID_{usr}})}$。

所以，$e(g,l^{-1})e(C_2^{-H(M)},h)e(C_1,g)=e(g,g)^{\theta\frac{f(\mathrm{ID_{usr}})}{\alpha-\mathrm{ID_{usr}}}}$。

B 可以计算得出：$(e(g,l^{-1})\ e(C_2^{-H(M)},h)\times e(C_1,g))^{1/(\theta f(\mathrm{ID_{usr}}))}=e(g,g)^{1/(\alpha-\mathrm{ID_{usr}})}$。

时间复杂度：模拟器B的主要时间消耗是计算私钥 $d_i=\prod_{j=0}^{q-1}g_j^{b_{ij}\theta}=g^{\theta f_i(\alpha)}$ 和 $l=\prod_{i=0}^{q}g_i^{c_i\theta}=g^{\theta F'(\alpha)}$，其中 $f_i(\alpha)$ 与 $F'(\alpha)$ 都是 $q-1$ 阶的多项式。每个 $f_i(\alpha)$ 或 $F'(\alpha)$ 的计算都需要 $O(q)$ 指数运算，而攻击者最多进行 q 次私钥请求，所以 $t=t'+O(t_{\exp}q^2)$。

证毕

4 在无线传感器网络中的应用

4.1 本方案的应用

在上述基于身份的签名方案的基础上，可以设计一个于无线传感器网络中的高效、安全的密钥分配与签名方案。该方案主要应用在无基站的无线传感器网络中，主要分为离线密钥分配和在线签名两部分。

(1) 离线密钥分配

首先，按照签名方案中的系统密钥生成算法，生成系统参数和主密钥。系统密钥生成算法的输出是 $\{q,G_1,G_2,e,g,g_1,h,\alpha\}$，其中 q 为一个质数，而 G_1、G_2 为两个阶为 q 的群；$e:G_1\times G_1\to G_2$ 是一个双线性映射；$\alpha\in Z_p^*$ 为系统的主密钥；$g,h\in_R G_1, g_1=g^{\alpha}\in G_1$ 为系统的公开参数。

本文使用传感器节点的一个唯一标识作为它的身份信息，这个唯一标识可能是节点的一个唯一的名称，或者网络地址，或者硬件地址等，这个身份信息就是该节点的公钥。使用系统的公开参数和系统的主密钥，对每个节点的身份信息按照签名方案中的用户密钥生成算法计算出每个节点的私钥。

然后将系统的公开参数和每个节点的私钥都存储在对应的节点中，在无基站的无线传感器网络中这一过程可以在节点制造过程中完成。

(2) 在线签名

当无线传感器网络在布置完成以后，每个节点内都存储了系统参数和自己的私钥，两个或多个节点间需要进行身份认证时，发送方可以使用自己的私钥对事先约定的认证数据按照签名方案中的消息签名算法进行签名。接收方用发送方的身份信息作为公钥，按照签名方案中的签名验证算法，对接收到的信息进行验证，从而确定发送方的身份。

4.2 与其他方案的比较

(1) 与基于对称密钥的认证方式比较

对称密钥算法在无线传感器网络中应用非常广泛，文献[1-4]都是对称密钥算法的应用。使用对称密钥算法的过程中，为了保障两个对话节点间的信息安全，对不同的节点对之间要使用不同的密钥，否则所有与被俘获节点使用相同密钥的节点都不安全，如预置全局密钥方案。当节点数目众多时，文献[1]由于对存储的巨大需求而不可行。文献[3-4]部分地解决了上述问题，但是文献[2-4]中被俘获节点达到一定数量或比例时，整个网络都不再安全，文献[4]中，需要中间节点的辅助，一旦中间节点被俘获，攻击者就有可能利用该节点与其他节点的信任关系将其他非法节点加入信任关系中，在文献[4]中提出了额外的算法和策略来解决这种问题。

使用本文所述的签名方案，则不会出现上述问题，当某个节点被俘获后，攻击者最多只能获取到该节点的私钥，并不能伪装成其他节点来进行下一步行动。

(2) 与基于证书的方案比较

基于证书的公钥算法在无线传感器网络中作为认证手段的应用，解决了对称密钥算法中密钥存储量的问题和中间节点的问题，但是也带来了新的问题，就是证书的存储和交换问题。证书确保了节点的身份，但是由于每个节点都有自己的证书，所以在节点间第一次会话时必须要传送证书信息，对于计算存储能力以及能量都非常有限的无线传感器网络节点来说，这是非常奢侈的。文献[13]利用部署的先验知识来解决上述问题，在存储量和能量消耗间取得了折中，在无法预知部署位置的应用中该方案就无法奏效。

基于身份的公钥算法有效地解决了上述问题，由于节点的公钥就是节点的身份信息本身，所以就不存在公钥与身份信息的绑定问题，因此不需要证书。而基于身份的公钥算法又具有与基于证书的公

钥算法相同的优点，因此，基于身份的方案比基于证书的方案更适用于无线传感器网络。

(3) 与现有方案的比较

文献[9]根据文献[7]提出了无线传感器网络中的密钥协商和加密方案。虽然文献[7]中也提出了签名方案，但是方案对节点的计算能力需求很大，不适合在无线传感器网络中的应用，如果使用加密方案来解决认证问题，在广播的情况下，会极大地增加发送节点的能耗。而文献[11]给出了无需随机预言机的标准模型下安全的签名方案，但是该方案对存储需求非常大，其公开参数包含了 $n_u + n_m + 5$ 个群元素。本文提出的方案中，系统参数只有3个群元素，并且在标准模型下给出了安全性证明。

5 总 结

无线传感器网络在现实生活中有着广泛的应用，由于其节点的处理能力、存储能力和通信能力等都十分有限，使得设计无线传感器网络的安全方案成为一项极富挑战性的工作。基于身份的签名方案既解决了对称加密算法的认证方案中的密钥存储问题和中间人攻击问题，也避免了基于证书的方案中证书的存储和交换问题。与现有方案相比，本文方案无需使用随机预言机模型，所需存储的参数也比现有文献[11]少，并且给出了标准模型下的安全性证明。所以本文提出的适用于无线传感器网络中的基于身份的签名算法是安全的、高效的。

参 考 文 献

[1] LAI B, KIM S, VERBAUWHEDE I. Scalable session key construction protocol for wireless sensor networks[C]// IEEE Workshop on Large Scale Real-Time and Embedded Systems (LARTES). Austin: IEEE Computer Society, 2002.

[2] BLOM R. An optimal class of symmetric key generation systems[C]//EUROCRYPT. Berlin: Springer-Verlag, 1984: 335-338.

[3] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//ACM Conference on Computer and Communications Security. New York: ACM, 2002: 41-47.

[4] CHAN H, PERRIG A, SONG D X. Random key predistribution schemes for sensor networks[C]//IEEE Symposium on Security and Privacy. Washington: IEEE Computer Society, 2003: 197-197.

[5] ROMAN R, ALCARAZ C. Applicability of public key infrastructures in wireless sensor networks[M/CD]. (2007-08-14)http:// www. springerlink. com/home/main.mpx..

[6] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//CRYPTO. Berlin: Springer-Verlag, 1984: 47-53.

[7] BONEH D, FRANKLIN M K. Identity-based encryption from the weil pairing[C]// CRYPTO. Berlin: Springer-Verlag, 2001: 213-229.

[8] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles [C]// EUROCRYPT. Berlin: Springer-Verlag, 2004, 223-238.

[9] GENG Y, Chun-ming R, CHRISTIAN V, et al. Identity-based key agreement and encryption for wireless sensor networks[J]. Journal of China Universities of Posts and Telecommunications, 2006, 13(4): 54-60.

[10] WATERS B. Effcient identity-based encryption without random oracles[C]//EUROCRYPT. Berlin: Springer, 2005: 114-127.

[11] PATERSON K G, SCHULDT J C N. Effcient identity-based signatures secure in the standard model[C]//ACISP. Berlin: Springer, 2006: 207-222.

[12] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups[J]. Journal of Cryptology. Berlin: Springer-Verlag, 2008, 21(2): 149-177.

[13] DU W, WANG R, NING P. An effcient scheme for authenticating public keys in sensor networks[C]// International Symposium on Mobile Ad Hoc Networking & Computing. Urbana-Champaign.New York: ACM, 2005: 58-67.

编 辑 张 俊