第 34 卷 第 1 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.1 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)01—0156—02 文献标识码：A 中图分类号：TP309

基于 ECC 的组合公钥技术的安全性分析

赵美玲，张少武
(信息工程大学电子技术学院，郑州 450004)

摘 要：分析了唐文等人提出的一种基于ECC(椭圆曲线密码体制)的组合公钥技术的安全性特点，给出了两种合谋攻击的方法。第 1 种方法称之为选择合谋攻击，一个用户与其选择的具有某些映射特点的$w(\geq 2)$个用户合谋，可以得到2^w-w-1 个不同用户的私钥。第 2 种方法称之为随机合谋攻击，两个合谋用户首先计算其公钥的差值 Δk_{21} 和 Δk_{12}，然后在公开的公钥因子矩阵中任意选取组合公钥，通过计算所选取的公钥与两个合谋用户之一的公钥的差值是否等于 Δk_{21} 或 Δk_{12}，从而达到攻击的目标。

关键词：公钥密码；私钥；椭圆曲线

Security Analysis of Elliptic Curve Cryptography-based Combined Public Key Technique

ZHAO Mei-ling, ZHANG Shao-wu
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004)

【Abstract】This paper analyzes the security of an elliptic curve cryptography-based combined public key technique due to Tang Wen and some others. Because of some security vulnerabilities of the proposed technique, it gives two kinds of collusion attack methods, and calls the first method as a choice collusion attack. if a customer chooses w customers with some mapping characteristics and colludes them, they will get the 2^w-w-1 other customers' private keys. And it calls the second method a random collusion attack. Two collusive customers first compute their public keys' difference Δk_{21} and Δk_{12}, and then they choose public key from public key factor matrix random. Suppose one of the differences between the chosen public key and the two collusive customers' key is equal to Δk_{21} or Δk_{12}, the attack succeeds.

【Key words】public-key cryptography; private key; elliptic curve

1 概述

自从Diffie和Hellman提出公钥密码体制以来，人们对公钥密码体制进行了广泛深入的研究[1-2]，不断提出基于新的困难问题的密码体制以满足不同的应用需求。1985 年，Koblitz和Miller分别在文献[3]和文献[4]中独立地提出了利用椭圆曲线上的点群来实现公钥加密系统的方法。2003 年，唐文等人在此基础上设计了一种基于椭圆曲线密码系统的组合公钥技术[5]。

本文分析了该技术的安全性特点，给出了两种合谋攻击的方法。第 1 种方法，称之为选择合谋攻击，一个用户与其选择的具有某些映射特点的$w(\geq 2)$个用户合谋，可以得到2^w-w-1 个不同用户的私钥。第 2 种方法称为随机合谋攻击，两个合谋用户首先计算其公钥的差值 Δk_{21} 和 Δk_{12}，然后在公开的公钥因子矩阵中任意选取组合公钥，通过计算所选取的公钥与两个合谋用户之一的公钥的差值是否等于 Δk_{21} 或 Δk_{12}，从而达到攻击的目标。

在文献[5]中，各用户的公钥不直接公布，只公布公钥因子矩阵，各用户的公钥通过公钥因子矩阵和相关映射计算出来，具体过程如下：

首先，在密钥管理中心生成公、私钥因子矩阵。私钥因子矩阵 ***SSK*** 中元素为整数标量 r_{ij}，公钥因子矩阵 ***PSK*** 中对应元素为 r_{ij} 对应的椭圆曲线上的点 $r_{ij}\cdot G$。公、私钥因子矩阵生成后，私钥因子矩阵保持秘密，而公钥因子矩阵予以公布。

$$\boldsymbol{SSK}=\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{pmatrix}_{m\times n}$$

$$\boldsymbol{PSK}=\begin{pmatrix} r_{11}\cdot G & \cdots & r_{1n}\cdot G \\ \vdots & \ddots & \vdots \\ r_{m1}\cdot G & \cdots & r_{mn}\cdot G \end{pmatrix}_{m\times n}$$

设映射算法 $F_i(X)$ 的 n 次映射为：F_i(用户名)mod m=map$i$，$1\leq I\leq n$。对用户 A 进行 n 层映射，获得 n 个映射值分别为 $(i_1,i_2,\cdots,i_n)$，则用户 A 的私钥为：$k_A=(r_{i_1 1}+r_{i_2 2}+\cdots+r_{i_n n})\bmod m$。由于公钥因子矩阵公开，映射算法 $F_i(X)$ 公开，因此当验证方需要获得用户 A 的公钥时，就可以计算出用户 A 的公钥 $PK_A=(r_{i_1,1}\cdot G+r_{i_2,2}\cdot G+\ldots+r_{i_n,n}\cdot G)$。

2 合谋攻击

从椭圆曲线密码体制的组合公钥技术的实现原理出发，本文将给出两种对椭圆曲线密码体制的组合公钥技术的合谋攻击。

2.1 第 1 种合谋攻击

第 1 种合谋攻击称为选择合谋攻击。

定义 1 设两个用户A_1和A_2经过n层映射后的映射值分

作者简介：赵美玲(1982－)，女，硕士研究生，主研方向：密码编码与分析；张少武，教授

收稿日期：2007-01-10 **E-mail：**pluam@126.com

别为($i_{11}, i_{12}, \cdots, i_{1n}$)和($i_{21}, i_{22}, \cdots, i_{2n}$)，若其中仅有$t$个位置的值不同，记为 $i_{1j_p} \neq i_{2j_p}$，p=1,2,⋯,t。则称用户A_1和用户A_2是($j_1, j_2, \cdots, j_t$)层不同的，或统称用户A_2与用户A_1是t层不 同的。

定义 2 设用户 A 和用户 B 是($j_1, j_2, \cdots, j_{t_1}$)层不同的，用户 A 和用户 C 是($s_1, s_2, \cdots, s_{t_2}$)层不同的，且集合{ $j_1, j_2, \cdots, j_{t_1}$ }和{ $s_1, s_2, \cdots, s_{t_2}$ }的交集为空，则称用户 B 和 C 与用户 A 是层互斥不同的。

定理 1 设用户 A 与用户 B 和用户 C 分别是($j_1, j_2, \cdots, j_{t_1}$)层不同和($s_1, s_2 \cdots, s_{t_2}$)层不同的，且用户 B 和用户 C 与用户 A 是层互斥不同的，则 3 个用户 A, B, C 合谋，可以得到与用户 A 是($j_1, j_2, \cdots, j_{t_1}, s_1, s_2, \cdots, s_{t_2}$)层不同的用户的私钥。

证明 设用户 A、B 和 C 的组合私钥分别为

$$k_0 = r_{i_{01}1} + r_{i_{02}2} + \cdots + r_{i_{0n}n}$$

$$k_1 = r_{i_{11}1} + r_{i_{12}2} + \cdots + r_{i_{1n}n}$$

$$k_2 = r_{i_{21}1} + r_{i_{22}2} + \cdots + r_{i_{2n}n}$$

于是得到

$$k_1 - k_0 = (r_{i_{1j_1}j_1} - r_{i_{0j_1}j_1}) + (r_{i_{1j_2}j_2} - r_{i_{0j_2}j_2}) + \cdots + (r_{i_{1j_{t1}}j_{t1}} - r_{i_{0j_{t1}}j_{t1}})$$

$$k_2 - k_0 = (r_{i_{2s_1}s_1} - r_{i_{0s_1}s_1}) + (r_{i_{2s_2}s_2} - r_{i_{0s_2}s_2}) + \cdots + (r_{i_{2s_{t2}}s_{t2}} - r_{i_{0s_{t2}}s_{t2}})$$

记集合 Ω ={ $j_1, j_2, \cdots, j_{t_1}, s_1, s_2, \cdots, s_{t_2}$ }，由互斥性得到

$$k_0 + (k_1 - k_0) + (k_2 - k_0) = k_1 + k_2 - k_0 = \sum_{p \notin \Omega} r_{i_{0p}p} + r_{i_{1j_1}j_1} + \cdots + r_{i_{1j_{t1}}j_{t1}} + r_{i_{2s_1}s_1} + \cdots + r_{i_{2s_{t2}}s_{t2}}$$

证毕

更进一步有

定理 2 设用户A与w(≥2)个用户A_s(s=1,2,⋯,w)分别是($j_{s1}, j_{s2}, \cdots, j_{st_s}$)层不同的，且这$w$个用户两两是层互斥不同的，则用户A与$w$个用户$A_1, A_2, \cdots, A_w$合谋，可以得到与用户A是($j_{1t_1}, \cdots, j_{1t_1}, j_{21}, \cdots, j_{2t_2}, \cdots, j_{w1}, \cdots, j_{wt_w}$)层不同的用户的私钥。

定理 2 由定理 1 的证明过程很容易得到。显然定理 1 是定理 2 中 w=2 的情形，由定理 1 和定理 2 可以得到：

定理 3 用户A 与w(≥2)个用户A_s(s=1,2,⋯,w) 分别是($j_{s1}, j_{s2}, \cdots, j_{st_s}$)层不同的，且这$w$个用户两两是层互斥不同的，则用户A与$w$个用户$A_1, A_2, \cdots, A_w$合谋，可以得到 2^w-w-1 个不同的用户私钥。

证明 由定理 1 和定理 2 知，用户A与满足定理条件的任意s(2≤s≤w)个用户合谋都可以得到一个用户的私钥，而s个用户有 $\binom{w}{s}$ 种不同的取法，不同的取法得到不同的用户私钥，从而可以得到 $\binom{w}{2} + \binom{w}{3} + \cdots + \binom{w}{w} = 2^w - w - 1$ 个不同的用户私钥。证毕

2.2 第 2 种合谋攻击

第 2 种合谋攻击称为随机合谋攻击。

设两个合谋用户 A 和 B 的私钥分别为 k_1 和 k_2，其差记为 $\Delta k = k_2 - k_1$，如果在私钥矩阵中存在一个组合私钥 k_3，使得 $k_3 - k_2 = k_2 - k_1$，从而有 $k_3 = 2k_2 - k_1$。k_3 的存在性可以由公开的公钥矩阵来验证。实际上，记 Δk 对应的用户 A 和 B 的公钥差为 ΔPk (= $Pk_2 - Pk_1$)，合谋用户 A 或 B 在公钥矩阵中任意取得一个公钥因子组合，得到一个组合公钥，记为 Pk_3，如果 $Pk_3 - Pk_2 = \Delta Pk$，则该公钥对应的私钥即为 $k_3 = 2k_2 - k_1$。本文给出如下合谋算法：

step1 两个合谋用户 A 和用户 B 计算其组合私钥的差 $\Delta k_{21} = k_2 - k_1$ 和 $\Delta k_{12} = k_1 - k_2$，对应的公钥差分别为 ΔPk_{21} 和 ΔPk_{12}；

step2 在公钥因子矩阵中任意取得一个组合公钥 Pk_3，如果 $Pk_3 - Pk_2 = \Delta Pk_{21}$，或 $Pk_3 - Pk_1 = \Delta Pk_{12}$，则该组合公钥对应的私钥为 $k_3 = 2k_2 - k_1$ 或 $k_3 = 2k_1 - k_2$。否则继续执行 step2。

假设两个合谋用户是第 j(1≤j≤n)层不同的，记其第 j 列的私钥因子分别为 $r_{i_1 j}$ 和 $r_{i_2 j}$，如果私钥因子矩阵中存在一个私钥因子 $r_{i_3 j}$，满足 $r_{i_3 j} - r_{i_2 j} = r_{i_2 j} - r_{i_1 j}$ (这一点可以由公开的公钥因子矩阵来验证)，这时合谋用户就可以由合谋算法得到一个与之第 j 层不同的用户私钥。

3 结束语

本文研究了文献[5]提出的一种基于椭圆曲线密码体制的组合公钥技术的安全性，给出了两种合谋攻击方法。结果表明，基于椭圆曲线密码体制的组合公钥技术难以抵抗用户间的合谋攻击。

参考文献

[1] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] Rivest R, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communication of ACM, 1978, 21(2): 120-126.

[3] Koblitz N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

[4] Miller V. Uses of Elliptic Curves in Cryptography[C]//Proc. of Conf. on Advances in Cryptology-Crypto'85. [S. l.]: IEEE Press, 1986: 417-426.

[5] 唐 文, 南相浩, 陈 钟. 基于椭圆曲线密码系统的组合公钥技术[J]. 计算机工程与应用, 2003, 39(21): 1-3.

（上接第 155 页）

3 结束语

分割 MAC 的 WLAN 网络已经逐渐成为应用的主流，这种模式可以提高系统的整体性能。在笔者设计的这种架构模型中应用 802.1X 和 802.11i 协议为用户提供认证与加密服务可以确保用户数据的可靠性和安全性。接下来进一步研究认证与密钥协商模块对 AP 切换的支持，以便系统内部实现 MAC 层无缝切换。

参考文献

[1] IEEE Std 802.11i-2004 IEEE Standard for Local and Metropolitan Area Networks Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) specifications Amendment 6: Medium Access Control(MAC) Security Enhancement[S]. 2004-07-23.

[2] IEEE Std 802.1X-2004 IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control[S]. 2004-12-13.

[3] Extensible Authentication Protocol(EAP)[S]. RFC 3748. 2004-06.

[4] Gast M. 802.11 无线网络权位指南[M]. 南京: 东南大学出版社, 2006.