行了改进，但仍无法有效地解决安全隐患。文献[12]运用同步数以及双向认证机制来保障系统的安全性，对各种威胁进行分析，保证了协议的安全性。文献[13]提出了一种轻量级认证密钥协商协议，该协议包含了身份认证、密钥协商和密钥更新 3 个阶段，通信实体双方先共享旧密钥及新密钥。一般情况下，该协议使用新密钥进行重要信息的交互，若认证失败，发起者则会利用旧密钥重新发起会话。

本文主要设计了基于二次剩余理论和 Hash 函数的智能电表认证协议。在协议的初始阶段，将电表 ID 的 Hash 函数值预置在电表标签中，不占用电表标签的计算空间；在协议的认证阶段，利用二次剩余理论和勒让德符号的性质实现了数据采集器对智能电表的认证；比较分析了该协议与常用的 RFID 认证协议的安全性能和计算效率；用 BAN 逻辑对协议的形式化进行了证明；对协议的非形式化攻击进行了分析。

2　相关数学概念

二次剩余的概念在密码技术中有着重要的地位，通过二次剩余理论加密的数据具有较高的安全性[14]。

定义 1(二次剩余)　设 n 是一个正整数，如果 $gcd(a,n)=1$ 且同余式 $x^2\equiv a(\mathrm{mod}\ n)$ 有解，则称 a 是 n 的二次剩余；否则称 a 是 n 的二次非剩余。

定义 2(勒让德符号)　设 p 是一个奇素数，a 是一个不能被 p 整除的整数，则勒让德符号 $[\frac{a}{p}]$ 被定义为：$[\frac{a}{p}]=1$ 代表 a 是 p 的二次剩余；$[\frac{a}{p}]=-1$ 代表 a 是 p 的二次非剩余。

对于同余式 $x^2\equiv a(\mathrm{mod}\ n)$，若以 x^2 取代 x，且 $(x^2)^2\equiv a(\mathrm{mod}\ n)$ 有解，那么很明显，这个解是一个完全平方 (x^2)。4 个可能的解中只有一个解是同余式中对模 n 的二次剩余。

定义 3(哈希函数)　哈希函数[15] $H:\{0,1\}^*\rightarrow\{0,1\}^n$ 又称杂凑函数或者散列函数，其主要功能是将任意长度的消息映射成固定长度的输出消息。一般地，输出消息的长度远小于输入消息的长度，因此可通过缩短消息长度来提高密码算法的效率。哈希函数具有单向性，即已知一个哈希值 h，在计算上无法找出一个输入值 x 使得式 $H(x)=h$ 成立。虽然在理论上 96 位或者更大长度的哈希函数可以计算出输入值，但是在实际有限的计算时间内这几乎不可能实现。

3　基于二次剩余理论的认证协议描述

最基本的智能电表信息采集系统一般由智能电表(SM)、数据采集器和后端服务器(MDMS)三部分构成，其结构如图 1 所示。

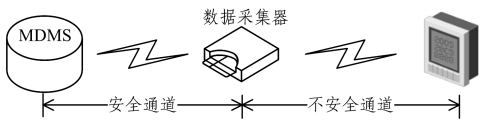

图 1　智能电表信息采集系统结构图

Fig. 1　Structure of smart meter information acquisition system

一般认为，数据采集器和 MDMS 之间的电力专用光纤网络是安全的，可以由现有的安全软件保障信息的安全传输；而数据采集器和智能电表之间的传输通道不安全。本文设计的认证协议中，Hash 运算、二次剩余计算和解密算法均在数据采集器中进行，电表标签只需存储初始信息，并进行少量的异或运算。协议的认证过程如图 2 所示。

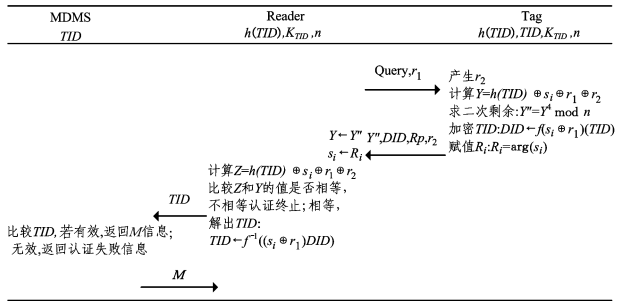

图 2　基于二次剩余理论的认证协议

Fig. 2　Authentication protocol based on quadratic residual theory

3.1　协议中的符号说明

协议中涉及的符号及其意义如下：Tag 为智能电表标签；Reader 为数据采集器；MDMS 为服务器；p 与 q 是两个大素数且 $p\equiv q\equiv 3(\mathrm{mod}\ 4)$；$n=pq$，$n$ 是正整数；$h(\cdot)$ 表示一个 Hash 函数；TID 表示电表标识符；K_{TID} 表示电表和数据采集器共享的密钥，$K_{TID}=s_1\parallel s_2\parallel\cdots\parallel s_m$，$s_i$ 是从 K_{TID} 中随机抽取的一组长为 n bit 的字符串；$\parallel$ 代表连接符，$\oplus$ 代表按位进行异或运算；r_i 代表协议中产生的随机数；$DID\leftarrow f_{(s_i\oplus r_1)}(TID)$ 代表加密后的电表标签标识符；$TID\leftarrow f^{-1}_{(s_i\oplus r_1)}(DID)$ 代表解密后的电表标签标识符；M 代表标签物品信息；$R_i=\arg(s_i)$ 表示将 s_i 转变为与随机数相同的进位制的赋值运算。

3.2　协议的执行过程

1)初始阶段

数据库和数据采集器分别与电表标签共享一些信息：数据库与标签共享标签标识符 TID；阅读器和标签共享密钥 K_{TID} 和 TID 的 Hash 值 $h(TID)$ 以及正整数 n。

2)执行阶段

步骤 1　数据采集器生成随机数 r_1，同时向电表发送认证信息 $Query$。

步骤 2　电表收到来自数据采集器的认证信息后，生成的随机数 r_2，并进行如下计算：

①$Y=h(TID)\oplus s_i\oplus r_1\oplus r_2$；

②$Y''=Y^4(\mathrm{mod}\ n)$；

③$DID\leftarrow f_{(s_i\oplus r_1)}(TID)$；

④$R_i=\arg(s_i)$；

⑤将 Y''，DID，r_2，R_i 发送给数据采集器。

步骤 3　数据采集器在收到 Y''，DID，r_2，R_i 后，进行如下计算：

①收到 Y'' 后，生成新的同余式 $X^2\equiv Y''(\mathrm{mod}\ n)$。设 $X=Y^2$，因为 $n=pq$，所以同余式 $X^2\equiv Y''(\mathrm{mod}\ n)$ 可以分解成同余式组 $\begin{cases}x^2\equiv Y''(\mathrm{mod}\ p)\\ x^2\equiv Y''(\mathrm{mod}\ q)\end{cases}$；已知 $p\equiv q\equiv 3(\mathrm{mod}\ 4)$，上述同余式组可以得到两个不同的解：$x\equiv\pm(Y'')^{(p+1)/4}(\mathrm{mod}\ p)$ 和 $x\equiv\pm(Y'')^{(q+1)/4}(\mathrm{mod}\ q)$)；然后利用中国余数定理解得：$\begin{cases}x\equiv\pm x_1(\mathrm{mod}\ n)\\ x\equiv\pm x_2(\mathrm{mod}\ n)\end{cases}$；又因为 $X=Y^2$，所以 $\begin{cases}x\equiv+x_1(\mathrm{mod}\ n)\\ x\equiv+x_2(\mathrm{mod}\ n)\end{cases}$。

因此，$Y=\sqrt{x_1}$ 或 $Y=\sqrt{x_2}$，此时利用勒让德符号解出唯一的 Y 值。

②通过 R_i 解出 s_i，然后计算 $Z=h(TID)\oplus s_i\oplus r_1\oplus r_2$，并比较 Z 是否与上一步得到的 Y 值相等，若不相等则认证终止。

③若 $Z=Y$，则数据采集器通过得到的 s_i 和自身所了解的 r_1 解密 DID，得到 TID，并将 TID 发送给 MDMS 数据库。

3)认证阶段

MDMS 数据库收到 TID 后，搜索数据库中是否有相同的 TID，以验证标签是否合法，若有相同的 TID，则将电表信息 M 发送给数据采集器；若数据库中没有相同的 TID，则验证电表标签无效，返回数据采集器失败的认证信息。

4 协议性能分析

4.1 协议的形式化分析

运用 BAN 逻辑[16]对协议进行安全分析。BAN 逻辑表达式及逻辑推理规则如表 1 和表 2 所列。

表 1 BAN 逻辑表达式

Table 1 BAN logic expressions

BAN 逻辑表达式	表达含义
$P\mid\equiv X$	P 信任 X
$P\mid\sim X$	P 产生过 X
$P\lhd X$	P 收到过 X
$P\mid\Rightarrow X$	P 对 X 有管辖权
$\sharp(X)$	X 是新鲜的
$\{X\}_K$	用密钥 K 加密 X 后得到的密文
$P\overset{K}{\leftrightarrow}Q$	P 和 Q 共享密钥 K

表 2 BAN 逻辑推理规则

Table 2 Inference rules of BAN logic

推理规则	BAN 逻辑表达式
消息含义规则	$\dfrac{P\mid\equiv Q\overset{K}{\leftrightarrow}P,P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X}$
临时值验证规则	$\dfrac{P\mid\equiv\sharp(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
仲裁规则	$\dfrac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$

协议包括数据采集器 R、电表标签 T 和数据库 S 3 个要素，R 与 T 在初始化阶段就共享一个密钥对，用 K 来表示。假设 R 与 S 之间为安全信道，用密钥 Key 来加密 R 与 S 之间的信息。

首先，建立协议的理想化模型：

Message1 $R\rightarrow T:\{r_1\}_K$

Message2 $T\rightarrow R:\{Y'',DID,r_2\}_K$

Message3 $R\rightarrow S:\{TID\}_{Key}$

Message4 $S\rightarrow R:\{M\}_{Key}$

然后，建立协议的初始假设集合：

$R\mid\equiv R\overset{K}{\leftrightarrow}T;T\mid\equiv T\overset{K}{\leftrightarrow}R;S\mid\equiv S\overset{Key}{\leftrightarrow}R;R\mid\equiv R\overset{Key}{\leftrightarrow}S;R\mid\equiv\sharp(DID);R\mid\equiv\sharp(Y'');R\mid\equiv\sharp(M);R\mid\equiv T\mid\Rightarrow DID;R\mid\equiv T\mid\Rightarrow Y'';R\mid\equiv S\mid\Rightarrow M;S\mid\equiv R\mid\Rightarrow TID;S\mid\equiv\sharp(TID)$

协议的正确性证明目标如下：

a)$R\mid\equiv DID$；b)$R\mid\equiv Y''$；c)$S\mid\equiv TID$；d)$R\mid\equiv M$。

证明过程如下：

1)消息 Message2 可得到 $R\lhd\{DID\}_K$，由假设 $R\mid\equiv T\overset{K}{\leftrightarrow}R$ 和消息含义规则可推出 $R\mid\equiv T\mid\sim DID$；由假设 $R\mid\equiv\sharp(DID)$ 和临时值验证规则可推出 $R\mid\equiv T\mid\equiv DID$；由假设 $R\mid\equiv T\mid\Rightarrow DID$ 和仲裁规则可推出 $R\mid\equiv DID$；同理 $R\mid\equiv Y''$。

2)消息 Message3 可得 $S\lhd\{TID\}_{Key}$，由假设 $S\mid\equiv S\overset{Key}{\leftrightarrow}R$ 和消息含义规则可推出 $S\mid\equiv R\mid\sim TID$；由假设 $S\mid\equiv\sharp(TID)$ 和临时值验证规则可推出 $S\mid\equiv R\mid\equiv TID$；由假设 $S\mid\equiv R\mid\Rightarrow TID$ 和仲裁规则可推出 $S\mid\equiv TID$。

3)消息 Message4 可得 $R\lhd\{M\}_{Key}$，由假设 $R\mid\equiv S\overset{Key}{\leftrightarrow}R$ 和消息含义规则可推出 $R\mid\equiv S\mid\sim M$；由假设 $R\mid\equiv\sharp(M)$ 和临时值验证规则可推出 $R\mid\equiv S\mid\equiv M$；由假设 $R\mid\equiv S\mid\Rightarrow M$ 和仲裁规则可推出 $R\mid\equiv M$。整个认证过程证明完毕。

由 BAN 逻辑形式化分析可以看出，本协议中 $R\mid\equiv DID$，$R\mid\equiv Y''$，$S\mid\equiv TID$，因此协议的安全性得到证明，能够实现预期假设。

4.2 协议的非形式化分析

1)隐私保护

首先，方案中采用求解二次剩余的方法来认证电表标签。利用大的复合数的因式分解难以被预测的性质，提高了数据加密的安全性，防止电表标签和数据采集器之间的信息被窃取；其次，本方案在电表标签和数据采集器初始化阶段就写入了一段 Hash 值，Hash 函数的单向、不可逆特性可以保证电表标签和数据采集器之间数据通信的前向安全性；最后，将电表标签 TID 作为关键词来查询 MDMS 中的数据信息，TID 值在认证过程中从未以明文的形式出现，因此避免了信息泄露。

2)抵抗重放攻击

协议中，密钥被分成 m 组 n bit 的字符串，从中随机选取一组字符串来实现计算和认证，因此当攻击者在协议中试图重放消息时，数据采集器在执行阶段会计算出两次相同的 Z 值，此时采集器认为遭受重放攻击并采取相应的安全措施。

3)位置攻击

电表标签标识符 TID 在协议中经过加密后变成 DID 进行传输，且对 TID 进行加密运算的字符串也是从密钥中随机抽取的字符串，攻击者无法预测，因此即使上次的数据被截获，攻击者仍不能预测下次通信的数据信息。

4)匿名性

电表标签 $DID\leftarrow f_{(s_p\oplus r_1)}(TID)$，在协议中参与认证的是 $h(TID)$，$Y=h(TID)\oplus s_p\oplus r_1\oplus r_2$，电表标签在认证的过程中都是匿名传输的。

5)中间人攻击

攻击者可以模仿数据采集器向电表标签发出 $Request$ 以及 r_1，并获得电表标签的返回信息 Y''，DID。但是由于 r_2 不知道 $h(TID)$，会导致下一步计算的 Y 和 Z 值与实际不符，得不到正确的 TID 值，不能成功实现认证，亦不会获得数据库给出的电表信息。

5 协议的性能分析

将本文所提出的协议与文献[8]和文献[13]所提出的协议进行性能比较，结果如表 3 所列。可以看出，本文提出的协议可抵抗重放攻击和恶意跟踪，并且具有前向安全性。

表 3　本文协议与其他协议的性能比较

Table 3　Performance comparison of proposed protocol and other protocols

协议	前向安全性	抗重放攻击	防止恶意跟踪
文献[8]的协议	√	×	×
文献[13]的协议	√	×	√
本文提出的协议	√	√	√

假设标签长度为 K，密钥和伪随机数的长度为 L，Hash 函数的长度为 H。文中所提协议的标签除了需要存储密钥和标签内容以外，还需要存储标签的 Hash 函数值。对本文提出的协议与文献[8]和文献[13]所提出的协议进行效率分析，结果如表 4 所列，其中，$PRNG$ 为生成随机数运算量；E 为加密运算量；D 为解密运算量；$Hash$ 为哈希运算量；R 为二次剩余运算量。可以看出，本协议仅通信 2 次。

表 4　本文协议与其他协议的效率分析

Table 4　Efficiency analysis of proposed protocol and other protocols

协议	标签存储空间	标签计算量	通信次数
文献[8]的协议	$2L+K$	$PRNG+E$	4
文献[13]的协议	$5L+K$	$PRNG+D+E+Hash$	5
本文提出的协议	$2L+K+H$	$PRNG+R+E$	2

一般的低成本标签有 5k 左右的门电路，其中有 10%～20%的门电路用于实现协议的安全功能。随机数发生器需要几百个门电路；Hash 函数需要 1700 个门电路[17]；分组密码算法需要 1400 个门电路；文中提出的协议不需要进行 Hash 运算，只是将标签 ID 的 Hash 函数值与随机数进行异或移位等运算，这在标签的承受范围之内。

结束语　本文针对基于 RFID 智能电表中的安全和隐私问题，利用二次剩余理论和 Hash 函数构造了电表标签和数据采集器之间的 RFID 系统认证协议。协议不需要大运算量的密码算法，只需要在初始阶段在电表标签和数据采集器中预置标签标识符的 Hash 函数值，并运用二次剩余理论来认证标签。通过 BAN 逻辑的分析方法，对协议的形式化进行证明，并对协议的非形式化问题进行分析，其中，协议能抵抗重放攻击和标签位置攻击。最后，将本文提出的协议与智能电表常用的认证协议进行分析和对比，结果表明，在满足隐私性和不可追踪性的前提下，本文协议计算量小、通信开销较低，可以保证用户个人隐私的安全性，满足新一代智能电表安全设计的要求。

参 考 文 献

[1] YU Y X, LUAN W P. Smart Grid[J]. Power System & Clean Energy, 2009, 127(9): 251-253.

[2] KHURANA H, HADLEY M, LU N, et al. Smart-Grid Security Issues[J]. IEEE Security & Privacy, 2010, 8(1): 81-85.

[3] SHARMA K, SAINI L M. Performance analysis of smart metering for smart grid: An overview[J]. Renewable & Sustainable Energy Reviews, 2015, 49: 720-735.

[4] ZHAO B, ZHAI F, LI T Y, et al. Secure Communication Protocol for Smart Meter Bidirectional Interaction System[J]. Automation of Electric Power System, 2016, 47(17): 93-98. (in Chinese)
赵兵，翟峰，李涛永，等. 适用于智能电表双向互动系统的安全通信协议[J]. 电力系统自动化，2016，47(17)：93-98.

[5] DUAN J H, CUI A J, ZHANG X, et al. The Network Information Security of Smart Grid Architecture[J]. Information Security and Technology, 2015(11): 52-54. (in Chinese)
段军红，崔阿军，张驯，等. 面向智能电网的网络信息安全架构[J]. 信息安全与技术，2015(11)：52-54.

[6] LIU X Y, ZHANG Q, LI Z M. A Survey on Information Security for Smart Grid[J]. Electric Power ICT, 2014, 12(4): 56-60. (in Chinese)
刘雪艳，张强，李战明. 智能电网信息安全研究综述[J]. 电力信息与通信技术，2014，12(4)：56-60.

[7] HAN Y N, LI F G. Research on combined public key cryptographic scheme for smart grid[J]. Journal of Cryptologic Research, 2016, 3(4): 340-351. (in Chinese)
韩亚楠，李发根. 适用于智能电网的组合公钥密码体制研究[J]. 密码学报，2016，3(4)：340-351.

[8] HU Y, DONG M C. Strengthening the security of network applications with SSL protocol[J]. Automation of Electiric Power Systems, 2002, 26(15): 70-77. (in Chinese)
胡炎，董名垂. 用 SSL 协议加强电力系统网络应用的安全性[J]. 电力系统自动化，2002，26(15)：70-77.

[9] GARCIA F D, JACOBS B. Privacy-friendly energy-metering via homomorphic encryption[M] // Security and Trust Management. Springer Berlin Heidelberg, 2010: 226-238.

[10] XUE R. IK-CPA security implies IE-CCA security in the random oracle model[J]. Science China (Information Sciences), 2013, 56(3): 179-189.

[11] HSIANG H C, KUO H C, SHIH W K. Security Enhancement for a Novel Mutual Authentication Scheme Based on Quadratic Residues for RFID Systems[C] // Second International Conference on Future Generation Communication and Networking, 2008(FGCN'08). IEEE, 2008: 197-200.

[12] XIAO H G, LI W, WU X R. A lightweight and efficient RFID authentication protocol based on synchronization code[J]. Computer Engineering & Science, 2016, 38(4): 673-678. (in Chinese)
肖红光，李为，巫小蓉. 基于同步数的轻量级高效 RFID 身份认证协议[J]. 计算机工程与科学，2016，38(4)：673-678.

[13] ZHAO B, GAO X, GAO P P, et al. A lightweight authenticated protocol with key agreement for power utilization information collecting[J]. Automation of Electric Power Systems, 2013, 37(12): 81-86. (in Chinese)
赵兵，高欣，郜盼盼，等. 适用于用电信息采集的轻量级认证密钥协商协议[J]. 电力系统自动化，2013，37(12)：81-86.

[14] XUAN X W, TENG J F, BAI Y. Enhanced RFID Authentication Protocol Based on Quardratic Residue[J]. Computer Engineering, 2012, 38(3): 124-125, 129. (in Chinese)
轩秀巍，滕建辅，白煜. 基于二次剩余的增强型 RFID 认证协议[J]. 计算机工程，2012，38(3)：124-125，129.

[15] ROSEN K H. Elementary Number Theory and Its Applications[M]. Beijing: China Machine Press, 2004.

[16] WANG Z C, XU D Y, WANG X F, et al. Reliability Analysis and Improvement of BAN Logic[J]. Computer Engineering, 2012, 38(17): 110-115. (in Chinese)
王正才，许道云，王晓峰，等. BAN 逻辑的可靠性分析与改进[J]. 计算机工程，2012，38(17)：110-115.

[17] BOYD C, MAO W. On a limitation of BAN logic[M] // Advances in Cryptology—EUROCRYPT'93. Springer Berlin Heidelberg, 1993: 240-247.