一个前向安全的基于身份的代理签密方案

于 刚,黄根勋
YU Gang,HUANG Gen-xun

信息工程大学 理学院,郑州 450001
School of Science,Information Engineering University,Zhengzhou 450001,China
E-mail:ygygang@126.com

YU Gang,HUANG Gen-xun.Forward secure identity based proxy-signcryption scheme.Computer Engineering and Applications,2008,44(2):157-159.

Abstract: Based on an identity based signcryption scheme proposed by Chen and Malone-Lee,an identity based proxy-signcryption scheme from pairings is proposed in this paper.The new scheme not only has the function of proxy signature scheme,but also has the advantage of identity based signcryption scheme.Only the intended recipient can recover the plaintext from the ciphertext,and the recipient can verify the validity of the proxy signature.As compared to the existing schemes,the new scheme provides both forward security and public verifiability.What's more,the new scheme is more convenient for application.

Key words: proxy-signcryption;identity based cryptography;forward secure;bilinear pairings;signcryption

摘 要: 借鉴Chen和Malone-Lee提出的基于身份的签密方案的思想，利用双线性对的特性构建出一个基于身份的代理签密方案。该方案既保持了基于身份签密的优点，又具有代理签名的功能，只有指定的接收者才能从密文中恢复消息，验证代理签名的有效性。与已有的方案相比，该方案同时具有前向安全性和公开验证性；并且新方案更适于应用。

关键词:代理签密;基于身份的密码;前向安全;双线性对;签密
文章编号:1002-8331(2008)02-0157-03 **文献标识码**:A **中图分类号**:TP309

1 引言

1996年,Mambo等人提出代理签名的概念。代理签名允许代理签名人代替原签名人(也称授权人)行使签名权。但是,代理签名仅能提供签名授权的认证而不能提供消息的保密性。为了既保密又认证的传输消息,Zheng于1997年提出了数字签密的概念,它不但能在一个合理的逻辑步骤内同时实现数字签名和加密两项功能,而且其计算量和通信成本都要低于传统的"先签名后加密"。Gamage等人于1999年提出第一个代理签密方案,代理签密结合了代理签名和签密两项功能,它将签密的权力授予代理签密人，然后代理签密人代替原签密人进行签密。1984年,Shamir提出基于身份的密码思想。在基于身份的密码系统中,为了减轻公钥证书的认证负担,用户的公钥直接从其身份信息(如姓名、身份证号、E-mail地址等)得到,而私钥则是由一个称为私钥生成中心(TA)的可信方生成。此思想一经提出便受到广泛关注，许多基于身份的密码协议被提出。2005年,Chen和Malone-Lee提出一个高效的基于身份的签密方案。基于身份的签密方案与代理签名方案有效结合产生基于身份的代理签密方案。一个基于身份的强代理签密应该具有以下安全性质:前向安全性、可公开验证性、可证安全、强不可伪造性、强可识别性、强不可否认性、防止滥用性等。第一个基于身份的代理签密方案由Li和Chen于2004年提出，但是文献[7]证明文献的方案不具有强不可伪造和前向安全的性质。文献给出了一个改进的方案和一个新方案,但改进后的方案仍然不具有前向安全性。张学军和王育民指出文献给出的新方案存在明显的错误,这种错误导致其新方案不可行。张等同时基于短签名给出了一个高效的代理签密方案。但是文献的方案中,私钥生成中心(TA)需要为每一个用户产生两个秘密钥,一个用于签密,另一个用于解签密。

本文利用双线性对提出了一个新的可公开验证和前向安全的签密方案。分析表明,新方案在保持了代理签密各种安全性质的条件下,效率非常高,更适合于应用。

2 相关知识和安全性要求

本章简要介绍双线性对的基础知识及其相关的困难问题。

设$(G,+)$为q阶加法循环群,$(V,\cdot)$为q阶乘法循环群。假定在G、V中计算离散对数问题是困难的。设$\hat{e}:G\times G\to V$是一个双线性映射,满足以下3条性质:

(1)双线性性:对于所有的$P,Q\in G$和所有的$a,b\in Z_q^*$,$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$。

(2)非退化性:存在$P,Q\in G$,满足$\hat{e}(P,Q)\neq 1$。

(3)可计算性:对所有的$P,Q\in G$,$\hat{e}(P,Q)$可以在多项式时

作者简介:于刚(1984-),男,硕士生,主要研究方向:密码协议分析、信息安全;黄根勋(1964-),男,副教授,硕士生导师,主要研究方向:应用数学、密码与信息安全。

间内有效计算出来。

本文的方案主要基于下面几个难题：

(1)椭圆曲线上的离散对数问题(ECDLP)：已知两个群元素 P 和 Q，找一个正整数 n，使得 $Q=nP$ 成立。

(2)双线性 Diffie-Hellman 问题(BDHP)：已知 P,aP,bP,cP，其中 $a,b,c\in Z_q^*$，计算 $\hat{e}(P,P)^{abc}$。

本文假设 ECDLP 和 BDHP 在 G、V 中是难解的，G 可以采用超奇异椭圆曲线上的加法群，双线性映射可以采用改进的 Weil 对或 Tate 对。

3 基于身份的代理签密方案的形式化定义

本章描述基于身份的代理签密方案的算法组成及其安全概念。

3.1 基于身份的代理签密方案的组成

一个基于身份的代理签密方案一般包含下面几个算法：

(1)系统初始化算法：由 TA 完成，输入安全参数 l^k，输出主密钥 S 和系统参数 $params$，TA 保密 S，公开 $params$。

(2)密钥生成算法：输入用户的身份 ID_u，TA 计算用户的私钥 S_u，并通过安全方式发送给用户。

(3)代理签密密钥生成算法：原签密人 Alice 生成一个许可证 m_w 来说明 Alice 和代理人 Park 之间的授权关系，同时也说明该授权关系的使用限制等内容。Park 收到许可证后生成代理签密密钥。

(4)代理签密算法：输入系统参数 $params$、明文 m、接收者 Bob 的身份 ID_B 和 Park 生成的代理签密密钥，输出密文。

(5)解签密算法：输入密文、系统参数 $params$，接收者的私钥，输出明文或符号，表示解签密失败。

3.2 基于身份的强代理签密方案应有的安全性质

一个基于身份的强代理签密方案应该具有以下安全性质：

(1)前向安全性(Forward Security)：即使代理签密人的私钥泄露，敌手仍然不能对以前签密过的密文进行解签密运算而得到明文。

(2)公开验证性(Public Verifiability)：第三方可以直接验证签密的明文来源，而不需要借助接收方的私钥。

(3)可证明安全性(Provable Security)：方案满足在适应性选择密文攻击下具有不可区分性和在适应性选择消息攻击下能抗存在性伪造。

(4)强不可伪造性(Strong Unforgeability)：除代理人以外的第三方包括授权人不能产生一个合法的代理签密。

(5)强可识别性(Strong Identifiability)：任何人能从一个代理签名中得知代理人的身份。

(6)强不可否认性(Strong Undeniability)：代理人一旦对一消息进行代理签密就不能否认。

(7)防止滥用(Prevention of Misuse)：代理人不能对未经授权的消息进行代理签密。

4 新的基于身份的代理签密方案

本章提出一个新的基于身份的代理签密方案，具体细节如下。

4.1 系统初始化

给定安全参数 l^k，TA 选取阶为 q 的加法循环群$(G,+)$和乘法循环群$(V,\cdot)$，群 G 的生成元 P，双线性映射 $\hat{e}:G\times G\to V$。定义三个安全 Hash 函数：$H_0:\{0,1\}^*\to G\backslash\{0\}$，$H_1:\{0,1\}^*\to Z_q^*$，$H_2:v\to\{0,1\}^{n+l}$，其中 n 是表示一个明文所需的比特数，l 是表示 G 中元素所需的比特数。然后 TA 随机选择主密钥 $S\in Z_q^*$，计算 $Q_{TA}=sP$。最后 TA 保密 s，公开系统参数 $G,V,q,\hat{e},H_0,H_1,H_2,Q_{TA},P$。

4.2 用户密钥的提取

用户 U 将其身份信息 ID_u 提交给 TA，TA 计算用户公钥 $Q_U=H_0(ID_U)$ 和私钥 $S_U=sQ_U$。则原签密人 Alice、代理签密人 Park、接收者 Bob 对应的公钥和私钥分别为(Q_A,S_A)、(Q_P,S_P)、(Q_B,S_B)。

4.3 代理签密密钥的生成

Alice 生成一个许可证 m_w 来说明 Alice 和代理人 Park 之间的授权关系，同时也说明该授权关系的使用限制等内容。Alice 计算 $h_1=H_1(m_w)$ 和 $Z=h_1S_A$。Alice 将(m_w,Z)发给 Park。Park 验证下面等式是否成立：$\hat{e}(Z,P)=\hat{e}(Q_{TA},Q_A)^{h_1}$。如果成立，则计算 $Z_P=Z+h_1S_P$，并将 Z_P 作为代理签密密钥。

4.4 代理签密

给 Bob 签密消息 $m\in\{0,1\}^n$，Park 首先随机选择 $k\in Z_q^*$，然后计算 $X=kQ_P$，$r=H_1(X\|m)$，$T=(k+r)S_P+Z_P$，$Q_B=H_0(ID_B)$，$w=\hat{e}(S_P,Q_B)^k$，$c=H_2(w)\oplus(T\|m)$，则 $\sigma=(m_w,c,X)$为 Park 代表 Alice 的代理签密。

4.5 解签密

收到 $\sigma=(m_w,c,X)$后，Bob 先计算 $w=\hat{e}(X,S_B)$，$T\|m=c\oplus H_2(w)$。然后计算 $r=H_1(X\|m)$，并验证下面等式是否成立：$\hat{e}(T,P)=\hat{e}(Q_{TA},X)\hat{e}(Q_{TA},Q_P)^r\hat{e}(Q_{TA},Q_P+Q_A)^{h_1}$，成立则接受 m，否则返回 $\perp$。

5 安全性质和效率分析

5.1 安全性质分析

(1)前向安全性：解签密需要知道 $w=\hat{e}(S_P,Q_B)^k$。但对于一个攻击来说，即使得到了代理签密者的私钥 S_P，想从 X 得到 k 是困难的，因为它相当于解 G 上的 ECDLP 问题。

公开验证性：当接收方与代理签密人之间存在分歧时，Bob 可以将(m,m_w,X,T)提交给第三方，第三方计算 $r=H_1(X\|m)$和 $h_1=H_1(m_w)$，验证 $\hat{e}(T,P)=\hat{e}(Q_{TA},X)\hat{e}(Q_{TA},Q_P)^r\hat{e}(Q_{TA},Q_P+Q_A)^{h_1}$ 是否成立。若是，则认为 m 确为 Park 给 Bob 签密的消息。

(3)可证明安全性：与文献[5]证明类似，可证明新方案满足在适应性选择密文攻击下具有不可区分性和在适应性选择消息攻击下能抗存在性伪造。

(4)强不可伪造性：因为主密钥 s 被 TA 秘密保存，通过 $Q_{TA}=sP$ 求解 s 相当于求解 ECDLP 问题。因此除 Park 以外的任何人(包括原签密人、签密接收者 Bob 和其他第三方)都不能建立有效的代理签密密钥。另外文献[7]中的几种攻击对新方案都无效。

(5)强可识别性：完整的代理签名(m,m_w,X,T)中有原签密人 Alice 的授权 m_w，任何人都能从 m_w 中确定代理签密人的身份。

(6)强不可否认性:由于授权 m_w 包含在有效的验证等式里,因此代理签密人不能随便更改 m_w,所以一旦代理签密人创建了一个有效的代理签密,他就不能否认。

(7)防止滥用:由于授权 m_w 包含在有效的验证等式里,因此代理签密人不能签署未经授权的消息,当然他不能把代理签密权利转给其他人。

5.2 效率分析

下面将本文的方案与张和王的方案[8]从计算复杂性进行比较,并将结果总结在表 1 中。表 1 中有关符号定义如下:P_a 表示双线性对运算,P_m 表示 G 中的标量乘运算,A_d 表示 G 中的点加运算,M_u 表示 V 上的乘运算,E_x 表示 V 上的指数运算。$x(+y)$ 表示需要 x 次双线性对运算,y 次双线性对预运算。

表 1 计算复杂性比较结果

方案	私钥	整个代理签密方案				
		E_x	A_d	P_a	P_m	M_u
文献[8]	2	7	3	3(+7)	3	4
本文方案	1	4	3	4(+3)	4	2

从表 1 可以看出除了增加了一个中的标量乘运算和一个对运算外(但对运算总数减少三个),其它运算均有减少。另外新方案仅需要一个密钥,给 TA 减轻了计算负担,同时也给用户储存私钥带来了方便,因此该方案更适合于应用。

6 结束语

本文主要提出了一个新的基于身份的代理签密方案,并且对本文方案的安全性质和效率进行了分析。与其它的基于身份的代理签密方案相比,该方案最大的特点在于同时具有前向安全性和可公开验证性,并且效率更高。与方案[8]相比本方案仅需要一个私钥,更适合应用。(收稿日期:2007 年 7 月)

参考文献:

[1] Mambo M,Usuda K,Okamoto E.Proxy signature:delegation of the power to sign messages[J].IEICE Trans Fundamentals E79-A,1996,9:1338-1353.

[2] Zheng Y.Digital signcryption or how to achieve cost (Signature & Encryption)≤Cost (Signature)+Cost (Encryption)[C]//LNCS 1294:CRYPTO'97.Berlin:Springer-Verlag,1997:165-179.

[3] Gamage C,Leiwo J,Zheng Y.An efficient scheme for secure message transmission using proxy-signcryption[C]//Edwards J.Proceedings of the 22nd Australasian Computer Science Conference.Auckland:Springer-Verlag,1999:420-431.

[4] Shamir A.Identity-based cryptosystems and signature schemes[C]//Blakley G R,Chaum D.LNCS 196:Advances in Cryptology-CRYPTO'84.Berlin:Springer-Verlag,1984:47-53.

[5] Chen L,Lee M.Improved identity-based signcryption[C]//Vaudenay S.LNCS3386:Public Key Cryptography-PKC2005.Berlin:Springer-Verlag,2005:362-379.

[6] Li Xiang-xue,Chen Ke-fei.Identity based proxy-signcryption scheme from pairings[C]//Proceedings of the IEEE International Conference on Services Computing(SCC 2004),2004:494-497.

[7] Wang Meng,Li Hui,Liu Zhi-jing.Efficient identity based proxy-signcryption schemes with forward security and public verifiability[C]//The Third International Conference on Networking and Mobile Computing (ICCNMC 2005).Berlin:Springer-Verlag,2005,3619:982-991.

[8] Zhang Xue-jun,Wang Yu-min.Efficient identity-based proxy signcryption[J].Computer Engineering and Applications,2007,43(3):109-111.

(上接 156 页)

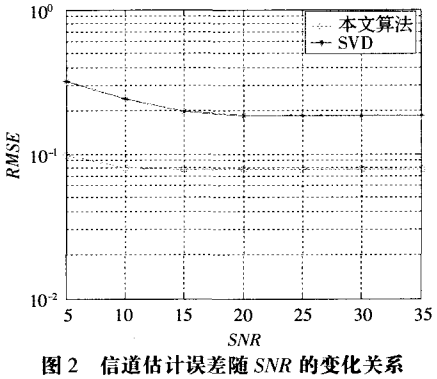

图 2 信道估计误差随 SNR 的变化关系

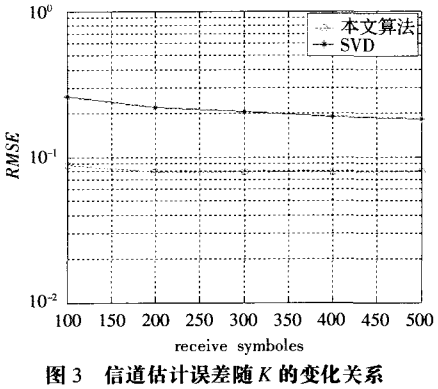

图 3 信道估计误差随 K 的变化关系

算法,该算法通过使用导频给出精确的信道初始值,并结合一种子空间跟踪算法来估计信道参数。该算法不仅提高了收敛速度,降低了计算复杂度。而且仿真结果也表明,有较好的估计精度,有助于改善信道的均衡性能。(收稿日期:2007 年 7 月)

参考文献:

[1] Muquet B,Wang Z,Giannakis G B,et al.Cyclic prefixing or zeros padding for wireless multicarrier transmissions? [J].IEEE Trans Commun,2002,50:2136-2148.

[2] Sandell M,Edfors O.A comparative study of pilot-based channel estimations for wireless OFDM [R].Research Report TULEA 1996:19,Div of Signal Processing,Lulea University of Technology,1996-09.

[3] Coleri S,Ergen M,Bahai A.Channel estimation techniques based on pilot arrangement in OFDM systems[J].IEEE Trans Broadcast,2002,48(3):223-229.

[4] Muquet B,de Courville M,Duhamel P.Subspace-based blind and semi-blind channel estimation for OFDM systems[J].IEEE Trans on Signal Processing,2002,50:1699-1712.

[5] Roy S,Li C.A subspace blind channel estimation method for OFDM systems without cyclic prefix[J].IEEE Trans Wireless Communication,2002,1(4):572-579.

[6] Altuna A J,Mulgrew B B,Badeau C R,et al.A fast adaptive method for subspace based blind channel estimation[C]//Proc of I-CASSP,2006:1121-1124.

[7] Golub G H,van Loan C F.Matrix computations [M].3rd ed.[S.l.]:Johns Hopkins University,1996.