

MV 群签密方案的安全性分析

曹嘉莉¹, 高崇志²

(1. 广东工业大学 应用数学学院, 广东 广州 510090 2 广州大学 信息与机电工程学院, 广东 广州 510006)

摘要: 利用 MV 群签密方案的安全漏洞构造具体的攻击: 给定一个有效的密文, 接收方中任何一个成员都可以伪装成发送方的成员产生其它有效的密文, 从而证明 MV 群签密方案不满足不可伪造性。

关键词: 群签密; 不可伪造性; 离散对数问题

中图分类号: TP309.7

文献标识码: A

文章编号: 1007-7162(2007)01-0026-03

常规的书信通信根据亲笔签名或印章来证明内容的真实性, 通过信封来防止他人的非法阅读. 在计算机通信中, 一种谨慎的习惯做法是利用带加密的数字签名, 即对消息先签名后加密. 1997 年, Zheng^[1]首次提出了数字签密 (Signcryption) 的概念. 数字签密能够在一个合理的逻辑步骤内同时实现签名和加密两项功能. 在安全参数相同的前提下, 其算法复杂度 (计算时间和通信带宽) 小于带加密的数字签名. 数字签密在诸如保密选举、电子拍卖等方面有着广阔的应用前景.

2000 年, Mu 和 Varadharajan 把群签名^[2]引入数字签密的研究, 提出了群签密^[3]的概念. 在 MV 群签密方案中, 成员可以代表各自所在的组织进行匿名的保密认证传输, 出现争议时由可信机构 (通常由发送方的群管理员担任) 识别出消息的真正发送者. 2003 年, Kwak 和 Moon^[4]认为, MV 群签密方案构造复杂, 可能存在安全漏洞, 但他们未能构造出具体的攻击方法.

事实上, 任意给定一个有效的密文, 由于发送方成员的私钥在密文中没有得到充分的保护, 因此接收方中任何一个成员都可以伪装成发送方的成员产生其它有效的密文. 本文将利用这一点构造具体的攻击, 从而证明 MV 群签密方案不满足不可伪造性.

1 MV 群签密方案

MV 群签密方案由以下步骤组成.

1.1 系统初始化

在初始化阶段, 群管理员负责生成系统参数, 包括大素数 p , $p-1$ 的素因子 q 以及 Z_p^* 中的 q 阶元素

g . 此时整个系统尚未完全建立, 只有当所有的成员都完成加入程序, 才能生成群公钥.

1.2 成员加入

群管理员为每个成员生成相应的私钥. 假设有 n 个成员, 成员与群管理员之间的通信都是安全的, 即秘密的和可认证的. 其加入过程如下: 秘密选取 $x_i \in Z_q$, $i = 1, 2, \dots, n$, 定义多项式

$$f(x) = \prod_{i=1}^n (x - x_i) = \sum_{i=0}^n \alpha_i x^i \bmod q,$$

把 $f(x)$ 展开并计算其各项系数 $\alpha_0, \dots, \alpha_n$ 的值. 定义

$$\alpha'_0 = \alpha_0, \alpha'_1 = \dots = \alpha'_{n-1} = \sum_{i=1}^{n-1} \alpha_i, \alpha'_n = \alpha_n,$$

$$\beta_i = g^{\alpha'_i}, i = 0, 1, \dots, n,$$

$$A_l = \sum_{i=1, j=1, i \neq j}^{n-1} \alpha_i x_j^l, l = 1, 2, \dots, n$$

秘密选取 $\delta \in Z_q^*$, 计算 $\delta^{-1} \pmod{q}$, $\beta_{n+1} = g^{\delta^{-1}} \bmod p$ 以及 $\rho_j = -\alpha_j \delta^{-1}$, $j = 1, 2, \dots, n$. 所有成员组成一个群 G , 群公钥定义为 $(\beta_0, \beta_1, \dots, \beta_{n+1})$. 第 l 个成员的私钥是 (x_l, ρ_l) .

假设通过上述系统初始化和成员加入过程建立了两个用户组织 G_A, G_B , 其成员人数分别为 n_A 和 n_B . G_A, G_B 的群公钥分别记作 $(\beta_0, \beta_1, \dots, \beta_{n_A+1})$ 和 $(\beta_0, \beta_1, \dots, \beta_{n_B+1})$.

1.3 签密算法

若 G_A 的成员 Alice 想以 G_A 的名义发送消息给 G_B , 她可以利用自己的私钥 (x_a, ρ_a) 对消息进行签密.

首先, 获取 G_B 的群公钥, 即 $(\beta_0, \beta_1, \dots, \beta_{n_B+1})$. 然后选取 $z \in Z_q$, 计算 $k = g^z \bmod p$, 把会话密钥 k 分成两个子密钥 k_1 和 k_2 . 设 $H(\cdot)$ 是标准的非碰撞

收稿日期: 2006-04-19

作者简介: 曹嘉莉 (1979-), 女, 助教, 主要研究方向为信息安全; 通讯作者: 高崇志 (1976-), 男, 讲师, 主要研究方向为信息与通信安全. E-mail: gzcynsure@msn.com

(collision free) 哈希函数, 计算

$$\begin{aligned} w &= H(m), r = H_{k_2}(m), \\ u_j &= \beta_j^w \bmod p, j = 1, 2, \dots, n_A, \\ s_j &= w(x_A^j - ru_j) \bmod q, j = 1, 2, \dots, n_A, \\ c_1 &\leftarrow (a_0, a_1, \dots, a_{n_B+1}) \leftarrow (g^{kr} \beta_0^w, \beta_1^w, \dots, \beta_{n_B+1}^w), \\ c_2 &\leftarrow (a_0, u_1, \dots, u_{n_A}, a_{n_A+1}) \leftarrow (g^{z-kr} \beta_0^w, u_1, \dots, u_{n_A}, \beta_{n_A+1}^w), \\ c_3 &= E_{k_1}(m). \end{aligned} \tag{*}$$

最后, 把 $(c_1, c_2, c_3, r, s_1, \dots, s_{n_A})$ 发送给 G_B .

1.4 解签密算法

接收方 G_B 的成员 Bob 可以代表 G_B 恢复消息: 首先获取发送方 G_A 的群公钥, 即 $(\beta_0, \beta_1, \dots, \beta_{n_A+1})$, 然后计算会话密钥

$$\begin{aligned} k &= \left[a_0 \left(\prod_{i=1}^{n_B} a_i^{x_i^b} \right) a_{n_B+1}^{\beta_b^0} \right] \left[a_0 \left(\prod_{j=1}^{n_A} u_j^{ru_j} \beta_j^s \right) a_{n_A+1} \right] = \\ &= \left[g^{kr} \beta_0^w \left(\prod_{i=1}^{n_B} \beta_i^{w x_i^b} \right) \beta_{n_B+1}^w \right] \left[g^{z-kr} \beta_0^w \left(\prod_{j=1}^{n_A} \beta_j^{w x_j^a} \right) \beta_{n_A+1}^w \right] = \\ &= \left[g^{kr} \left(g^{\sum_{i=1}^{n_B} a_i' x_i^b - A_b} \right)^w \right] \left[g^{z-kr} \left(g^{\sum_{j=1}^{n_A} a_j' x_j^a - A_a} \right)^w \right] = \\ &= g^{kr} g^{z-kr} = g^z \bmod p, \end{aligned}$$

把 k 分成两个子密钥 k_1 和 k_2 计算 $m = D_{k_1}(c_3)$, $w = H(m)$, 验证等式 $r = H_{k_2}(m)$, $a_0 = g^{kr} \beta_0^w \bmod p$, $a_0 = kg^{-kr} \beta_0^w \bmod p$ 是否成立. 如果成立, 则接受该消息, 并认为发送方就是 G_A .

2 安全性分析

一般的观点认为, 基于离散对数假设^[5]的 ElGamal 密码算法^[6]在实际应用中也是安全的. 因为 a_0 和 a_0 是 ElGamal 型的密文, 所以 MV 群签密方案可以看作 ElGamal 密码算法的变型. 根据这个假设, Mu 等人对所提出的群签密方案进行了详细的安全性讨论 (但没有给出严格的安全性证明). 他们声称该方案满足不可伪造性、匿名性以及保密性. 文献 [3] 认为, 在验证过程中输入发送方的群公钥可以保证只有合法的成员才能代表发送方产生有效的密文; 如果把哈希函数 $H(\bullet)$ 看成一个随机预言机, 在合法成员的私钥没有泄露的前提下, 该方案满足不可伪造性. 如果 Alice 没有在 s_j 中嵌入 x_w , Bob 就不能从密文中恢复消息. 换句话说, 要产生有效的密文, 发送方的成员必须在密文中嵌入自己的私钥.

MV 群签密方案确实满足保密性. 如果一个不属于 G_B 的攻击者可以从密文中恢复出原始消息, 那意味着他至少成功解决了某一个离散对数问题, 这就与离散对数假设相矛盾. 因此, 恢复消息唯一计算可

行的办法是得到接收方合法成员的私钥 (x_b, θ) . 遗憾的是, MV 群签密方案并不满足不可伪造性和匿名性. Kwak 和 Moon^[4]就已经指出, 群管理员的诚信关系到整个系统的安全——他掌握所有成员的私钥, 因此他可以毫不费力地伪装成组织中任何一个成员; 除此以外, 群管理员也往往成为其他攻击者的攻击目标.

事实上, 根据 s_j 的定义, Bob 可以通过计算得到 x_A^j 的值, 其中 $j = 1, 2, \dots, n_A$. 此外, Bob 还可以计算出 $\beta_{n_A+1}^w (= (a_{n_A+1})^{w-1} \bmod p)$. 由于 Alice 的私钥 x_a 没有得到充分的保护, 因此 Bob 就可以伪装成 Alice 产生任意消息的有效密文. 在下一节中, 我们将利用这一点构造具体的攻击方法, 从而证明 MV 群签密方案不满足不可伪造性. 更为严重的是, 如果 Alice 的私钥 x_a 与 Alice 的身份标识之间的关联是公开的话, 那么 Alice 作为 G_A 成员的身份也随之暴露, 匿名性也不满足.

3 攻击方法的具体实现

给定一个由 Alice 产生的有效密文 $(c_1, c_2, c_3, r, s_1, \dots, s_{n_A})$, 接收方中任何一个成员 (例如 Bob) 首先对密文进行解签密, 得到一系列的中间结果, 然后选取一个新的消息 m' , 计算

$$\begin{aligned} w' &= H(m'), r' = H_{k_2}(m'), \\ u_j' &= u_j^{w-w'} \bmod p, \\ s_j' &= w'(w^{-1} s_j + ru_j - r' u_j') \bmod q, j = 1, 2, \dots, n_A, \\ c_1' &\leftarrow (a_0', a_1', \dots, a_{n_B+1}') \leftarrow (g^{kr'} \beta_0^{w'}, \beta_1^{w'}, \dots, \beta_{n_B+1}^{w'}), \\ c_2' &\leftarrow (a_0', u_1', \dots, u_{n_A}', a_{n_A+1}') \leftarrow \\ &\quad (kg^{-kr'} \beta_0^{w'}, u_1', \dots, u_{n_A}', (a_{n_A+1}')^{w-w'}), \\ c_3' &= E_{k_1}(m'). \end{aligned}$$

最后, 把 $(c_1', c_2', c_3', r', s_1', \dots, s_{n_A}')$ 发送给 G_B 中的其他成员, 并宣称该消息的发送方是 G_A .

下面验证 $(c_1', c_2', c_3', r', s_1', \dots, s_{n_A}')$ 是关于消息 m' 的有效密文, 一定可以通过解签密算法的验证. 因为

$$\begin{aligned} u_j' &= u_j^{w-w'} = (\beta_j^w)^{w-w'} = \beta_j^{w'} \bmod p, \\ s_j' &= w'(w^{-1} s_j + ru_j - r' u_j') = \\ &= w'(x_A^j - r' u_j') \bmod q, j = 1, 2, \dots, n_A, \\ (a_{n_A+1}')^{w-w'} &= (\beta_{n_A+1}^w)^{w-w'} = \beta_{n_A+1}^{w'} \bmod p, \\ k &= g^z \bmod p, \end{aligned}$$

所以 G_B 中的其他成员 (例如 Carol) 收到 $(c_1', c_2', c_3', r', s_1', \dots, s_{n_A}')$ 后, 同样可以计算出会话密钥

$$k = \left[a_0' \left(\prod_{i=1}^{n_B} a_i'^{x_i^b} \right) a_{n_B+1}'^{\beta_b^0} \right] \left[a_0' \left(\prod_{j=1}^{n_A} u_j'^{ru_j'} \beta_j'^{s_j'} \right) a_{n_A+1}' \right] =$$

$$\left[g^{kr'} \beta_0' \left(\prod_{i=1}^{n_B} \beta_i^{x_i'} \right) \beta_{n_B+1}' \right] \left[g^{z-kr'} \beta_0' \left(\prod_{j=1}^{n_A} \beta_j^{x_j'} \right) \beta_{n_A+1}' \right] =$$

$$\left[g^{kr'} \left(g^{\sum_{i=0}^{n_B} \alpha_i' x_i - A_b} \right)^{w'} \right] \left[g^{z-kr'} \left(g^{\sum_{j=0}^{n_A} \alpha_j' x_j - A_a} \right)^{w'} \right] =$$

$$g^{kr'} g^{z-kr'} = g^z \bmod p.$$

把 k 分成两个子密钥 k_1 和 k_2 , 计算 $m' = D_{k_1}(c_3')$, $w' = H(m')$, 并且可以验证等式 $r' = H_{k_2}(m')$, $a_0' = g^{kr'} \beta_0' \bmod p$, $a_0' = g^{z-kr'} \beta_0' \bmod p$ 一定成立, 因此 Carol 接受该消息, 并认为发送方就是 G_A . Alice 无法证明密文 $(c_1', c_2', c_3', r', s_1', \dots, s_{n_A}')$ 是伪造的.

4 结论与展望

本文通过构造具体的攻击证明了 MV 群签密方案不满足不可伪造性. 本文还进一步指出, 如果发送方成员的私钥与身份标识之间的关联是公开的话, 那么发送方成员的身份也随之暴露, 匿名性也不满足.

群签密的研究从提出到现在才短短 6 年的时间, 与群签密有关的数字签密和群签名的研究已经取得一些成果, 但还不够完善, 因此对群签密的研究正处于初级阶段. 鉴于现有群签密方案存在的缺陷, 以下问题很值得作进一步的探讨:

1) 寻找支持动态成员管理的群签密方案, 即系统建立后允许成员的加入或撤销. 现有的方案如果

增加/删除成员或者更改原有成员的私钥, 需要重新建立系统, 改变群公钥, 效率低.

2) 设计出适用于大群体的群签密方案, 群公钥和密文的长度应独立于成员的人数, 并且签密/解签密算法的计算复杂度不依赖于成员的人数.

参考文献:

- [1] Yuliang Zheng. Digital Signcryption or How to Achieve Cost (Signature & Encryption) $\ll$ Cost(Signature) + Cost(Encryption) [J]. CRYPTO'97, Lecture Notes in Computer Science 1997, 1294: 165-179.
- [2] David Chaum, Eugene van Heyst. Group Signatures [J]. EUROCRYPT'91, Lecture Notes in Computer Science 1991, 547: 257-265.
- [3] Yimur Vijay Varadharajan. Distributed Signcryption [J]. NDPCRYPT 2000, Lecture Notes in Computer Science 2000, 1977: 155-164.
- [4] Dong Jin Kwak, Sang-Jae Moon. Efficient Distributed Signcryption Scheme as Group Signcryption [J]. ACNS 2003, Lecture Notes in Computer Science 2003, 2846: 403-417.
- [5] Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C [M]. New York, NY, USA: John Wiley & Sons Inc., 1996.
- [6] T Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

Cryptanalysis of Mu-Varadharajan Group Signcryption Scheme

CAO Jia-li¹, GAO Chong-zhi²

(1 Faculty of Applied Mathematics Guangdong University of Technology, Guangzhou 510090, China)

2 School of Information and Mechanical Electronics Engineering, Guangzhou University, Guangzhou 510006, China)

Abstract This paper demonstrates a concrete attack to show that the MV group signcryption scheme fails to have unforgeability. Our attack allows a dishonest receiver to forge a valid ciphertext as if the genuine sender generated it.

Key words group signcryption; unforgeability; discrete logarithm problem