文章编号:1001 - 9081(2009)09 - 2351 - 04

安全有效的无线传感器网络匿名通信方案

章志明[1],邓建刚[3],邹成武[2],余 敏[2]
(1. 江西师范大学 软件学院,南昌 330022; 2. 江西师范大学 计算机信息工程学院,南昌 330022;
3. 江西师范大学 科技处,南昌 330022)
(zzm_9650@163.com)

摘 要:随着无线传感器网络(WSN)的广泛应用,在某些场合不仅需要保证传送信息的安全性,还需要保证节点在传送信息过程中的匿名性和私有性,如何设计出安全有效的无线传感器网络匿名通信协议已成为当前研究的热点。使用双线性函数的双线性对,哈希函数和异或运算提出了一种可验证安全的无线传感器网络匿名通信方案,方案不仅能满足匿名通信的基本要求,而且大大提高系统的计算复杂度和存储复杂度,更适合无线传感器网络。

关键词:无线传感器网络;匿名通信;节点身份;双线性对
中图分类号: TP393 **文献标志码**:A

Secure and effective anonymous communication scheme for wireless sensor network

ZHANG Zhi-ming[1], DENG Jian-gang[3], ZOU Cheng-wu[2], YU min[2]
(1. *School of software, Jiangxi Normal University, Nanchang Jiangxi* 330022, *China*;
2. *School of Computer and Information Engineering, Jiangxi Normal University, Nanchang Jiangxi* 330022, *China*;
3. *Science and Technology Research Place, Jiangxi Normal University, Nanchang Jiangxi* 330022, *China*)

Abstract: With the widespread applications of large scale distributed Wireless Sensor Network (WSN), in some situations, the security of WSN involves not only the security of sending data by sensors, but also the anonymity and privacy during the sending process. How to design a secure efficient anonymous communication scheme for wireless sensor network has become a research hotspot. Using bilinear pairing, hash function and different operation, a scheme of validated secure anonymous communication was proposed. Through the analysis and improvement, this scheme can not only satisfy the basic requirement of anonymous communication, but also improve distinctly the complexity of computation and storage, and it is more suitable for wireless sensor network.

Key words: Wireless Sensor Network (WSN); anonymous communication; node-ID; bilinear pairing

0 引言

随着传感器与计算机等技术的发展,无线传感器网络(Wireless Sensor Network, WSN)的应用已越来越广泛。在许多 WSN 的应用如国防军事等领域中,当一个节点传送敏感信息给基站时,不仅需要保证传送信息的安全性,节点的身份和位置等信息也需隐藏,因为窃听者可以通过分析节点间的通信从而获得节点的身份等信息,从而摧毁或捕获被标识的节点,最终使整个网络瘫痪。无线传感器网络的匿名通信是指通过一定的方法将传感器节点间的通信关系加以隐藏,使窃听者不能获知或推测任何一方传感器节点的身份和双方的通信关系。无线传感器网络的匿名性根据所要隐藏信息的不同,可将匿名保护分为:发送方匿名(Sender Anonymity),接收方匿名(Receiver Anonymity)和收发双方无关联(Unlinkability between Sender and Receiver)。

关于传统网络匿名通信问题的研究,近年来已成国内外研究的热点并取得了丰硕的研究成果,但由 WSN 的能量、存储和带宽都严格受限,传统的基于洋葱路由等匿名通信协议都无法在无线传感器网络中直接应用。对于如何保护无线传感器网络和移动自组(Ad Hoc)网络的匿名通信,近年来已成国内外研究的热点。文献[1-3]对移动 Ad Hoc 网络的匿名路由问题进行了深入研究,在文献[1]中,目的节点的身份泄露给了路由的中间节点,文献[2]所提出的算法虽然具有较高的安全性与较好的匿名性,但是它不适用于敌手能力较强的环境。文献[3]提出了一种安全匿名的多径移动自组网络路由协议,很好地实现了通信者身份匿名、位置隐藏与路由不可追踪,但该协议采用了公钥密码体制和 Bloom Filter 等技术,并不适用于无线传感器网络。文献[4]利用假名机制提出了两个无线传感器网络匿名通信方案,方案一为每个节点提供了一个伪名集合,当节点需要发送信息时,从伪名集合中随机选取一个假名作为它的身份,另一个方案利用哈希函数产生节点的假名身份。这两个方案在假设节点之间共享的密钥不会被窃听者捕获的情况下都能提供很好的安全匿名性,并且每个节点为了达到匿名通信目的需要存储许多参数。文献[5]使用哈希函数链提出两个无线传感器网络匿名通信方法,但这两个方案都需要每个节点存贮并维护一张路由信息

收稿日期:2009-02-03;**修回日期**:2009-03-20。 **基金项目**:国家 973 计划项目(2007CB316505;2006CB303000);科技型中小企业技术创新基金资助项目(07C26213600564);江西省科技支撑计划项目。

作者简介:章志明(1978-),男,江西临川人,讲师,硕士,主要研究方向:网络信息安全、无线传感器网络; 邓建刚(1977-),男,江西高安人,讲师,硕士,主要研究方向:信息安全、网络计算技术; 邹成武(1980-),男,江西临川人,助教,硕士,主要研究方向:网络信息安全、无线传感器网络; 余敏(1964-),女,江西南昌人,教授,博士,主要研究方向:网络信息安全、分布式系统与移动计算、无线传感器网络。

表,当随着网络节点数增加所需存储空间急剧增加,不适合大规模分布式无线传感器网络。为了保持具有较高的安全匿名性同时,提高系统的存储性,本文使用双线性函数的双线性对计算节点与节点之间,节点与基站之间共享密钥,然后利用共享的会话密钥构提出了一种安全有效的无线传感器网络匿名通信方案。在路由建立过程中隐藏通信节点的身份信息,只有被选中路径上的节点才能获得完整的路由信息,方案采用对称密钥机制替代公钥签名机制,降低了通信所需的能耗。

1 双线性函数

1.1 双线性对

双线性对[6]是基于身份的密码体制中非常重要的概念,双线性映射可以从椭圆曲线中的 Weil Pairing 或 Tate Pairing 构造得到。设 G_1 和 G_2 是阶为素数 q 的群,其中 G_1 为加法群,G_2 为乘法群,P 为 G_1 的生成元,设群 G_1 和 G_2 中离散对数问题是困难的。双线性对是指满足以下性质的一个映射 $e:G_1 \times G_1 \rightarrow G_2$。

1) 双线性。① 对任意 $P,Q,R \in G_1$,有 $e(P,Q+R) = e(P,Q)e(P,R)$,$e(P+Q,R) = e(P,R)e(Q,R)$;② 对任意 $P,Q \in G_1$,$a,b \in Z_q$,有 $e(aP,bQ) = e(P,Q)^{ab} = e(abP,Q)$。

2) 非退化性。存在 $P,Q \in G_1$,满足 $e(P,Q) \neq 1$。

3) 可计算性。对任意 $P,Q \in G_1$,存在有效的多项式时间算法计算 $e(P,Q)$。

1.2 双线性对难解问题

1) 离散对数问题(Discrete Logarithm Problem, DLP)。对任意 $P,Q \in G_1$,求解一个整数 n,满足 $Q = nP$,称为离散对数问题,假设在群 G_1 和 G_2 中离散对数问题是困难的。

2) 判定性 Diffie-Hellman 问题(Decisional Diffie-Hellman Problem, DDHP)。对任意 $P,a,b,c \in G_1$,给定 (P, aP, bP, cP),决定 $c = ab \bmod q$ 是否成立。

3) 计算性 Diffie-Hellman 问题(Computational Diffie-Hellman Problem, CDHP)。对任意 $P,a,b \in G_1$,给定 (P, aP, bP),计算 abP。

如果在群 G 中 DDHP 是易解的而 CDHP 是难解的,那么群 G 称为 Gap Diffie-Hellman 群。因为可以通过 $e(P, cP) = e(aP, bP)$ 来决定 DDHP,但没有有效的算法来计算 abP,所以 G_1 是一个 Gap Diffie-Hellman 群。

2 基于双线性对的匿名通信方案

2.1 系统网络模型

系统由 N 个传感器节点和一个基站组成。基站是整个无线传感器网络与外界网络的接口,将接收来自无线传感器网络中节点发送过来的所有数据,并给网络中的节点发送操作指令等安全信息,基站一般作为无线传感器网络的控制中心,而且处理能力、内存及无线发射功率都不受限制,普通节点只需采集周围环境的数据并发往基站。系统为每个节点分配一个身份随机数 ID_i 作为唯一身份标识。基站保存全网拓扑信息,每次路由时以系统匿名需求与网络生存时间最大化为约束条件选取路径,节点与节点之间,节点与基站之共享一个对称密钥。

本文定义匿名路由要达到如下目标。

1) 身份机密性。任何中间路由节点都不知道通信的发送方(源)与接收方(目的)的真实身份,并且发送方和接收方也不知道中间路由节点的真实身份。

2) 位置机密性。发送方与接收方的位置不会被其他节点知道,路由节点不能获得到源与目的的距离,即中间转发节点不可判断到发送方和接收方节点的跳数。

3) 路由的匿名性。不能通过追踪发送信息包来发现发送方和接收方的节点,即第三方难以推断源与目的之间的通信传输模式。

2.2 符号说明

Q 表示一个大素数;G_1 表示大素数 q 的加法群;G_2 表示大素数 q 的乘法群;e 表示满足 $G_1 \times G_1 \rightarrow G_2$ 的一个双线性映射;S_i 表示表示普通节点 i;BS 表示表示基站;ID_i 表示节点 S_i 的唯一身份标识;ID_{BS} 表示基站的唯一身份标识;$h(\cdot)$ 表示一个强密码 hash 函数,该函数把节点 ID 映射到 G_1 中的一个元素;$\|$ 表示串接;$K_{i,j}$ 表示节点 i 和节点 j 之间的共享密钥;$E_{K_{i,j}}(m)$ 表示用密钥 K_{ij} 加密信息 m;ST 表示一个堆栈,存储路由点的相关信息;SP 表示一个堆栈,存储用于验证路由信息是否被修改的相关信息;$\oplus$ 表示异或运算。

2.3 系统初始化

1) 基站选择系统参数为 $q,G_1,G_2,e:G_1 \times G_1 \rightarrow G_2$ 以及一个强密码 hash 函数 $h(\cdot):\{0,1\} \rightarrow G_1$。

2) 为每个节点 S_i 选择一个身份随机数 ID_i 并计算其公钥为 $H(ID_i)$,私钥为 $qh(ID_i)$,并把 $(ID_i,h(ID_i),qh(ID_i),G_1,G_2,e:G_1 \times G_1 \rightarrow G_2,h(\cdot))$ 嵌入节点内,基站保存加法群上的大素数 q。

2.4 匿名通信协议

在将所有的传感器节点部署完毕后,假设基站要与节点 S_i 进行匿名通信,基站首先通过算法 1 产生路由信息 $M = E_{KBS,1}(h(ID_1) \| ST \| SP \| T_0) \| h(ID_{BS}) \| Dt$(其中 $\|$ 表示连接运算,$h(ID_{BS})$ 为基站的身份哈希值,$h(ID_1)$ 为路由路径上转发的第一个节点,ST 为一个路由堆栈,存储了其他路由点的相关信息,SP 为一个路由堆栈,SP 和 T_1 中存储了用于验证路由信息是否被修改的相关信息,$K_{BS,1}$ 表示基站与节点 S_1 之间的共享密钥,Dt 表示经过某种加密运算后发送给目的节点的信息。),然后广播出去,节点 S_1 得到信息 M 后通过算法2进行路由信息的转发,依次类推路由路径上的其他路由节点重复执行算法2,直到目的节点 S_i 最后得到源节点发送的信息 Dt,整个匿名通信结束。

算法 1 路由信息初始化算法

输入:基站、网络节点集合 $\{BS,S_1,S_2,\cdots,S_n\}$ 和基站、各节点的身份哈希值 $\{h(ID_{BS}),h(ID_1),h(ID_2),\cdots,h(ID_n)\}$;

输出:路由信息 $M = E_{KBS,1}(h(ID_1) \| ST \| SP \| T_0) \| h(ID_{BS}) \| Dt$;

```
Begin
1) Add the S_j into the routing set V;
    // 选择一条到节点 S_i 的路径(BS, S_1, S_2, ···, S_{i-2}, S_{i-1}, S_i);
2) K_1 = h(ID_BS) ⊕ h(ID_1) ⊕ h(ID_2);
3) For m = 1 to i - 2
4) K_{m+1} = h(ID_m) ⊕ h(ID_{m+1}) ⊕ h(ID_{m+2});
5) Initial(ST);                    // 初始化一个路由堆栈 ST
6) For m = n; to m = 1
   ST. Push(K_m);                  // 依次把 K_m 压入路由堆栈 ST 中
7) T_0 = h(ID_BS);
8) L_0 = h(T_0);
9) For m = 0 to i - 1
10) T_{m+1} = T_m ⊕ h(ID_{m+1});
11) L_{m+1} = h(T_{m+1}); // 依次得到 L_1 = h(h(ID_BS) ⊕ h(ID_1))、
```

//$L_2 = h(h(ID_{BS}) \oplus h(ID_1) \oplus h(ID_2))$、…、$L_i =$
//$h(h(ID_{BS}) \oplus h(ID_1) \oplus \cdots \oplus h(ID_i))$

12) Initial(SP); // 初始化一个路由堆栈 SP

13) For $m = n$ to 1

14) $SP.Push(L_m)$; // 依次把 L_m 压入路由堆栈 SP 中

15) $K_{BS,1} = e(qh(ID_{BS}), h(ID_1))$; // 基站利用双线性函数
// 的双线性对计算与节点 S_1 之间的共享密钥

16) $M = E_{K_{BS,1}}(h(ID_1) \| ST \| SP \| T_0) \| h(ID_{BS}) \| Dt$;
// 产生路由信息 M

End

算法 2　节点 S_j 转发来自 S_{j-1} 的路由信息

输入:路由信息 $M = E_{K_{j-1,j}}(h(ID_j) \| ST \| SP \| T_{j-1}) \| h(ID_{j-1}) \| Dt$;

输出:路由信息 $M' = E_{K_{i,i+1}}(h(ID_{j+1}) \| ST' \| SP' \| T_j) \| h(ID_j) \| Dt$;

Begin

1) $K_{j-1,j} = e(h(ID_{j-1}), qh(ID_j))$; // 节点 S_j 从 M 中取出
//$qh(ID_{j-1})$,计算与 S_{j-1} 之间共享的密钥 $K_{j,j-1} =$
//$e(h(ID_{j-1}), qh(ID_j))$,根据双线性函数的双线性对性质有
//$K_{j,j-1} = e(h(ID_{j-1}), qh(ID_j)) = e(h(ID_{j-1}), h(ID_j))^q =$
//$e(qh(ID_{j-1}), h(ID_j)) = K_{j-1,j}$

2) Use $K_{j-1,j}$ decrypt the $E_{K_{j-1,j}}(h(ID_j) \| ST \| SP \| T_{j-1})$;
// 使用 $K_{j-1,j}$ 解密信息

3) S_jGet the $T = h(ID_j)$ from the $E_{K_{j-1,j}}(h(ID_j) \| ST \| SP \| T_{j-1})$;

4) S_j Compares $h(ID_j)$ with the encrypted $T = h(ID_j)$;

5) If the check passes go to 7);

6) else stop and send Error message;

7) $L_j = SP.Get(L_j) = h(h(ID_{BS}) \oplus h(ID_1) \oplus \cdots \oplus h(ID_j))$;
// 取出路由堆栈 SP 栈顶元素 L_j

8) $SP' = SP.Pop(L_j)$; // 栈顶元素 L_j 出栈,形成新栈 SP'

9) $T_j = T_{j-1} \oplus h(ID_j)$; // 计算 $T_j = T_{j-1} \oplus h(ID_j) =$
//$h(ID_{BS}) \oplus h(ID_1) \oplus \cdots \oplus h(ID_j)$

10) if($L_j == h(T_j)$)

11) go to 13); // 如果 $L_j == h(T_j)$,则一切合法

12) else stop and send Error message; // 如果 $L_j != h(T_j)$,则受
// 到攻击,路由中止,并发送相关的错误信息

13) $K_j = ST.Get(K_j)$; // 取出路由堆栈 ST 栈顶元素 K_j

14) $ST' = ST.Pop(K_j)$; // 栈顶元素 K_j 出栈,形成新栈 ST'

15) $h(ID_{j+1}) = h(ID_{j-1}) \oplus h(ID_j) \oplus K_j = h(ID_{j-1}) \oplus h(ID_j) \oplus h(ID_{j-1}) \oplus h(ID_j) \oplus h(ID_{j+1})$; // 用得到的 S_{j-1} 身份哈希
//值 $h(ID_{j-1})$、自己的身份哈希值 $h(ID_j)$ 和 K_j 进行异或运算
//得到下一个路由节点 S_{j+1} 的身份哈希值 $h(ID_{j+1})$

16) $K_{j,j+1} = e(qh(ID_j), h(ID_{j+1}))$; // 基站利用双线性函数的双
// 线性对计算与节点 S_{j+1} 之间的共享密钥

17) $M' = E_{K_{i,i+1}}(h(ID_{j+1}) \| ST' \| SP' \| T_j) \| h(ID_j) \| Dt$;
// 产生新的路由信息 M'

18) Broadcast the M';

End

2.5　匿名性与安全性分析

2.5.1　匿名性分析

本方案的每个路由节点(包括源节点和目的节点)的真实身份 ID 是用一个强密码 hash 函数映射到 G_1 中,路由上的任意路由节点只知道它的前驱路由节点和后继路由节点的假名信息,同样发送方从路由信息中得到的也是接收方的身份 ID 用 hash 函数 hash 得到的一个假名,从而保证了路由节点的身份机密性。

当节点 S_{j+1} 取得 S_j 节点发送的路由信息包,利用得到的上一个节点身份的哈希值 $h(ID_j)$、自己节点的身份哈希值 $h(ID_{j+1})$ 和 K_{j+1} 进行异或运算只能得到下一个路由节点的身份哈希值 $h(ID_{j+2})$,并不能得知其他路由节点的信息,更不能得到源节点和目的节点的任何信息,从而保证源节点和目的节的位置机密性,即中间转发节点不可能判断到发送方和接收方节点的跳数。

只有路由路径上正确的路由节点才能解密得到正确的路由信息,假设节点 S_j 的下一个路由节点为 S_{j+1},因为路由信息是用 S_j 和 S_{j+1} 这两个节点共享的密钥 $K_{j,j+1}$ 加密的,只有节点 S_{j+1} 才能正确解密出路由信息,其他任何节点都不能得到路由信息,从而保证了路由的匿名性:不能通过追踪发送信息包来发现发送方和接收方的节点,即第三方难以推断源与目的节点之间的通信传输模式。

2.5.2　安全性分析

方案的安全性是建立在求解椭圆曲线离散对数问题和计算性 Diffie-Hellman 问题的基础之上。当窃听者获得节点的公钥 $H(ID_i)$ 时,它想求解节点的私钥 $qH(ID_i)$ 是不可能的,因为它不知道保存在基站中的加法群上大素数 q。即使当窃听者捕获了节点 i,从而获得了节点的公钥和私钥对 $(h(ID_i), qh(ID_i))$,但它要求解出 q 是不可能的,因为它将面临求解椭圆曲线离散对数问题和计算性 Diffie-Hellman 问题,所以即使捕获了一些节点,其他节点的私钥 $qh(ID_j)$ 仍是安全的。

1) 抗被动攻击。当窃听者获得路由信息包时,虽然能取得了上一节点的身份哈希值 $h(ID_{j-1})$,但没有当前路由节点的哈希值 $h(ID_j)$,不能获得与上一节点的共享密钥 $K_{j,j-1}$,从而不能正确解密出完整的路由信息,所以方案保证只有合法的路由节点才能得到正确的路由信息。

2) 抗主动攻击。文献[4]利用假名机制提出了两个无线传感器网络匿名通信方案,这两个方案在假设节点之间共享的密钥不会被窃听者捕获的情况下能提供很好的安全匿名性。然而,传感器节点一般被部署在不安全的环境中,我们需要考虑节点之间共享密钥被捕获情况下如何保证节点的匿名通信。在本方案中假设窃听者捕获了当前路由节点 S_j 并获得与上一路由节点的共享密钥 $K_{j,j-1}$,窃听者使用密钥 $K_{j,j-1}$ 并通过算法 2 也仅能获得下一路由节点的哈希值 $h(ID_{j+1})$,并不能获得其他路由节点的任何信息,更不能获得源节点和目的节点的信息。假设窃听者想跳过下一个路由节点 S_{j+1} 并把下一个路由节点设为 S_k,窃听者根据算法 2 计算 $T_j = T_{j-1} \oplus h(ID_j) = h(ID_{BS}) \oplus h(ID_1) \oplus \cdots \oplus h(ID_{j-1}) \oplus h(ID_j)$ 等信息,形成新的路由信息 $M' = E_{K_{i,k}}(h(ID_k) \| ST' \| SP' \| T_j) \| h(ID_j) \| Dt$ 并广播出去,当节点 S_k 收到路由信息后根据算法 2 取出堆栈 SP 的栈顶元素 $L_{j+1} = SP.Get(L_j) = h(h(ID_{BS}) \oplus h(ID_1) \oplus \cdots \oplus h(ID_j) \oplus h(ID_{j+1}))$,计算 $T_k = T_j \oplus h(ID_k) = h(ID_{BS}) \oplus h(ID_1) \oplus \cdots \oplus h(ID_{j-1}) \oplus h(ID_j) \oplus h(ID_k)$,然后比较 L_{j+1} 是否与 $h(T_k)$ 相等,很显然 $L_{j+1} != h(T_k)$,则 S_k 知道路由信息被修改,然后向网络广播路由信息被修改的信号。

3) 最小的信息泄露。路由上的任意路由节点只知道它的前驱路由节点和后继路由节点的假名信息,路由上其他节点的信息对它来说都是透明的。

4) 可验证性。路由上的任意路由节点都能确认它是路由路径上的一部分,并且路由上的每一路由节点都能确认路由信息确实来自于它的前驱路由节点。因为路由信息是用前驱路由节点和当前路节点共享的密钥进行加密的,只有当前合法的路由节点才能解密路由信息。

2.6 性能分析

在计算复杂度方面,本方案的中间路由节点只是计算两次异或运算、几个Hash函数、两次对称密钥的运算,对称密码体制下的一次解密和一次加密。由于对称密码体制和Hash函数实现的速度要远远快于基于公钥密码体制的匿名通信方案[3],因此,以上这些计算的计算复杂度是非常低的。

在存储复杂度方面,文献[4]的方案为了达到匿名通信目的,每个节点需要的存储量为$6k+7kN$,其中k表示大小为k位的伪名空间,N为当前节点的邻接节点个数。假设一个无线传感器网络有1000个节点,伪名空间大小为64 b,每个节点的邻接节点平均为100个则每个节点需的存储量为$6\times64+7\times64\times100=45184$ b $=5648$ B $=5.6$ KB,如果有10000个节点,则存储量为$6\times64+7\times64\times1000=54.7$ KB,可见随着网络规模增加,方案所需存储量也呈线性增加,并不太适用于资源受限的传感器网络。文献[5]使用哈希函数链提出两个无线传感器网络匿名通信方法,但这两个方案都需要每个节点存贮并维护一张邻接节点信息表,当随着网络节点数增加所需存储空间也急剧增加,不适合大规模分布式无线传感器网络。在本文提出的方案中,每个节点S_i仅需存储$(ID_i, h(ID_i), qh(ID_i), G_1, G_2, e: G_1\times G_1\rightarrow G_2, h(\cdot))$,每个符号表示的意思如2.2节所示,需要的存储量为一个与网络大小无关的常量。

3 结语

本文使用双线性函数的双线性对,哈希函数和异或运算提出了一种可验证安全的无线传感器网络匿名通信方案。方案在路由建立过程中隐藏通信节点的身份信息,只有被选中路径上的节点才能获得完整的路由信息,方案采用对称密钥机制替代公钥签名机制,在保持具有较高的安全性和匿名性同时,大大提高系统的计算复杂度和存储复杂度。本文的下一步工作将进一步在网络仿真平台上对路由建立时间与数据包发送迟延进行仿真,以全面评价该方案的性能。

参考文献:

[1] KONG J, HONG X. ANODR: Anonymous on demand routing with untraceable routes for mobile Ad-Hoc networks [C]// MobiHoc'03: Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Annapolis, MD, USA: ACM Press, 2003: 291-302.

[2] ZHU BO, WAN ZHI-GUO, KANKANHALLI M S, *et al*. Anonymous secure routing in mobile Ad-Hoc networks [C]// Proceedings of the 29th Annual IEEE Inter national Conference on Local Computer Networks. Tampa, USA: IEEE Computer Society, 2004: 102-108.

[3] 章洋,范植华,何晓新,等.移动自组网络中多径路由的匿名安全[J].电子学报, 2005,33(11): 2022-2029.

[4] MISRA S, XUE G. Efficient anonymity schemes for clustered wireless sensor networks[J]. International Journal of Sensor Networks, 2006, 1(1/2): 50-63.

[5] YI OU-YANG, LE ZHENG-YI, XU YU-RONG, *et al*. Providing anonymity in wireless sensor networks [C]// Proceedings of the 2007 IEEE International Conference on Pervasive Services. Washington, DC: IEEE Computer Society, 2007: 145-148.

[6] BARRETO P S L M, KIM H Y, LYNN B, *et al*. Efficient algorithms for pairing-based cryptosystems [C]// Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, LNCS 2442. Berlin: Springer-Verlag, 2002: 354-368.

(上接第2343页)

复杂度,val_{time}为验证时间复杂度。将本文的签名方案与其他方案进行比较,见表1所示。

表1 四种方案的密钥长度、签名长度及时间复杂度比较

运算	本文方案	文献[6]方案	文献[7]方案	文献[8]方案
Lpk	$[\log n]+2[\log p]$	$n[\log n]+[\log p]$	$[\log p]+T$	$[\log n]+[\log p]$
Lsk	$[\log n]$	$[\log n]$	$[\log n]+T$	$[\log n]$
$Lsig$	$2[\log n]$	$[\log n]+[\log p]$	$3[\log n]$	$[\log n]+[\log p]$
sig_{time}	$T_{exp}+3T_{mod}$	$T_{exp}+2T_{mod}$	$T_{exp}+4T_{mod}+T_{ath}$	$2T_{exp}+3T_{mod}$
val_{time}	$T_{exp}+2T_{mod}$	$[\log n](T_{exp}+T_{mod})$	$2T_{exp}+[\log t]T_{mod}$	$2T_{exp}+3T_{mod}$

表1中,计算公钥$Lpk=(n,p)$,其长度为$[\log n]+[\log p]$,模指数运算T_{exp}为计算如$y\equiv g^x \bmod p$的时间,模乘运算T_{mod}为计算如$s_1=xe+k \bmod n$的时间,逆运算T_{ath}为计算如$k^{-1} \bmod n$的时间。从表1可以看出,本文中的方案与文献[6-8]中方案相比具有签名密钥短、计算时间复杂度小等优点。

4 结语

本文提出了一个新的签名方案,从新的角度将素数域上的离散对数和椭圆曲线结合起来,基于椭圆曲线离散对数的签名方案,可以大大提高数字签名的安全性和性能,它的安全性同时基于这两个困难问题的求解,达到了设计要求。并且,将本文方案与其他签名方案进行了比较,具有较快的运行速度和较好的安全性。随着计算机技术的发展,减少基于双难题签名方案的复杂度,以及如何提高签名方案的效率将是今后深入研究的内容。

参考文献:

[1] KOBLITZ N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209.

[2] MENEZES A J, VAN OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography[M]. 胡磊,王鹏,译. 北京:电子工业出版社, 2005.

[3] WILLIAM S. Cryptography and network security principles and practices [M]. 孟庆树,王丽娜,傅建明,等译. 4版. 北京:电子工业出版社, 2007.

[4] 胡向东,魏琴芳.应用密码学教程[M].北京:电子工业出版社,2005.

[5] 王衍波,薛通.应用密码学[M].北京:机械工业出版社.2003.

[6] 贾晓芸,罗守山,袁超伟.一种新的基于离散对数的签名方案[J].西安电子科技大学学报:自然科学版, 2008,35(2): 352-354.

[7] 吴秋新,杨义先,胡正名.同时基于离散对数和素因子分解的新的数字签名方案[J].北京邮电大学学报, 2001,24(1): 61-64.

[8] 任俊伟,林东岱.一种基于因数分解和离散对数的签名算法的分析与改进[J].计算机工程与应用, 2005,41(7): 132-135.