* 1

一种适于 Ad hoc 网络恶意节点处理的多接收者签密算法

魏　靓，　郑连清，　张串绒，　崔晓臣
(空军工程大学电讯工程学院,陕西　西安　710077)

摘要　基于身份的多接收者签密算法是基于身份签密算法的扩展,是近来研究的热点。首先基于双线性对提出一个基于身份的多接收者签密算法,并对其安全性和效率进行了分析和比较;结果表明:在随机预言机模型下,该算法是可被证明安全的,而且其计算量和传输量小、效率高,特别适合 Ad hoc 网络的安全通信。最后,以处理 Ad hoc 网络中恶意节点为例,阐述了将基于身份的多接收者签密算法用于 Ad hoc 网络安全通信的方法。同时,这种签密算法的提出能更好地满足实际应用的高安全需求,具有一定应用价值。

关键词　Ad hoc 网络;多接收者签密;可证明安全;基于身份;双线性对
DOI　10.3969/j.issn.1009－3516.2011.01.015
中图分类号　TN918.1　　**文献标识码**　A　　**文章编号**　1009－3516(2011)01－0068－05

移动 Ad hoc 网络(Mobile Ad Hoc Network, MANET)是由若干无线移动节点组成的不依赖于任何固定基础设施,通过节点间的相互协作进行网络互联的一种临时性自组织系统[1]。它具有广阔的应用前景,但由于其动态拓扑、无线通信的特点,容易遭受各种安全威胁,因而 Ad hoc 网络的安全是亟待解决的问题,尤其如何处理恶意节点是研究的热点,这就要求为此设计专门的安全算法。

签密能够在一个逻辑步骤内同时完成签名和加密 2 项工程,而且其通信成本和计算量远远低于传统的"先签名后加密"。多接收者签密以安全和认证的方式广播一个消息给多个接收者,每个接收者都可以独自解签并获得明文。在处理 Ad hoc 网络恶意节点时,需要将信息同时发送给多名接收者,并且要确保信息的机密性和可认证性,因此构建一种基于身份的多接收者签密算法,对提高 Ad hoc 网络的安全性和效率具有重要作用。

1　多接收者签密算法的形式化定义

1.1　安全概念

一个基于身份的多接收者签密算法由以下 4 部分组成[2]:①系统建立;②密钥提取;③签密;④解签密。文献[3]定义了一种基于身份签密算法的安全概念,具体如下:

定义 1　保密性:如果没有任何多项式有界的敌手以一个不可忽略的优势赢得以下游戏,则称一个基于身份的多接收者签密算法在适应性选择密文攻击下是不可区分的(IND－IBMRSC－CCA2)。

1)初始化阶段:挑战者 C 输入安全参数 k,运行系统建立算法,并将系统参数 params 发送给敌手 A。

2)询问阶段:敌手 A 执行以下多项式有界次适应性询问。①密钥提取询问:敌手 A 选择一个身份 ID_U,挑战者 C 计算 $S_u=\mathrm{Extract}(\mathrm{ID}_U)$ 并将结果发给 A。②签密询问:敌手 A 选择一个身份 ID_i 和多个 $\mathrm{ID}_j(j=1,2,\cdots,n)$,一个明文 m。挑战者 C 计算 $\sigma=\mathrm{signcrypt}(m,S_{\mathrm{ID}_i},(\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n))$,并将结果 σ 发送给 A。③解签密询问:A 选择一个身份 ID_i 和一个密文 σ。挑战者 C 首先计算私钥 $S_{ID_j}=\mathrm{Extract}(\mathrm{ID}_j)(j\in[1,n])$ 并发送

* **收稿日期**:2010－09－06
基金项目:国家自然科学基金资助项目(60873233);陕西省科技攻关基金资助项目(2008－k04－21)
作者简介:魏　靓(1980－),女,山东青岛人,博士生,主要从事无线网络安全、密码学研究.
E－mail:weijing0619@163.com

unsigncrypt(σ, S_{ID_j}, ID_i)的结果给敌手 A。

3)敌手 A 输出 2 个相同长度的明文 m_0, m_1 以及 1 个身份 ID_A。ID_A 不能是在 2)中已经执行过密钥提取询问的身份。挑战者 C 随机选择 1 个 $b \in \{0,1\}$,计算 $\sigma = \text{signcrypt}(m, S_A, (ID_1, ID_2, \cdots, ID_n))$,将 σ 发送给 A。

4)猜测阶段:A 像 2)中那样,再次执行多项式有界次询问。但是它不能对 ID_A 和 $ID_i (i \in [1,n])$ 执行私钥提取询问,也不能对密文 σ 执行解签密询问。

5)最后阶段:A 输出一个值 b作为对 b 的猜测。如果 $b' = b$,A 赢得游戏。那么 A 赢得上述游戏的优势定义为 $\text{Adv}(A) = |2P[b' = b] - 1|$。

定义 2　不可伪造性:如果不存在任何多项式有界的敌手以一个不可忽略的优势赢得以下游戏,则称一个基于身份的多接收者签密方案在适应性选择消息攻击下是存在性不可伪造的(EUF - IBMRSC - CMA)。

1)初始化阶段:挑战者 C 输入安全参数 k,运行系统建立算法,并将系统参数 params 发送给敌手 A。

2)询问阶段:A 类似保密性定义中那样执行多项式有界次询问。

3)最后阶段:A 输出一个新元组$(\sigma, ID_A, (ID_1, ID_2, \cdots, ID_n))$,且这个新元组不是询问阶段签密预言机的输出,$ID_A$ 也不是询问阶段的密钥提取预言机的输出。如果 unsigncrypt(σ, ID_A, S_{ID_j})的结果不是符号 $\perp$,则 A 赢得游戏。A 的优势为他获胜的概率:$\text{Adv}(k) = \Pr[\text{win}(A)]$

1.2　双线性对

令 G_1 为由 P 生成的循环加法群,阶为 q,G_2 为具有相同阶 q 的循环乘法群,a, b 是 Z_q^* 中的元素。双线性对[4]是指满足下列性质的一个映射 $e: G_1 \times G_1 \to G_2$:

1) 双线性性:对 $\forall P, Q \in G_1$,有 $e(aP, bQ) = e(P, Q)^{ab}$;

2) 非退化性:若 $P \in G_1$,对于 $\forall Q \in G_1$,只有 $P = o$ 时,才有 $e(P, Q) = 1$;

3) 可计算性:对 $\forall P, Q \in G_1$,存在有效的算法计算 $e(P, Q)$。

双线性(Diffie - Hellman, BDH):对于 $a, b, c \in Z_q^*$,由 $<P, aP, bP, cP>$ 计算 $e(P, P)^{abc}$。

确定性双线性(Diffie - Hellman, DBDH):对于 $a, b, c \in Z_q^*$,由 $<P, aP, bP, cP>$ 和 $h \in G_2$ 判断 $h = e(P, P)^{abc}$ 是否成立。

2　基于身份的多接收者签密算法(IDMRSC)

系统参数:给定一个安全参数 k,PKG 选择椭圆曲线上 2 个阶为 q 的循环群$(G_1, +)$和$(G_2, \cdot)$,G_1 的生成元为 P,$e: G_1 \times G_1 \to G_2$ 为一个双线性映射。PKG 随机选择一个主密钥 $s \in Z_q^*$,计算 $P_{pub} = sP$,一个安全的对称密码算法(E, D),3 个安全的 Hash 函数 $H_1: \{0,1\}^{l_1} \to G_1$, $H_2: \{0,1\}^l \times G_1 \to Z_q^*$ 以及 $H_3: G_2 \to (0,1)^l$,其中 l_1 是身份 ID 的比特长度,l 是明文比特长度。PKG 公布系统参数 params = $\{G_1, G_2, n, e, P, P_{pub}, H_1, H_2, H_3\}$,并保密主密钥 s。

密钥提取:给定一个用户 U 的身份 ID_U,PKG 计算该用户的私钥 $S_U = sQ_U$,其中,$Q_U = H_1(ID_U)$ 为该用户的公钥。

签密:为了发送消息 m 给 n 个身份为$(ID_{R_1}, ID_{R_2}, \cdots, ID_{R_n})$的接收者,Alice 执行以下的步骤:

①随机选择 $r \in Z_q^*$,$K \in (0,1)^l$;②计算 $U = rP$ 和 $h_1 = H_2(U \| m)$;③计算 $Z = rP_{pub} + h_1 S_A$;④计算 $V = E_K(m \| Z)$;⑤计算 $N_i = K \oplus H_3(\omega)$,其中 $\omega = e(rP_{pub}, Q_{R_i}) (i = 1, 2, \cdots, n)$。

密文为 $\sigma = (U, V, N_1, N_2, \cdots, N_n, L)$,$L$ 是一个标签,包含了 N_i 是怎样联系到每个接收者的信息。

解签密:当收到 σ,身份为 $ID_{R_i} (i \in [1,n])$的接收者执行以下步骤:①根据 L 找到适当的 N_i;②计算 $\omega = e(U, S_R)$;③计算 $K = N_i \oplus H_3(\omega)$;④恢复消息 $m \| Z = D_K(V)$;⑤计算 $h_1 = H_2(U \| m)$;⑥当且仅当等式 $e(Z, P) = e(U + h_1 Q_A, P_{pub})$ 成立时接受此消息,否则返回符号 $\perp$。

算法的正确性证明: $\omega = e(rP_{pub}, Q_{R_i}) = e(rsP, Q_{R_i}) = e(rP, sQ_{R_i}) = e(U, S_{R_i}))$

$e(Z, P) = e(rP_{pub} + h_1 S_A, P) = e(rsP + h_1 sQ_A, P) = e(rP + h_1 Q_A, sP) = e(U + h_1 Q_A, P_{pub})$

3 安全性分析与性能评价

3.1 安全性分析

3.1.1 机密性

结论 1 在随机预言模型中,若存在一个 IND-IBMRSC-CCA 敌手 A 能够在 t 时间内,以 ε 的优势赢得**定义 1** 中的游戏,那么,就存在一个算法 Γ(它最多能进行 q_{H_i} 次 H_i 询问($i=1,2,3$),q_E 次密钥提取询问,q_S 次签密询问和 q_U 次解签密询问)能够在 $t' < t + (q_s + 3q_U)t_e$ 时间内,以 $\varepsilon' > \varepsilon \frac{1}{C_{q_1}^n}\frac{1}{q_2}\left(1-q_s\frac{q_2+q_3}{2^k}\right)\left(1-\frac{q_2 q_u}{2^k}\right)$ 的优势解决 BDH 问题,其中 t_e 表示计算一次双线性对运算所需要的时间。

证明:我们假设 Γ 接收一个 BDH 问题的随机实例$(P,aP,bP,(c_1P,c_2P,\cdots,c_nP))$。他的目标是计算出 $e(P,P)^{abc_i}(i\in[1,n])$是否成立,算法 Γ 将敌手 A 作为它的子程序利用。A 向 Γ 询问随机预言 $H_i(i=1,2,3)$,Γ 维持 3 个列表 L_1,L_2,L_3 来存储这些回答。Γ 把包括 $P_{\text{pub}}=aP$ 的系统参数发送给 A(Γ 并不知道 a,这个值模拟 *PKG* 的主密钥)。假设 A 不会做重复的询问。

H_1 询问:敌手 A 对 H_1 进行多项式有限次询问。若 $\mathrm{ID}=\mathrm{ID}_{R_i}^*(i=1,2,..,n)$,则回答 $H_1(\mathrm{ID}_{R_i}^*)=c_iP$,否则,对于其他的 ID 询问,$\Gamma$ 从 Z_q^* 中随机取一值 d_e,计算 $Q=d_eP$,并将(ID_e,d_e)添加到 L_1 中,给出回答值 Q。

H_2 询问:对于一个 $H_2(U_e\|m_e)$ 询问,Γ 首先检查列表 L_2 中是否存在$(U_e\|m_e,h_{1e})$,如果含有该条目,Γ 把回答 h_{1e} 输出给 A;否则,从 Z_q^* 中随机选择一个 h_1,将$(U_e\|m_e,h_1)$添加到 L_2 中并输出 h_1 给 A。

H_3 询问:对于一个 $H_2(\omega_e)$ 询问,Γ 首先检查列表 L_3 中是否存在(ω_e,h_e),如果含有该条目,Γ 把回答 h_e 输出给 A;否则,从 $\{0,1\}^n$ 中选择一个随机串 h,将(ω_e,h)添加到 L_3 中。

密钥提取询问:当 A 询问 Extract(ID)时,如果 $\mathrm{ID}=\mathrm{ID}_{R_i}^*(i\in[1,n])$,那么 Γ 将失败并终止模拟;否则,在列表 L_1 选中查找对应的条目(ID_e,d_e),Γ 计算 ID 的公钥 $Q_e=d_eP$ 和私钥 $S_e=d_eP_{\text{pub}}=d_eaP$ 并发给 A。

签密询问:A 选择一个明文 m,发送者身份 ID_A 和接收者 $\mathrm{ID}_{R_i}(i=1,2,\cdots,n)$进行签密询问。情况 1:如果 $\mathrm{ID}_A\neq\mathrm{ID}_{R_i}^*(i\in[1,n])$,$\Gamma$ 可以通过密钥提取算法计算出 Q_A 和私钥 S_A,然后简单地运行签密运算即可。情况 2:如果 $\mathrm{ID}_A=\mathrm{ID}_{R_i}^*$,$\mathrm{ID}_{R_i}\neq\mathrm{ID}_{R_i}^*(i\in[1,n])$,$\Gamma$ 按如下过程模拟签密:首先从 Z_q^* 中随机选取 r 和 h_1,计算 $U'\leftarrow h_1(P-Q_A)$,$Z'\leftarrow h_1P_{\text{pub}}$,将$(U1\|m,h_1)$添加到 L_2 中,然后在 L_1 中找到$(\mathrm{ID}_{R_i},d_{ei})$,根据密钥提取询问得到 $Q_{R_i}\leftarrow d_{ei}P$ 和 $S_{R_i}\leftarrow d_{ei}P_{\text{pub}}\leftarrow d_{ei}aP$,计算 $\omega'\leftarrow e(U',S_{R_i})$,选取 $K'\in(0,1)^*$,计算 $N_i'\leftarrow K'\oplus H_3(\omega')$($H_3(\omega')$可以从上述的 H_3 询问获得),最后计算 $V'\leftarrow E_{K'}(m\|Z')$ 并将签密密文 $\sigma=(U',V',N_1',N_2',\cdots,N_n',L)$ 发送给 A。

解签密询问:A 对一个密文 $\sigma=(U',V',N_1',N_2',\cdots,N_n',L)$ 和发送者身份 ID_A 进行解签密询问,当 $\mathrm{ID}_{R_i}\neq\mathrm{ID}_{R_i}^*(i\in[1,n])$时,$\Gamma$ 首先计算 $\omega'\leftarrow e(U',S_{R_i})$(定义 $H_3(\omega')=h'$),查找(ω',h')是否在 L_3 中,如果 L_3 条目中存在这个二元组,则计算 $K'\leftarrow N_i'\oplus H_3(\omega')$,$m\|Z'\leftarrow D_{K'}(V')$,$h_1'\leftarrow H_2(U1\|m)$,然后遍历列表 L_2,如果找到一个二元组$(U1\|m,h_1')$并使得 $e(Z',P)=e(U'+h_1'Q_A,P_{\text{pub}})$ 成立,则解签密恢复出 m;如果不存在这样一个二元组,Γ 返回符号 $\perp$。当 $\mathrm{ID}_{R_i}=\mathrm{ID}_{R_i}^*(i\in[1,n])$时,遍历中 L_3 的条目(ω_e,h),对于每一个 ω_e 计算 $K'\leftarrow N_i'\oplus H_3(\omega_e)$,$m\|Z'\leftarrow D_{K'}(V')$,得到 m,如果 $U1\|m$ 是 L_2 中的元素,则计算 $h_1'\leftarrow H_2(U1\|m)$,如果等式 $e(Z',P)=e(U'+h_1'Q_A,P_{\text{pub}})$ 成立,则返回消息 m。

在第 1 阶段末,A 输出 2 个明文 m_0 和 m_1,一个发送者身份 ID_A,要求进行接收者身份为$(\mathrm{ID}_{R_1},\mathrm{ID}_{R_2},\cdots,\mathrm{ID}_{R_n})$的密文挑战。如果$(\mathrm{ID}_{R_1},\mathrm{ID}_{R_2},\cdots,\mathrm{ID}_{R_n})\neq(\mathrm{ID}_{R_1}^*,\mathrm{ID}_{R_2}^*,\cdots,\mathrm{ID}_{R_n}^*)$,则 Γ 终止模拟。否则,Γ 随机选择 $b\in\{0,1\}$进行签密 m_b,令 $U^*=bP$,随机选择 $N_1^*,N_2^*,\cdots,N_n^*\in\{0,1\}^n$,$V^*\in\{0,1\}$,提交挑战密文 $\sigma^*=(U^*,V^*,N_1^*,N_2^*,\cdots,N_n^*,L)$ 给 A。

A 经过第 2 轮的询问,这些询问同第 1 轮相同。在模拟最后,A 产生 1 个 b' 作为对 b 的猜测。如果 $b'=b$,Γ 输出 $\omega^*=e(U^*,S_{R_i}^*)=e(bP,caP)=e(P,P)^{abc_i}$ 作为 BDH 问题的答案,否则 Γ 没有解决问题。

下面计算 Γ 成功的概率。如果 A 在第 1 阶段对 $\mathrm{ID}_{R_i}^*(i\in[1,2,\cdots,n])$执行 Extract 询问,$\Gamma$ 将失败。A 选择 $\mathrm{ID}_{R_i}^*(i\in[1,2,\cdots,n])$的方法有 $C_{q_1}^n$ 种,因此不对 $\mathrm{ID}_{R_i}^*$ 执行 Extract 询问的概率大于 $1/C_{q_1}^n$。在第 2 阶段,

如果 A 对 $\omega = e(P,P)^{abc_i}$ 进行 H_3 询问,Γ 将失效,在对 H_3 的 q_3 次询问中 A 不对 $\omega = e(P,P)^{abc}$ 进行 H_3 询问的概率大于 $1/q_2$。在对签密的 q_s 次询问中,失败的概率最多为 $q_s(q_2+q_3)2^k$。一个合法的密文在解签密询问中被拒绝的概率为 $q_3 q_u/2^k$,所以 Γ 的成功解决 BDH 问题的概率至少是 $\varepsilon \frac{1}{C_{q_1}^n}\frac{1}{q_2}\left(1-q_s\frac{q_2+q_3}{2^k}\right)\left(1-\frac{q_3 q_u}{2^k}\right)$。在 Γ 计算时间方面,每次签密询问需要 1 次双线性对运算,解签密询问需要 3 次双线性对运算。

3.1.2　不可伪造性

我们的方案在适应性选择消息攻击下能抗存在性伪造。如果一个敌手能伪造我们的签名,则它也能够伪造签名方案,这个方案是 Hess 方案[5]的一个变体。

3.1.3　公开验证性

只需提交 (m,U,V,K) 给第 3 方验证者,验证者计算 $h_1 = H_2(U\|m)$,$m\|Z = D_K(V)$,检验等式 $e(Z,P) = e(U+h_1 Q_A, P_{pub})$ 是否成立即可,此过程不需要接收者的私钥。

3.1.4　前向安全性

如果 Alice 的私钥 S_A 泄露,敌人也不能计算出 ω 的值,因而得不到以前的会话内容,所以方案满足前向安全性。

3.1.5　不可否认性

既然本文的签密方案是不可伪造的,如果接收者能出示消息的签名,则 Alice 就无法否认发送过这个消息。

3.2　效率分析

与已有基于身份的签密算法签密 n 次相比,我们的方案有更高的效率。用 P,M,E 来分别表示双线性对,标量乘和指数运算。表 1 给出我们的方案与使用目前已有的 3 个重要基于身份的签密算法[4,6-7]签密 n 次的效率比较,可以看出我们的方案高效得多(本文没有考虑预计算)。

表 1　效率比较

Tab. 1　The efficiency compares

方案	计算量	通信量
方案[4]	$4nM+nE+3nP$	$2n\|G_1\|+n\|m\|$
方案[6]	$3nM+6nP$	$n\|G_1\|+n\|m\|+n\|q\|$
方案[7]	$4nM+3nE+5nP$	$2n\|G_1\|+n\|m\|$
本文中的方案	$4M+(2n+2)P$	$\|G_1\|+\|m\|+nl$

4　IDMRSC 在处理 Ad hoc 网络恶意节点中的应用

对 Ad hoc 网络来说,任意节点都有被破坏或俘获的可能。为了抵抗被俘获节点的内部攻击,采用下面的措施:假定每个节点都具有某种监视机制,例如入侵检测机制,可以监视其一跳邻居节点[8]。每个节点维护一种恶意节点列表,表中每项包括的内容有:<被投诉节点 ID,被投诉节点状态 state,被投诉次数 count,投诉节点列表 List>,其中被投诉节点状态 state 为恶意或可疑。根据具体安全需求,选定门限值 k_1。如果某节点被投诉次数 count 大于 k_1 则认为该节点可能已被敌人俘获,将被投诉节点的状态置为“恶意”,否则被投诉节点状态为“可疑”。投诉节点列表 List 记录着所有投诉者的 ID。

当一个节点 A 发现其邻居节点 B 有恶意行为,需要发送警告消息 Warning $<ID_B>$ 广播至全网,此时采用文中给出的多接收者签密算法,警告信息 m = Warning $<ID_B>$,接收者为 $ID_1, ID_2, \cdots, ID_n$,节点执行 singcrypt$(m, S_A, (ID_1, ID_2, \cdots, ID_n))$,得到签密密文 σ。每一个接收者收到密文后,运行 unsigncrypt(σ, ID_A, S_{ID_i}) 得到警告消息。首先检查恶意节点列表看投诉节点状态是否为可疑,是则丢弃该消息,否则继续。然后验证签名,如果签名不正确,则认为该投诉无效,否则继续。如果被投诉节点未在恶意节点列表中,则为该节点建立表项,并将投诉节点列入该节点的投诉列表中,将被投诉次数置为 1,状态置为可疑;否则(被投诉节点已经在恶意节点列表中),将被投诉节点的被投诉次数加 1,将投诉节点列入该节点的投诉列表中,并检查 count 是否达到门限值 k_1,如果 count 已经达到门限值,则该节点的状态被标识被“恶意”。由于采用多接收者的签密算法,无需为每一个接收者发送一次签密消息,从而减少了计算量和通信量,节省了带宽资源,适合在 Ad hoc 环境下运行。

5 结束语

在随机预言机模型下,利用本文提出的多接收者签密算法可抗适应性选择密文与身份攻击,且满足不可伪造性、前向安全性和公开验证性,与使用已有签密算法签密多次相比,其低计算量和传输需求能很好地满足 Ad hoc 网络通信的要求。基于身份的多接收者签密算法不仅适于处理 Ad hoc 网络中恶意节点的问题,而且适用于国家政府或情报部门签署机密文件发送给一些特定的机构或具有一定级别的官员,因而应该得到广泛的应用。

参考文献:

[1] 陈林星,曾曦,曹毅. 移动 Ad hoc 网络[M]. 北京:电子工业出版社,2006.
CHEN Linxing, ZENG Xi, CAO Yi. Mobile Ad hoc network [M]. Beijing: Electronic industry publishing house, 2006. (in Chinese)

[2] Du H Z, Wen Q Y. An efficient identity - based multi - recipient signcrypytion scheme [J]. Journal of Shenzhen university science and engineering, 2009, 26(2): 127 - 132.

[3] Libert B, Quisqusater J. A new identity based signcryption schemes from pairings [C]//2003 IEEE information theory workshop. Paris: IEEE press, 2003: 155 - 158.

[4] 张串绒,张玉清. 基于身份的前向安全和可公开验证签密方案[J]. 空军工程大学学报:自然科学版, 2009, 10(3): 78 - 81.
ZHANG Chuanrong, ZHANG Yuqing. Identity based signcryption scheme with forward security and public verifiability[J]. Journal of air force engineering university: natural science edition, 2009, 10(3): 78 - 81. (in Chinese)

[5] Florian, Hess. Efficient identity based signature schemes based on pairings[J]. Computer science, 2003, 2595: 310 - 324.

[6] Sherman S W, Chow S M, Lucas C K, et al. Efficient forward and provably secure ID - based signcryption scheme with public verifiability and public ciphertext authenticity[C]//Information security and cryptology ICISC 2003, LNCS 2971. Berlin: Springer - verlag, 2004: 352 - 369.

[7] 李发根,胡予濮,李刚. 一个高效的基于身份的签密方案[J]. 计算机学报, 2006, 29(9): 1641 - 1647.
LI Fagen, HU Yupu, LI Gang. An efficient identity - base signcryption scheme[J]. Journal of computers, 2006, 29(9): 1641 - 1647. (in Chinese)

[8] 李光松,韩文报. 分簇 Ad hoc 网络的密钥管理[J]. 计算机科学, 2006, 33(2): 79 - 84.
LI Guangsong, HAN Wenbao. Cluster - based key management in Ad hoc networksp[J]. Computer science, 2006, 33(2): 79 - 84. (in Chinese)

(编辑:徐楠楠)

Multi - recipient Signcryption Algorithm for Dealing with Malicious Nodes of Ad hoc Networks

WEI Jing, ZHENG Lian - qing, ZHANG Chuan - rong, CUI Xiao - chen
(Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China)

Abstract: Identity - based multi - recipient signcryption (IDMRSC) is an extension of identity - based signcryption. At first, a new IDMRSC algorithm is proposed based on bilinear pairings and its security and efficiency are analyzed. The result shows that the algorithm is provable secure in the random oracle model. Furthermore, the algorithm is significantly efficient and of low computation cost and communication overhead, and is very suitable for secure communication in Ad hoc networks. Finally, the method of using IDMRSC algorithm to deal with malicious nodes in Ad hoc networks is expounded. This IDMRSC algorithm can meet the high level secure requirement in practical application and therefore, is of a certain practical value in application.

Key words: Ad hoc networks; multi - recipient signcryption; provable security; identity - based; bilinear pairing