份的签名方案

" d S Ä 和上节中基于分级身份签名方案的初始化相同 公开参数为0 - 1 其中 为 : 的私钥 同时定义哈希函数7 +0 1^C 以及随机选择

á 4 | 由第 (= 层发放给第 (层用户&+随机选择 . . 第 (层用户 % < % %= %&私钥为+ % <

$(D $&< % % (& (D &

& 用户 % 的私钥为 % < $(D $& 用户 % 对文件 进行签名 选择一个随机数 . C 计算 5 <

和6 < 7 5& 则签名为 < 6 5&

£ 给定 % 以及签名 < 6 5& 验证如下等式+ 6&< & % % (& 5 7 5&&

若等式成立 则此签名有效 否则签名无效

ç Ø 假设 D & . 4 ? 假设在群 成立 那么这个基于分级身份的签名方案在给定攻击身份 选择消息攻击下就是 - - D ——& &安全的 其中 E = - D - && - - 分别是询问私钥和签名的次数 指的是下一次指数运算所需要的最大时间

证明+假设一个攻击者能够成功伪造签名 那么就可以构造一个算法 , 解决 D & . 4 ? 问题 首先任意给定算法 , 如下的一个 D & . 4 ? 问题+ < / < / = < / = < / D < / D (D < / D 要求 / D 6 在得到系统参数之前公布他将攻击的目标身份 % < % % (& . (, 则根据目标身份在后面的 = (层都添加 , 令 < 选择一个随机 . . 令 < 然后选择 并计算 < 8 = D 同时选择 . . 令 < % C = D 然后将这些参数给攻击者 模拟者的私钥 未知& 4 / < D

6 首先进行 -7 次7 函数的询问 - 次% 私钥提取的询问和- 次签名的询问 模拟技巧和过程和定理 的证明非常类似 在此省略 最后 可以得到 如果 D = . 4 ? 假设成立 新的基于分级身份的签名方案就是安全的

9 ²

本文提出两个效率更高的基于分级身份的签名方案 第一个新的基于分级身份的签名方案在随机应答模型下是给定身份攻击下安全的 即使攻击者选择明文和身份进行攻击 同时 它的安全性是基于计算4 2'$ $(' 困难假设的 新方案效率是目前方案中效率最高的 特别是它的签名算法只需要两次指数运算 并且安全性证明不依赖于分叉原理 从而安全归约的效率很高 同时 本文第一次提出了一个签名长度与签名者身份的深度无关的基于分级身份的签名方案

• I Ó D

8 9 / F @)$ **+ , -$) '&+0* -+-*$" -) - * &$ -'%&" $-8 9 : ?! @ > GF 4 1) 7) 1 '$- >&+0* (+ >@ A &' $$) - 8 > 9 G/ / 0& $&& 7 >/ ; =

8 9 . A ? 4 @ : F) $ * *+ , -$) $ ' &+0* 2&" *%$ #$ (0 & 8 9 : $) 1 '$- >&+0* (+ >@ A &' $$) -8>9 G/ / 0& $&& >/ =

8 9 . A ? 4 . A! ? H ?2' $ * -$($ * 1$ 4 -$' &$) $ **+ , -$) $ ' &+0* # *% * &) " &' ($- 8 9 > > >%&- * > F ? / >) 1 '$- >&+0* (+ ?G@A >@ &' $$) - 8>9 / # *6$&( ) / 0& $&& >/ = 7

8 9 . A ? 4 . A! ? H / $ &$) $ * *+ , -$) $ ' &+0* # *% * &) " &' ($- 8 9 @ : F **%$# :) 1 '$- >&+0* (+ >@ A &' $$) - 8 > 9 G/ / 0& $&& >/ =

8 9 . A ? 4 : " 0& 1$) $2' $ ' + 2 &>> -$' &$ ' &+0 * -+-*$' - , (* -) $ * *+ , -$) $ ' &+0* 8 9 F ? ? ?/ (2&$) 0 ' - >&+0* (+ > @ &' $$) -8>9 G/ / 0& $&& >/ ; 7 =

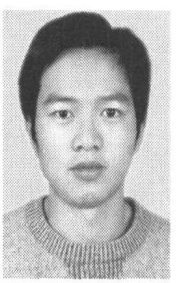
8; 9 ? @ > / B?@ ?@ $&& % (4 , -$) ' &+0* &0%+8 9 ? ! ( ) 1 '$- >&+0* (+ / >@ 8>9 $# $ ( ) / 0& $&& >/ 7= ; ;

8 9 . A ? 4 . A! ? H A ? $&& %' ( ) $ * *+ , -$) $ ' &+0* # *% ' -* * - 6$ ' 0%$&&$3* 8 9 >@ F ?@ @ ()) 1 '$- >&+0* (+ ?G@A>@ &' $$) -8>9 4 $ " &5 / 0& $&& >/ = ;

879 ! $# %$&&%' (4 , -$) ' &+0 * -+-*$') >> -$' &$: ?8 9 AG H , $* (; ?G> &' $$) -8>9 : A@? / 0& $&& ; >/ ; =

8 9 > A / F G > : ! G / F > A : / $' &$ $&& '%' ( ) $ **+ . -$) / * &$) *- 00(' * 8 9 0$6 1 $& $* (> >/ &' $$) - 8>9 / 0 / 0& $&& >/ ; 7 =

T € e º



Ù É 男 博士研究生 7 年生 江西人 年在西南师范大学数学系获理学学士学位 年起在中山大学数学与计算科学学院硕博连读 现在香港中文大学信息工程系任助理研究员 主要研究领域是密码学 感兴趣的方向是各类签名体制 基于身份的密码系统 包括基于身份的签名和加密

? " (-+-I (J + % ' " '

f Z S 男 副教授 生于 年 月 ; 年在烟台师范学院数学系获得理学学士学位 年在上海同济大学应用数学系获得理学硕士学位 年在西安电子科技大学通信工程学院获得密码学博士学位 现在中山大学电子与通信工程系任教 主要研究方向为椭圆曲线密码学 基于身份的密码系统

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net