一种基于身份一次性公钥的构造

张 胜 徐国爱 胡正名 杨义先
(北京邮电大学信息安全中心126信箱 北京 1000876)

摘 要 该文利用基于身份的密码系统，构造一个一次性公钥，来解决Internet通信的匿名性问题。在该系统中，用户只需由可信中心颁发一次私钥，而在每次活动时自己生成不同的公钥，通过与之对应的签名方案，在认证用户身份的同时，保证用户的匿名性和多次活动之间的不可联系性。另外，在必要时，可以联合可信中心揭示用户的真实身份，以防止用户的恶意活动。

关键词 保密通信，匿名性，基于身份，一次性公钥，双线性映射
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)08-1412-03

Construction of the One-Off Public Key Based on Identity

Zhang Sheng Xu Guo-ai Hu Zheng-ming Yang Yi-xian
(*Information Security Center, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract In order to resolve the problem of Internet communication anonymity, the paper constructs one-off public key using identity-based cryptography. In this system, user only needs TC(Trust Center) issuing the private key one time, and he can generate his different public keys when uses it. So it can ensure the user's anonymity and the disconnection among the user's actions. And TC can reveal the user's identity to preventing the user committing when occasion requires.

Key words Secret communication, Anonymity, Identity-based, One-off public key, Bilinear map

1 引言

随着Internet的普及，特别是随着电子商务的不断发展，越来越多的人用它进行私人通信或与商务活动有关的通信。与现时生活中一样，人们在网上进行私人通信或商务活动时，个人的隐私也应当得到保护。然而，众所周知，Internet并不提供个人的隐私保护，网络窃听者可以轻而易举地截获通信数据，从而知道谁和谁在通信。因此，许多人开始进行Internet上的匿名通信研究，为通信方提供隐私保护。其中一种方案是用户使用临时身份或加密永久身份来实现，但是较长时间使用相同的临时身份或加密了的永久身份会暴露用户不同活动之间的联系。另一种方案是使用基于证书的公钥系统，同样地，这种方案也使得用户的不同活动仍然可以由用户的公钥和证书联系起来。还有一种方案是在电子商务中常用的盲签名，然而盲签名的匿名性在保护个人隐私的同时，给犯罪分子带来了可乘之机。

为了既保护个人的隐私，又避免犯罪，最近人们又提出了很多方案。文献[1]指出可通过每个用户使用多个公私钥和证书来实现，显然这一方案极其繁琐。文献[2]提出了笔名证书 (Pseudonym certificate) 的概念，指出通过该方案可使证书的身份与责任相分离，从而实现安全的匿名通信，但并没有提出一个真正的方案。文献[3]利用RSA (Rivest、Shamir和Adleman联合提出的公钥密码系统) 和Fiat-Shamir身份鉴别方案提出基于ID的一次性盲公钥，来保证用户的匿名性和用户多次活动的不可联系性。然而，该一次性盲公钥不能防止用户伪造公钥信息进行欺骗，并且由于使用RSA，在计算和存储能力受限的移动终端上实施起来具有一定的困难。

本文基于文献[3]一次性盲公钥的思想，利用文献[4]基于身份的密码系统，构造一个基于身份的一次性公钥，来解决Internet 通信的匿名性问题。在该系统中，可信中心只需给用户颁发一次私钥，而用户在每次使用时可以随机生成不同的公钥，该公私钥可用对应的签名方案对消息进行签名，从而保证用户的匿名性和用户多次活动的不可联系性。同时，在必要时，可以联合可信中心，来揭示用户的真实身份，以防止用户的恶意活动。另外，该一次性公钥可以防止用户伪造公钥信息进行欺骗，并且使用椭圆曲线，方便在移动终端上实施。

2 基于身份的密码系统

基于身份的密码系统首先由Shamir[5]提出。使用基于身份的密码系统，用户的公钥即是自己的身份，可以由任何人根据其身份计算出来，而用户的私钥由可信中心 (Trust Center, TC) 产生。最近，利用椭圆曲线上Weil对 (Weil Pairing)的双线性性质[6]，几个基于身份的密码系统被构造出来，包括基于身份的加密方案[7]和基于身份的数字签名方案[4,

2004-12-01 收到，2005-05-08 改回
国家自然科学基金(60372094)资助课题

[8]。它们的理论基础是椭圆曲线，Diffie-Hellman问题，CDHP，DDHP，GDH群，双线性映射，双线性Diffie-Hellman假设和Weil对。

文献[4]构造了一个基于身份公钥的签名方案，该方案包含 3 方：可信中心、签名者和验证者。分为 4 个阶段：系统初始化、用户注册、签名与验证签名。设 G_1， G_2 分别是阶为 q 的加法群和乘法群，其中 q 是素数，在 G_1， G_2 中离散对数问题都是难解的。设 $\hat{e}$ 是 $G_1 \times G_2$ 到 G_2 的一个双线性映射。通常 G_1 为有限域 F_q 上的椭圆曲线有理点群的一个加法子群，G_2 为这个有限域的一个乘法子群，双线性映射 $\hat{e}$ 由椭圆曲线上的 Weil 对派生得到。设 ID 是个标识用户身份的一个字符串，H_1，H_2 是公开的哈希函数，H_1：$\{0,1\}^* \to G_1$，H_2：$\{0,1\}^* \times G_2 \to F_q$。

(1) 系统初始化　可信中心 TC 随机选择 $P \in G_1$，$s \in F_q$，计算 $P_{\mathrm{TC}} = s\ P$。公开 P 和 P_{TC}，秘密保存 s。P_{TC} 为系统公钥，s 为系统私钥(亦称系统主密钥)，系统中所有用户的私钥均由它生成。

(2) 用户注册　假设用户 A 身份信息为 ID_A，用户 A 注册时首先将 ID_A 送给 TC。TC 认证 A 的身份，如果合法，则计算 $Q_A = H_1(\mathrm{ID}_A)$和 sQ_A，并将 sQ_A 通过安全渠道送给 A。A 计算 $Q_A = H_1(\mathrm{ID}_A)$，A 的公钥 $P_A = Q_A$，私钥 $S_A = sQ_A$。

(3) 签名　为了签名一个消息 M，选择 $P_1 \in G_1$，$k \in F_q$ 计算 $w = \hat{e}(P_1, P)^k$，$v = H_2(M, w)$，$U = v\ S_A + kP_1$，签名为(U, w)。

(4) 验证签名　计算 $\hat{e}(U, P)$，$\hat{e}(P_A, P_{\mathrm{TC}})^v$，验算下列等式是否成立 $\hat{e}(U, P) = \hat{e}(P_A, P_{\mathrm{TC}})^v w$。

3　一次性公钥的构造

(1) 系统初始化　可信中心 TC 选择 $P \in G_1$，$s \in F_q$，计算 $P_{\mathrm{TC}} = sP$。公开 P 和 P_{TC}，秘密保存 s。P_{TC} 为系统公钥，s 为系统私钥。

(2) 用户注册　假设用户 A 身份信息为 ID_A，选择 $t \in F_q$ 并秘密保存，计算 $Q_A = H_1(\mathrm{ID}_A)$，tQ_A，tP，然后将 ID_A，tQ_A，tP 送给 TC。

(a) TC 首先认证 A 的身份并检查 tP 是否与其他用户相同，然后计算 $Q_A = H_1(\mathrm{ID}_A)$，验证等式 $\hat{e}(tQ_A, P) = \hat{e}(Q_A, tP)$是否成立。如成立，将 tP 和 ID_A 保存起来，用作日后确认 A 的身份。然后计算 sQ_A 和 $M_A = s(s.tQ_A + sQ_A)$，将 sQ_A 和 M_A 通过安全渠道送给 A；

(b) A 的私钥为 $S_A = sQ_A$，A 秘密保存 M_A。显然 M_A 只能从 TC 得到，无法自己生成。

(3) 一次性公钥　任意选择 $r \in F_q$，计算 $P_A = rQ_A$，$u_A = r(sQ_A)$，$v_A = rt(sQ_A)$，$w_A = rtQ_A$，则$(P_A, u_A, v_A, w_A, rM_A)$称为 A 的一次性公钥。如果 A 要与 B 进行通信，需要将该一次性公钥送给 B。B 首先验证一次性公钥的有效性，然后通过与之对应的签名方案对 A 进行身份认证。对一次性公钥的有效性验证描述如下：

(a) B 验证等式 $\hat{e}(u_A, P) = \hat{e}(P_A, P_{\mathrm{TC}})$和 $\hat{e}(v_A, P) = \hat{e}(w_A, P_{\mathrm{TC}})$是否成立。如成立，则证明 A 已在 TC 注册过。

事实上，

$$\hat{e}(u_A, P) = \hat{e}(r(sQ_A), P) = \hat{e}(rQ_A, sP) = \hat{e}(P_A, P_{\mathrm{TC}})$$

$$\hat{e}(v_A, P) = \hat{e}(rt(sQ_A), P) = \hat{e}(rtQ_A, sP) = \hat{e}(w_A, P_{\mathrm{TC}})$$

如果上列两式成立，则说明 u_A，v_A 都含有系统主密钥，因此 A 在 TC 注册过。

(b) B 验证等式 $\hat{e}(rM_A, P) = \hat{e}(u_A, P_{\mathrm{TC}}) \cdot \hat{e}(v_A, P_{\mathrm{TC}})$ 是否成立。如成立，则确信 TC 在必要时可以揭示出 A 的身份。

事实上，$\hat{e}(rM_A, P) = \hat{e}(rsstQ_A + rssQ_A, P) = \hat{e}(rsstQ_A, P)\,\hat{e}(rssQ_A, P) = \hat{e}(rstQ_A, sP)\,\hat{e}(rsQ_A, sP) = \hat{e}(v_A, P_{\mathrm{TC}})\,\hat{e}(u_A, P_{\mathrm{TC}})$。

如果上式成立，则说明 $rM_A = su_A + sv_A$。而 u_A, v_A 也都含有系统主密钥，因此用户 A 自己无法独立生成 su_A，sv_A，因而也就无法独立生成 rM_A，只能通过从 TC 得到的 M_A 与某个随机数相乘来生成。由于 $M_A = s(s.tQ_A + sQ_A)$且用户 A 无法伪造，因此 v_A 与 u_A 之间相差 t。而 TC 中保存了与 A 相关的 tP 等信息，所以用户 B 可以确信 TC 在必要时通过 u_A，v_A 能够揭示出用户 A 的身份。

(4) 签名　为了签名一个消息 M，选择 $P_1 \in G_1$，$k \in F_q$，计算 $w = \hat{e}(P_1, P)^k$，$v = H_2(M, w)$，$U = rvS_A + kP_1$，签名为(U, w)。

(5) 验证签名　计算 $\hat{e}(U, P)$，$\hat{e}(P_A, P_{\mathrm{TC}})^v$，验算下列等式是否成立 $\hat{e}(U, P) = \hat{e}(P_A, P_{\mathrm{TC}})^v \cdot w$。

事实上，$\hat{e}(U, P) = \hat{e}(rvS_A + kP_1, P) = \hat{e}(rvS_A, P) \cdot \hat{e}(kP_1, P) = \hat{e}(rsQ_A, P)^v \cdot \hat{e}(P_1, P))^k = \hat{e}(rQ_A, sP)^v \cdot w = \hat{e} \cdot (P_A, P_{\mathrm{TC}})^v \cdot w$

4　安全性分析

(1) 一次性公钥的匿名性　用户 A 的一次性公钥为$(P_A, u_A, v_A, w_A, rM_A)$，它们都经过了随机数 r 的处理，因此没有向用户 B 泄漏任何有关 A 的私钥和 w_A 的信息。并且，在上述 A 向 B 证明自己身份的过程中，B 仅能知道 A 已在可信中心 TC 注册过，并确信 TC 能揭示 A 的真实身份。只要 A 不取相同的 r，每次的$(P_A, u_A, v_A, w_A, rM_A)$就不会相同。因此，用户 B 自己无法得知 A 的真实身份，并且用户 A 的不同活动之间也没有任何联系。

在必要时，用户 B 可以与可信中心 TC 合作，来揭示用户 A 某次活动的真实身份。用户 B 只需将 u_A，v_A 送给 TC，由 TC 来揭示 A 的身份。因为 TC 中保存了用户 A 对应的 ID_A, tP，通过验证等式 $\hat{e}(v_A, P) = \hat{e}(u_A, tP)$是否成立，来揭示 A 的身份。事实上，$\hat{e}(v_A, P) = \hat{e}(rt(sQ_A), P) = \hat{e}(r(sQ_A), tP) = \hat{e}(u_A, tP)$。因此，这既保证了用户 A 的活动具有匿名性和不可追踪性，也保证了用户 A 不能进行恶

意的活动。

(2) 一次性公钥的不可欺骗性　用户 A 不能使用虚假的公钥信息对用户 B 进行欺骗。首先，用户 A 无法伪造 rM_A。因为 B 通过验证等式 $\hat{e}(u_A, P) = \hat{e}(P_A, P_{TC})$和 $\hat{e}(v_A, P) = \hat{e}(w_A, P_{TC})$，可以得知 u_A, v_A 含有系统主密钥。通过验证等式 $\hat{e}(rM_A, P) = \hat{e}(u_A, P_{TC})\hat{e}(v_A, P_{TC})$，可以得知 $rM_A = su_A + sv_A$。因为 u_A， v_A 也都含有系统主密钥，因此用户 A 自己无法独立生成 su_A， sv_A，因而也就无法独立生成 rM_A，只能通过从TC得到的 M_A 与某个随机数相乘来生成。因为 A 无法伪造 M_A，因此也就无法伪造 rM_A。

如果 A 伪造了 u_A 或 v_A， B 通过验证等式 $\hat{e}(rM_A, P) = \hat{e}(u_A, P_{TC})\hat{e}(v_A, P_{TC})$是否成立可以立即发现。同样地，如果 A 伪造了 P_A 或 w_A，B 通过验证等式 $\hat{e}(u_A, P) = \hat{e}(P_A, P_{TC})$ 和 $\hat{e}(v_A, P) = \hat{e}(w_A, P_{TC})$是否成立也可以立即发现。

用户 A 也无法伪造信息 tQ_A， tP 进行注册。因为 TC 会检查 tP 是否和其他用户相同，并且通过验证等式 $\hat{e}(tQ_A, P) = \hat{e}(Q_A, tP)$判断注册信息是否正确。因此，该一次性公钥具有不可欺骗性。

5 结束语

本文利用基于身份的密码系统，构造一个一次性公钥。在该系统中，用户只需由可信中心颁发一次私钥，而在每次活动时自己生成不同的公钥，从而保证用户的匿名性和多次活动之间的不可联系性。同时，在必要时，可以联合可信中心揭示用户的真实身份，以防止用户的恶意活动。另外，该系统使用基于身份的公钥，相对于基于证书的公钥，无需保存、传送和管理证书，也不需验证证书的有效性，并且使用椭圆曲线，方便在计算和存储能力受限的移动终端上实施，是解决 Internet 通信匿名性问题一个可行的方案。

参 考 文 献

[1] 冯登国. 电子商务中的安全认证问题[R]. 北京:中国科技大学研究生院, 1997: 23−27.

[2] Herreweghen E. Secure anonymous signature-based transactions [A]. Proceedings of ESORICS 2000[C]. London, UK, Springer-Verlag, 2000: 55−71.

[3] 张秋璞, 郭宝安. 基于 ID 的一次性盲公钥[J]. 电子学报, 2003, 31(5): 769−771.

[4] Hess F. Exponent group signature schemes and efficient identity based signature schemes based on pairing[EB/OL]. Available from http://epring.iacr.org, 2002.

[5] Shamir A. Identity-base cryptosystems and signature schemes[C]. Proc. of Crypto'84, Lecture Notes in Computer Science, Springer-Verlag, 1984, Vol. 196: 47−53.

[6] Silverman J H. The arithmetic of elliptic curves[D]. Graduate Texts in Mathematic, Springer -Verlag, 1986: 106: 96−99.

[7] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]. In:Proc Crypto 2001, LNCS, Springer-Verlag, 2001: 2139: 213−229.

[8] Paterson K. ID-based signatures from pairing on elliptic curves [EB/OL]. Available from http://epring.iacr.org, 2002.

张　胜： 男，1974 年生，博士生，研究方向为密码学与网络安全.

徐国爱： 男，1972 年生，副教授，研究方向为密码学与网络安全.

胡正名： 男，1931 年生，教授，博士生导师，研究方向为编码密码学.

杨义先： 男，1961 年生，教授，博士生导师，研究方向为编码密码学与信息安全.