应用于无线传感器网络的门限环签名方案

肖俊芳[1]，**廖剑**[2]，**曾贵华**[3]

（1. 工业和信息化部电子科学技术情报研究所，北京 100040；
2. 普天信息技术研究院有限公司 北京 100080；3. 上海交通大学 电子工程系，上海 200030）

摘 要：针对节点的能量损耗、通信带宽、存储空间等有严格限制的无线传感器网络环境，基于双线性配对，本文提出门限签名方案。在假设计算 Diffie-Hellman 问题困难的前提下，利用规约到矛盾的方法给出在随机预言机模型下的严格安全性证明。此外所提的方案具备群合作条件下应有的顽健性，可以进行多签，满足分布式并行计算等特点，非常适应于无线传感器网络。

关键词：无线传感器网络；配对密码术；门限环签名；安全性证明

中图分类号：TN915; TP301 **文献标识码**：A **文章编号**：1000-436X(2012)03-0075-07

Threshold ring signature for wireless sensor networks

XIAO Jun-fang[1], LIAO Jian[2], ZENG Gui-hua[3]

(1. Electronic Technology Information Research Institute MIIT, Beijing 100040, China; 2. Potevio Institute of Technology Co. Ltd., Beijing 100080, China;
3. School of Electronic and Engineering, Shanghai Jiaoton niversity, Shanghai 200030, China)

Abstract: Compared with traditional network, the wireless sensor nodes are limited in the storage, mobility, computation, energy, and so on. A threshold ring signature scheme suitable for wireless sensor networks based on bilinear pairings was proposed. Assuming the abstrusity of computational Diffie-Hellman problem, the secure proof was shown in the model of random oracles using the reduction to the contravention. Proposed scheme also had other characteristics,such as robustness, multi-signature and parallel computation.

Key words: wireless sensor networks; pairing-based cryptography; threshold ring signature; security analysis

1 引言

无线传感器网络（WSN）广泛应用于军事、环境监测、医疗、智能建筑和其他商业领域。在无线传感器网络中，网络规模颇为庞大，节点数目较多；节点在电池能量、计算能力和存储容量方面都有限制；节点因能量耗尽而失效或离开都是非常常见的现象。这些特点给无线传感器网络安全协议的设计提出了更高的要求，安全成为制约无线传感器网络进一步广泛应用的关键。

环签名首先由 Rivest 等[1]提出。在一般环签名的应用场景中，节点群的规模及相应的 PKI（公钥体系）对节点能量和性能消耗影响较大。针对无线传感器网络的特点，安全协议的选取受到通信带宽、存储空间、计算量、能量消耗和抵御各种已知安全攻击等方面的影响，因此设计合适的环签名方案，由一个经常变化的子群代替整个群完成签名，才更加适合无线传感器网络。

Crescenzo 提出在自组织网络中应该注意的 2 个基本安全问题[2]。第一，单个节点的失效，即避免由于关键节点的失效而导致严重的系统事件；第二，服务的可用性，即某个服务请求被提出时，系

收稿日期：2010-08-12；**修回日期**：2011-02-03
基金项目：国家自然科学基金资助项目（60970109）
Foundation Item: The National Natural Science Foundation of China (60970109)

统能确保足够的节点资源来满足服务需求。Stefaan[3]提出一个可以使多个节点相互协作去认证信息的方案，但是该方案需要一个节点起到完全的支撑整个系统运行的作用。一旦该节点失效，对于整个系统将是灾难性的。Liu 引入新的概念－联系性[4]，并针对自组织网络提出第一个具备联系性的环签名（LSAG）方案。但是 LSAG 方案中架构的(*t*,*n*)门限环签名方案需要每个节点生成一个环签名，然后再将所有节点生成的*n*个签名组合，形成(*t*,*n*)门限环签名，使得每个节点的计算量和存储空间的消耗都非常大。Qi[5]采用门限密码学中的(*t*,*n*)秘密共享方法，提高了基于身份的加密签名(IBES)系统中密钥生成中心(PKG)的可信性，并应用于无线传感器网络。Tony 提出第一个盲自发匿名群签名（SAG， spontaneous anonymous group）[6]，在此方案的基础上，架构(*t*,*n*)门限环盲签名。在环签名的架构基础上，Javier 针对自组织网络的通用接入架构[7]，提出一个环签名架构。基于该方案 Javier 也提出了门限签名方案，并且给出了安全性证明，包括正确性、匿名性以及在选择消息攻击模式下抵御存在性伪造。Bresson[8]首次改进了 Rivest[1]环签名方案的模型，随后将该模型扩展应用至门限签名方案和 ad hoc 群。此外 Bresson 还给出了具有较高性能的环签名方案，并给出在随机预言机模型下的安全性证明。

本文基于双线性配对提出一个新的门限签名方案可适用于无线传感器网络，同时给出正确性、匿名性和抵御存在性伪造的证明。在假设计算 Diffie-Hellman（CDH, computational Diffie-Hellman）问题困难的前提下，给出在随机预言机模型下的安全性证明，结论证明本文所提的方案可以在自适应选择消息攻击模式下抵御存在性伪造。除此之外本文所提方案还具备以下特点。

1) 顽健性：群合作的条件下可以在合作生成签名的过程中检测所有节点是否运行错误的行为和步骤，同时可以防御一些恶意的节点对整个群造成的影响。

2) 多签：群内的所有节点可以自由选择自己需要发布的消息，在签名中可以一次性对所有的消息进行签名。多签现在被广泛应用于移动代理、招投标、电子投票、数字彩票、电子现金等方面。

3) 满足分布式并行计算要求：所有参与签名节点可以并行地计算自己的部分签名，然后将部分签名组合成为门限签名。无需像传统的环签名，需要参与签名的节点一个接着一个生成部分签名，这样才可以组成一个环。该方法产生一个环签名需要的时间非常长，增加了能量的消耗；并且如果某个节点失效，需要重新定义群内参与签名的节点次序，浪费较多的资源。因此本文提出的门限环签名方案非常适合无线传感器等网络。

2 门限环签名的语法及安全模型

一个门限环签名方案应该包含至少 3 个算法(Setup,Sign,Verify)，算法定义如下。

1) Setup 算法：该算法是一个 PPT（probabilistic polynomial time）算法，它的表达式为：$Setup(1^k, N) = \{P_{\text{pub}}, s, \bigcup_{i\in\{1,\perp,n\}} P_{\text{PK}}^i, S_{\text{SK}}^i\}$。

2) Sign 算法：该算法是一个 PPT 算法，它的表达式为：$Sign(1^k, N, m, P_{\text{pub}}, s, \bigcup_{i\in\{1,\perp,n\}} P_{\text{PK}}^i, S_{\text{SK}}^i) = d$。

3) Verify 算法：通常是确定性算法，是对*Sign*算法的输出进行有效性的检验，输出是 Ture 或者 False。该算法的表达式为：$Verify(1^k, N, m, P_{\text{pub}}, \bigcup_{i\in\{1,\perp,n\}} P_{\text{PK}}^i, d) = \{0,1\}$。

以上定义的门限环签名方案是一个最简化的版本。对于门限环签名方案至少需要有 3 个方面的要求：正确性、匿名性和抵御存在性伪造。

与 Benoit[9]、Sherman[10]定义类似，本文给出门限环签名的安全模型：定义在随机预言机模型下，宣称一个 (t,n) 门限环签名方案可以抵御自适应选择消息攻击，那么应该不存在一个多项式边界的伪造者（polynomially bounded forger）以不可忽略的概率完成如下的游戏。

1) 伪造者 F 从节点群 N 中任意选取 $t-1$ 个目标节点，这些节点可以与 F 一起参与伪造。F 可以从挑战者 C 处得到部分私钥 S_{SK}^i。

2) 在安全参数 k 的作用下，C 运行 Setup 算法，然后将系统参与发送给 F。

3) F 进行多项式边界次散列函数和签名询问。F 可以根据 C 返回的结果动态地调整询问值。

4) F 输出一个有效的签名。

F 输出一个关于消息 m 的门限环签名，在有 n 个节点的群内至少需要 t 个节点参与签名。在游戏中有 2 个要求：①消息 m 在之前的签名和随机预言机询问中没有被涉及到；②少于 t 个节点的密钥被 F 获取。当伪造的签名可以通过签名验证算法，那么 F 赢得这个游戏。

3　改进的门限环签名方案

针对无线传感器网络的特点，本节提出改进的门限环签名方案，在签名的构建部分包括准备、签名和验证 3 个步骤。随后对改进的门限环签名方案进行顽健性分析，给出参与签名的节点在签名过程中如何检测错误的发生。最后基于改进的门限环签名方案，本节提出实现多方数字签名的方法。

3.1　改进的门限环签名算法

假设在一个无线传感器网络群内有 n 个节点，用符号 S 表示，同时在 WSN 群内架构一个公钥生成器（PKG），该 PKG 可以离线预先生成各节点的公私钥对。

3.1.1　Setup 算法

1) 选定系统安全参数 k，输出 q 阶加法群 G_1 和 q 阶乘法群 G_2，双线性映射 $e: G_1 \times G_1 \to G_2$，此处 q 是 k bit 的素数。

2) PKG 随机选择 G_1 的生成元 P，随机选择 $s \in_R Z_q^*$，计算并公布公钥 $P_{\text{pub}} = sP$，随机选择 $s' \in_R Z_q^*$，计算并公布 $Q = s'P$。

3) PKG 生成一个 t 阶多项式：

$$f(x) = s + a_1 x + a_2 x^2 + \mathrm{L} + a_{t-1} x^{t-1} \tag{1}$$

其中，随机选择 $a_1, \mathrm{L}, a_{t-1} \in_R Z_q^*$。

4) PKG 为 WSN 中每一个节点生成公钥 $P_{\text{PK}}^i = f(i)P$，其中 $i = 1, \mathrm{L}, n$。

5) 定义密码散列函数 $H: \{0,1\}^* \times G_1 \to Z_q^*$，其中 $\{0,1\}^*$ 表示任意长度的数据。

6) 消息明文空间 $m \in \{0,1\}^*$。

7) PKG 将 s 作为系统私钥，输出系统参数 $params: \{q, G_1, G_2, e(\cdot,\cdot), P, Q, P_{\text{pub}}, P_{\text{PK}}^1, \mathrm{L}, P_{\text{PK}}^n, H\}$。

8) 在每个节点得到相应的私钥之前，WSN 群内每个节点 $S_k \in \{1, \mathrm{L}, n\}$ 都可以检查

$$\sum\nolimits_{i \in S_k} L_i P_{\text{PK}}^i = P_{\text{pub}} \tag{2}$$

是否成立，此处拉格朗日系数 $L_i = \prod_{\substack{j \neq i \\ j \in S}} \frac{j}{j-i}$，参与签名的节点有 $|S_k| = t$ 个。

9) PKG 计算每个节点 $i \in \{1, \mathrm{L}, n\}$ 的私钥 $S_{\text{SK}}^i = f(i)Q$，并通过安全信道将每个节点对应的公私钥对 $\{P_{\text{PK}}^i, S_{\text{SK}}^i\}$ 发给对应的节点 i。

3.1.2　Sign 算法

为了不失一般性，假设 WSN 群中编号为 $\{1, \mathrm{L}, t\}$ 的节点参与环签名的生成，编号为 $\{t+1, \mathrm{L}, n\}$ 的节点不参与环签名的生成。

1) 编号为 $\{1, \mathrm{L}, t\}$ 的节点进行的步骤如下：对于 $j \in \{1, \mathrm{L}, t\}$ 的节点，随机选择 $r_i \in_R Z_q^*$，然后计算 $U_i = r_i P$，随后通过认证的通道将 U_i 发给其他所有的节点。

2) 编号为 $\{1, \mathrm{L}, t\}$ 中的任意一个节点或者其他任意一个实体（只要不将其他参与签名节点的身份暴露即可）进行的步骤如下：对于 $j \in \{t+1, \mathrm{L}, n\}$ 的节点，随机选择 $r_j \in_R Z_q^*$，计算

$$U_j = r_j P \tag{3}$$

$$h_j = H(m \| S \| \bigcup\nolimits_{k=1}^n U_k) \tag{4}$$

$$V_j = L_j^{-1}(r_j + h_j)^{-1} r_j Q \tag{5}$$

此处 S 表示 WSN 群中参与签名的 n 个节点的身份；随后将 (U_j, V_j) 公布；最后计算并公布 $U' = \sum_{j=t+1}^n U_j$，$U'' = \sum_{j=t+1}^n r_j Q$。

3) 编号为 $\{1, \mathrm{L}, t\}$ 的节点进行的步骤如下：对于 $j \in \{1, \mathrm{L}, t\}$ 的节点，计算

$$h_i = H(m \| S \| \bigcup\nolimits_{k=1}^n U_k) \tag{6}$$

$$V_i = (r_i + h_i)^{-1} S_{\text{SK}}^i - L_i^{-1} t^{-1} (r_i + h_i)^{-1} U'' \tag{7}$$

4) WSN 群 S 输出针对某个特定消息 m 的环签名 $d = \{m, \bigcup_{k=1}^n U_k, \bigcup_{k=1}^n V_k\}$。

3.1.3　Verify 算法

验证者需要 2 个条件检验关于签名 $d = \{m, \bigcup_{k=1}^n U_k, \bigcup_{k=1}^n V_k\}$ 是否有效：第一，d 是关于消息 m 的签名；第二，d 是 WSN 群至少 t 个签名者共同参与生成的。验证者判断的流程如下。

1) 对于 $k \in (1, \mathrm{L}, n)$，验证者计算 $h_k = H(m \| S \| \bigcup_{k=1}^n U_k)$。

2) 验证者检验等式

$$\prod\nolimits_{i=1}^n e(L_i V_i, U_i + h_i P) = e(Q, P_{\text{pub}}) \tag{8}$$

是否成立。如果成立，则签名 d 是有效的，否则为无效的签名。

3.2　顽健性分析

在 WSN 群体签名方案中顽健性指的是参与其中的任何节点可以方便地检测出自己或者其他节

点的行为或者计算是否发生错误。顽健性对于能量受限的无线传感器网络等自组织网络来说是非常有意义的，一旦某个参与签名的节点发生了错误，该节点可以对计算的结果进行检查验证并且加以改正。因此群体签名方案中顽健性可以减少某个节点发生错误的几率，避免因错误导致的通信数据量、计算等带来的能量消耗。针对本节提出的环签名方案，顽健性应该具备以下特征。

1) 避免到最后生成签名时才发现生成的签名是无效的。

2) 在签名的生成过程中，每个参与签名的节点应该可以检验自身的错误。

在 Setup 算法阶段的步骤 8）中，实际上已经在进行顽健性检查，每个节点需要计算公钥是否是有效，进一步判断参与签名的群体 S 是否合法。

在 Sign 算法阶段中，所有的节点 $\{1,\mathrm{L},n\}$ 在步骤 3）结束后，获得部分签名 $d_i=\{h_i,U_i,V_i\}$，因此节点 j 可以计算等式

$$e(V_i,U_i+h_iP)=e(Q,P_{\mathrm{PK}}^i-L_i^{-1}t^{-1}U') \tag{9}$$

是否成立。如果成立则该节点生成的部分签名是正确的，否则该节点重新进行计算。

3.3 多签方案

与其他的群签名方案相比较，本节提出的环签名方案可以使 WSN 群中不同的签名者对多个不同的消息同时进行签名。在网络规模较大的密码学应用环境中，如果 WSN 群内有签名者想发布一个特别的信息，但是不想暴露到底是哪一个签名者发布的，最有效的方式就是生成一个包含不同消息的群签名。

一个典型的应用场景就是 Yao[11]提出一个对“offer privacy”的定义，应用于移动代理环境中，例如：有一群应标者参与某个项目的竞争性投标，每个应标者给出他们的报价。为防止应标者抵赖，需要应标者对这个报价进行签名，保证该报价的不可伪造性。其他应标方可以看到该标价，最后招标方公布胜出的应标者身份，但是其他竞标失败的应标者无法得知其真实的身份。针对这种应用环境，需要一个带 offer privacy 的多签方案，本文提出的环签名方案略加改动，即可实现该多签方案。

1) Setup 算法

与改进门限环签名算法一样。

2) Sign 算法

设定与改进门限环签名算法一样，不同流程是在步骤 2）和步骤 3）中，对于 $j\in\{1,\mathrm{L},n\}$ 的节点，选取消息 m_i，计算 $h_i=H(m_i\|S\|\bigcup_{k=1}^{n}U_k)$；在步骤 4）中，WSN 群 S 输出针对消息 $\{m_1,\mathrm{L},m_n\}$ 的环签名 $d=\{m_1,\mathrm{L},m_n,\bigcup_{k=1}^{n}U_k,\bigcup_{k=1}^{n}V_k\}$。

3) Verify 算法

对于 $k\in(1,\mathrm{L},n)$，验证者计算 $h_k=H(m_k\|S\|U_k)$，检验等式

$$\prod_{i=1}^{n}e(L_iV_i,U_i+h_iP)=e(Q,P_{\mathrm{pub}}) \tag{10}$$

是否成立。如果成立，则签名 d 是有效的，否则为无效的签名。

4 安全性证明

当前在很多论文中都提出了从 Diffie-Hellman 问题到签名方案的规约[3,8~10,12]，这些规约的方法是很有效的。本节首先给出正确性推导；环签名方案必须保证真正产生签名的节点是匿名的，因此本节随后给出匿名性分析；最后在假设计算 Diffie-Hellman 问题难解的前提下，根据随机预言模型给出安全性证明。

4.1 正确性

在门限环签名方案中签名和验证阶段应该保持一致性，推导过程如下。

$$\begin{aligned}
&\prod_{i=1}^{n}e(L_iV_i,U_i+h_iP)\\
&=\prod_{i=1}^{t}e(L_iV_i,U_i+h_iP)\prod_{j=t+1}^{n}e(L_iV_i,U_i+h_iP)\\
&=\prod_{i=1}^{t}e(L_i((r_i+h_i)^{-1}S_{\mathrm{SK}}^i-L_i^{-1}t^{-1}(r_i+h_i)^{-1}U''),r_iP+h_iP)\cdot\\
&\quad\prod_{j=t+1}^{n}e(L_jL_j^{-1}(r_i+h_i)^{-1}r_jQ,r_jP+h_jP)\\
&=\prod_{i=1}^{t}e(L_iS_{\mathrm{SK}}^i-t^{-1}U'',P)\prod_{j=t+1}^{n}e(r_jQ,P)\\
&=e(\sum_{i=1}^{t}L_iS_{\mathrm{SK}}^{\mathrm{i}}-U'',P)e(\sum_{j=t+1}^{n}r_jQ,P)\\
&=e(\sum_{i=1}^{t}(L_if(i)Q-r_iQ),P)e(Q,\sum_{j=t+1}^{n}r_jP)\\
&=e(Q,\sum_{i=1}^{t}L_iP_{\mathrm{PK}}^i-U')e(Q,U')\\
&=e(Q,\sum_{i=1}^{t}L_iP_{\mathrm{PK}}^i)\\
&=e(Q,P_{\mathrm{pub}})
\end{aligned}\tag{11}$$

4.2 匿名性

环签名方案的特点之一就是匿名性，即外界无法猜测真正发布签名的节点。在有 n 个节点的群内，外界猜测签名者的身份，猜对的概率应该是 $1/n$。对于 (t,n) 门限环签名方案，外界需要从 n 个节点中猜测出 t 个真正参与签名的节点，猜测正确的概率

应该是 $\prod_{i=0}^{t-1}(t-i)/(n-i)$。

对于 $i\in\{1,\mathrm{L},t\}, j\in\{t+1,\mathrm{L},n\}$，$\{r_i\}\cup\{r_j\}$ 是从 Z_q^* 域中随机选取的，因此 $\{U_i=r_iP\}\cup\{U_j=r_jP\}$ 在域 G_1 内也是随机分布的。由于 $U'=\sum_{j=t+1}^{n}U_j$，$U''=\sum_{j=t+1}^{n}r_jQ$，因此 (U',U'') 在域 G_1 内也是随机分布的。在随机预言模型中，一般假设所有的散列函数的映射都是理论上完全随机的。$\{U_i\}\cup\{U_j\}$ 是随机预言机 H 的输入并且在域 G_1 内是随机分布的，因此随机预言机 H 的输出 $\{h_i\}\cup\{h_j\}$ 在 Z_q^* 域内也是随机分布的。

对于 t 阶多项式 $f(x)=s+a_1x+a_2x^2+\mathrm{L}+a_{t-1}x^{t-1}$，其中，$a_1,\mathrm{L},a_{t-1}\in_R Z_q^*$ 是随机选择的，因此每个节点的私钥 $S_{\mathrm{SK}}^i=f(i)Q$ 在域 G_1 内是随机分布的，并且与 $\{r_i\}$ 和 $\{h_i\}$ 是分布独立的。因此可以推断出 $\{V_i=(r_i+h_i)^{-1}S_{\mathrm{SK}}^i-L_i^{-1}t^{-1}(r_i+h_i)^{-1}U''\}\cup\{V_j=L_j^{-1}(r_j+h_j)^{-1}r_jQ\}$ 在域 G_1 内是随机分布的。

从 n 个签名者的群 S 内任意选取 t 个签名者，对于某个消息 m，签名 $\{\bigcup_{k=1}^{n}U_k,\bigcup_{k=1}^{n}V_k\}$ 都是独立且均匀随机分布。因此可以推导出敌手或者外界猜测正确生成门限环签名的 t 个签名者的概率不会超过 $\prod_{i=0}^{t-1}(t-i)/(n-i)$。

4.3　抵御存在性伪造

假定挑战者 C（挑战 CDH 问题）接收到 CDH 问题的一个随机实例 (P,aP,bP)，用 (P,A,B) 表示。挑战者 C 在不知道 a 和 b 的情况下被要求计算出 abP。挑战者 C 与概率多项式时间（PPT，probabilistic polynomial time）的伪造者 F 玩下面的游戏，在完成该游戏之后，利用伪造者 F 得到的返回信息去解决 CDH 问题。在游戏的过程中伪造者 F 可以向挑战者 C 询问随机预言机 H、密钥提取和签名的应答。

在一个 (t,n) 门限方案中，对一个秘密 a 可以利用拉格朗日系数很容易地将其分为 $\{a_1,a_2,\mathrm{L},a_n\}$。假设在一个 WSN 群 S 中任意挑选一个子群 $S_i=\{i_1,i_2,\mathrm{L},i_t\}\subset\{1,\mathrm{L},n\}$，对于任意 $i\in\{1,\mathrm{L},n\}\backslash S_i$，都可容易地计算系数 $l_{i_1},l_{i_2},\mathrm{L},l_{i_t}\in Z_q^*$ 使得等式 $a=\sum_{j=1}^{t}l_{i_j}a_{i_j}$ 成立。现在挑战者 C 和伪造者 F 开始进行如下的交互。

伪造者 F 从 WSN 群 S 中任意挑选一个有 $t-1$ 个节点的子群 S' 作为攻破的对象。为了不失一般性，假设子群 S' 包括编号为 $\{1,2,\mathrm{L},t-1\}$ 的节点。挑战者 C 进行如下步骤。

1) 随机选择 $a_1,a_2,\mathrm{L},a_{t-1}\in_R Z_q^*$。

2) 计算对应的系数 l_{i_j}，并计算 $P_{\mathrm{PK}}^i=l_{i_0}P_{\mathrm{pub}}+\sum_{j=1}^{t-1}l_{i_j}a_jP$，此处 $i=t,\mathrm{L},n$。

3) 计算 $P_{\mathrm{PK}}^i=a_iP$，此处 $i=1,\mathrm{L},t-1$。

4) 将每个节点对应的公钥 $P_{\mathrm{PK}}^i\ (i=1,\mathrm{L},n)$ 发送给伪造者 F。

对于任意一个子群 $S\in\{1,\mathrm{L},n\}$，并且子群的规模 $|S|=t$，等式 $\sum_{i\in S}L_iP_{\mathrm{PK}}^i=P_{\mathrm{pub}}$ 都是成立的。注意到挑战者 C 同样可以计算节点的私钥 $S_{\mathrm{SK}}^i=c_iQ\ (i=1,\mathrm{L},t-1)$，并将该私钥发往伪造者 F。显然，在一个有效的签名 $V_i=V_i^1+V_i^2=(r_i+h_i)^{-1}S_{\mathrm{SK}}^i-L_i^{-1}t^{-1}(r_i+h_i)^{-1}U''$ 中，V_i^1 实际上是关于 r_i 和 h_i 的签名，并且 V_i^2 是关于 U'' 的签名。因此伪造一个有效的签名 V_i 实际上就是输出一个有效的签名 V_i^1。因此可以理解为，如果一个伪造者可以输出一个有效的签名 V_i^1，那么可以很容易地伪造签名 V_i^2。但是伪造者 F 无法以一个不可忽略的概率（non-negligible probability）伪造一个合法的签名 V_i^1。

在交互之中，伪造者 F 将向挑战者 C 询问最多 q_H 次随机语言机 H 的输出答案，并询问最多 q_S 次消息/签名对，2 次询问都是相对独立进行的。粗略的讲，这些回答都是随机生成的，因此为了保证回答的一致性，挑战者 C 需要维护相应的列表保存自己的回答，以免碰撞的发生，避免伪造者 F 发现挑战者 C 的破绽。

随后伪造者 F 可以通过挑战者 C 向签名的预言机（signature oracle）发起询问。为了使得分析简单化，本节先讨论如何伪造一个有效的 V_i^1。假设第 $i\ (1\leqslant i\leqslant q_S)$ 次询问的输入是 (m_i,r_i,U_i)，伪造者 F 得到相应的签名 V_i^2。最后伪造者 F 输出一个新的签名 (m',U_i,V_i^2)。如果消息 m' 没有在前面的询问中出现，并且等式 $e(V_i^2,U_i+h_iP)=e(Q,P_{\mathrm{PK}}^i)$ 成立，那么可以宣称伪造者 F 以不可忽略的概率攻破改进的门限环签名方案。现在伪造者 F 进行类似文献[12]中的流程如下。

假设一个算法 A 执行自适应选择消息攻击改进

的门限环签名方案，并以不可忽略的概率攻破本文提出的签名方案。现构建一个算法 B 进行如下步骤。

1) 选择一个整数 $x \in \{1,2,\mathrm{L},q_S\}$。定义 $Sign(H_2(m_i,r_i,U_i)) = V_i^1$。

2) 对于 $i = 1,2,\mathrm{L},q_S$，算法 B 回应算法 A 对随机预言机 H 和签名预言机的询问。如果 $i = x$，算法 B 使用 m_x 代替 m。

3) 算法 A 输出 (m',U_i,V_i^n)。

4) 如果 $m' = m$，则签名 V_i^1 是有效的，算法 B 输出 (m,U_i,V_i^2)；否则输出“失败”并结束整个流程。

注意到 x 是随机选取的，算法 A 无法从询问的结果中得到关于 x 的任何信息。同样，只要 H 是一个随机预言机，那么算法 A 不通过询问随机预言机 H 而生成一个有效输出的概率是 $1/2^k$。设定 $P_{\mathrm{PK}}^i = A = aP$ 作为公钥，并且使得 $Q = bP$，此处挑战者 C 不知道 a 和 b 的数值。假设 $V_i^1 = (r_i + h_i)^{-1} S_{\mathrm{SK}}^i \leftarrow bP$，可以做出如下的推导：

$$V_i^1 = (r_i + h_i)^{-1} aQ \leftrightarrow V_i^1 = (r_i + h_i)^{-1} abP$$
$$\leftrightarrow abP = (r_i + h_i) bP \leftrightarrow abP = bU_i + h_i bP \quad (12)$$

从式(12)最后一步的推导可以得出结论，abP 是可以计算出来的，即解决了计算 Diffie-Hellman 问题。实际上，CDH 问题以目前的计算能力是无法解决的，与已知的事实是矛盾的。从文献[13]中，可以得到结论：敌手伪造一个有效签名的概率是可以忽略的。也就是伪造者 F 无法以不可忽略的概率生成一个有效的签名 V_i^1，进而伪造签名 V_i 的概率也是可以忽略的，从而改进的门限环签名可以抵御自适应选择消息攻击。

5 效率分析

Bresson[8]提出门限环签名方案，(t,n)门限环签名的长度是 $[2^t(n+t)\mathrm{lb}\,n]l$ bit，此处 l 是安全参数。然而本文提出的改进(t,n)门限环签名方案的签名长度是 $[2n]k$ bit，此处 k 是安全参数。一般来说，双线性配对采用的是椭圆曲线算法的 160bit 的密钥长度，而其他一般采用 1024bit。显而易见，即使采用的安全参数都是一样长度位数的前提下，本文提出的改进门限环签名方案的签名长度依然要短很多。而且在节点群个数增长的情况下，尤其是参与签名的节点数增长的情况下，Bresson 的签名长度成指数增长，而本文提出的门限环签名长度只是线性增长。

计算量较难评估，可以先考虑计算量最大的操作，如散列函数计算次数、环签名等式的验证、双线性配对计算，分别用 H、C 和 e 表示。Bresson 方案在签名生成阶段的计算量是 $2tC + (2^t \mathrm{lb}n)H$，即需要进行 $2t$ 次环签名等式验证计算和 $2^t \mathrm{lb}n$ 次散列函数运算；在签名验证阶段计算量是 $tC + (2^t \mathrm{lb}n)H$。本文提出的门限环签名方案在签名生成阶段计算量是 nH，在签名验证阶段计算量是 $nH + (n+1)e$。

表 1 计算量对比

方案	签名长度	计算量	
		签名生成阶段	签名验证阶段
Bresson 的方案	$[2^t(n+t)\mathrm{lb}n]l$	$2tC + (2^t \mathrm{lb}n)H$	$tC + (2^t \mathrm{lb}n)H$
本文提出的方案	$[2n]k$	nH	$nH + (n+1)e$

本文仿真实验运行在 Redhat9.0 环境下，以 NS2 平台为主，进行无线传感器的网络模拟，仿真 Bresson 所提方案和本文方案的能量消耗。初始网络规模为 10 个节点，随机部署。后续节点个数依次递增为 20 个、50 个、80 个直到 120 个。网络均采用 SMAC 协议和 AODV 路由协议，底层数据通信的能量消耗暂未计入，2 种方案分别独立地仿真 20 次，分别模拟在不同网络规模下的签名生成和验证，计算每个节点消耗功率的平均值作为最后的结果。在每次仿真中，每个节点初始能量 1 000J，门限值 t=n/10，在不同网络规模下的能量消耗如图 1 所示。

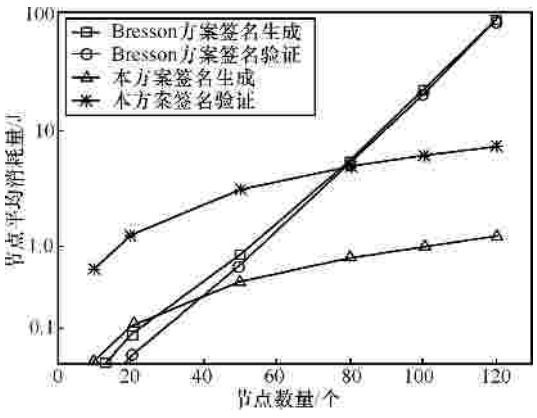

图 1 不同节点规模的平均能量消耗比较

在图 1 的比较中，纵坐标采用对数比例，可以看出在节点规模达到 50 个的时候，本文方案的签

名生成和 Bresson 方案基本持平；在节点规模达到 80 个时，本方案签名生成只有 Bresson 方案的 1/6，但是签名验证的能量消耗与 Bresson 方案持平；节点规模达到 100 个的时候，本方案签名生成只有 Bresson 方案的 1/20，签名验证只有 Bresson 方案的 1/3；节点规模达到 120 个的时候，本方案签名生成只有 Bresson 方案的 1/70，签名验证只有 Bresson 方案的 1/12。因此 Bresson 的方案计算量随着参与签名节点数量成指数增长，而本文提出的门限环签名方案计算量与群的规模成线性增长。因此在群内节点个数规模越大的时候本文提出的环签名方案计算量优势越明显。

此外本文提出的门限环签名方案可以进行并行计算，即参与签名的节点可以并行地生成部分签名，然后再将部分签名共同生成门限环签名，本文称为并行生成算法。但是绝大部分的门限环签名方案，包括 Bresson 的方案，需要参与签名的节点一个接着一个生成部分签名，这样才可以组成一个环，本文称为串行生成算法。串行生成算法产生一个环签名需要的时间非常长，增加了能量的消耗；并且如果某个节点失效，需要重新定义群内参与签名的节点次序，浪费较多的资源。因此本文提出的门限环签名方案非常适合无线传感器等自组织网络。

6　结束语

基于双线性配对，本文提出一个适用于无线传感器网络的门限签名方案，并在假设计算 Diffie-Hellman 问题困难的前提下，利用规约到矛盾的方法给出在随机预言机模型下的安全性证明。与传统的网络相比，无线传感器网络规模较大，网络节点随时可能失效，同时新旧节点的加入非常频繁，而且无线传感器网络在存储空间、移动性、计算能力和能量等方面限制，因此在需要采用认证、签名等安全技术时，本文所提的门限方案更加适合无线传感器网络。此外，本文所提方案还具有以下特点：第一，满足群合作的条件下应该具备的顽健性，可以在合作生成签名的过程中检测所有节点是否运行错误的行为和步骤，同时可以防御一些恶意的节点对整个群造成的影响；第二，多签，即群内的所有节点可以自由选择自己需要发布的消息，在签名中可以一次性对所有的消息进行签名；第三，满足分布式并行计算要求，所有参与签名节点可以并行地计算自己的部分签名，然后将部分签名组合成为门限签名。

参考文献：

[1] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret[A]. Proc ASIACRYPT'2001[C]. Berlin, Heidelberg, New York: Springer-Verlag, 2001. 552-565.

[2] GIOVANNI D C, GONZALO A, RENWEI G. Threshold cryptography in mobile ad hoc networks[A]. SCN 2004[C]. Berlin, Heidelberg, New York: Springer-Verlag, 2005. 91-104.

[3] STEFAAN S, BART P. Efficient cooperative signatures: a novel authentication scheme for sensor networks[A]. SPC 2005[C]. Berlin Heidelberg, New York: Springer-Verlag, 2005. 86-100.

[4] LIU J K, WEI V K, WONG D S. Linkable spontaneous anonymous group signature for ad hoc groups[A]. ACISP 2004[C]. Berlin, Heidelberg, New York: Springer- Verlag, 2004. 325-335.

[5] QI Z H, Y G, CHEN W, *et al*, One threshold and identity based encryption-signature scheme for WSN[J]. Journal of Nanjing University of Posts and Telecommunication(Natural Science), 2009, 29(5): 14-20.

[6] TONY K C, FUNG K, LIU J K, *et al*. Blind spontaneous anonymous group signatures for ad hoc groups[A]. ESAS 2004[C]. Springer-Verlag, Berlin Heidelberg New York, 2005. 82-94.

[7] JAVIER H, GERMAN S. Ring signature schemes for general Ad-Hoc access structures[A]. ESAS 2004[C]. Berlin, Heidelberg, New York: Springer-Verlag, 2005. 54-65.

[8] BRESSON E, STERN J, SZYDLO M. Threshold ring signatures and applications to ad-hoc groups[A]. Proc CRYPTO 2002[C]. Berlin, Heidelberg, New York: Springer- Verlag, 2002. 465-480.

[9] BENOIT L, QUISQUATER J J. Efficient revocation and threshold pairing based cryptosystems[A]. Proceedings of the Annual ACM Symposium on Principles of Distributed Computing (PODC 2003)[C]. New York, 2003. 163-171.

[10] SHERMAN C, LUCAS C K, YIU S M. Identity Based Threshold Ring Signature[A]. ICISC 2004[C]. Berlin, Heidelberg, New York: Springer-Verlag, 2005. 218-232.

[11] YAO M, MATT H, GREG M, *et al*. A mobile agent system providing offer privacy[A]. ACISP2004[C]. Berlin, Heidelberg, New York: Springer-Verlag, 2004. 301-312.

[12] LIAO J, XIAO J f, QI Y H, *et al*. ID-based signature scheme without trusted PKG[A]. CISC 2005[C]. Berlin, Heidelberg, New York: Springer-Verlag, 2005. 53-62.

（下转第 89 页）