一种改进的超轻量级RFID所有权转移协议

沈金伟 凌 捷
(广东工业大学计算机学院 广州 510006)

摘 要 针对RFID所有权转移协议中存在的拒绝服务攻击漏洞,提出了一种改进的超轻量级RFID所有权转移协议,并给出了基于GNY逻辑的协议安全性证明。通过改进协议的交互方式,实现了阅读器和标签的双向认证功能,解决了攻击者重放消息造成的拒绝服务攻击漏洞等问题,提高了阅读器和标签在开放环境中通信的保密性。对协议的安全性分析和性能比较分析表明,该协议不仅满足所有权转移的安全要求,而且具有超轻量的特点,适合于移动身份认证环境中的实际应用。

关键词 RFID,拒绝服务攻击,超轻量级,所有权转移议,GNY逻辑

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.026

Improved Ultra-lightweight Authentication of Ownership Transfer Protocol for RFID Tag

SHEN Jin-wei LING Jie
(College of Computer Science, Guangdong University of Technology, Guangzhou 510006, China)

Abstract Aiming at the securing hole of current ownership transfer protocol, a ultra-lightweight RFID mutual authentication of ownership transfer protocol was proposed. The formal proof of the proposed authentication protocol was given based on GNY logic. It improves the reader and the tag in an open environment confidentiality of communications, which not only solves problems of Denial of Service (DoS) that are produced when the attacker replays the message, but also achieves the reader and the tag mutual authentication function through changing protocols interact. This paper analyzed the security and compared the performance of the protocol. The results show that the proposed protocol not only satisfies the security requirements of transfer of ownership, but also has the characteristics of ultra-lightweight, which indicates that it is suitable for actual mobile authentication environment.

Keywords RFID, DoS attack, Ultra-lightweigh, Ownership transfer protocol, GNY logic

1 引言

射频识别(Radio Frequency Identification,RFID)技术是利用射频信号在开放环境中自动识别对象并获取相关数据的技术,具有非接触、非视觉范围读写、寿命长等特点。由于受到无线传输、信号广播、终端硬件等因素的影响,RFID安全与隐私问题成为制约其发展的重要因素。在RFID标签的生命期内,它的所有者经常需要发生改变,在所有权转移过程中,RFID标签的安全和隐私问题尤显突出。生产者将RFID标签嵌入商品,再将该商品出售给批发商,批发商再卖给零售商,最后消费者购买该商品;在上述商品流通的过程中,经过了多次所有权转移过程[1]。如果某一用户得到商品,他就获得了商品的所有权,用户必须得到商品上标签的信息,才能使用RFID标签的功能,这就涉及到标签的所有权转换问题,即标签的上一个拥有者需要把标签信息安全地告知给标签的下一个所有者,让标签的新用户获得标签的信息内容和信息的后续使用权,另一方面,该标签的旧消息对新所有者是完全屏蔽的,在所有权转移成功之后,标签的上一任所有者就失去了标签的控制权;同时,方案也要满足RFID系统的其他安全性和隐私性需求。由于标签计算能力弱、存储能力低,目前大多数的RFID标签转移协议都难以满足实际应用的要求。因此,设计安全、低成本的RFID双向认证协议成为亟待解决的研究课题。

2 相关工作

2005年,Molnar等人提出了标签的所有权转换问题,并提出一种可以实现RFID标签所有权转移功能的协议[2],该协议基于密钥树的假名协议来实现用户的隐私保护。在协议中,假设可信中心(Trusted Center,TC)对原标签所有者授权了标签的k个假名,则新所有者读取标签的第$k+1$个授权假名,从而实现标签的所有权转移过程。该方案的主要缺点是标签的原所有者与新所有者需要有一个共同的可信中心,从而限制了该协议的实际使用范围。

2006年,Osaka等人基于Hash函数和对称密码体制,提

到稿日期:2013-12-10 返修日期:2014-03-07 本文受广东省战略性新兴产业核心技术攻关项目(2012A010701004),广东省自然科学基金重点项目(S2012020011071),广东省教育部产学研合作项目(2012B091000037,2012B091000041)资助。

沈金伟(1987—),硕士,主要研究方向为网络与信息安全技术、物联网安全技术,E-mail:jwshengz@163.com;凌 捷(1964—),博士,教授,主要研究方向为网络信息安全技术、云计算安全技术、物联网安全技术。

出了一种 RFID 标签所有权转换协议[3]。在该协议中，标签与阅读器完成双向认证通信后，通过改变对称密钥，可以保护用户的隐私，并实现所有权转移功能。但是该协议存在不少安全缺陷，首先该协议不能抵抗拒绝服务攻击(DoS)；其次该协议不满足不可追踪性：攻击者通过向受害标签发送上一次的随机数认证请求，能获得相同的标签响应，进而造成标签的隐私泄露。

2007 年，Fouladgar 等人提出了一种简单有效的所有权转移方法：在 RFID 系统中，原所有者的数据库把标签的信息传输给新用户的数据库，新用户通过阅读器向新数据库发出所有权转换请求，后台验证标签身份通过后，新数据库发送秘密消息，通过阅读器转发给标签，完成所有权转换过程[4]。但该协议不能抵抗重放攻击、假冒攻击，并且有隐私泄漏的风险。

2010 年，Kulseng 等人基于物理不可克隆(PUF)技术和线性反馈移位寄存器(LFSR)功能，提出了一种所有权转移协议[5]。该协议与其他基于 Hash 函数的协议相比，效率更高；但协议的安全性有待证明。

2011 年，金永明等人在文献[6]中提出了一种轻量级所有权转移协议，并认为该协议具有抗重放攻击、抗拒绝服务攻击(异步攻击)、抗中间人攻击等常见攻击方式的能力，但本文的研究发现，文献[6]协议在抵抗拒绝服务攻击以及抵抗标签端重放攻击方面存在缺陷。

2012 年，Albert 等人提出了一种在标签数据更新阶段实现所有权转移的方案[7]，该方案不但实现了 RFID 标签所有权的转移和恢复功能，而且具有可扩展性；该方案可以抵抗重放攻击、终端(服务器或标签)模拟攻击、拒绝服务攻击；但是对于其他常见攻击(如窃听、追踪、异步等)的安全性没有验证。

2013 年，Robin 等人提出一种符合 EPC C1G2 标准的所有权转移方案[8]，该方案基于二次剩余(quadratic residue)问题设计了两种环境(open loop 和 closed loop)下的协议，用以抵抗异步攻击造成的拒绝服务攻击等常见攻击；而且与其他协议的仿真结果对比说明，该方案中的两种协议都具有良好的性能；但是没有经过实际环境的检测。

本文针对文献[6]协议中的缺陷，提出了一种改进的可抵抗拒绝服务攻击的超轻量级所有权转移协议，给出了基于 GNY 逻辑的协议安全性证明。

3 针对所有权转移协议的攻击

3.1 拒绝服务攻击

文献[6]的协议是基于 SQUASH 方案提出的。在协议的初始状态中，标签保存公钥 t_i，读写器保存本次认证的私钥、公钥(s_i，t_i)，上次认证的私钥、公钥(u_i，v_i)。文献[6]中声称协议可以抗拒绝服务攻击，但是本文研究发现，攻击者重放窃听到的消息，可以通过标签的身份验证，获取标签的信任，然后与标签交换数据，从而导致读写器和标签两边的公钥无法匹配，使协议失效。具体攻击过程如下：

第 1 轮通信：攻击者窃听通信过程，记录消息($M_1 \parallel N_1$)和($P_1 \parallel Q_1$)，并截获消息($P_1 \parallel Q_1$)；此时后台数据库(database)已经更新数据，而标签(tag)因为没有收到消息未更新的数据，所以两端的数据情况为：

Database：$(S_{i+1}, t_{i+1}), (s_i, t_i)$

Tag：t_i

第 2 轮通信：标签与后台正常通信，此时两端的数据情况为：

Database：$(S_{i+2}, t_{i+2}), (s_i, t_i)$

Tag：t_{i+2}

第 3 轮通信：攻击者发送($M_1 \parallel N_1$)数据给阅读器，阅读器返回数据($P_3 \parallel Q_3$)，此时两端的数据为：

Database：$(S_{i+3}, t_{i+3}), (s_i, t_i)$

Tag：t_{i+2}

第 4 次通信：阅读器发送 request 请求，标签返回($M_2 \parallel N_2$)，此时读写器使用公钥 t_{i+3} 验证标签用公钥 t_{i+2} 加密的数据，验证没通过，协议失效。

3.2 重放攻击

攻击者窃听到正常通信过程，记录消息($M_1 \parallel N_1 \parallel P_1 \parallel Q_1$)，并截获消息($P_1 \parallel Q_1$)，然后在标签下一次与读写器通信之前，攻击者发送 request 认证请求，收到消息($M_2 \parallel N_2$)，接着重放消息($P_1 \parallel Q_1$)，标签认证攻击者身份通过，攻击实施成功。

4 改进的超轻量级所有权转移协议

在 RFID 标签的所有权转移过程中必须满足以下安全与隐私要求：(1)所有权转移后，原所有者失去标签的控制权；(2)新所有者 RFID 标签所有权转移成功后，不能访问原标签所有者的数据；(3)所有权转移协议可以抵抗中间人攻击、异步攻击等常见攻击方式[6]。根据上述要求，本文提出了一种“先认证后授权”的所有权转移过程，并设计了相应的协议。

在文献[6]协议中，由于通信双方没有实现双向认证功能，攻击者重放记录的上次通信过程中的消息，就可以顺利通过标签的身份认证，然后与标签交换数据，造成了拒绝服务攻击漏洞；而且标签需要具备随机数发生器硬件，增加了标签的成本。针对这些不足，本文提出了一种新的超轻量级 RFID 双向认证协议，将标签保存数据 N_x 作为标签的随机数来完成认证过程，N_x 保持动态刷新，并通过 MIXBITS(x，y)函数[9]增加了数据的随机性，从而使标签具有不需要随机数发生器也可以产生随机数的能力，减少了标签端的硬件成本，实现了超轻量级的功能；同时标签端保存假名 IDS 数据，减少了后端服务器的计算量。改进后的协议如图 1 所示。

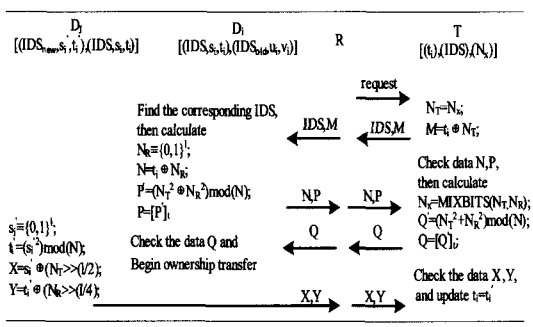

图 1 改进的超轻量级 RFID 所有权转移协议

在协议的初始状态中，后端数据库保存数据(IDS，s_i，t_i)，标签保存数据(t_i，IDS，N_x)，其中 D_i 表示原所有者的数据，D_j 表示新所有者的数据。协议的具体执行过程如下：

Step1：读写器发送 request 请求给标签。

Step2：标签收到阅读器的请求消息后，计算 $N_T = N_x$，$M = t_i \oplus N_t$；返回 $IDS \parallel M$。

Step3：读写器收到消息之后，在数据库中查找 $IDS=IDS_{new}$，或 $IDS=IDS_{old}$，查找成功之后，产生随机数 N_R，利用对应的 t_i，计算 $N_T=M\oplus t_i$，$N=t_i\oplus N_R$，$P'=(N_T^2\oplus N_R^2)\bmod(N)$，$P=[P']_t$。然后读写器发送消息 $N\|P$ 给标签。其中 $[P']_t$ 表示取数据 P' 的前 t 位，N 是 Rabin 加密方案中的梅森数[10]。

Step4：标签接收到消息之后，根据 N 计算出 N_R 和 P_x，并用计算结果 P_x 验证消息中的数据 P；如果验证成功，则标签认证阅读器通过，更新数据 $N_x=MIXBITS(N_T,N_R)$，计算 $Q'=(N_T^2+N_R^2)\bmod(N)$，$Q=[Q']_t$；并发送消息 Q 给阅读器。

Step5：阅读器收到消息并验证标签合法性成功后，开始所有权转移过程：新所有者数据库产生随机数 s_{i+1}，计算 $t_{i+1}=(s_{i+1})^2\bmod(N)$，$X=s_{i+1}\oplus(N_T>>l/2)$，$Y=t_{i+1}\oplus(N_T\gg l/4)$；更新数据 $IDS_{old}=IDS$，$u_i=s_i$，$v_i=t_i$，$IDS_{new}=IDS\oplus N_T\oplus N_R$，$s_i=s_{i+1}$，$t_i=t_{i+1}$；将消息 $X\|Y$ 发送给标签。其中 $>>$ 表示循环右移运算，l 表示密钥长度。

Step6：标签收到消息验证并验证成功之后，更新数据 $IDS=IDS\oplus N_T\oplus N_R$，$t_i=Y\oplus(N_R>>l/4)$。

5 改进协议形式化证明

GNY 逻辑是一种分析密码协议安全性的逻辑化方法，它是在 BAN 逻辑的基础上进行扩展和改进后提出的一种形式化分析工具，其规则直观、精确。本文根据协议的形式化模型和初始化假设，利用逻辑推导规则进行推理，逐步推断得到了协议的形式化证明。

5.1 协议形式化模型

用逻辑语言描述本文协议中的消息，其形式化模型如图 2 所示。

Msg1 $R\lhd *IDS,*[N_T]_K$

Msg2 $T\lhd *[N_T]_K,*F_1(N_R,N_T)$

Msg3 $R\lhd *F_2(N_R,N_T)$

Msg4 $T\lhd *F_3(S_i,N_T),*F_4(t_i',N_R)$

图 2 本文协议的形式化模型图

5.2 协议的初始化假设和证明目标

协议的初始化假设如图 3 所示。在本文协议中，使用 T、R 表示主体，即标签(T)、阅读器(R)。Init1、Init2 表示标签、阅读器的拥有；Init3、Init4 表示标签、阅读器对数据新鲜性的相信；Init5、Init6 表示标签和阅读器彼此相信 K 是双方的共享秘密，Init7、Init8 表示标签与阅读器相信各自的信息是可以识别的。

Init1 $T\in(IDS,K,N_t)$

Init2 $R\in(IDS,K)$

Init3 $T|\equiv\#(IDS,N_T,K)$

Init4 $R|\equiv\#(IDS,N_R,K)$

Init5 $T|\equiv R\overset{K}{\leftrightarrow}T$

Init6 $R|\equiv T\overset{K}{\leftrightarrow}R$

Init7 $T|\equiv\phi(N_T,IDS)$

Init8 $R|\equiv\phi(N_R)$

图 3 本文协议的初始化假设协议图

本文协议的证明目标如图 4 所示，主要有 5 个：阅读器对标签的身份信息 IDS 的识别；标签对阅读器拥有共享秘密 K 的相信；阅读器对标签拥有共享秘密 K 的相信；标签对交互信息新鲜性的相信。

G1 $R|\equiv\phi(IDS)$

G2 $T|\equiv R\in K$

G3 $R|\equiv T\in K$

G4 $T|\equiv R|\sim\#F_1(s_i',N_T),\#F_2(t_i',N_R)$

图 4 本文协议的证明目标

5.3 基于 GNY 逻辑的协议证明

本文协议的证明是在初始化假设基础上，针对协议形式化模型中的消息逐个进行的。证明过程遵循文献[11]中的逻辑推理规则，包括如下几步：

(1)从图 2 中 Msg1 开始进行形式化分析，由接受规则 T4 和初始化假设 Init2 得到 $R\lhd N_T$；然后验证收到的 IDS 与阅读器后台数据库的 IDS 是否匹配，如果匹配成功，则读写器预认证标签成功，即 $R|\equiv\phi(IDS)$；预期目标 G1 实现。由 Init8 和可识别规则 F1 可知 $R|\equiv\phi(N_R,K)$，结合 Init2，Init6，Init8 和消息解析规则 I1，有 $R|\equiv T\in K$，预期目标 G3 实现。

(2)标签收到消息 Msg2：由初始化假设 Init1：$T\in(K,IDS)$ 和被告知规则 $T4$ 和 $T5$，有 $T\lhd F(N_R,IDS)$，$T\lhd N_r$；标签验证消息成功后，则表明标签预认证读写器成功，即有 $T|\equiv\phi(N_R)$；根据可识别规则 R1 可知，$T|\equiv\phi(N_R,IDS)$，$T|\equiv\phi F(N_R,IDS)$；又由初始化假设 Init4 和新鲜性规则 F1 可得 $T|\equiv\#(N_R,IDS)$，再由应用规则 F1 得到 $T|\equiv\#F(N_R,IDS)$；根据形式化消息 Msg2，初始化假设 Init1：$T\in K$，Init5 和消息解析规则 I1，有 $T|\equiv R\in K$。至此，预期目标 G2 实现。

(3)标签收到消息 Msg4：后台数据库认证 Msg3 消息成功后，开始所有权转移过程。根据初始化假设 Init3：$T|\equiv\#N_T$ 和新鲜性规则 F1，可知有 $T|\equiv\#(S_{i+1},N_T)$，继续使用规则 F1 有 $T|\equiv\#F(S_{i+1},N_T)$；同理，根据初始化假设 Init4：$T|\equiv\#N_R$ 和新鲜性规则 F1，可知有 $T|\equiv\#(t_{i+1},N_R)$，继续使用规则 F1 有 $T|\equiv\#F(t_{i+1},N_R)$；预期目标 G4 得以实现。

6 安全性分析和性能比较

6.1 安全性分析

本文提出的改进的超轻量级 RFID 协议的安全性分析如下：

(1)抗重放攻击：本文协议中，标签和阅读器实现了双向认证功能。标签用动态数据 N_x 加密消息，并将消息发送给阅读器验证标签身份；一旦协议中标签收到消息后，N_x 就会刷新数据，假设攻击者重放上次记录的消息，则此时阅读器验证 $P^*=P$ 不成功，协议终止，攻击失败。

(2)抗拒绝服务攻击：假设初始状态两端的 IDS 数据情况如下：

Database：(IDS,s_i,t_i)，(IDS_{old},u_i,v_i)

Tag：(IDS,t_i,N_{x+1})

攻击者对本文协议发起拒绝服务攻击，过程如下：

第 1 轮通信：攻击者窃听通信过程，记录消息 $(M_1\|N_1\|P_1\|Q_1\|X_1\|Y_1)$，并截获消息 $(X_1\|Y_1)$，此时读写器已经更新数据 $(IDS_{new},s_{i+1},t_{i+1})$，标签因为没有收到消息 $(X_1\|Y_1)$，除 N_x 外，不更新其他数据。因此读写器和标签两端数据如下：

Reader：$(IDS_{new+1},s_{i+1},t_{i+1})$，$(IDS,s_i,t_i)$

Tag：(IDS,t_i,N_{x+1})

第 2 轮通信：阅读器与标签正常通信，此时两端的 IDS 数据情况为：

Reader：$(IDS_{new+2}, s_{i+2}, t_{i+2})$，$(IDS, s_i, t_i)$

Tag：$(IDS_{new+2}, t_{i+2}, N_{x+2})$

第 3 轮通信：攻击者发送 request 请求，收到标签返回的 $(IDS_{new+2} \| M_{i+2})$ 消息之后，重放第一轮窃听到的消息 $(N_{i+2} \| P_{i+2})$，由于此时标签中的 N_x 数据已经更新，标签验证消息 $P^*_{i+2} \neq P_{i+2}$，协议终止，攻击失败。

攻击者使用重放攻击的方式来攻击文献[6]协议，可能造成协议失效，将其用来攻击本文协议则是无效的，最终协议能正常执行。主要原因是文献[6]协议中，阅读器单向认证标签，而在改进的协议中，通过增加通信过程，实现了阅读器和标签的双向认证；而且标签用动态数据 N_x 来加密消息，N_x 在收到标签消息后就会刷新数据，这样协议中的消息具有了时效性，协议就可以防重放攻击，同时拒绝服务攻击也失效了。

6.2 性能比较

本文从通信量、计算量、标签上的存储量 3 方面对文献[6]协议、文献[7]协议、文献[8]方案中的两种协议（closed loop 协议和 open loop 协议）与本文协议进行比较。5 种协议标签上的存储量不同：文献[6]协议中标签端保存数据 t_i；文献[7]协议标签端保存数据 ik、uk、id；文献[8]方案中的两种协议标签端保存的数据是一样的，都是 $h(\mathrm{TID})$、K_{TID}、r、n；本文协议中标签端保存数据 IDS、t_i、N_x。假设 3 种协议的单位消息长度相同都为 L，文献[6]协议的通信量为 $3L$；文献[7]协议的通信量为 $5L$；文献[8]方案中的两种方案的通信量都是 $7L$；本文协议的通信量为 $5L$。当协议执行完毕时，5 种协议标签计算量比较结果如表 1 所列。设每次计算操作消耗的时间单位为 $T(s)$，协议中的密钥长度是 l；两种协议的计算量比较如表 1 所列。

表 1 两种协议的计算量比较结果表

协议	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
A	0T	2T	1T	0T	0T	0T	0T	0T	2T
B	1T	1T	0T	0T	4T	0T	0T	3T	1T
C	0T	19T	0T	0T	5T	3T	1T	5T	2T
D	0T	20T	0T	0T	6T	3T	0T	5T	2T
E	1T	2T	1T	1T	0T	0T	0T	0T	2T

注：(1)表示"+"操作；(2)表示"⊕"操作；(3)表示 SQUASH 方案操作；(4)表示 MIXBITS(x,y)函数操作；(5)表示 Hash(哈希)操作；(6)表示 mod(求余)操作；(7)表示 CRC(循环校验)操作；(8)表示 PRNG(伪随机数发生器)操作；(9)表示比较操作。A 表示文献[6]协议方案；B 表示文献[7]协议方案；C 表示文献[8]中的 closed loop 协议方案；D 表示文献[8]中的 open loop 协议方案；E 表示表示本文协议方案。

结束语 本文通过分析现有的 RFID 所有权转移协议，针对文献[6]协议的缺陷，提出了一种改进的超轻量级 RFID 所有权转移协议，该协议实现了阅读器和标签的双向认证功能，并基于 GNY 逻辑给出了协议的形式化证明。对协议的安全性分析和性能比较表明，本文协议可以抵抗拒绝服务攻击、重放攻击等常见攻击方式；协议中标签端没有使用伪随机数发生器，实现了超轻量的特性。与现有一些方案比较表明，本文协议具有更高的安全性、更少的硬件成本，可以满足低成本 RFID 系统的应用需求。

参 考 文 献

[1] 邵婧，陈越，常振华. RFID 标签所有权转换模式及协议设计[J]. 计算机工程，2009，35(15)：143-145

[2] Molnar D，Soppera A，Wagner D. A Scalable，Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags[C]// Proc. of SAC'05. Kingston，Jamaica：Springer-Verlag，2005：276-290

[3] Osaka K，Takagi T，Yamazaki K，et al. An Efficient and Secure RFID Security Method with Ownership Transfer[C]// Proc. of CIS'06. Springer-Verlag，2006：778-787

[4] Fouladgar S，Afifi H. An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags[C]// Proc. of the 1st International Workshop on RFID Technology. Vienna，Austria，2007

[5] Kulseng L，Yu Zhen，Wei Ya-wen，et al. Lightweight mutual authentication and ownership transfer for RFID systems [C]// Proc of the 29th Conf on Computer Communications IEEE INFOCOM 2010. Piscataway，NJ：IEEE，2010：1-5

[6] 金永明，孙惠平，关志，等. RFID 标签所有权转移协议研究[J]. 计算机研究与发展，2011，48(8)：1400-1405

[7] Fernandez-Mir A，Trujillo-Rasua R，Castella-Roca J，et al. A Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation. RFID，Security and Privacy，LNCS，2012，7055：147-162

[8] Doss R，Zhou Wan-lei，Yu Shui. Secure RFID Tag Ownership Transfer Based on Quadratic Residues[J]. IEEE Transcations on information forensics and security，2013，8(2)：390-401

[9] 彭朋，赵一鸣，韩伟力，等. 一种超轻量级的 RFID 双向认证协议[J]. 计算机工程，2011，37(16)：140-142

[10] Shamir A. SQUASH-A new MAC with provable security properties for constrained devices such as RFID tags [C]// LNCS 5086：Proc of 15th Annual Fast Software Encryption Workshop. Springer，2008：144-157

[11] 李杰. RFID 安全认证协议研究与设计[D]. 西安：西安电子科技大学，2012：40-46

(上接第 100 页)

[18] Yao A. Protocols for secure computation [C]// Proceeding of the 23th IEEE Symposium on Foundations of Computer Science. IEEE Computer Society Press，Los Alamitos，USA，1982：160-164

[19] 杨庚，王江涛，程宏兵，等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报，2007，35(1)：180-184

[20] 刘梦君，刘树波，刘泓晖，等. 异构无线传感器网络动态混合密钥管理方案研究[J]. 山东大学学报：理学版，2012，47(11)：67-73

[21] 郭萍，张宏，傅德胜，等. 一种混合轻量型无线传感器网络公钥密码方案[J]. 计算机科学，2012，39(1)：69-81

[22] Boneh D，Franklin M. Identity-based encryption from the Weil pairing [C]// Advances in Cryptology，CRYPTO 2001，Lecture Notes in Computer Science. Berlin：Springer-Verlag，2001，2139：213-229

[23] Groat M M，Hey W，Forrest S. KIPDA：k-indistinguishable privacy-preserving data aggregation in wireless sensor networks [C]// 30th IEEE International Conference on Computer Communications. Shanghai，China，2011：2024-2032