一种无线传感器网络双向认证协议设计及证明

郭 萍 傅德胜 成亚萍 展 翔
(南京信息工程大学计算机与软件学院 南京 210044)

摘 要 构建了一种适用于无线传感器网络的用户与传感器节点间的双向认证协议。分析表明,协议所用算法克服了基于身份公钥的机制中第三方私钥托管问题,并简化了传统基于证书的机制产生及验证证书的复杂性。系统初始化完成后,用户与传感器节点间的双向认证无需可信第三方参与,认证协议简单高效、通信量少。采用BAN(Burrows-Abadi-Needham)逻辑证明协议的完备性、正确性及安全性。

关键词 无线传感器网络(WSN),双向认证,BAN逻辑
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.021

Design and Proof of Bilateral Authentication Protocol for Wireless Sensor Network

GUO Ping FU De-sheng CHENG Ya-ping ZHAN Xiang
(School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing 210044, China)

Abstract A bilateral authentication protocol between users and sensor nodes was proposed for WSN(wireless sensor network). Analysis shows that authentication protocol not only avoids the drawback of private key escrow in the identity-based system, but also achieves the advantage of simplifying complication of producing and verifying public key in traditional certificate-based system. Moreover, the authentication protocol doesn't need TTP(Trusted Third Party), is efficient and has less communications. Finally, the integrity, correction and security of protocol were proved with BAN logic formal method.

Keywords Wireless sensor network (WSN), Bilateral authentication, BAN logic

1 引言

无线传感器网络(WSN)是目前的研究热点,无基础设施支持,可迅速在某区域内部署很多低成本的传感器节点,用来监测环境并通过无线链路向基站报告,是一种非常灵活的无线网络结构。WSN适合用于敌对环境或大规模地理区域,在军用及民用领域得到广泛的应用,如目标跟踪、战场侦查及野外环境监视。一些特殊的应用包括:(1)军事领域。WSN特别适用于军事方面,如战场上,传感器节点可以用来监控敌军的汽车流量,或者跟踪它们的位置,然后把信息送回基站。(2)环境监测。传感网可被部署在不同环境领域来监测环境数据的变化。例如:可监控森林火灾情况,或者可被随机散落在污染环境中,向基站汇报原始的污染数据。

随着传感器网络技术的发展,越来越多的基于非对称密码(即公钥密码)技术的认证机制被用于WSN[1-4]。文献[1]证明了在8MHz主频、8bits处理能力的CPU上运行RSA与ECC公钥密码算法的可行性;文献[3]则在4kB内存、7.38MHz的传感器节点上实现了ECC-160bits公钥算法;文献[4]则重点研究如何设计更适用公钥算法的硬件,以便在WSN的节点上使用。文献[5]提出基于RSA的TinyPK认证方案,较方便地实现了WSN的实体认证,但是该方案存在单点失效问题。文献[6]提出的强用户认证协议采用了一种全局认证形式,将单点认证转化为n个节点认证,提高了网络的容侵性。这个认证协议安全强度较高,但对拒绝服务攻击没有较好的防御措施。文献[7]提出基于ECC算法的WSN认证及访问控制协议,可以支持新节点动态地加入WSN,在访问控制的过程中建立密钥从而与其邻居节点协商会话密钥。该方案虽然比文献[6]具有更高的效率,节省存储及带宽,但需要同时配置的两个传感节点具有相同的引导时间,且假设每个节点在被攻陷前具有相同的容忍间隔,这对于大多数实际应用太苛刻。基于证书公钥认证机制虽然不需要事先分配密钥,节点身份与其公钥绑定明确,节点间安全的通信链路方便建立,会话密钥的协商也较容易,但是如何安全地向所有节点分发其私钥是问题所在。文献[8]特别指出基于身份的认证机制尤其适合于WSN,因为它有以下优点:(1)克服了基于证书公钥机制中繁重的证书管理,无需证书开销,采用隐式密钥认证;(2)身份信息可由地理信息、IP地址或ID号充当,有时候在实际应用中很有意义。文献[9]设计一个基于BF-IBE(Boneh and Franklin Identity-Based Encryption)[10]的节点间可认证的密钥协商协议。文献[11]提出一个适用于

到稿日期:2014-08-15 返修日期:2014-09-20 本文受中国气象局项目(2014MC16),江苏大学生创新基金(201410300049)资助。
郭 萍(1973-),女,博士,讲师,主要研究方向为无线网络安全、无线认证及加密技术,E-mail:ziyyou@yeah.net;傅德胜(1951-),男,博士生导师,主要研究方向为信息安全、信息隐藏;成亚萍(1968-),女,硕士,副教授,主要研究方向为数字水印、图像处理;展 翔(1979-),女,硕士,讲师,主要研究方向为数据挖掘。

WSN 的节点协商会话密钥的协议。文献[12]提出一个以位置信息为身份的 WSN 安全机制。文献[13]对基于身份的密码体制在 WSN 中的应用进行可行性研究。在 WSN 中应用公钥算法，虽然最近研究都对其给予了肯定，但是还应仔细设计，尽量减少各种能耗。

本文提出一种无线传感器网络节点与漫游用户间的双向认证协议，第 2 节详细描述协议工作过程；第 3 节采用 BAN 逻辑对所提协议的安全性进行证明；最后总结全文。

2 协议详述

本文采用轻量级密码思想[14,15]结合椭圆黄线密码系统，设计传感节点及漫游用户间的双向认证协议，所用符号及意义如表 1 所列。

表 1 符号释意表

符号	释意	符号	释意
SK	私钥	ID	身份信息
PK	公钥	Sign	签名算法
$PK^{(Master)}$	主公钥	h( )	单向哈希函数
$PK^{(Slavery)}$	辅公钥	R	随机数
MU	移动用户	Ksession	会话密钥
SN	传感器节点	E( )	加密算法
Cert	证书	D( )	解密算法

2.1 系统参数说明及初始化

系统初始化过程如下，更多椭圆曲线密码系统产生密钥的细节详见文献[16]：

1. TTP(Trust Third Party，可信第三方)选取椭圆曲线群 $GF(p)$ 上的线 E，p 是大素数，P 是 E 的基点，q 是一个大素数且是 P 的生成元。

2. TTP 产生 n 个私钥 $x_1, x_2, \cdots, x_n \in GF(q)$，生成系统主私钥：$X=(x_1, x_2, \cdots, x_n)$。

3. 与系统主私钥相对应，产生 n 个公钥组成系统主公钥 $Y=(y_1, y_2, \cdots, y_n)$，其中：$y_i = x_i P$，$1 \leqslant i < n$。

4. TTP 选择碰撞避免的单向哈希函数 $h: \{0,1\}^* \rightarrow \{0,1\}^n$，发布系统公共参数集 K 为 $\{Y, P, p, q, h(\cdot)\}$。

5. TTP 执行算法，输入系统参数 $\{Y, P, p, q, h(\cdot)\}$，输出 TTP 的公/私钥对 (PK_{TTP}, SK_{TTP})。$SK_{TTP} = \sum_{i=1}^{n} h_i(str_{TTP}) x_i$，其中 str_{TTP} 是产生 TTP 公/私钥对的语义，$h_i(str_{TTP})$ 是 $h(str_{TTP})$ 的第 i 个比特，$PK_{TTP} = SK_{TTP} P = \sum_{i=1}^{n} h_i(str_{TTP}) y_i$。

6. 用户执行算法，输入系统参数 $\{Y, P, p, q, h(\cdot)\}$，输出用户的主公钥/私钥对 $(PK_{MU}^{(Master)}, SK_{MU})$。$SK_{MU} = \sum_{i=1}^{n} h_i(str_{MU}) x_i$，其中 str_{MU} 是产生用户主公钥/私钥对的语义，$h_i(str_{MU})$ 是 $h(str_{MU})$ 的第 i 个比特，$PK_{MU}^{(Master)} = SK_{MU} P = \sum_{i=1}^{n} h_i(str_{MU}) y_i$。同理产生传感器节点的主公钥/私钥对 $(PK_{SN_i}^{(Master)}, SK_{SN_i})$。

2.2 MU 与传感器节点 SN_i 之间的双向认证协议及会话密钥协商

若 MU 通过 TTP 的认证，进入到传感器网络，得到所有传感器节点的认可，一般情况下无需再认证。但 MU 需要直接与某节点通信进行数据加密传输等操作时，应该先与传感器节点进行双向认证同时协商会话密钥。协议设计的前提是 MU 和传感器节点 SN_i 双方彼此都不知道对方的公钥，但他们都已经拥有初始化过程由 TTP 签名的公/私钥对，且双方都知道 TTP 的证书及其公钥。本协议在 MU 和传感器节点 SN_i 之间展开，不需再与 TTP 进行通信。

1. MU 向传感器网络节点 SN_i 请求通信，发送 TTP 的证书及辅公钥 $PK_{MU}^{(Slavery)}$ 给对方 $MU \rightarrow SN_i: \{Cert_{TTP}, PK_{MU}^{(Slavery)}, h(ID_{MU} | PK_{MU}^{(Master)})\}$，表明是经 TTP 注册的合法用户。

2. SN_i 确认 TTP 的证书，并用 TTP 的公钥解密 MU 辅公钥 $PK_{MU}^{(Slavery)}$ $(PK_{MU}^{(Slavery)} = Sign_{SK_{TTP}}(ID_{MU} | PK_{MU}^{(Master)}))$，得到 MU 的身份及主公钥信息，用相同的散列函数计算 $h'(ID_{MU} | PK_{MU}^{(Master)})$ 并与 MU 发来的散列值相比较，若相同则验证 MU 是经 TTP 注册的合法用户，予以响应，产生随机数 R_{SN_i}，与辅公钥一起发给 MU：$SN_i \rightarrow MU: \{R_{SN_i}, PK_{SN_i}^{(Slavery)}\}$。

3. MU 收到 SN_i 发来的消息后，用 TTP 的公钥解密 $PK_{SN_i}^{(Slavery)}$ $(PK_{SN_i}^{(Slavery)} = Sign_{SK_{TTP}}(ID_{SN_i} | PK_{SN_i}^{(Master)}))$，获得 SN_i 的主公钥。产生随机数 $K_{session}$ 作为会话密钥，同时也是挑战信息，然后计算 $s_{MU} = Sign_{SK_{MU}}(h(K_{session} | PK_{MU}^{(Slavery)} | R_{SN_i})$，发送 $MU \rightarrow SN_i: a = E_{PK_{SN_i}^{(Master)}}(K_{session}, PK_{MU}^{(Slavery)}, R_{SN_i}, s_{MU})$，$a$ 是用传感器节点的主公钥对 $(K_{session}, PK_{MU}^{(Slavery)}, R_{SN_i}, s_{MU})$ 进行加密运算。

4. SN_i 收到 a 后，首先用私钥解密 a 得到 $(K_{session}, PK_{MU}^{(Slavery)}, R_{SN_i}, s_{MU})$，检查 $R_{SN_i} = R'_{SN_i}$ 是否成立，若成立，用 TTP 的公钥解密 $PK_{MU}^{(Slavery)}$ $(PK_{MU}^{(Slavery)} = Sign_{SK_{LCA}}(ID_{MU} | PK_{MU}^{(Master)}))$，获得 MU 的主公钥，并用该公钥通过 MU 的验证签名算法检验签名 $s_{MU} = Sign_{SK_{MU}}(h(K_{session} | PK_{MU}^{(Slavery)} | R_{SN_i}))$ 是否成立，若成立，则会话密钥 $K_{session}$ 得到确认；用私钥计算签名 $s_{SN_i} = Sign_{SK_{SN_i}}(h(K_{session}))$，用 MU 的主公钥加密并发送 $SN_i \rightarrow MU: b = E_{PK_{MU}^{(Master)}}(K_{session}, s_{SN_i})$。

5. MU 收到 b 后，用私钥解密得到 $K_{session}$，s_{SN_i}，检查 $K_{session} = K'_{session}$ 是否成立，若成立，则 SN_i 的身份得到验证；MU 在第 2 步中已获取 SN_i 的主公钥，用验证签名算法来验证签名 $s_{SN_i} = Sign_{SK_{SN_i}}(h(K_{session}))$ 是否成立，若成立，会话密钥 $K_{session}$ 得到确认。

通过以上 5 步，双方进行了双向认证并确认了会话密钥。以上过程如图 1 所示。

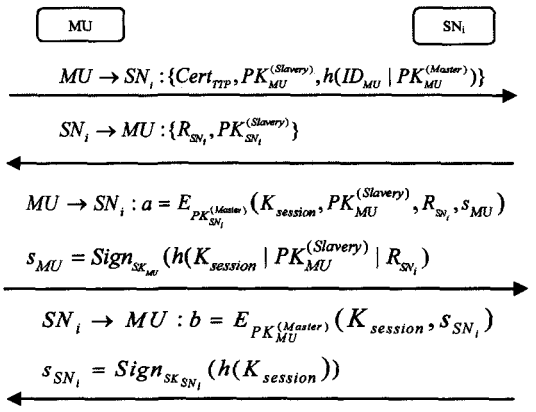

图 1 MU 与传感器节点 SN_i 之间的双向认证过程

3 BAN 逻辑分析双向认证协议的安全性

本节使用 BAN(Burrows-Abadi-Needham)[17] 逻辑对所

提 MU 与传感节点间的双向认证协议进行安全性证明。

1. 证明所使用逻辑规则[17]

$$(1)\frac{P|\equiv\xrightarrow{K}Q,P\lhd\{X\}_K^{-1}}{P|\equiv Q|\sim X}$$

规则表示：如果 P 相信 K 是 Q 的公钥，且 P 看见过 Q 使用 K^{-1} 加密消息 X，则 P 相信 Q 说过 X。

$$(2)\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

规则表示：如果 P 相信 X 是新鲜的，且 P 相信 Q 说过 X，则 P 相信 Q 相信 X。

$$(3)\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$$

规则表示：如果 P 相信 Q 拥有对 X 的权威性，且 P 相信 Q 相信 X，则 P 相信 X。

$$(4)\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$$

规则表示：如果 P 相信 X 是新鲜的，则 P 相信 (X,Y) 是新鲜的。

$$(5)\frac{P|\equiv(X,Y)}{P|\equiv X}$$

规则表示：如果 P 相信 (X,Y)，则 P 相信 X。

2. 初始假设

协议中，MU 与传感节点间的认证不需 TTP 的参与（但需要 TTP 的证书），因此可认为 TTP 是可信的，主公钥/私钥由 MU 或节点自己产生，但辅公钥经 TTP 签名生成，只要能证明签名是合法的，即可认为主公钥及辅公钥均是可信的。故可以做出初始假设如下：

(1) $SN|\equiv\#PK_{MU}^{(Slavery)}$；

(2) $MU|\equiv\#PK_{MU}^{(Slavery)}$；

(3) $SN|\equiv TTP|\Rightarrow PK_I^{(Slavery)},I=MU,SN$；

(4) $SN|\equiv TTP|\Rightarrow PK_I^{(Matter)},I=MU,SN$；

3. MU 与节点 SN 间协议根据逻辑规则推理

原协议中第 1 步 $MU\rightarrow SN_i:\{Cert_{TTP},PK_{MU}^{(Slavery)},h(ID_{MU}|PK_{MU}^{(Master)})\}$，推理如下：

Message1：

$$\frac{SN|\equiv|\xrightarrow{Cert_{TTP}}TTP,SN\lhd PK_{MU}^{(Slavery)}}{\dfrac{SN|\equiv TTP|(PK_{MU}^{(Slavery)}),SN|\equiv\#PK_{MU}^{(Slavery)}}{SN|\equiv TTP|\equiv(PK_{MU}^{(Slavery)})}}$$

根据初始假设，SN 相信 $Cert_{TTP}$ 是 TTP 的证书，且 SN 看到 $PK_{MU}^{(Slavery)}(=Sign_{SK_{TTP}}(ID_{MU}|PK_{MU}^{(Master)}))$，根据规则(1)可得 $SN|\equiv TTP|(PK_{MU}^{(Slavery)})$。$SN|\equiv\#PK_{MU}^{(Slavery)}$ 是初始假设(1)，由规则(2)可得 $SN|\equiv TTP|\equiv(PK_{MU}^{(Slavery)})$，故协议第 1 步得到 SN 相信 TTP 相信 $PK_{MU}^{(Slavery)}$，也意味着 SN 相信 MU 的身份 ID_{MU} 及其主公钥 $PK_{MU}^{(Master)}$。

原协议中第 2 步 $SN\rightarrow MU:\{R_{SN},PK_{SN}^{(Slavery)}\}$，推理如下：

Message2：

$$\frac{MU|\equiv|\xrightarrow{Cert_{TTP}}TTP,MU\lhd PK_{SN}^{(Slavery)}}{\dfrac{MU|\equiv TTP|(PK_{SN}^{(Slavery)}),MU|\equiv\#[PK_{SN}^{(Slavery)},R_{SN}]}{MU|\equiv TTP|\equiv(PK_{SN}^{(Slavery)})}}$$

根据初始假设，MU 相信 $Cert_{TTP}$ 是 TTP 的证书，且 MU 看到 $PK_{SN}^{(Slavery)}(=Sign_{SK_{TTP}}(ID_{SN}|PK_{SN}^{(Master)}))$，根据规则(1)可得 $MU|\equiv TTP|(PK_{SN}^{(Slavery)})$。$MU|\equiv\#PK_{MU}^{(Slavery)}$ 是初始假设(2)且 R_{SN} 是随机数，由规则(2)可得 $SN|\equiv TTP|\equiv(PK_{MU}^{(Slavery)})$，故协议第 2 步得到 MU 相信 TTP 相信 $PK_{SN}^{(Slavery)}$，也意味着 MU 相信 SN 的身份 ID_{SN} 及其主公钥 $PK_{SN}^{(Master)}$。

原协议中第 3 步 $MU\rightarrow SN:a=E_{PK_{SN}^{(Master)}}(K_{session},PK_{MU}^{(Slavery)},R_{SN},s_{MU})$，推理如下：

Message3：

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{SN|\equiv TTP|\equiv(PK_{MU}^{(Master)}),SN|\equiv TTP\Rightarrow(PK_{MU}^{(Master)})}{SN|\equiv(\xrightarrow{PK_{MU}^{(Master)}}MU),SN\lhd E_{PK_{SN}^{(Master)}}(K_{session},PK_{MU}^{(Slavery)},R_{SN},s_{MU})}}{SN|\equiv MU|E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}],SN|\equiv\#(R_{SN})}}{SN|\equiv MU|\equiv E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}],SN|\equiv MU\Rightarrow E_{PK_{SN}^{(Master)}}[K_{session},R_{MU}]}}{SN|\equiv E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}],SN|\equiv|\xrightarrow{PK_{SN}^{(Master)}}SN}}{SN|\equiv[K_{session},R_{SN}]}}{SN|\equiv K_{session}}$$

根据第 1 步，SN 相信 MU 的身份 ID_{MU} 及其主公钥 $PK_{MU}^{(Master)}$。由规则(3)，$SN|\equiv TTP|\equiv(PK_{MU}^{(Slavery)})$ 和初始假设(3)，可得 $SN|\equiv(\xrightarrow{PK_{MU}^{(Master)}}MU)$，且 SN 看到 $E_{PK_{SN}^{(Master)}}(K_{session},PK_{MU}^{(Slavery)},R_{SN},s_{MU})$，根据规则(1)可得：$SN|\equiv MU|E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}]$，根据初始假设(3)，$SN$ 相信 R_{SN} 是新鲜的，则根据规则(4)可知 $SN|\equiv\#(K_{session},R_{SN})$，由于 $SN|\equiv MU|E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}]$，根据规则(2)可得：$SN|\equiv MU|\equiv E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}]$，而 MU 拥有对 $E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}]$ 的权威性，故 $SN|\equiv MU\Rightarrow E_{PK_{SN}^{(Master)}}[K_{session},R_{MU}]$，根据规则(3)，可得 $SN|\equiv E_{PK_{SN}^{(Master)}}[K_{session},R_{SN}]$。$SN$ 相信 $PK_{SN}^{(Master)}$ 是自己的主公钥，故根据规则(5)可知：$SN|\equiv[K_{session},R_{SN}]$。再由规则(5)，得到安全目标 $SN|\equiv K_{session}$，即 SN 相信 $K_{session}$。

原协议中第 4 步 $SN_i\rightarrow MU:b=E_{PK_{MU}^{(Master)}}(K_{session},s_{SN_i})$，推理如下：

Message4：

$$\frac{\dfrac{\dfrac{\dfrac{MU|\equiv TTP|\equiv(PK_{SN}^{(Master)}),MU\equiv TTP\Rightarrow(PK_{SN}^{(Master)})}{MU|\equiv(\xrightarrow{PK_{SN}^{(Master)}}SN),MU\lhd E_{PK_{MU}^{(Master)}}(K_{session},s_{SN})}}{MU|\equiv SN|E_{PK_{MU}^{(Master)}}[K_{session},s_{SN}],SN|\equiv\#(s_{SN})}}{MU|\equiv SN|\equiv E_{PK_{MU}^{(Master)}}[K_{session},s_{SN}],SN|\equiv K_{session}}}{MU|\equiv SN|\equiv K_{session}}$$

根据第 2 步，MU 相信 SN 的身份 ID_{SN} 及其主公钥 $PK_{SN}^{(Master)}$。由规则(3)，$MU|\equiv TTP|\equiv(PK_{SN}^{(Slavery)})$ 和初始假设(3)，可得 $MU|\equiv(\xrightarrow{PK_{SN}^{(Master)}}SN)$，且 MU 看到 $E_{PK_{MU}^{(Master)}}(K_{session},s_{SN})$。根据规则(1)可得：$MU|\equiv SN|E_{PK_{MU}^{(Master)}}[K_{session},s_{SN}]$，根据初始假设，$MU$ 相信 s_{SN} 是新鲜的，根据规则(4)可得：$MU|\equiv SN|\equiv E_{PK_{MU}^{(Master)}}[K_{session},s_{SN}]$，而 MU 相信 $PK_{MU}^{(Master)}$ 是自己的主公钥，且由第 3 步得 $SN|\equiv K_{session}$，由规则(5)得到安全目标 $MU|\equiv SN|\equiv K_{session}$。

由上证明过程可知，MU 与传感节点密钥协商过程是安全的。同理，可证 TTP 与 MU/节点或两个欲通信的节点间的密钥协商过程是安全的。

结束语 本文结合轻量级密码思想，设计了一种无线传感器节点与漫游用户间的双向认证协议，所用算法克服了基于身份公钥机制中第三方私钥托管问题，又简化了传统基于证书机制产生及验证证书的复杂性，简单高效，通信量少，适用于资源受限的无线传感器网络。最后，采用 BAN 逻辑证明了协议的完备性、正确性及安全性。

（下转第 130 页）

根据图 11 和图 12 的实验结果可以得到，优化前的 TWINE 系统所需加密速率为：Minimum period =45.421ns；优化后的 TWINE 系统所需加密速率为：Minimum period = 9.690ns；由此可以得出，优化后的 TWINE 密码算法在系统速率上提高了 5 倍左右。

Design statistics:
Minimum period: 45.421ns (Maximum frequency: 22.016MHz)
Maximum path delay from/to any node: 4.883ns
Maximum net delay: 0.838ns
Analysis completed Fri Feb 21 12:12:00 2014

图 11 原始 TWINE 加密速率实验数据

Design statistics:
Minimum period: 9.690ns (Maximum frequency: 103.199MHz)
Maximum path delay from/to any node: 4.455ns
Maximum net delay: 0.838ns
Analysis completed Fri Feb 21 11:22:34 2014

图 12 优化后的 TWINE 加密速率实验数据

结束语 随着物联网的应用越来越深入，特别是在目前的各种智能卡芯片越来越轻薄的情况下，如何更有效地减少加密算法在智能卡上的实现面积是一个重要课题。因此如何对 TWINE 密码算法进行硬件面积优化是必要的课题。本文对 TWINE 密码算法的结构进行优化，在面积减少的同时也保证了加密效率。

参 考 文 献

[1] Suzaki T, Minematsu K, Morioka S, et al. TWINE: A light weight, versatile block cipher[C]// Proceeding of ECRYPT Workshop on Lightweight Cryptography. Louvain-la-Neuve, Belgium, 2011:146-169

[2] Çoban M, Karakoç F, Bozta ş Ö. Biclique cryptanalysis of TWINE[C]// Proceeding of Cryptology and Network Security. Darmstadt, Germany, 2012:43-55

[3] 陈佳康. 密码学算法的优化与应用[D]. 北京：北京邮电大学，2013

[4] 惠越超，汪一鸣. 基于 S 盒优化的轻量级加密算法设计[J]. 通信技术，2010,43(5):103-106

[5] 何德彪，胡进，陈建华. 基于 FPGA 的高速 AES 实现[J]. 华中科技大学学报：自然科学版，2010,38(2):101-104

[6] Kundi D S, Aziz A, Ikram N. Resource efficient implementation of T-Boxes in AES on Virtex-5 FPGA[J]. Information Processing Letters, 2010, 110(10):373-377

[7] Li C Y, Chien C F, Hong J H, et al. An efficient area-delay product design for mixcolumns/ Invmixcolumns in AES[C]// Proceeding of 2008 IEEE Computer Society Annual Symposium on VLSI. Montpellier, France, 2008:503-506

[8] 李浪，李仁发，邹祎，等. PRESENT 密码硬件语言实现及其优化研究[J]. 小型微型计算机系统，2013,34(10):2272-2275

(上接第 102 页)

参 考 文 献

[1] Gura N, Patel A, Wander A, et al. Comparing Elliptic Curve Cryptography and RSA on 8bit CPUs[J]. CHES, 2004(8):11-13

[2] Hill J, Szewczyk R, Woo R, et al. System Architecture Directions for Networked Sensors[C]// Proceeding of Architectural Support for Programming Languages and Operating Systems. Quintana Roo, USA: IEEE Publisher, 2000:93-104

[3] Malan D J, Welsh M, Smith M D. Implementing Public-Key Infrastructure for Sensor Networks [J]. ACM Transactions on Sensor Networks, 2008, 4(4):1-23

[4] Levis P, Madden S, Polastre J, et al. TinyOS: An operating system for sensor networks [EB/OL]. 2004-6-18[2014-7-9]. http://www.cs.berkeley.edu/~culler/AIIT/papers/TinyOS/levis06tinyos.pdf

[5] Watro R, Kong D, Sue F C, et al. TinyPK: Securing Sensor Networks with Public Key Technology[C]// Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. Miami, USA: IEEE Publisher, 2004:59-64

[6] Benenson Z, Gedicke N, Raivio O. Realizing Robust User Authentication in Sensor Networks[C]// Proceedings of Workshop on Real-World Wireless Sensor Networks. LNSC4582, Palma de Mallorca, Spain: Springer-Verlag, 2005:556-566

[7] Zhou Y, Zhang Y, Fang Y. Access Control in Wireless Sensor Networks [J]. Ad hoc Networks, 2007(5):3-13

[8] Oliveira L B, Dahab R, Lopez J. Identity-Based Encryption for Sensor Networks[C]// Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops. San Francisco, USA: IEEE Publisher, 2012: 290-294

[9] Cheng Hai-bin, Yang Guan. An Authenticated Identity-based Key Establishment and Encryption Scheme for Wireless Sensor Networks[J]. The Journal of China Universities of Posts and Telecommunications, 2012, 13(2):31-38

[10] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]// Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, Britain: Springer-Verlag, 2001:213-229

[11] 杨庚，程宏兵. 一种有效的无线传感器网络密钥协商方案[J]. 电子学报，2008,36(7):1389-1395

[12] Zhang Yi-he, Liu Wei, Lou Wu Jun, et al. Location-based Compromise-tolerant Security Mechanisms for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 24(2):247-260

[13] Kampanakis P T. Identity-based Cryptography Feasibility & Applications in Next Generation Sensor Networks[EB/OL]. 2011-11-6[2014-7-9]. http://www.lib.ncsu.edu/theses/available/etd-08042007-125351/unrestricted/etd.pdf

[14] Dong Xiao-lei, Wei Li-fei, Zhu Hao-jin, et al. EP2DF: an efficient privacy-preserving date-forwarding scheme for service-oriented vehicular Ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(2):580-591

[15] 郭萍，傅德胜，朱节中，等. 无线 MESH 轻量级容侵方案[J]. 计算机科学，2013,40(12):200-206

[16] Brown D R. SEC 2: Recommended Elliptic Curve Domain Parameters[EB/OL]. 2011-11-8[2014-7-10]. http://www.secg.org/download/aid-784/sec2-v2.pdf

[17] Burrows M, Abadi M, Needham R. Logic of Authentication [J]. ACM Transactions on Computer Systems, 1990(8):18-36