一种适合于低成本标签的 RFID 双向认证协议

赵跃华, 王益维, 李晓聪
(江苏大学 计算机科学与通信工程学院, 江苏 镇江 212013)

摘 要: 在分析现有一些 RFID 认证协议的基础上,提出了一种新的适合低成本标签的双向认证协议,并对其进行了 SMV 模型检测形式化证明和性能分析。结果表明该认证协议具有认证性、保密性和完整性,能够满足低成本标签的安全需求,并且在安全性能提高的同时仍具有较好的执行性能。

关键词: 低成本标签; 射频识别; 安全协议; 认证; SMV 模型检测
中图分类号: TN915.08 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1885-04
doi:10.3969/j.issn.1001-3695.2010.05.080

New RFID mutual authentication protocol for low-cost tags

ZHAO Yue-hua, WANG Yi-wei, LI Xiao-cong
(*School of Computer Science & Telecommunications Engineering, Jiangsu University, Zhenjiang Jiangsu* 212013, *China*)

Abstract: Based on the analysis of some existing RFID authentication protocols, this paper proposed a new mutual authentication protocol for low-cost tags, and did the formal proof using SMV model checking and performance analysis of this protocol. The results show that the authentication protocol satisfies the requirements of authentication, confidentiality and integrity, and can meet the security needs of low-cost tags, in addition, the scheme also has a good performance.

Key words: low-cost tags; RFID(radio frequency identification); security protocol; authentication; SMV model checking

RFID(射频识别)是一种通过射频信号自动识别目标并获取相关数据的非接触式自动识别技术。近几年来,RFID 技术在国内外发展非常迅速,并且在各个领域得到了广泛的应用。随着 RFID 的应用不断扩大,它所面临的非法访问、跟踪、窃听、伪造、物理攻击、数据演绎、窜改、重放等安全问题日益突出。尤其在低成本 RFID 应用场合,标签受成本制约,标签芯片一般只有几千个门电路,而用于安全的资源十分有限。这些特殊性使得低成本标签不支持现有成熟的加密体制[1],这给认证协议的设计带来了极大的挑战。在 EPCglobal 公布的 EPC Class-1 Generation-2(以下简称 EPC-C1G2)协议中,虽然使用 32 bit 访问口令实现对读写器的认证[2],但是访问口令的传输使用简单的加密方法,访问口令很容易被攻击者通过窃听计算得到。一旦访问口令被攻击者获取,标签就可以被任意窜改。EPC-C1G2 标准中的安全体制还不能提供较好的安全保障,低成本标签要得到大规模的应用必须解决其安全问题。认证技术是解决 RFID 安全的关键之一,只有合法的读写器通过认证后才能对标签进行读写操作,同样只有合法的标签才能与读写器进行通信。目前,对于低成本 RFID 系统认证协议的研究已经成为 RFID 技术中研究的热点之一。

1 已有的适合低成本标签的认证方案

近几年来,针对 RFID 安全隐私问题,国内外学者已经提出了许多安全协议,但是他们大多数使用了 hash 函数或加密函数,符合低成本标签的方案并不多,仅有极少的协议能够满足要求。文献[3]中 Duc 等人提出了一个读写器和标签相互认证的协议,该协议实现比较容易,只涉及一些简单的逻辑运算和随机函数运算。但数据同步更新是该机制的主要安全隐患所在,它会带来 DoS 攻击(不能识别合法和非法的标签)、重放攻击、不能保证前向安全性等安全问题。文献[4]中 Chien 等人在文献[3]基础上提出了相互认证协议,它克服了在 Duc 方案中存在的 DoS 攻击,不能检测伪装标签,不能保证前向安全性等缺陷。但由于在该方案中对 CRC 的使用不当,留下了很大的安全隐患,该方案存在不能明确识别标签、标签假冒、读写器假冒、跟踪和自动非同步等问题[5]。在文献[6]中 Konidola 等人提出了 TRMA(tag-reader mutual authentication scheme)协议,但 Lim 等人[7]发现了 TRMA 协议存在一些安全缺陷,被动攻击者通过监听几轮通信数据并进行相关分析就可以获得访问口令 APwd。2007 年 Konidola 等人[8]又提出了 TRMA 的升级版本 TRMA+,它克服了 TRMA 协议不能抵制被动攻击的缺陷。TRMA+和 TRMA 在协议流程上是一样的,只是在密钥的计算方法上有所不同。但是 Peris-Lopez 等人[9]发现被动攻击获取 APwd 和 KPwd 密钥的可能性很大,获取的概率为 $p(\mathrm{APwd_M}) < 2^{-5}$, $p(\mathrm{APwd_L}) < 2^{-2}$, $p(\mathrm{KPwd}) < 2^{-2}$。在文献[10]中 Chien 提出了适合低成本标签的 SASI(strong authentication and strong integrity)协议,但是 Chien 等人的 SASI 协议被发现也存在一些安全缺陷。Sun 等人在文献[11]提出该协议中循环左移运算 $\mathrm{Rot}(x,y)$ 如果在循环 $y=0$ 位的情况下会造成非同步攻击,泄露标签的 ID。这些方案都存在一定的安全隐患,还不能应用到实际的低成本 RFID 系统中。

2 基于动态密钥的双向认证协议

本文在综合已有各种方案[2~4,6,8,10]的基础上,提出了一种

收稿日期: 2009-08-05; **修回日期**: 2009-10-21

作者简介:赵跃华(1958-),男,江苏苏州人,教授,博士,主要研究方向为信息安全(zhaoyh@ujs.edu.cn);王益维(1983-),男,江苏盐城人,硕士研究生,主要研究方向为无线通信安全;李晓聪(1985-),女,安徽淮北人,硕士研究生,主要研究方向为信息安全、空间数据库技术.

基于动态密钥的双向认证方案,该方案改进了已有方案的不足之处,并通过形式化证明和安全性分析,说明改进方案是安全的并能达到较好的安全性能。

2.1　认证过程

初始时,每个标签在出厂前随机选择一个 32 bit 访问口令 APwd、一个 32 bit 销毁口令 KPwd、一个 32 bit 密钥 K、电子产品编码 EPC 和协议控制码 PC 一起存储在标签和后台数据库中。在认证时,标签先发送一个匿名 IDS 给读写器,读写器从后台数据库中查找到相应信息后发送访问口令来验证读写器,同样标签也发送访问口令来验证标签。具体认证过程如图 1 所示。其中,‖ 表示级联运算符;K_M 表示 K 的高 16 bit;K_L 表示 K 的低 16 bit。

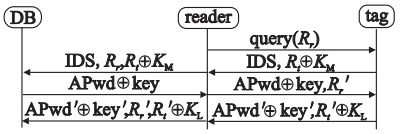

图1　本文的认证方案

认证过程如下:

a)R→T。读写器向标签发送询问请求 query,参数为 R_r。

b)DB←R←T。标签产生随机数 R_t,并计算 IDS = [CRC(EPC ‖ R_r) ‖ CRC(PC ‖ R_t)]⊕K,然后将(IDS,R_t⊕K_M)发送给读写器,读写器将(IDS,R_r,R_t⊕K_M)转发给后台数据库。后台数据库根据该读写器的权限,遍历其权限内的标签数据查找是否存在[CRC(EPC ‖ R_r) ‖ CRC(PC ‖ R_t)]⊕K == IDS。如果找到,提取出对应的 EPC、APwd、KPwd、K 等信息,并转到 c);否则,结束认证。

c)DB→R→T。后台数据库利用 K_M 解密 R_t,根据 APwd、KPwd 和 R_r 计算出密钥 key,再将 APwd 和 key 异或后发送给读写器,读写器发送 APwd⊕key 和一个新的 16 bit 随机数 R_r′给标签。标签收到 APwd⊕key 后,根据标签存储的 APwd′、KPwd′和随机数 R_r、R_t 计算出密钥 key 来解密密文,验证读写器发送的 APwd 和标签内存储的 APwd′是否一致,如果一致,则读写器通过认证,并转 d);否则,认证失败,停止操作。

d)DB←R←T。标签生成新的随机数 R_t′,利用 R_r′和 R_t′生成新的密钥 key′加密标签中存储的 APwd′发送给读写器,同时也将 R_t′⊕K_L 发送给读写器。读写器再将 APwd′⊕key′、R_r′和 R_t′⊕K_L 转发给后台数据库,后台数据库用 K_L 解密出 R_t′后,根据 APwd、KPwd、R_r′和生成 key′来解密 APwd′⊕key′,验证标签发送的 APwd′与后台数据库存储的 APwd 是否一致,如果一致,则标签通过认证;否则,认证失败,停止操作。

2.2　匿名 *IDS* 的构造

CRC 的作用与散列算法大致相同,但是 CRC 并不是严格意义上的散列算法。CRC 是一种线性运算,Duc 和 Chien 的两个认证方案都使用了 EPC 标准中 16 bit 的 CRC-CCITT[2]。在文献[12]中列举了大量的数据,它们的 EPC、K 都不同,但计算出来的 M_1 = CRC(EPC ‖ N_1 ‖ N_2)⊕K_n 都是一样的,这样后台数据库根本无法识别出标签的 M_1 对应于哪个 EPC,如果出现这种情况,那么认证协议就失去了意义。出现这种情况主要是因为对 CRC 的使用不当,CRC-CCITT 结果只有 16 bit,那么对应的 M_1 最多也只有 65 536 个。当标签数量急剧上升时,无法识别的概率会大大增加。根据生日悖论[13]理论可知,从符合离散均匀分布的区间[1,d]随机取出 n 个整数, 至少 2 个数字有相同的概率:

$$p(n;d)=\begin{cases}1-\prod_{k=1}^{n-1}\left(1-\frac{k}{d}\right) & n\leqslant d\\ 1 & n>d\end{cases}$$

在 Chien 等人的协议中,当标签数量达到 300 时,出现无法识别的概率为 50%;当标签数量达到 580 时,出现无法识别的概率为 90%;当数量达到 800 时,概率为 100%。具体概率分布如图 2(a)所示。

通过 16 bit 的 CRC 来表示标签的匿名是不符合实际情况的。所以在本文新方案中使用的两个 16 bit 的 CRC 级联成一个 32 bit 的数据,并且与 32 的密钥 K 异或后作为匿名 IDS。当 IDS 为 32 bit 时,结果可以有 2^{32} 个,当标签数量达到 77 200 时,无法识别的概率才达到 50%;当标签数量达到 140 000 时,无法识别的概率才达到 90%;当标签数量达到 200 000 时,无法识别的概率才达到 100%,具体概率分布如图 2(b)所示。可见本文所使用的 32 bit IDS 能够表示更多的标签,在标签数量较少的情况下,发生碰撞导致无法识别的概率很小。

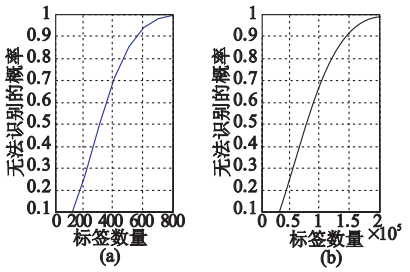

图2　无法识别标签概率分布图

2.3　密钥 *key* 的构造算法

密钥 key 的构造思想:用 APwd 从 16 bit 随机数 R_r 和 16 bit 随机数 R_t 中各选出 8 bit 数据来构成密钥 key 的低 16 bit,用 KPwd 从 16 bit 随机数 R_r 和 16 bit 随机数 R_t 中各选出 8 bit 数据来构成密钥 key 的高 16 bit,这样密钥 key 能达到 32 bit 的长度,在传输访问口令时无须进行两次传输,而且密钥的 key 的构造只有授权读写器和合法标签知道。

下面以 Apwd 为例说明如何构造密钥 key 的低 16 bit,当授权读写器与标签建立连接后,读写器和标签中都存储一组数据[EPC、K、APwd、KPwd],对于每个 EPC 都有一组[K、Apwd、KPwd]相对应。设访问口令 APwd 的二进制形式为 APwd = $(a_0a_1a_2a_3\cdots a_{28}a_{29}a_{30}a_{31})_B$、十六进制形式为 APwd = $(b_0b_1\cdots b_6b_7)_H$、十进制形式为 APwd = $(c_0c_1\cdots c_6c_7)_D$。

随机数 R_r 和 R_t 的二进制形式为 $R_r=(r_0r_1\cdots r_{14}r_{15})_B$,$R_t=(t_0t_1\cdots t_{14}t_{15})_B$。密钥 key 的二进制形式为 key = $(k_0k_1\cdots k_{14}k_{15})_B$。那么密钥 key 的计算方法为

$$k_0=r_{c_0},k_1=r_{c_1},\cdots,k_7=r_{c_7},k_8=t_{c_0},k_9=t_{c_1},\cdots,k_{15}=t_{c_7}$$

总的表达式为

$$k_i=\begin{cases}r_{c_i} & 0\leqslant i\leqslant 7\\ t_{c_i-8} & 8\leqslant i\leqslant 15\end{cases}$$

比如 APwd = $(13A6,9CFD)_H$,R_r = (0010,1100,1011,1011),R_t = (1101,0110,1001,1101),图 3 为密钥 key 的构造流程,其结果为 key[0-15] = (0010,0110,1101,0111)。由 KPwd 构造密钥 key 的高 16 bit 过程与此类似,这里不再阐述。

3　协议的 SMV 模型检测形式化分析

模型检测已被证明是分析密码协议的一种非常成功的途

径。SMV(symbolic model verifier,符号化模型检测)[14]是一个功能强大的符号化模型检验工具,在安全协议验证方面有强大的优势。在利用 SMV 软件进行安全协议的验证时首先要建立该协议的模型,然后将其要验证的安全属性用 CTL(computation tree logic,分支时态逻辑)语言进行描述作为模型的输入,最后通过系统有限状态的遍历输出验证的结果,如果系统具有给定的安全属性则输出 true;否则,输出 false,并显示不满足安全属性的反例。

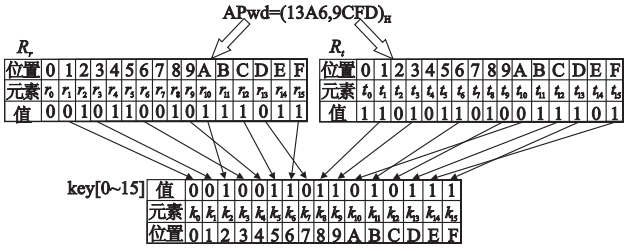

图3　密钥key低16 bit的构造流程

3.1　协议建模

在本文的认证协议中包括读写器 R、标签 T 和后台数据库 DB 三个主体,为了简化协议验证的过程,假设读写器与后台数据库之间的通信是安全的(这种假设在 RFID 安全协议的研究中是常用的,并且符合实际情况),这样只需验证读写器与标签之间的认证协议即可。为了验证协议的安全漏洞,加入入侵者 I,他可以窃听到系统内任何主体所发出的消息,并可以重放这些消息,或从消息中提取知识,根据这些知识伪造新的消息。

R 和 T 的有限状态转换如图 4 所示(其中,! 表示发送消息;? 表示接收消息;ε 表示自动进入下一状态)。R 和 T 的状态结合分别为{Idle、G_msg1、W_msg2、G_msg3、W_msg4、Finished}和{Idle、W_msg1、G_msg2、W_msg3、G_msg4、Finished},协议的发起者 R 从初始状态 Idle 开始,自动转换到 G_msg1 状态产生消息 1,并在发送消息 1 后进入 W_msg2 状态等待消息 2;当接收到消息 2 后进入 G_msg3 状态产生消息 3;并在发送消息 3 后进入 W_msg4 状态等待消息 4;当接收到消息 4 后转换到 Finished 状态,响应者 T 的过程和 R 相似,当 R 和 T 都进入 Finished 状态后,就执行了一次密钥分配协议。

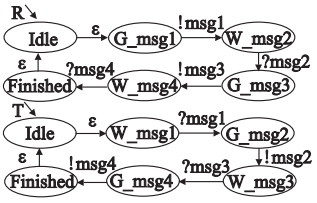

图4　R和T的状态转换图

入侵者 I 可以冒充每一个合法主体的行为,其状态转移图比较复杂,在此不对其有限状态进行显示建模而在相应程序中应用 SMV 输入语言对其能力进行描述。

3.2　协议安全属性的 CTL 描述

认证协议的目的是确保通信双方都是合法的。对认证协议的安全要求包括:a)认证性。通信双方能够相互认证对方的身份。b)保密性。保证非法主体不能获知认证的机密信息。c)完整性。保证双方的认证消息中途未被修改。

对于保密性和完整性的 CTL 分别描述如下:

a) AG((Reader.BegInit_count >= Tag.EndResp_count)&(Tag.BegResp_count >= Reader.EndInit_count));

b) AG(~((Intruder.get_Rr=1)&(Intruder.get_Rt=1)));

c) AG((Reader.state_init=Finished)&(Tag.state_resp=Finished))。

3.3　协议的验证结果

将上述各主体状态转换图所对应的程序和系统安全属性的 CTL 公式,保存为".smv"文件,输入到 SMV 工具中,运行 SMV 之后,得到各个安全属性的验证结果如图 5 所示。结果均为真,表明该认证协议具有认证性、保密性和完整性。

Property	Result
(AG((Reader.BeIint_count>=Tag.EndResp_count)&(Tag.BegResp_count>=Rea	true
(AG(~((Intruder.get_Rr=1)&(Intruder.get_Rt=1))))	true
(AG((Reader.state init=Finshed)&(Tag.state_resp=Finished)))	true

图5　改进方案的验证结果

4　协议的性能分析

从安全角度出发,本文提出的新的认证方案安全性比已有方案有了很大程度提高。表 1 为各种方案的性能比较。本文方案的具体安全性能如下:

a)本文方案中 EPC 没有在信道中直接传输,而是通过发送匿名的 IDS 来发送标签的身份,不会引起跟踪、隐私泄露等问题。

b)本文方案是一个双向认证协议,只有授权的合法读写器和合法的标签才能成功通过认证;否则,只要有一方非法,认证就不能通过。

c)用于认证的访问口令在传输时采用的是一次一密,可以防止重放攻击和中间人攻击,另外也无须考虑密钥的同步更新问题。

d)加密访问口令的密钥 key 由读写器和标签产生的随机数共同决定,攻击者无法获取密钥。而且在 EPC-C1G2 标准中密钥由标签单独产生,由于标签中产生的随机数是伪随机数,是按一定的规律产生的,随机数的质量不高,易产生弱密钥。

e)改进方案每次认证的数据没有相关性,IDS、密钥 key 均与两个随机数有关,前后两次产生的随机数关联性很小,即有前一次随机数猜测下一次随机数的概率很小。攻击者通过窃听每次的认证消息无法获取有用的信息,从而能够保证前向安全性。

表 1　本文方案与已有方案的安全性能比较

协议	跟踪	非法访问	标签假冒	重放	同步攻击	前向安全
EPC-C1G2	×	×	×	×	√	×
Duc	√	√	√	×	×	×
Chien	√	√	√	×	×	×
TRMA +	×	√	√	√	√	×
SASI	√	√	√	×	×	√
本文方案	√	√	√	√	√	√

从硬件实现复杂度的角度考虑,改进方案中没有使用计算复杂的加密算法,认证时,标签只需使用五次 XOR 操作、两个 16 bit 伪随机数、两次 CRC 计算和两次密钥的构造,在构造密钥时只需多消耗一些存储空间,所以实现仍比较简单。另外,由于每次加密的数据只有 32 bit,使用的是 XOR 操作,执行速度比较快。但是安全性能的提高也带来了其他性能的降低,如发送匿名 IDS 会增加后台数据库的查找时间,并且大量的计算会消耗后台数据库的资源,对于无须防跟踪的应用场合,仍建议使用直接发送 EPC 来代替发送 IDS。另外,标签的 IDS 需要计算两个 CRC,这也将会给标签增加一定的计算量。由于硬件环境的限制,本文只对认证方案进行了软件仿真,本文方案

和已有其他方案在 OPNET 下的仿真结果如表 2 所示,可以看出本文提出的方案在执行时间、信道利用率和队列延迟上均处于中间水平,并没有大大降低协议的执行性能,本文提出的认证方案在保证安全性的同时,也能够达到较好的执行性能,具有实用性。

表 2 本文方案与已有方案的仿真结果

协议	执行时间/s	读写器的无线信道利用率		队列延迟/s
		发射信道/%	接收信道/%	
EPC-C1G2	0.86	5.3	13.8	0.006 3
Duc	0.35	1.8	4.6	0.006 8
Chien	0.33	1.8	4.6	0.006 8
TRMA +	0.94	4.1	13.2	0.016 9
SASI	0.32	2.7	4.7	0.003 4
本文方案	0.45	2.7	6.6	0.008 5

5 结束语

在本文提出的基于动态密钥的双向认证协议中,标签每次发送一个匿名 IDS 给读写器,这样可以防止非法跟踪;在发送认证消息时,设计了一个密钥构造算法用于加密认证消息,密钥只有读写器和标签知道并且密钥是动态更新的;该协议能够实现对读写器和标签的双向认证,可以确保通信双方的合法性。通过对协议进行 SMV 形式化分析,结果显示该协议具有认证性、保密性和完整性。另外,该协议能够抵制跟踪、非法访问、标签假冒、DoS、重放、前向安全等攻击,并且具有硬件实现简单、运算速度快等特点,能够在低成本标签中实现。目前对低成本 RFID 安全技术的研究还处于初级阶段,现有的一些成果都是局部的、零星的、不系统的,还不能真正完全解决低成本 RFID 的安全问题。如何设计安全、实用、低成本的 RFID 安全协议仍是以后研究的重点。

参考文献:

[1] KARTHIKEYAN S, NESTERENKO M. RFID security without extensive cryptography[C]// Proc of ACM Workshop on Security of Ad hoc and Sensor Networks. Alexandria, VA: ACM, 2005: 63-67.

[2] EPC™ Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860MHz ~ 960MHz version 1.0.9[S]. 2005.

[3] DUC D N, PARK J, LEE H, *et al*. Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning[C]// Proc of Symposium on Cryptography and Information Security. 2006.

[4] CHIEN H Y, CHEN C H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards[J]. Computer Standards & Interfaces, 2007, 29(2): 254-259.

[5] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR, *et al*. Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard[J]. Computer Standards & Interfaces, 2009, 31(2): 372-380.

[6] KONIDALA D M, KIM K. Auto-ID labs white paper WP-HARDWARE033, RFID tag-reader mutual authentication scheme utilizing tag's access password[S]. 2007.

[7] LIM T L, LI T. Addressing the weakness in a lightweight RFID tag-reader mutual authentication scheme[C]// Proc of IEEE Int'l Global Telecommunications Conference(GLOBECOM). 2007: 59-63.

[8] KONIDALA D M, KIM Z, KIM K. A simple and cost-effective RFID tag-reader mutual authentication scheme[C]// Proc of RFIDSec. 2007: 141-152.

[9] PERIS-LOPEZ P, LI Tie-yan, LIM T-Lee, *et al*. Vulnerability analysis of a mutual authentication scheme under the EPC Class-1 Generation-2 Standard[C]// Proc of RFIDsec. 2008: 9-11.

[10] CHIEN H Y. SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity[J]. IEEE Trans on Dependable and Secure Computing, 2007, 4(4): 337-340.

[11] SUN H M, TING W C, WANG K H. On the security of chien's ultralightweight RFID authentication protocol[R/OL]. (2008). http://eprint.iacr.org/2008/083.

[12] PERIS-LOPEZ P. Lightweight cryptography in radio frequency identification (RFID) Systems[EB/OL]. (2008). http://pperis.host22.com/pperis/thesis/index.html.

[13] Birthday paradox[EB/OL]. http://en.wikipedia.org/wiki/Birthday_paradox.

[14] SMV[EB/OL]. http://www.kenmcmil.com/.

(上接第 1884 页)秘密份额,减轻了分发者的计算负担,避免了分发者的欺诈。安全性分析表明,新方案可以抵抗各种秘密共享的常见攻击;性能分析表明,新方案比 ZZZ 和 SC 方案在计算量和公开值方面都有优势。由于系统的所有通信都在公开信道中进行,新方案更加适用于不可能建立安全信道的实际环境中。

参考文献:

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22 (11): 612-613.

[2] BLAKLEY G. Safeguarding cryptographic keys [C]// Proc of AFIPS National Computer Conference. New York: AFIPS Press, 1979: 313-317.

[3] CHOR B, GOLDWASSER S, MICALI S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults [C]// Proc of the 26th IEEE Symposium on Foundations of Computer Science. Portland: IEEE, 1985: 251-260.

[4] DEHKORDI M, MASHHADI S. An efficient threshold verifiable multi-secret sharing [J]. Computer Standards & Interfaces, 2008, 30 (3): 187-190.

[5] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing [C]// Proc of the 28th IEEE Symposium on Foundations of Computer Science. Canada: IEEE, 1987: 22-27.

[6] HWANG R, CHANG C. An on-line secret sharing scheme for multi-secrets [J]. Computer Communications, 1998, 21 (3): 1170-1176.

[7] SHAO J, CAO Z. A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme [J]. Applied Mathematics and Computation, 2005, 168 (1): 135-140.

[8] YANG C, CHANG T, HWANG M. A (t, n) multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151 (6): 483-490.

[9] ZHAO J, ZHANG J, ZHAO R. A practical verifiable multi-secret sharing scheme [J]. Computer Standards and Interfaces, 2007, 29 (1): 138-141.

[10] DEHKORDI M, MASHHADI S. An efficient threshold verifiable multi-secret sharing [J]. Computer Standards & Interfaces, 2008, 30 (3): 187-190.