基于模糊属性的广播签名算法

朱 莉,杨 庚,陈 伟
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:基于双线性映射与多序列DHE假设,提出了一种基于模糊属性的广播签名算法。在基于模糊属性的签名方案中,对消息签名的属性集 S 与验证此签名的属性集 W 必须满足条件 $|S \cap W| \geqslant t$,t 是门限值,在过去的签名方案中,t 的值是预先设定不变的;而在文中提出的算法中,门限 t 值可以根据不同的需要而动态地设定。在计算量方面,设每组最多有 m 个用户,则验证签名所要计算的双线性对为 $m+1$ 个,降低了对用户计算能力的要求。此外本算法可以实现固定大小的密钥及密文,这有利于提高安全传输的性能。

关键词:双线性映射;多序列DHE假设;模糊属性;广播签名;门限
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)11-0123-05

Fuzzy Identity-Based Broadcast Signature Algorithm

ZHU Li, YANG Geng, CHEN Wei
(College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: Proposes a novel efficient broadcast signature algorithm according to fuzzy identities, based on the bilinear maps and multi-sequence of Diffie-Hellman exponents assumption. The fuzzy identity-based signatures, which allow a user with the private key for identity W to verify a message signature signed for identity S if and only if W and S are within a certain distance judged by threshold t. In the former signature schemes, the threshold t is static, but in the algorithm this paper puts forward, the threshold t is dynamic according to different demands. Besides, this algorithm can get constant keys and the ciphertext, which is in favor of promoting the performance of transmission.

Key words: bilinear maps; MS-DHE assumption; fuzzy identity; broadcast signature; threshold

0 引 言

随着计算机及网络通信技术的快速发展,数字签名技术扮演着越来越重要的角色。数字签名是电子和数字化环境下对传统手写签名的模拟,用以实现传统手写签名的功能。数字签名所具有的不可伪造性,可以用于消息来源的认证,消息完整性检测,防止对发送过的消息进行的抵赖等应用需求。因此,数字签名技术以其能提供认证、完整性和不可否认性而成为信息安全的关键技术之一。文中基于双线性映射与多序列DHE(Multi-Sequence of Diffie-Hellman Exponents Assumption)假设[1]提出了一种基于模糊属性的广播签名算法(FI-BSA: Fuzzy Identity-based broadcast signature algorithm)。

对数字签名的研究是与对公钥密码的研究同时开始的。1976年Diffie和Hellman不仅提出了公钥加密的思想,同时也提出了数字签名的思想。1978年Rivest, Shamir和Adleman基于大素数分解困难性给出了著名的RSA签名方案。在此后的二十几年中,新的数字签名方案如雨后春笋般涌现。

Sahai和Waters于2005年,在身份认证的基础上提出了模糊属性的概念。基于身份的概念最早由Shamir于1984年提出。这种算法的基本思想是公钥可以是任何唯一的字符串,如E-mail地址、身份证或其他标识。其优点是公钥可识别,通常不需要PKI系统的证书发放。尽管在Shamir之后人们也提出了多种实现技术,但直到2001年Boneh和Franklin才给出了以椭圆曲线实现该算法,其计算量远远小于传统的公钥密码体系。此后,以此为基础,根据需要提出了多种不同的签名方案[2~5]。而在模糊身份(基于属性)认证方式中,代表用户身份的不再是任意的字符串,而是

收稿日期:2009-03-05;**修回日期**:2009-06-21
基金项目:国家自然科学基金(60873231);江苏省高校自然科学基金(08KJB520006);江苏省"六大人才高峰"基金(06-E-044)
作者简介:朱 莉(1984-),女,硕士研究生,研究方向为计算机通信与网络、信息安全;杨 庚,教授,博士生导师,加拿大Laval大学博士,Monteral大学博士后,研究方向为计算机通信与网络、网络安全、分布与并行计算等。

由一个集合,其中集合中的每个元素都是描述用户身份的字符串。这种签名体制的一个重要的优点是容错性好,支持生物识别技术。在这种认证方式中,签名者所进行签名的私钥与代表其身份的一组属性相联系,而验证其签名的密钥与另一组属性 w' 相联系,而只有 w 和 w' 在设定的相似度之内才可以被认证。对基于属性的签名方式的研究已引起人们的高度重视[6~8]。

但是,由于广播签名的特殊性,其签名密钥必须与一组验证私钥相联系,因此其签名密钥往往比较复杂,而其签名密文也因为要包含接收者的相关信息,导致密文长度较长,这同时增加了传输过程中的不安全因素。例如以往基于属性的签名认证,其签名、验证密钥及密文长度都是线性增长的;且算法在签名验证时计算量大,对验证用户的计算能力及存储能力要求高;在实现用户成员的动态管理上非常复杂。而文中的基于模糊属性的动态门限签名算法,其思想来源于文献[1]。此 FIBSA 签名算法包括了基于属性的签名及门限签名的思想,与以往的基于属性的签名算法相比,可以实现固定大小的密文,且发送者可以动态地确定接收者的属性集合;与传统的门限概念相比,其门限值不是事先设定的,而是根据签名消息的重要性来设定;此外,本算法可以便捷地实现用户的动态加入。

1 预备知识

文中所提出的算法主要基于双线性对及 MS-DHE 的假设问题,而 MS-DHE 假设保证了此算法的安全性,即不可抵赖性、不可伪造性。

1.1 双线性映射

设 G_1, G_2 为阶数同为 P 的加法循环群,G_T 是阶数为 P 的乘法循环群。双线性映射对

$e: G_1 \times G_2 \to G_T$ 满足以下特性:

(1) 双映射性(bilinear maping):对于任意的 $G \in G_1, H \in G_2$ 及 $a, b \in Z_p$,有 $e(aG, bH) = e(G, H)^{ab}$;

(2) 非退化性(non-degenerate):g, h 分别为 G_1, G_2 的生成元,有 $e(g, h) \neq 1$;

(3) 可计算性(computability):存在有效的算法可以计算出 $e(G, H)$,其中 $G \in G_1, H \in G_2$。

记双线性映射系统为元组:

$S = (p, G_1, G_2, G_T, e(.\ ,\ .))$

在密码学中有三种类型的双线性映射:

i) 对称双线性映射:$G_1 = G_2$ 或者二者之间存在同构,逆也是可以计算的,即 $\Psi: G_2 \to G_1$。

ii) 非对称双线性映射:存在同构算法 $\Psi: G_2 \to G_1$,但它逆的计算是困难的。

iii) 不相关的双线性映射:G_1, G_2 之间不存在有效的同构关系。

1.2 MS-DHE 假设的几个有关定义

Diffie-Hellman Exponent 假设[9]是 2005 年由 Boneh, Boyen 和 Coh 共同提出的。虽然它仅适用于对称和非对称又线性映射,但可很容易地把它扩展到第三种更为一般的情况。下面对 DHE 假设简单介绍:

设 $S = (p, G_1, G_2, G_T, e(.\ ,\ .))$ 为对称双线性映射系统,$G_1 = G_2 = G$。令 g_0 为 G 的生成元,$g_0 \in G$,$g = e(g_0, g_0) \in G_T$。随机选取两个正整数 l, m 和两个 l 元组 P, Q,每个元组中的任意一个元素都是一个 F_p 中的 m 维向量,即 $P, Q \in F_p[X_1, X_2, \cdots, X_m]^m$。在此记为 $P = (p_1, p_2, \cdots, p_l)$ 和 $Q = (q_1, q_2, \cdots, q_l)$。

函数 $h: F_p \to \Omega^s$ 和向量 $(x_1, \cdots, x_m) \in F_p^m$,记

$h(P(x_1, \cdots, x_m)) = (h(p_1(x_1, \cdots, x_m)), \cdots, h(p_l(x_1, \cdots, x_m)))$。

以下定义一种线性组合为 F:

$$F = \sum_{1 \leqslant i,j \leqslant l} a_{i,j} p_i p_j + \sum_{1 \leqslant i \leqslant l} b_i q_i$$

其中 $a_{i,j}, b_i \in Z_p$。则 F 依赖于 (P, Q)。

下面给出几个定义。定义如下:

定义 1[9] (P, Q, F) - GDHE(General DHE) 问题。给定向量 $H(x_1, \cdots, x_m) = ([P(x_1, \cdots, x_m)]G_0, g^{Q(x_1, \cdots, x_m)}) \in G^l \times G_T^l$,计算 $g^{F(x_1, \cdots, x_m)}$。

定义 2[9] $((P, Q, F)$ - GDHE) 的判定问题即 $((P, Q, F)$ - GDDHE(General Decision DHE))。给出 $H(x_1, \cdots, x_m) \in G^l \times G_T^l$,对于任意的 $T \in G_T$,判定 T 是否等于 $g^{F(x_1, \cdots, x_m)}$。

$((P, Q, F)$ - GDHE) 及 $((P, Q, F)$ - GDDHE) 问题的安全性证明见文献[1]和[9]。

定义 3[1] $((l, m, t)$ - MS-DHE) 的判定问题。即 $((l, m, t)$ - MS-DDHE)。给定正整数 l, m, t,$S = (p, G_1, G_2, G_T, e(.\ ,\ .))$ 及 $g_0 \in G_1, h_0 \in G_2$。任意选择两个素质的多项式 f、g,其阶分别为 l, m,每个多项式具有不相同的根,分别为 $x_1, \cdots, x_l$,和 $y_1, \cdots, y_m$,几个指数序列分别为:

$$x_1, \cdots, x_l, y_1, \cdots, y_m, g_0, g_0^{\gamma}, \cdots, g_0^{f^{t+2}}, g_0^{k \cdot \gamma \cdot f(\gamma)},$$

$$g_0, g_0^{a \cdot \gamma}, \cdots, g_0^{a \cdot \gamma^{2t+1}}, h_0, h_0^{\gamma}, \cdots, h_0^{\gamma^{m-2}}$$

$$h_0^{a}, h_0^{a \cdot \gamma}, \cdots, h_0^{a \cdot \gamma^{2m-1}}$$

且给定 $T \in G_T$,判定 T 是否等于 $e(g_0, h_0)^{k \cdot f(\gamma)}$。

定理 1[1](安全性) 任意的随机算法 A,它对 G_1, G_2, G_T 和双线性系统 $e(.\ ,\ .)$ 访问的次数一共为 q_G 次,则

$$\mathrm{Adv}^{\mathrm{ms\text{-}ddhe}}(l,m,t)\leqslant\frac{(q_G+4(l+t)+6m+4)^2+d}{2p}$$

其中,$d=4(l+t)+6m+2$。

2 FIBSA

FIBSA作为一种广播签名算法,利用基于身份验证的思想,即广播发送者将要广播的数据发送给特殊身份标识的用户。每个用户的身份标识都是一组属性集 w,设广播发送者发送的数据签名所用的身份标识为属性集为 w',且设门限为 t,即当且仅当验证的属性集 S 与签名所用的属性集S的交集的大小至少为t时,才能正确地对消息进行验证。在此过程中,与以往不同的是,门限 t 的设定不是预先设定不变的,而是根据具体消息的重要程度来适当选择。且此签名所生成的密文大小固定,较之以前的算法,减少了密文在传输过程中的不安全因素。下面将介绍 FIBSA 算法的各个步骤,并定义该算法符合的安全模型。

2.1 FIBSA 算法

FIBSA广播签名算法主要包括五个主要过程,分别是系统初始化、私钥的提取过程、对消息进行签名、用户对报文的可用性进行验证和用户验证签名的过程。其描述如下:

(1)初始化 Setup(λ) 过程:输入安全参数 λ,生成系统参数 Param = (MK,PK,VK),其中 MK 为主密钥,只为广播发送者拥有,对其他任何用户均是不可见的,它主要负责用户成员的动态加入,及用户验证私钥的提取。而 PK 和 VK 均为公共密钥,对所有用户均可见。PK 主要用在广播发送者对所发送的消息进行签名及接收用户对消息的可用性进行判断的过程中,VK 是消息的接收者利用它来验证消息的真伪。

(2) 私钥的提取 KeyExtract(MK):这个过程同时也是用户的加入过程,任意加入的用户所拥有的属性集合为 W,广播发送者为其生成验证所需要的私钥。设任一属性 $i\in W$,则广播发送者任意选择 $x\in Z_p^*$,则该属性的公钥为 $apk=x$,私钥为 $ask=g^{\frac{1}{\gamma+x}}$。

(3) 对消息签名 Sign(PK,M,S,t):广播发送者利用公共密钥 PK 对消息M 进行签名,在这个过程中输入还包括签名所用的属性集(或者是所所用到的属性的公钥集合)及验证门限 t。输出密文 $C=(Hdr,S,t)$,其中 $Hdr=(C_1,C_2,\sigma)$,含有对信息 M 所生成的签名信息。

(4) 验证消息的可用性 Validate(PK,C):用户接收到消息后,不是立即进行签名的验证,而是首先验证该消息是否可用。用户根据双线性对的有关性质,对消息进行判断,如果结果为真,则继续进行签名的验证,否则丢弃该消息。

(5) 验证签名 Verify(VK,C,M):首先,用户选择验证签名所需的属性集合 $|T|=t=|W\cap S|$,利用属性集合中每一个属性的私钥对签名进行验证,如果结果为真,则接收该消息,否则丢弃。

2.2 安全模型

此 FIBSA 算法所满足的安全模型的定义如下,其详细证明请见第四部分。

(1)正确性:FIBSA 签名算法的正确性即合法用户能够正确地验证由广播者发送的合法信息。

(2)不可抵赖性:FIBSA 签名算法由广播者签名发送的合法信息,且合法用户验证通过,发送者无法否认信息是由自己签名发送的。

(3)不可伪造性:FIBSA 签名算法的不可伪造性即指广播者所签名的信息不能由任意第三方在验证者无法识别的情况下重新签名。

不可伪造性这一安全性要求,可以用以下的这个对弈来模拟其过程。对弈中有攻击者 A 和防御者 C 两个主要角色。具体过程如下:

a. 初始化 Setup(λ):由防御者 C 运行此算法的初始化过程,C 接受一个整数λ 为安全参数,生成管理主密钥 MK,和签名密钥 PK 及验证密钥 VK,并且将 PK、VK 发送给攻击者 A。

b. 阶段 1:攻击者 A 运行私钥提取算法 KeyExtract(MK) 生成广播域中的用户,设用户为 U,属性集合为 W,攻击者 A 为W 中的任意一个属性生成相关的密钥。

c. 伪造签名:防御者 C 声明其签名用的属性集合为S^*,并设验证门限为 t^*。C 随机地选择$b\leftarrow\{0,1\}$ 并且计算出签名 $(\sigma_0,Hdr^*)=\mathrm{Sign}(PK,S^*,t^*,M)$,然后 C 在签名所在的域中随机地选择σ_1,防御者 C 将 (σ_b,Hdr^*) 发送给攻击者 A。

在此过程中有一个限制条件,签名属性集合 S^*,最多只能包含攻击者生成的用户 U 的属性集合 W 中的t^*-1 个属性,即 $|S^*\cap W|\leqslant t^*-1$。

d. 阶段 2:攻击者 A 运行阶段 1 和算法 Verify(VK),且用户 U 的属性集W 与S^* 最多有 t^*-1 个相同的属性。攻击者 A 猜测出b',并将 b' 发送给 C。

e. 防御者 C 判断$b'=b$ 是否成立。

如果 $b'=b$,则可以认为攻击者赢得了这场对弈。记攻击者获胜的概率为

$$Pr_A^{UF}(\lambda)=|Pr[b'=b]-\frac{1}{2}|=$$

$$|Pr[b'=1\mid b=1]-Pr[b'=1\mid b=0]$$

3 算法的详细描述

以模糊身份认证为基础，利用双线性对及 GDHE 假设，提出了 FIBSA 广播签名算法，此算法所得出的签名密文不随属性的增加而迅速增长，使得在特殊的传输环境下数据传输的安全性提高。与之前基于模糊身份认证算法一个明显的区别在于，门限不是固定不变的，而是在消息发送时由发送者根据具体情况设定的，这为处理不同安全级别的消息提供了极大的灵活性。由下面的过程可见，此算法的另一显著特征为步骤 4，验证消息的可用性，这不仅增加了算法的健壮性，也将某些非法签名提前过滤掉，节省了系统资源。

3.1 初始化 Setup(λ)过程

输入一个随机整数 λ 为安全参数，广播发送者首先构造一个椭圆曲线上的双线性映射系统：$S=(P,G,G_1,G_2,G_T,e(.,.))$，其中 G_1,G_2,G_T 的阶均为 P，且 $|P|=\lambda$。群 G_1,G_2 的生成元为 $g\in G_1,h\in G_2$。在域中 Z_p^* 随机选择 γ,α，且令集合 $D=\{d_i\}_{i=1}^{m-1},d_i\in Z_p$，其中 m 为整数，是验证签名时所需要属性的最大数目。最后自 Z_p^* 中随机选择一组随机数列 $\{t_i\}_{i=1}^n$。

由此广播者给出主密钥为 $MK=(g,\gamma,\alpha)$，签名密钥为 $PK=(m,u,v,h^\alpha,\{h^{\alpha\cdot\gamma^i}\}_{i=1}^{2m-1},D)$ 以及验证密钥 $VK=(m,h,\{h^{\gamma^i}\}_{i=1}^{m-2},D)$，其中 $u=g^{\gamma\cdot\alpha},v=e(g,h)^\alpha$。

3.2 私钥提取 KeyExtract(MK)过程

对于任意一个用户，设其属性集为 w，属性 $\forall i\in w$ 广播发送者为其生成公钥 $apk=x\in Z_p^*$（x 是在域 Z_p^* 中未被选择的值中随机选择的），而此属性的相关私钥为 $ask=g^{\frac{1}{\gamma+x}}$。属性的公钥会在对消息生成签名时，用作标识验证所需要的属性，而其私钥则用在对消息签名进行验证的过程中。

3.3 对消息签名 Sign(PK,S,t,M)过程

设消息 M 为 n 位的有序序列，即 $M=(u_1u_2\cdots u_n)\in\{0,1\}^n$。利用系统参数 PK，给定此消息所需要的属性集合 $S=(apk=x_1,\cdots,x_s)$ 及门限值 $t,t\leqslant s=|S|\leqslant m$，Sign 算法随机选择 $k\in Z_p^*$，并且计算出 $Hdr=(C_1,C_2,\sigma)$，令

$$p=t_0\prod_{i=1}^{n}t_i^{u_i},\text{则}$$

$$C_1=u^{-k},$$

$$C_2=h^{k\cdot\alpha\cdot\prod_{x\in S}(r+x_i)\cdot\prod_{x\in D_{m+t-s-1}}(r+x)},\sigma=v^{kp}$$

将含有签名的密文 $C=(Hdr,S,t)$ 广播给接收者。

3.4 验证消息的可用性 Validate(PK,C)过程

接收者接收到含有签名的密文 C 后，利用系统公钥 PK，经过简单的计算可以检测此密文是否可用，其计算过程如下：

令 $C'_1=u^{-1},C'_2=h^{\alpha\cdot\prod_{x\in SUD_{m+t-s-1}}(\gamma+x)}$

计算 $e(C_1,C'_2)=e(C'_1,C_2)$ 是否成立。

如果此等式成立，则继续后面的步骤，否则丢弃该数据包。

3.5 用户验证签名 Verify(CK,C,M)过程

接收用户接收到并验证含有签名的密文 C，设此用户所拥有的属性集合为 W，则当且仅当 $|W\cap S|\geqslant t$ 时，才可以验证此签名。任取集合 $T\in|W\cap S|$ 且 $|T|=t$。

利用各个属性的私钥计算出：

$$L=e(g,C_2)^{\frac{1}{(\gamma+x_1)(\gamma+x_2)\cdots(\gamma+x_t)}}\in G_T$$

在此过程中，需要利用算法 Aggregate[10]，下面将简单介绍如何得出需要的值 L。

已知 $x_1,x_2,\cdots,x_t$ 和 $\sigma_i=e(g,C_2)^{\frac{1}{\gamma+x_i}},1\leqslant i\leqslant t$，及任意 (j,β)

则

$$L_{j,\beta}=\sigma_\beta^{\frac{1}{(\gamma+x_1)\cdots(\gamma+x_j)}}=e(g,C_2)^{\frac{1}{\gamma+x_\beta}\cdot\frac{1}{(\gamma+x_1)\cdots(\gamma+x_j)}}$$

Aggregate 算法包含计算：

$$L_{j,\beta},j=1,2,\cdots,t-1,\beta=j+1,\cdots,t$$

$$L_{j,\beta}=\left(\frac{L_{j-1,j}}{L_{j-1,\beta}}\right)^{\frac{1}{x_\beta-x_j}}$$

则 $L_t=L_{t-1,t}=e(g,C_2)^{\frac{1}{(r+x_1)(r+x_2)\cdots(r+x_t)}}$

已知 $M=(u_1u_2\cdots u_n)\in\{0,1\}^n$，可得

$$p'=t_0\prod_{i=1}^{n}t_i^{u_i'}$$

另 $\sigma'=(L\cdot e(C_1,h^{P_{(T,S)}(\gamma)}))^{c(T,S)^{-1}}$

其中 $P_{(T,S)}(\gamma)$ 为一个 $m-2$ 多项式，

$$P_{(T,S)}(\gamma)=\frac{1}{\gamma}\cdot\left(\prod_{x\in SUD_{m+t-s-1}-T}(\gamma+x)-C(T,S)\right)$$

$$C(T,S)=\prod_{x\in SUD_{m+t-s-1}-T}x$$

验证 $\sigma'^{P'}=\sigma$ 是否成立。

4 FIBSA 算法的有效性分析

基于模糊属性的签名中，当且仅当签名属性集 S 与验证此签名的属性集合 W 的交集至少含有 t 个属性时，才能正确验证消息的签名。而此处 t 值的设定，在以往的签名方案中，是固定不变的，而在文中提出的 FIBSA 签名算法中，可以根据消息重要性的不同而设定门限 t 的值。此外，文中的签名方案，可以实现固定大小的密钥及密文，这提高了在传输过程中的安全性，特别是在无线传感器等环境下，这种特征更为重要。而

计算量较文献[2]也有改进。其中算法[6,7]所提出的算法基于属性的签名,设每个用户所拥有的属性数量为 U,则其签名密钥和验证密钥的长度均与属性数量成正比,其计算量同样比较复杂,一般要计算一组属性大小的双线性对;设文献[2]中,每个用户用来标识身份的属性个数依然为 m,则在验证签名算法中,需要计算的双线性对为 $3m$,而在 FIBSA 中仅仅需要计算 $m+1$ 次。它们之间的详细差别请见表 1。

表 1　FIBSA 算法与文献[2,6,7]算法的比较

算法	密钥/密文长度			计算复杂度		动态
	λsk	λtk	λc	签名	验证/双线性对	门限
文献[6]	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	$O(\max(l,t))$	L	否
文献[7]	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	3	$O(\lvert u\rvert)$	否
文献[2]	$k\cdot\lvert m\rvert$	无	$k\cdot\lvert m\rvert$	$O(m)$	$3m$	否
FIBSA	constant	constant	constant	$O(m)$	$m+1$	是

5　结束语

FIBSA 签名算法由于其签名密文是固定大小的,且计算量也比较小,因此对资源的要求不高,可以用于资源受限的网络,如 Ad-hoc,WSNs 中。下一步的工作将进一步降低在验证签名时算法的复杂性。

参考文献:

[1] Delerabl'ee C', Pointcheval D. Dynamic Threshold Public-Key Encryption[C]//Wagner D. Advances in Cryptology-Proceedings of CRYPTO2008. Santa Barbara, California, USA: Springer-Verlag, 2008: 317-334.

[2] Yang Piyi, Gao Zhenfu, Dong Xiaolei. Fuzzy identity based signature. Cryptology ePrint Archive: Report 2008/002[EB/OL]. 2008. http://eprint.iacr.org/2008/002.pdf.

[3] ZHU ZhenChao, ZHANG Yuqing, WANG Fengjiao. An Efficient Identity-based Ring Signcryption Scheme. Cryptology ePrint Archive: Report 2008/254[EB/OL]. 2008. http://eprint.iacr.org/2008/254.pdf.

[4] Selvi S S D, Vivek S S, Karuturi N N. Cryptanalysis of Bohio et al.'s ID-Based Broadcast Signcryption (IBBSC) cheme for Wireless Ad-hoc Networks. Cryptology ePrint Archive: Report 2008/247[EB/OL]. 2008. http://eprint.iacr.org/2008/247.pdf.

[5] Sun Xun, Li Jian-hua, Chen Gong-liang, et al. Identity-Based Directed Signature Scheme from bilinear maps. Cryptology ePrint Archive: Report 2008/305[EB/OL]. 2008. http://eprint.iacr.org/2008/305.pdf.

[6] Li Jin, Kim Kwangjo. Attribute-Based Ring Signatures. Cryptology ePrint Archive: Report 2008/394[EB/OL]. 2008. http://eprint.iacr.org/2008/305.pdf.

[7] Maji H, Prabhakaran M, Rosulek M. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance. Cryptology ePrint Archive: Report 2008/328[EB/OL]. 2008. http://eprint.iacr.org/2008/328.pdf.

[8] Khader D. Attribute Based Group Signatures. Cryptology ePrint Archive: Report 2007/159[EB/OL]. 2007. http://eprint.iacr.org/2007/159.pdf.

[9] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext[C]//In Cramer R. EUROCRYPT 2005. Berlin, Germany: Springer-Verlag, 2005: 440-456.

[10] Delerabl'ee C', Paillier P, Pointcheval D. Fully collusion Secure Dynamic Broadcast Encryption with Constan-size Ciphertexts or Decryption Keys[C]//Takagi T, Okamoto T, Okamoto E, et al. Proceedings of the first International Conference on Pairing-based Cryptography (2007). [s. l.]: Springer-Verlag, 2007: 39-59.

(上接第 118 页)

频率、数据传输阶段时间长度等,需要进一步定量分析,今后需要在这方面继续研究。

参考文献:

[1] 任丰原,黄海宁,林　闯. 无线传感器网络[J]. 软件学报, 2003,14(7):1282-1291.

[2] 崔　莉,苗　勇,赵　泽,等. 无线传感器网络研究进展[J]. 计算机研究与发展,2005,42(1):163-174.

[3] 杨菊英,吕光宏. 无线传感器网络分层路由协议研究[J]. 计算机技术与发展,2008,18(6):115-118.

[4] Akkaya K, Younis M. A Survey of Routing Protocols in Wireless Sensor Networks[J]. Ad Hoc Networks, 2005, 3(3): 325-349.

[5] Heinzelman W B, Chandraskan A P, Blakrisshnan H. An Application Specific Protocol Architecture for Wireless Microsensor Networks[J]. IEEE Trans. on Wireless Communications, 2002, 1(4): 660-670.

[6] Lindsey S, Raghavendra C S, Sivalingam K M. Data Gathering Algorithms in Sensor Networks Using Energy Metrics[J]. IEEE Transactions on Parallel and Distributed Systems, 2002, 13(9): 924-935.

[7] Chen Jing, Yu Fengqi. An Uniformly Distributed Adaptive Clustering Hierarchy Routing Protocol[C]//In Proceedings of the 2007 IEEE International Conference on Integration Technology. Shenzhen: [s. n.], 2007: 628-632.

[8] 王　娟,王汝传,孙力娟. 数据融合在传感器网络协议中的节能性分析[J]. 计算机技术与发展,2006,16(11):4-6.