学校编码：10384　　分类号_____密级 _____

学　　号：200223011　　UDC_____

厦　门　大　学

硕　士　学　位　论　文

一种无证书的环签名方案和一个基于身份的多重签名方案

A Certificateless Ring Signature Scheme and An ID-Based Multisignature Scheme from Multilinear Forms

吴问娣

指导教师姓名：　曾　吉　文　教授

专　业　名　称：　基　础　数　学

论文提交日期：　2005　年　4　月

论文答辩日期：　2005　年　6　月

学位授予日期：　2005　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2005 年 4 月

一种无证书的环签名方案和一个基于身份的多重签名方案
吴问娣
指导教师 曾吉文教授
厦门大学

厦门大学学位论文

的学位论文　　人　导师指导　　的

人　论文　　的　个人　　的

文　　方　　人　　和　　论

文　　的　　和

人　签名：

年　月

签名 密码学的重 问 一 的 和身份
证 基于 密码 和 密码 签名
密码 的 签名的 和 一 的
于 密码 和 的 一 证 的
的 密码 证书方 证 的
证书的 和 的 的一个
的问 一 基于身份的 密码 ID-PKC 证
书问 的 身份的 一方
ID-PKC 一个 的 密 问 个 重
ID-PKC 一个基于身份的签名方案 PKG
的签名 的签名 的 2003 年
密会 Al-Riyami 和 Paterson 一种 的 无证书的
密码 CL-PKC CL-PKC 证书问 密 问
文 种类 的 签名方案 的
分 一种 ： 无证书的 密码 一种无
证书的环签名方案 证 无 名的
的 Diffie Hellman 问 的 方案
的 方案的 [9] 的基于身份的环签名
种 ：一种 多 基于身份
的 多重签名方案 的 基于 Diffie Hellman 问

：环签名 多重签名

Abstract

Digital signature, one of the important applications of public key cryptosystem, can be used to protect data integrity and authenticate the identity of the sender of a message. It plays an important role in the electronic transactions. Public Key Cryptography (PKC)is gaining a considerable attention because it can assure the security requirements of many applications. To guarantee the authenticity of public key, there is a need to provide an assurance to the user about the relationship between a public key and the authority of the holder of the corresponding private key. In traditional Public Key Cryptography,this assurance is delivered in the form of certificate,essentially a signature by a Certification Authority(CA)on a public key. However, the management of infrastructure (supporting certificates) is the main complaint against traditional PKC. While Identity-Based PKC can eliminate this troublesome infrastructure, the key escrow of user's private key is inherent in identity-based PKC. Recently, a new PKC paradigm called the certificateless PKC was introduced, it eliminates the need of certificates and retains the desirable properties of identity-based PKC without key escrow problem.

In this paper, we propose a certificateless ring signature scheme, based on the bilinear pairings, which provides unconditional anonymity ,and we analyze this scheme which is existentially unforgeable under adaptive chose-message attacks, in the random oracle model, assuming that the Generalized computational Diffie-Hellman problem is hard to solve. We propose an ID-based broadcasting multisignature scheme from multilinear forms and its security bases on the hardness of the computational Diffie-Hellman problem.

Key words: Ring Signature Public Key Cryptography Multisignature.

Contents

第一章 引 言

的 人 的
一个 的 种 大 于 的
的 签名 一种 的 的重
分 签名 一种 一个 签名的方
方 的签名 人 无 的一
的 签名 的一种证 基于 密码
和 签名 密码 的 签名
的 和 一 的 于 签名的 主
密码 的 签名的 于 的 密码
分 的 密码 基于身份的 密码 [1]和 的无
证书的 密码 [2] 种 密码 的 签名方
案 种类 的 签名方案

密码 的 Diffie 和 Hellman 于 1976 年 的
密码 1977 年 Rivest Shamir 和 Adleman
名的 RSA 密码 基于分 大 的 问 人 基
于 的 的 问 大 的 密码 的
的密码 的密码 方 一个 密密
密 于 密 密 导 一 密 分 问 ：
于一个密码 密密 分
N 个 的 C_N^2 个 密密 一个 密
密密 密 密密 密的 密码
密 分 分 问 分 和
一个 的 名 的 的

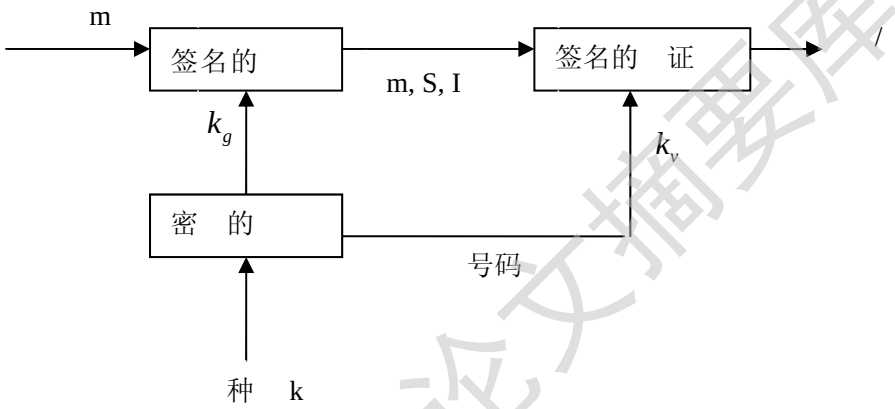
签名 (人) 密 一 密的
的 密 的 一
密 密文 密的人 密码 个
问 的 的 证书方
证书 和 的 一 证
的 证书的 和 的 的一
个 的问 一 1984 年 Shamir 一个基于身份的
于 的 的方 的问 基于身份的
ID-PKC , 的 身份的 一方
的 IP E mail 的身份证号 的 一个
的 方 KGC ID-PKC 一个
的 密 问 的 KGC 和分
个 重 ID-PKC 一个基于身份的
密方案 KGC 密 密文 的问 一个基于身份的
签名方案 KGC 的签名 的签名 的
个问 的方 一 2003 年 密会 Al-Riyami 和
Paterson 一种 的 无证书的 CL-PKC
CL-PKC ID-PKC 密 问 CL-PKC
一个 方 KGC ID-PKC 的 KGC CL-PKC 的
KGC 的 的 分 的
的 密 和 分 个 基于身份的
的身份 于 的 和 ID-PKC
无证书 签名 的
ID-PKC 的
的 密码 签名 的 证 证 的
个 大 多的 和 和

的

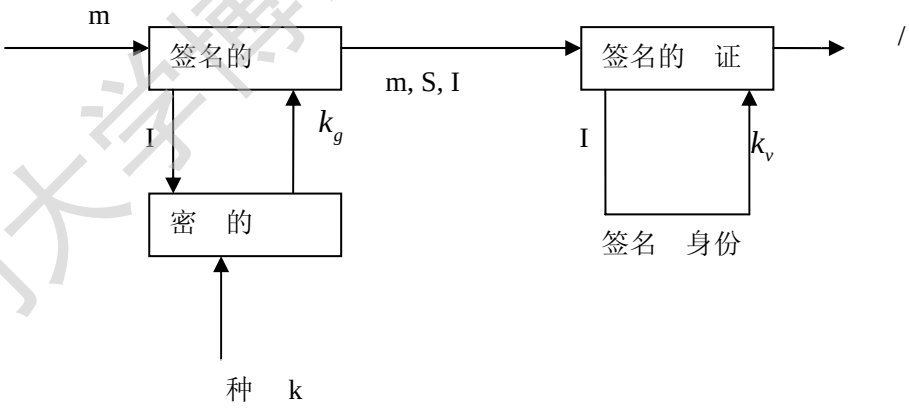
签名方案和基于身份的签名方案　　的

签名密　k_g　　m 签名　　m　　签名 S 和签名　的身份 I 一

证　　证　　证密　k_v　　证签名



(a)　　签名方案



b　基于身份的签名方案

签名方案和基于身份的签名方案　　的

证 的签名 的 签名分 名
签名和 名签名 一 签名 名签名 签名
和环签名 名签名 环签名
人于 2001 年 一 [3] 人 的重 [5
8] 一签名 一个签名 一个 的
环 Ring 的 和 人的 个环
一个 签名 员的 证 个签
名 个环的 个 员 的 的
的签名 无 名 环签名的 种
无 名 的一 环 环签名
于 签名 环签名 的 的
和 问
文 一种 ID-PKC
的 密码 的无证书的环签名方案 基于 Schnorr 的签
名方案 [3] 证 方案 的
Diffie-Hellman 问 的
的
于环签名人 的环签名 文
4 人 密 和 一个基于 的
的环签名方案 证 个方案 的 密 密
0 1 ^{l} 的一个 的
人 4 的方案 环签名方案
个基于 的环签名方案 一个基于 的 门 环签
名方案 人 一个 的环签名 个
于 类 的 的 的
和 一 的环签名方案的

证 方案 的 的 D C

和 8 的 一个基于身份的环签名

方案 的方案的 一个 的证

和 一个基于身份的 证 的环签名方案

一类签名方案 签名 多个 一

签名和 证 多个 一 签名的签名 多重签

名 10 签名 的 多重签名方案 分 类：一类 多重

签名方案 一类 多重签名方案

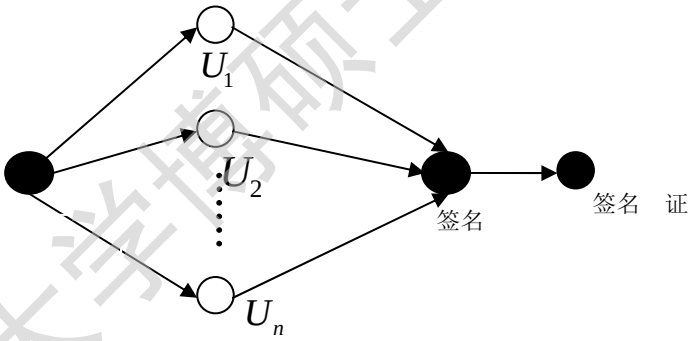
多重签名方案 签名 签名 和

签名 证 一位签名 签名

签名 签名 签名 签名

签名 证 签名 证 证多重签名的 多

重签名方案



1 4年 一种 多重 签名方案 文

一种 多 的基于身份的 多重签名方

案

第二章　预备知识和基本概念

§2.1　双线性对和多线性映射的知识

G_1　　的一个　　的　环　　G_2

一个　　的　环　　G_1和G_2　　问

的

1　　$e:G_1\times G_1\to G_2$　一个　　11　　：

1　　：　　$P,Q\in G_1,a,b\in Z_p$　　$e(aP,bQ)=e(P,Q)^{ab}$

Z_q　　的　　类

2　　：　　P　$Q\in G_1$　　P　Q　　1_{G_2}

3　　：　　P　$Q\in G_1$　　一个　　的　　P　Q

G_1　G_2　　的一个　　的　　12

G_1　　F_p　　的　　的一个　　G_2

$F_{p^2}^*$的　　一个

≡2　3 的　　3 的　　1　　F_p　方

$y^2=x^3+1$的　　F_{p^r}　　F_{p^r}　　的

：

1　　x^3+1　F_p　的一个　　F_p　　1 个　　无

∈　F_p　一个　　的　G_1　　的　的

2　　$1\neq\zeta\in F_{p^2}$　x^3-1　0　F_{p^2}　一个　　$\Phi(x,y)=(\zeta x,y)$

$E\left(F_{p^2}\right)$ 的一个 (x,y) $E\left(F_{p^2}\right)$ 的

$\forall$ $\in$ F_p $\Phi(Q)\in E(F_{P^2})$ $\Phi(Q)\notin E(F_p)$

$\in$ F_p $\Phi(Q)\in E(F_{p^2})$ 无 的

3 $P\in G_1,\Phi(P)$ 无 的 的 于 $Z_q\times Z_q$

$Z_q\times Z_q$ $E[q]$

G_2 一个 的 $F_{p^2}^*$ 的一个 $E(F_{p^2})$ 的

$E[q]\times E[q]\to G_2$ $\forall$ $\in$ F_p

$e(Q,P)=1$ 一个 的

：$G_1\times G_1\to G_2$ $\Phi(Q)$ 的 个

文 12 13 14 的 和

一个 的 于 多的密码 1

2 $e_n:G_1^n\to G_2$ 一个 ：

1 多 ： a_1 a_n Z_q P_1 P_n G_1

$$e_n(a_1P_1,\mathrm{L}\ ,a_nP_n)=e_n(P_1,\mathrm{L}\ ,P_n)^{a_1\mathrm{L}\ a_n}$$

2 ： G_1的一个 e_n G_2的

3 ： P_1 P_n G_1 一个 的

e_n P_1 P_n

于多 密码学 的 1

H_1 $\{0,1\}^*$ G_1^* H_2 $\{0,1\}^*$ Z_q^* 个 的

方案的 基于的 个 问 ：

一个 的

D 问 CD $\in Z_q^*$ P P

$P \in G$ P

的 D 问 CD $\in Z_q^*$ P P

$Q \in G$ Q

答 Q P CD CD CD CD

的一个 的 多 个问

§2.2 签名方案的一般定义

一 1 一个 签名方案主 个 签名

和 证 签名 一个 密 签名 签一个 导 的签

名 一个 的 证 证 一 签名 证 签名

一个 的 答 一个 签名方案

的 重 ：

1 的 的一个 的

2 的 签名 的一个 的

3 的 密 的一个 的 密

4 和 分 签名 和 证 一个$k \in K$ 一个

签名 $Sig_k(\cdot) \in S$ 和一个 的 证 $Ver_k(\cdot,\cdot) \in V$ 一个

$Sig_k(\cdot) \in S$ $P \to A$ 的 和 $Ver_k(\cdot,\cdot) \in V$ $P \times A \to \{$ $\}$ 的

一个 $x \in P$ 和 一个签名

$y \in A$ $Ver_k(x,y) =$ $y = Sig_k(x)$ 一个$k \in K$

$Sig_k(\cdot)$ 和 $Ver_k(\cdot,\cdot)$ 多 $Sig_k(\cdot)$ 一个 密的

$Ver_k(\cdot,\cdot)$ 一个 的 证 $Ver_k(\cdot,\cdot)$ 签名

$Sig_k(\cdot)$ 多 的 于

一个　　密　的　　签名 $Sig_k(x)$

人　　个签名　签名方案　　的

§2.3 Schnorr 数字签名方案的描述

一个　　Z_p　的　　问　　的　　1 的

一个大　　$\alpha \in Z_p^*$　　p　　1 的 q　　$P=\{0,1\}^*$　$A=Z_q \times Z_q$

$$K=\{(p,q,\alpha,a,\beta):\beta \equiv \alpha^a \pmod p\}$$

$1 \le a \le q-1$　　p　q　α,β　　a　　$h:\{0,1\}^* \to Z_q$

的

于 $K=(p,q,\alpha,a,\beta)$ 和一个　密的　　$k,1 \le k \le q-1$

$$sig_k(x,k)=(\gamma,\delta)$$

$\gamma=h(x\|\alpha^k)$　　$\delta=k+a\gamma \bmod q$

于 $x \in \{0,1\}^*$ 和 $\gamma,\delta \in Z_q$　　证　　的　　的：

$$ver_k(x,(\gamma,\delta))=true \Leftrightarrow h(x\|\alpha^\delta \beta^{-\gamma})=\gamma$$

$\alpha^\delta \beta^{-\gamma} \equiv \alpha^k \pmod p$　　证　　签名

一个

$q=101, p=78q+1=7879$　3　　Z_{7879}^*　的一个

$\alpha=3^{78} \bmod 7879=170$　　α　　1 的

$\beta=\alpha^a \bmod 7879=4567$

签名　　0

$\alpha^k \bmod p=170^{50} \bmod 7879=2518$

一　　$h(x\|2518)$　　的　　2 18　　位