

一种基于 Waters-IBE 的在线/离线加密方案

王昱菲, 杨 庚

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要: 针对无线传感器网络中传感器节点能量和计算能力的局限性, 本文在 Waters-IBE 的基础上, 提出了一种基于身份的在线/离线加密算法. 该算法将加密过程划分为两个阶段: 离线阶段和在线阶段. 离线阶段由 PKG 或基站完成, 在获得接收者身份和将要加密的消息之前可进行大量复杂运算; 在线阶段在节点中只需进行简单运算就可加密消息. 在完全模型下可证明算法是 CPA 安全的. 仿真实验表明, 算法减轻了节点中的运算量并降低了运算时间, 从而更加适用于无线传感器网络.

关键词: 在线/离线加密; 基于身份; Waters-IBE; 无线传感器网络

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)11-0042-03

A Scheme of Online/Offline Encryption Based on Waters-IBE

WANG Yu-fei, YANG Geng

(College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: In this paper, we propose an identity-based online/offline encryption based on Waters-IBE, because of the limited computation and storage power of sensor nodes. This algorithm splits the encryption process into two phases: the offline and online parts. In the offline stage, all heavy computation can be done by PKG or base station prior to knowing the message and the recipient, the online stage can be conducted efficiently with some light computation to encrypt a message once the message and the recipient's identity become available. We have proved this algorithm could reach CPA security under the full model. What's more, the simulation results indicate that our algorithm reduces the requirement of computation and decrease the computation time in sensor nodes, so it is more suitable for applications in wireless sensor network.

Key words: online/offline encryption; identity-based; Waters-IBE; wireless sensor network

1 引言

无线传感器网络是由大量传感器节点自组织形成的无线网络, 由于无线通信的特性, 无线传感器网络易受攻击, 所以对于敏感数据的隐私保护成为首要任务. 传感器节点在存储量、能耗、计算能力方面的局限性要求加密算法计算量小且低能耗. 文献[1]首先提出基于身份的加密的理念和第一个基于身份的签名方案. 文献[2]提出了基于身份的“在线/离线”签名算法. 文献[3]提出了基于身份的在线/离线

加密算法.

目前基于身份的在线/离线加密方案 (Identity-Based Online/Offline Encryption, IBOOE) 通常有四种, Guo, Mu, Chen 提出了最早的两个 IBOOE 方案^[3]. 文献[4]在随机预言机模型下提出了第一种 IBOOE 方案, 达到 CPA 安全. 文献[5]基于选择身份模型提出了限制接收者个数 n 的 RB-OOIBE 方案.

本文对现有的 IBE 算法 Waters-IBE^[6] 进行改进, 在完全模型下给出了一种有效的 IBOOE 算法,

收稿日期: 2012-05-10; 修回日期: 2012-06-16

基金项目: 国家自然科学基金项目 (60873231); 江苏省自然科学基金项目 (BK2009426); 江苏省研究生培养创新工程项目 (CXLX11_0416, CXZZ11_0402, CXZZ_0402, CX10B_195Z)

解密过程只需 4 次配对,存储需求更少,计算量更小,经证明达到 CPA 安全。

2 预备知识

2.1 双线性映射

G 和 G_T 是两个阶为 p 的乘法循环群,其中 p 为素数, g 是 G 的一个生成元。如果映射 $e: G \times G \rightarrow G_T$ 满足下列条件,则称 e 为双线性映射^[1]:

- (1) 如果对所有的 $x, y \in G, a, b \in Z$, 都有 $e(x^a, y^b) = e(x, y)^{ab}$ 。
- (2) 非退化性: 存在 $P, Q \in G$, 使得 $e(P, Q) \neq 1$ 。
- (3) 可计算性: 有一个多项式时间算法来计算 $e(P, Q)$ 。

2.2 复杂性假设

判定性 BDH 问题: 挑战者随机选取 $a, b, c, z \in Z_p$ 并抛掷硬币 β 。如果 $\beta=1$ 则输出元组 $(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^{abc})$ 。否则, 如果 $\beta=0$, 挑战者输出元组 $(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^z)$ 。接下来敌手必须给出对 β 的猜测值 β' 。如果 $|Pr[B(g, g^a, g^b, g^c, e(g, g)^{abc})=1] - Pr[B(g, g^a, g^b, g^c, e(g, g)^z)=1]| > 2\epsilon$, 那么敌手 B 能以至少 ϵ 的优势解决判定性 BDH 问题^[6]。

判定性 BDH 假设: 如果不存在多项式时间敌手能以至少 ϵ 的优势解决上述 BDH 问题, 那么就认为判定性 BDH 问题成立。

3 WSN 中基于身份的在线/离线加密方案具体实现

令 G, G_T 为 p 阶循环群, $e: G \times G \rightarrow G_T$ 是双线性映射。用户的身份被表示为一个 n 比特的字符串。 p 是一个大素数, 以确保 G, G_T 中的离散对数问题难解。

在此, 我们提出一种 WSN 中基于 Waters-IBE 的在线/离线加密的具体实现方案:

Setup: KGC(Key Generation Center) 执行以下操作:

随机选取 $\alpha \in Z_p$, 从 G 中随机选取一生成元 g , 令 $g_1 = g^\alpha$ 。从 G 中随机选取元素 g_2, u' 以及 $u_1, u_2, \dots, u_n$ 。记 $U = (u_1, u_2, \dots, u_n)$ 。

公开参数是 $\text{params} = (g, g_1, g_2, u', U, D)$, 主密钥 $\text{msk} = g_2^\alpha$ 。

KeyGen: 用户身份 $ID \in \{0, 1\}^n$, 令 v 为用户身

份的比特表示, v_i 是 v 的第 i 比特, $V \subseteq \{1, 2, \dots, n\}$ 是使得 $v_i = 1$ 的 i 的集合。为了生成用户的私钥, KGC 首先随机选取 Z_p 中的一个元素 r , 然后生成相应的私钥 d_v 如下:

$$d_v = (g_2^\alpha (u' \prod_{i \in V} u_i)^r, g^r).$$

Offline-Encrypt: 随机选取 $t \in Z_p, h \in G$ 。

$$C_{of} = \langle e(g_1, g_2)^t, g^t, e(g_1, h)^t, g^r, h^\alpha g_1^r \rangle \\ = \langle c_1', c_2, c_3, c_4, c_5 \rangle$$

存储 C_{of}, t 供在线加密阶段使用。

Online-Encrypt: 发送者对于消息 $M \in \{0, 1\}^n$ 和身份为 ID 的接收者, 计算 $Q_{ID} = u' \prod_{i \in V} u_i$ 。

$$\text{输出 } C_m = \langle M \cdot e(g_1, g_2)^t, Q_{ID} \rangle = \langle c_1, c_6 \rangle.$$

对应于身份 ID 的最终密文是:

$$C_v = \langle M \cdot e(g_1, g_2)^t, g^t, e(g_1, h)^t, g^r, h^\alpha g_1^r, \\ Q_{ID} \rangle = \langle c_1, c_2, c_3, c_4, c_5, c_6 \rangle$$

Decrypt: $C_v = \langle c_1, c_2, c_3, c_4, c_5, c_6 \rangle$ 是身份 $ID \in \{0, 1\}^n$ 的有效密文。接收者利用其私钥 d_{ID} 解密 C_v 。

验证等式是否成立: $c_3 = \frac{e(c_2, c_5)}{e(c_2^\alpha, c_4)}$ 。如果不成立, 输出 $\perp$; 否则, 计算消息 $M = c_1 \cdot \frac{e(d_2, c_6)^t}{e(d_1, c_2)^t}$ 。

解密正确性:

$$c_1 \cdot \frac{e(d_2, c_6)^t}{e(d_1, c_2)^t} = M \cdot e(g_1, g_2)^t \cdot \frac{e(g^r, Q_{ID})^t}{e(g_2^\alpha Q_{ID}^r, g^t)} \\ = M \cdot e(g_1, g_2)^t \cdot \frac{e(g^r, Q_{ID}^t)}{e(g_2^\alpha, g^t) e(Q_{ID}^r, g^t)} = M$$

一致性验证:

$$\frac{e(c_2, c_5)}{e(c_2^\alpha, c_4)} = \frac{e(g^t, h^\alpha g_1^r)}{e(g^{t\alpha}, g^r)} \\ = \frac{e(g^t, h^\alpha) e(g^t, g_1^r)}{e(g_1^t, g^r)} = e(g^t, h^\alpha) \\ = e(g_1, h)^t = c_3$$

4 安全性证明

定理 如果判定性 $(t + O(\epsilon^{-2} \ln(\epsilon^{-1}) \lambda^{-1} \ln(\lambda^{-1})), \frac{\epsilon}{32(n+1)q})$ BDH 假设成立, 其中 $\lambda = \frac{1}{8(n+1)q}$, 那么以上 IBOOE 方案是 (t, q, ϵ) 安全的。

证明: 假设存在一个 (t, q, ϵ) -敌手 A 挑战该方案, 我们构建一个挑战者 B 来进行判定性 BDH 游戏攻击。挑战者 B 接收 BDH 挑战攻击 $(g, A=g^a, B=g^b, C=g^c, Z)$, 无论挑战者攻击是不是 BDH 元组都输出一个猜测值 β' , 挑战者执行以下步骤:

Setup: 挑战者首先设置一个整数 $m=4q$, 并从 0 到 n 之间随机选取一个整数 k , 然后选取一个长度为 n 的随机向量 $\vec{x}=(x_i)$, 其中 $\vec{x}$ 中的元素是均匀地从 0 到 $m-1$ 之间随机选取的, x' 也是均匀地从 0 到 $m-1$ 之间随机选取的. 令 X^* 表示 $(x', \vec{x})$ 对. 另外挑战者还随机选取 $y' \in Z_p$ 和一个长度为 n 的向量 $\vec{y}=(y_i)$, 其中 $\vec{y}$ 中的元素是在 Z_p 中随机选取的. 这些值都是由挑战者本身保存的. 同样, 对于身份 v , 令 $V \subseteq \{1, \dots, n\}$ 是所有 $v_i=1$ 的 i 的集合.

为简化分析, 我们需要定义三个函数:

$$\begin{aligned} F(v) &= (p - mk) + x' + \sum_{i \in v} x_i, \\ J(v) &= y' + \sum_{i \in v} y_i \\ K(v) &= \begin{cases} 0, & \text{if } x' + \sum_{i \in v} x_i \equiv 0 \pmod{m} \\ 1, & \text{otherwise} \end{cases} \end{aligned}$$

挑战者赋值 $g_1=A, g_2=B$, 然后赋值公共参数 $u' = g_2^{p-km+x} g^{x'}$, $u_i = g_2^{x_i} g^{y_i}$. 从敌手的角度来看公共参数的分配和真实的算法其实是一样的.

Phase 1. 敌手 A 发起私钥查询. 假设敌手对身份 v 发起查询. 如果 $K(v)=0$, 挑战者终止, 并且随机选取 β' 作为对挑战者的 β 的猜想. 否则, 挑战者选取一个随机数 $r \in Z_p$. 基于 BB IBE 的方法, 挑战者生成私钥

$$d = (d_0, d_1) = \left(g_1^{\frac{-J(v)}{F(v)}} (u' \prod_{i \in v} u_i)^r, g_1^{\frac{-1}{F(v)}} g^r \right).$$

令 $\tilde{r} = r - \frac{a}{F(v)}$, 于是有

$$\begin{aligned} d_0 &= g_1^{\frac{-J(v)}{F(v)}} (u' \prod_{i \in v} u_i)^r \\ &= g_1^{\frac{-J(v)}{F(v)}} (g_2^{F(v)} g^{J(v)})^r \\ &= g_2^a (g_2^{F(v)} g^{J(v)})^{-\frac{a}{F(v)}} (g_2^{F(v)} g^{J(v)})^r \\ &= g_2^a (u' \prod_{i \in v} u_i)^{r - \frac{a}{F(v)}} = g_2^a (u' \prod_{i \in v} u_i)^{\tilde{r}} \end{aligned}$$

此外, 有 $d_1 = g_1^{\frac{-1}{F(v)}} g^r = g^{r - \frac{a}{F(v)}} = g^{\tilde{r}}$.

当且仅当 $F(v) \neq 0 \pmod{p}$ 时, 挑战者才能进行这个运算. 为了简化分析, 在充分条件 $K(v) \neq 0$ 下, 挑战者只是继续 (而不是终止) 运算. (如果有 $K(v) \neq 0$ 就意味着 $F(v) \neq 0 \pmod{p}$, 因为对于任何合理值 p, n, m , 可以假定 $p > nm$.)

Challenge: 敌手提交两条消息 $M_0, M_1 \in G_1$ 和一个身份 v^* . 如果 $x' + \sum_{i \in v^*} x_i \neq km$, 那么挑战者终止并提交一个 β' 的随机猜想值. 否则, 有 $F(v^*) \equiv 0 \pmod{p}$, 挑战者将抛出硬币 γ , 产生密文 $T = (ZM_\gamma, C, C^{J(v^*)})$.

假设给定挑战者一个 BDH 元组 $Z = e(g, g)^{abc}$. 那么有 $T = (e(g, g)^{abc} M_\gamma, g^c, g^{C^{J(v^*)}}) = (e(g_1, g_2)^c M_\gamma, g^c, (u' \prod_{i \in v^*} u_i)^c)$. 我们看到 T 是 M_γ 的有效密文.

否则, Z 是 G 的一个随机元素. 那么这种情况下密文就不会给出挑战者选择 γ 的任何消息.

Phase 2. 重复 Phase 1 阶段的相同步骤.

Guess. 最后, 敌手输出对于 γ 的猜测 γ' .

Artificial Abort. 此时挑战者仍然无法使用敌手的输出结果. 敌手成功的概率与挑战者需要终止的概率关联在一起. 这个结论是由于两个不同的 q 次私钥查询集合会以不同的概率引起挑战者终止.

在最坏的情况下, 模拟中会担心 $\Pr[\gamma = \gamma' | \neg \text{abort}] - \frac{1}{2} = 0$ (或是可忽略的值), 即使对于不可忽略的值 ϵ 也有 $\Pr[\gamma = \gamma'] - \frac{1}{2} = \epsilon$.

挑战者强制所有导致模拟终止的查询集的概率设定为 $(1-\lambda)$, 其中 $(1-\lambda)$ 是此阶段之前引起挑战者终止私钥查询的集合的概率下界.

令 $\vec{v} = \{v_1, \dots, v_q\}$ 表示 Phase 1 和 Phase 2 进行的私钥查询, v^* 表示挑战身份, $V^* \subseteq \{1, \dots, n\}$ 是所有满足 $v_i^* = 1$ 的 i 的集合.

首先, 定义函数 $\tau(X', \vec{v}, v^*)$, 其中 X' 是模拟值 $x', x_1, \dots, x_n$ 的集合, $\tau(X', \vec{v}, v^*) =$

$$\begin{cases} 0, & \text{if } \bigwedge_{i=1}^q K(v_i) = 1 \wedge x' + \sum_{i \in v^*} x_i = km \\ 1, & \text{otherwise} \end{cases}$$

如果对于一个给定的模拟值 X' , 私钥和挑战查询 $\vec{v}, v^*$ 并没有导致挑战者终止, 那么函数 $\tau(X', \vec{v}, v^*)$ 的值将为 0. 对于一个给定的查询集 $\vec{v}, v^*$, 分析概率 $\eta = \Pr_{X'}[\tau(X', \vec{v}, v^*) = 0]$.

挑战者通过随机选择 X' 对概率 η 进行 $O(\epsilon^{-2} \ln(\epsilon^{-1}) \lambda^{-1} \ln(\lambda^{-1}))$ 次取样, 并通过运行 $\tau(X', \vec{v}, v^*)$ 来估计值 η' . 采样不需要敌手再次运行. 令 $\lambda = \frac{1}{8nq}$ 为不终止任何查询集的概率的下界. 如果 $\eta' \geq \lambda$, 挑战者将以概率 $\frac{\eta' - \lambda}{\eta'}$ 终止并接受一个随机猜想值 β' . 否则挑战者不会终止.

如果挑战者此刻没有终止, 它会检查敌手的猜测是否 $\gamma' = \gamma$. 如果 $\gamma' = \gamma$ 挑战者输出一个猜想值 $\beta' = 1$, 否则输出 $\beta = 0$.

证毕.

(下转第 49 页)

成对资源节点的授权. 该方案很好的解决了具有去中心化及动态性强的 P2P 网络环境下的访问控制问题. 最后, 在 P2P 文件共享应用场景下, 设计和实现了 TRACM 模型的原型系统, 经测试系统运行良好, 从而证明了方案的可行性、高效性和正确性.

参考文献:

- [1] Maruoka M, Nemati A G, Barolli V, et al. Role-based access control in peer-to-peer (P2P) societies[C] // Proceedings of the 22nd International Conference on Advanced Information Networking and Applications. Okinawa, Japan; IEEE, 2008: 495-500.
- [2] Lu J, Li R, Lu Z, et al, A role-based access control architecture for P2P file-sharing systems using primary/backup strategy[C] // Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China; IEEE, 2009: 700-703.
- [3] Diep N N, Hung L X, Zhung Y, et al, Enforcing access control using risk assessment[C] // Proceedings of the Fourth European Conference on Universal Multi-service Networks, Toulouse, France; IEEE, 2007: 419-424.
- [4] 李俊青, 谢圣献, 刘广亮, 等. P2P 网络基于蚁群优化

的动态细粒度访问控制框架[J]. 微电子学与计算机, 2008, 25(10): 30-33.

- [5] 刘义春, 张焕国. 基于 Bayesian 信任网络的 P2P 访问控制[J]. 小型微型计算机系统, 2011, 32(6): 1059-1063.
- [6] Chen D H, Le J J, Wei J Y. A peer-to-peer access control management based on web of trust[C] // Proceedings of the International Conference on Future Computer and Communication, Kuala Lumpur, Malaysia; IEEE, 2009: 192-194.
- [7] Bo L. Trust degree based access control for social networks[C] // Proceedings of the International Conference on Security and Cryptography, Athens, Greece; IEEE, 2010: 43-48.
- [8] Wu Z P, Wu H. Access control and resource allocation for peer-to-peer video streaming based on fuzzy logic[J]. Advances in Intelligent and Soft Computing, 2010(75): 237-244.

作者简介:

李致远 男, (1981—), 博士, 讲师. 研究方向为 P2P 网络安全、物联网.

毕俊蕾 女, (1981—), 硕士, 讲师. 研究方向为无线传感器网络、网络安全.

(上接第 44 页)

5 结束语

本文提出了一种新的基于身份的在线/离线加密算法. 简化了节点内部的加密过程, 复杂运算由外部设备计算, 形成离线密文分发给需要发送消息的节点, 供其在在线加密阶段使用. 仿真实验结果与理论分析一致, 证实了本文算法的优势. 与当前几种在线/离线加密算法相比的结果是密文长度较短, 需要的存储量较小, 并在完全模型下可证明达到 CPA 安全. 因此该算法适用于无线传感器网络.

参考文献:

- [1] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C] // Kilian, J. (ed.) CRYPTO 2001. LNCS, Springer, Heidelberg. 2011(2139): 213-229.
- [2] Sun D, Mu Y, Willy S. A generic construction of identity-based online/offline signcryption [C] // ISPA 2008. Australid, Sydney, 2008: 707-712.
- [3] Guo F, Mu Y, Chen Z. Identity-based online/offline

encryption[C] // FC 2008. LNCS, Springer, Heidelberg. 2008(5143): 247-261.

- [4] Liu J, Zhou J. An efficient identity-based online/offline encryption scheme[C] // ACNS, Springer, Heidelberg. 2009(5536): 156-167.
- [5] Chu C, Liu J, Zhou J, et al. Practical ID-based encryption for wireless sensor network[C] // ASIACCS' 10. China; Beijing, 2010.
- [6] Waters R. Efficient identity base encryption without random oracles[C] // Eurocrypt 2005. LNCS 3494. Berlin; Spriner-Verlag. 2005: 114-127.

作者简介:

王昱菲 女, (1988—), 硕士研究生. 研究方向为无线传感器网络、信息安全、计算机通信与网络.



杨庚 男, (1961—), 教授, 博士生导师. 研究方向为无线传感器网络、计算机通信与网络、信息安全.