

基于椭圆曲线密码体制的 (t, n) 门限签密方案*

戴元军, 杨 成

(北京邮电大学 信息安全中心, 北京 100876)

摘要: 首先提出一个基于椭圆曲线密码体制的签密方案。该方案是数字签名和公钥加密的有机集成, 除了具有认证性、保密性外, 还具有计算量与通信量小等特点。在此基础上, 构造了一个基于椭圆曲线密码体制的 (t, n) 门限签密方案。该方案具有数据传输安全、鲁棒性、通信代价更小、执行效率更高等特点。还给出两种方案的安全性分析。

关键词: 签密; 门限; 椭圆曲线密码; 离散对数问题

中图法分类号: TN918.4

文献标识码: A

文章编号: 1001-3695(2004)09-0142-02

(t, n) Threshold Signature Encryption Scheme Based on Ellipse Curve Cryptosystem

DAI Yuan-jun, YANG Cheng

(Information Security Center, Beijing University of Posts & Telecommunications, Beijing 100876, China)

Abstract: In this paper, a signature encryption scheme based on ellipse curve cryptosystem is proposed. The scheme perfectly integrates digital signature scheme with public key cryptosystem, it has authentication, secrecy, less computation cost and less communication cost. Then we use a threshold scheme to construct a (t, n) threshold signature encryption scheme based ellipse curve cryptosystem. The scheme has more secrecy of data transmission, robustness, requires less communication cost and performs efficiently etc. The security analysis of two scheme is proposed.

Key words: Signature Encryption; Threshold; Ellipse Curve Cryptosystem; Discrete Logarithm Problem(DLP)

1 引言

签密是指能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能, 而其计算代价要远远低于“先签名后加密”, 因而它是实现既保密又认证地传输及存储消息的较为理想的方法^[1]。由于在诸如电子现金支付系统、安全认证地密钥生成、Internet 上的安全多发送信息传输及可认证的密钥恢复等许多方面都需要既保密又认证地消息传输, 因此签密有着广阔的应用范围。本文提出一个基于椭圆曲线密码体制的签密方案。该方案是数字签名和公钥加密的有机集成, 能够抵抗文献[2, 3]所提出的攻击, 并具有认证性、保密性和接收方的匿名性等特点。

门限数字签名是门限密码学的重要组成部分, 其概念是由 Boyd C^[4], Desmedt Y 和 Frankel Y^[5]等人的工作引入的。门限签名的主要目标是将团体的数字签名密钥以 (t, n) 门限方案的方式分散给多人管理。它有如下优点^[6-8]: 攻击者若想得到签名密钥, 必须得到 t 个子密钥, 这是很困难的; 即使某些成员不合作、不愿意出示子密钥, 泄露、篡改子密钥或子密钥丢失也不会影响签名消息的认证与恢复; 实现权利分配, 避免滥

用职权。如公司重大的决定需要由董事会中多个董事成员共同签名才能有效。基于我们所提出的签密方案和门限方案的思想, 我们构造了一个新的基于椭圆密码体制的 (t, n) 门限签密方案。该方案除了具有保密性、认证性与鲁棒性外, 还具有门限方案的优点。

2 基于椭圆曲线密码体制的签密方案

该方案分为三个阶段: 系统初始化阶段、签密阶段和签密消息验证恢复阶段。它由一个可信中心 CA、签密者 A 和接收者 B 来实施。

2.1 系统初始化阶段

该方案的安全参数如下:

(1) 可信中心 CA 选取有限域 F_q 上一条安全的椭圆曲线 $E(F_q)$, 保证该椭圆曲线的离散对数问题是难解的。在 $E(F_q)$ 上选一基点 G , G 的阶数为 n (n 为一个大素数)。

(2) 签密者 A 和接收者 B 为系统中的两个用户。A 和 B 分别选取 $d_A \in \{1, 2, \dots, n-1\}$ 和 $d_B \in \{1, 2, \dots, n-1\}$ 作为私钥, 计算 $Y_A = d_A \cdot G \in E(F_q)$ 和 $Y_B = d_B \cdot G \in E(F_q)$ 作为公钥, 并发送给 CA。

(3) CA 公开 $E(F_q), G, n, Y_A, Y_B$ 。

2.2 签密阶段

签密者 A 对消息 M 签密并发送给指定的接收者 B。首先签密者 A 选取随机数 $k \in \{1, 2, \dots, n-1\}$, 并计算 $V_1 = k \cdot G$,

收稿日期: 2003-06-30; 修返日期: 2003-12-09

基金项目: 国家“863”计划资助项目(2002AA143041); 国家“973”基金资助项目(1999035804); 国家自然科学基金资助项目(60073049, 90204017)

$V_2 = k \cdot Y_B$ 和 $v = F_x(V_1 + V_2) \bmod n$, 这里 $F_x(V_1 + V_2)$ 是取椭圆曲线上点 $(V_1 + V_2)$ 的 x 坐标的函数; 然后计算签密消息 (r, s) 如下:

$$r = M \cdot v \quad (1)$$

$$s = k + d_A \cdot r \bmod n \quad (2)$$

A 发送 (V_1, r, s) 给 B, 这里的 (r, s) 是 M 的签密消息, 因为消息被隐藏在 r 中。

2.3 签密消息的验证恢复阶段

接收者 B 接收到签密消息 (r, s) 及 V_1 后, 计算:

$$V_1 = s \cdot G - r \cdot Y_A \quad (3)$$

$$V_2 = x_B \cdot V_1 \quad (4)$$

首先通过验证 $V_1 = V_1$ 是否成立来验证签密消息 (r, s) 的有效性, 因为如果签密消息 (r, s) 有效, 则有 $V_1 = s \cdot G - r \cdot Y_A = (s - r d_A) \cdot G = k \cdot G$ 和 $V_2 = x_B \cdot V_1 = k \cdot Y_B$ 成立。然后接收者 B 计算 $v = F_x(V_1 + V_2) \bmod n$, 恢复消息 $M = r \cdot v^{-1}$ 。若签密者 A 遵循签密阶段的步骤, 则指定的接收者 B 能够正确地恢复签密消息 M 。

2.4 安全性分析

(1) 攻击者想从签密者 A 的公钥 Y_A 求得私钥 d_A 等价于求解椭圆曲线离散对数问题 (ECDLP)。

(2) 接收者 B 由签密消息 (r, s) 及式 (2) 无法获得 A 的私钥 d_A , 因为 k 是未知的, 欲从 V_1 及 G 中求得 k 等价于求解 ECDLP 问题。同理, 攻击者即使监听到 (V_1, r, s) 也无法获得 A 的私钥 d_A 及 k 。

(3) 攻击者想伪造签密消息 (r, s) 是不可能的, 他可以试探选取 $k \in \{1, 2, \dots, n-1\}$ 由式 (1) 计算 r , 但由式 (2) 求 s 是不可能的, 因为签密者 A 的私钥 d_A 是不可知的。

(4) 只有接收者 B 才能恢复消息, 因为由式 (4) 只有知道 B 的私钥 d_B 才能求得 V_2 , 进而恢复消息 M 。攻击者无法由 B 的公钥 Y_B 计算出 B 的私钥 d_B , 所以无法恢复出消息 M 。

3 基于椭圆曲线密码体制的(t, n) 门限签密方案

方案分为三个阶段: 系统初始化阶段、门限签密阶段和签密消息的恢复阶段。它由一个可信中心 CA, n 个签密者和一个接收者 B 来实施。

3.1 系统初始化阶段

该方案的安全参数如下:

(1) 可信系统 CA 选取有限域 F_q 上一条安全的椭圆曲线 $E(F_q)$, 保证该椭圆曲线的离散对数问题是难解的。在 $E(F_q)$ 上选一基点 G , G 的阶数为 n (n 为一个素数)。

(2) 令组 $Q = \{P_1, P_2, \dots, P_n\}$ 是 n 个签密者的集合, 签密者 $P_i (i = 1, 2, \dots, n)$ 的身份标识 ID_i 是不等于零的正整数, 且不同的签密者 P_i 具有不同的身份标识 ID_i , 即当 $i \neq j$ 时, $ID_i \neq ID_j (i, j = 1, 2, \dots, n)$ 。

(3) CA 随机选取 $d_Q \in \{1, 2, \dots, n-1\}$ 作为组 Q 的私钥, 组 Q 的公钥为 $Y_Q = d_Q \cdot G \in E(F_q)$ 。然后, CA 随机产生 $t-1$ 次多项式:

$$f(x) = d_Q + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1} \bmod n$$

分别计算组 Q 中签密者 $P_i \in Q$ 的私钥与公钥为:

$$d_i = f(ID_i) \quad Y_i = d_i \cdot G$$

(4) CA 通过安全信道发送 $d_i (i = 1, 2, \dots, n)$ 给 $P_i \in Q$, 并且公开参数 $E(F_q), G, n, Y_Q, Y_i$ 和 $ID_i (i = 1, 2, \dots, n)$ 。

3.2 门限签密阶段

假设组 $Q = \{P_1, P_2, \dots, P_n\}$ 中的 t 个签密者, 不妨设为 P_1, P_2, \dots, P_t 对消息 M 签密并发送给接收者 P_B 。签密步骤如下:

(1) 首先签密者 $P_i (i = 1, 2, \dots, t)$ 随机选取 $K_i \in \{1, 2, \dots, n-1\}$ 并计算 $V_{i1} = K_i \cdot G$, 然后 $P_i (i = 1, 2, \dots, t)$ 发送 (V_{i1}, V_{i2}) 给签密合成者。

(2) 签密合成者通过验证 $V_{i1} = V_{j1} (i = j)$ 是否成立来检查 P_i, P_j 在步骤 (1) 是否选择了相同的随机数。如果 P_i, P_j 选择了相同的随机数, 则通知它们重新选取新的随机数并计算 (V_{i1}, V_{i2}) ; 否则, 签密合成者计算 $T_1 = \sum_{i=1}^t V_{i1}, V_{i1}, T_2 = \sum_{i=1}^t V_{i2}$ 和 $v = F_x(T_1 + T_2) \bmod n$, 这里 $F_x(T_1 + T_2)$ 是取椭圆曲线上点 $(T_1 + T_2)$ 的 x 坐标的函数。然后计算 $R = M \cdot v$, 并广播 R 。

(3) 签密者 $P_i (i = 1, 2, \dots, t)$ 计算 $s_i = k_i + R \cdot d_i \cdot C_i \bmod n$, 其中 $C_i = \prod_{j=1, j \neq i}^t (ID_j - ID_i)^{-1} \bmod n$ 。最后, 签密者 $P_i (i = 1, \dots, t)$ 发送 s_i 给签密合成者。

(4) 签密合成者接收到部分签密消息 s_i 后, 通过验证如下等式 $s_i \cdot G - Y_i \cdot R \cdot C_i = V_{i1}$ 是否成立来验证部分签密消息 s_i 的有效性, 其中 $C_i = \prod_{j=1, j \neq i}^t (ID_j - ID_i)^{-1} \bmod n$ 。如果所有的部分签密消息 s_i 都是有效的, 则签密合成者计算 $S = \sum_{i=1}^t s_i \bmod n$, 并且发送签密消息对 (R, S) 给接收者 P_B 。

3.3 签密消息的恢复阶段

接收者 P_B 接收到签密消息对 (R, S) 后, 首先计算 $T_1 = S \cdot G - Y_G \cdot R$ 和 $T_2 = T_1 \cdot d_B$, 然后计算 $v = F_x(T_1 + T_2) \bmod n$, 并恢复消息 $M = R \cdot v^{-1}$ 。如果组 Q 成员在签密过程中遵循门限签密阶段的步骤, 则指定接收者 P_B 能够正确地恢复签密消息 M 。

3.4 基于椭圆曲线密码体制的门限签密方案的安全性分析

(1) 该方案的安全性是基于求解有限域上椭圆曲线密码离散对数问题 (ECDLP) 的困难性和门限方案的安全性。

(2) 该方案中攻击者无法从步骤 (3) 中的 $s_i = k_i + R \cdot d_i \cdot C_i \bmod n$ 求得子私钥 d_i , 因为 k_i 是未知的, 而由步骤 (1) 中的 (V_{i1}, V_{i2}) 求 k_i 是不可能的, 这等价于求解椭圆曲线密码的离散对数问题。同样, 也无法由公钥 $Y_Q, Y_i (i = 1, 2, \dots, n)$ 求得组的私钥 d_Q 和签密者的私钥 d_i 。

(3) 该方案中通过步骤 (4) 来验证部分签密消息的有效性, 能够发现签名者 $P_i (i = 1, 2, \dots, t)$ 是否篡改子密钥进行欺骗, 并且能够容忍 $n-t$ 个签名者不合作或用篡改的子密钥签密消息, 从而该方案具有门限方案的鲁棒性。

(4) 接收者或签密合成者试图对伪造消息 M 进行门限签密的攻击是不可能的, 接收者或签密合成者可以随机选取 $k_i \in \{1, 2, \dots, t\}$ 能够计算 R , 但是他不能构造部分签密消息 s_i 使得 $s_i = k_i + R \cdot d_i \cdot C_i \bmod n$, 因为他不知道签密成员 P_i 的私钥 d_i , 若他要从 $s_i \cdot G - Y_i \cdot R \cdot C_i = V_{i1}$ 中求解 s_i , 则等价于求解 ECDLP 问题。

(5) 无法进行合谋攻击, 任意 $t-1$ 或少于 (下转第 146 页)

5 流过滤技术

流过滤是东软集团提出的一种新型防火墙技术架构,它融基于状态的包过滤技术与基于内容的深度包检测技术为一体,提供了一个较好的应用防御解决方案。它以状态监测技术为基础,但在此基础上进行了改进。其基本的原理是:以状态包过滤的形态实现应用层的保护能力。通过内嵌的专门实现的 TCP/IP 协议栈,实现了透明的应用信息过滤机制。

流过滤技术的关键在于其架构中的专用 TCP/IP 协议栈。这个协议栈是一个标准的 TCP 协议的实现,依据 TCP 协议的定义对出入防火墙的数据包进行了完整的重组,重组后的数据流交给应用层过滤逻辑进行过滤,从而可以有效地识别并拦截应用层的攻击企图。

在这种机制下,从防火墙外部看,仍然是包过滤的形态,工作在链路层或 IP 层,在规则允许下,两端可以直接访问。但是,任何一个被规则允许的访问在防火墙内部都存在两个完全独立的 TCP 会话,数据以“流”的方式从一个会话流向另一个会话。由于防火墙的应用层策略位于流的中间,因此可以在任何时候代替服务器或客户端参与应用层的会话,从而起到了与应用代理防火墙相同的控制能力。如在对 SMTP 协议的处理中,系统可以在透明网桥的模式下实现完全的对邮件的存储转发,并实现丰富的对 SMTP 协议的各种攻击的防范功能。流过滤的示意图如图 4 所示。

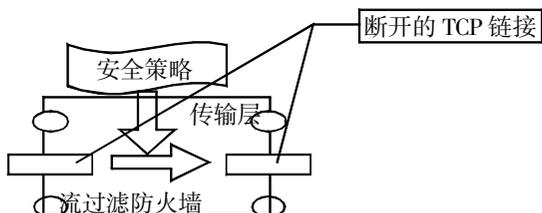


图 4 流过滤示意图

流过滤的结构继承了包过滤防火墙的应用透明的特点,非常容易部署,而且具有很好的应用防御能力。流过滤的另一个优势在于性能,完全为过滤和转发目的而重新实现的 TCP 协议栈相对于以自身服务为目的的操作系统中的 TCP 协议栈来说,消耗资源更少且更加高效,可以说流过滤采用专用的 TCP 协议栈解决了内容过滤障碍的问题,大大提高了防火墙处理速度。

6 结束语

本文从分析数据包结构出发,提出包过滤技术的核心问题是选取哪些字段信息,以及如何有效地利用这些字段信息并结合访问控制列表来执行包过滤操作,并尽可能地提高安全控制力度。在此基础上,分析了包过滤技术的两种发展趋势。我们看到,两种技术取长补短,相互融合,也是一种发展趋势。

参考文献:

[1] Douglas E Comer. 用 TCP/IP 进行网际互连 [M] . 林瑶, 等. 北京: 电子工业出版社, 2001.

[2] Guido Van Rooij. Real Stateful TCP Packet Filtering in IP Filter [EB/OL] . <http://citeseer.nj.nec.com/correct/491783>.

[3] Richard Stiennon. Deep Packet Inspection: Next Phase of Firewall Evolution [EB/OL] . http://www.gartner.com/DisplayDocument?doc_cd=111579.

[4] 曹斌. 网络防火墙的体系结构 [EB/OL] . <http://neteye.neusoft.com/Docs/News/html/20010913112353854/htmlfile/20010913112353854.html>.

[5] 费宗莲. 防火墙倾向内容过滤 [EB/OL] . <http://media.ccidnet.com/media/ciw/1169/c2301.html>.

[6] 流过滤技术分析 [EB/OL] . <http://neteye.neusoft.com/Docs/News/html/20011212131209304/htmlfile/20011212131209304.html>.

作者简介:

翟钰, 硕士研究生, 主要研究领域为网络信息安全; 武舒凡, 硕士研究生, 主要研究领域为通信技术; 胡建武, 主要研究领域为自动控制。

(上接第 143 页) $t - 1$ 个签密者无法重构 $t - 1$ 次多项式 $f(x)$, 也就不能合谋得到签密者的私钥 $d_i (i = 1, 2, \dots, t)$ 及组的私钥 d_0 。

(6) 在该方案中 t 个签密者用他们的子密钥对消息进行部分签密, 然后把部分签密(而不是子密钥)发送给签密合成者。签密合成者把这些部分签密合成为签密消息, 但他没有得到签密的子密钥, 也无法合成组的私钥, 这样就克服了签密合成者的欺骗。

4 结束语

本文首先提出一个基于椭圆曲线密码体制的签密方案, 该方案是数字签名和公钥加密的有机集成, 具有认证性、保密性、和计算量与通信量比较小等特点。然后基于所提出的签密方案和门限方案的思想, 构造了一个新的基于椭圆密码体制的 (t, n) 门限签密方案。该方案除了具有保密性、认证性与鲁棒性外, 还具有通信量小、执行效率高等优点。我们还可以利用文献 [8, 9] 中的密钥分配方法, 把本文的方案进一步改进为没有可信中心的门限签密方案, 限于篇幅我们将在另文中给出详细方案。

本文是在导师杨义先教授的精心指导下完成的, 特此致谢。

参考文献:

[1] Cheng Y L. Signcryption and Its Application in Efficient Public Key Solutions [C] . Proceedings of Information Security Workshop (ISW

'97) . Springer-Verlag, 1997. 201-218.

[2] Lin C - C, Lai H C - S. Cryptanalysis of Nyberg-rueppel 's Message Recovery Scheme [J] . IEEE Communications Letters, 2000, 4 (7) : 231-232.

[3] Miyaji A. Another Countermeasure to Forgeries over Message Recovery Signature [J] . IEICE Trans Fundamentals, 1997, E80 -A (11) : 2191-2200.

[4] Boyd C. Digital Multisignatures [C] . Cryptography and Coding. Clarendon Press, 1986. 241-246.

[5] Desmedt Y, Frankel Y, Threshold Cryptosystems [C] . Proc. CRYPTO ' 89, Springer-Verlag, 1990. 307-315.

[6] Shamir A. How to Share a Secret. Commun [J] . ACM, 1979, 24 (11) : 612-613.

[7] Desmedt Y, Frankel Y. Threshold Cryptosystems [C] . Brassard Ged, Advances in Cryptology-CRYPTO '89 Proceedings. Lecture Notes in Computer Science 435, Berlin: Springer-Verlag, 1990. 307-315.

[8] T P Pedersen. A Threshold Cryptosystem without a Trusted Party [C] . Proc. of Eurocrypt '91, Lecture Notes in Computer Science 547, Springer-Verlag, 1991. 221-238.

[9] C Park, K Kurosawa. New ElGamal Type Threshold Digital Signature Scheme [J] . IEICE Trans. Fundamentals, 1996, E79 -A (1) : 86-93.

作者简介:

戴元军 (1974 -), 博士生, 研究方向为密码学、电子支付、信息安全; 杨成, 博士生, 研究方向为密码学、信息安全、信息隐藏。