面向医疗物联网的匿名认证协议

刘英军, 罗洋, 杨钰均, 刘媛妮

引用本文

刘英军, 罗洋, 杨钰均, 刘媛妮.面向医疗物联网的匿名认证协议[J]. 计算机科学, 2023, 50(8): 359-364.

LIU Yingjun, LUO Yang, YANG Yujun, LIU Yuanni. Anonymous Authentication Protocol for Medical Internet of Things [J]. Computer Science, 2023, 50(8): 359-364.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220700151

面向医疗物联网的匿名认证协议

刘英军[1]　罗　洋[2]　杨钰均[2]　刘媛妮[3]
1 工业和信息化部产业发展促进中心　北京 100846
2 重庆邮电大学计算机科学与技术学院　重庆 400065
3 重庆邮电大学网络空间安全与信息法学院　重庆 400065
(liuyingjun@idpc.org.cn)

摘　要　随着物联网技术的不断成熟,其开始被频繁地应用于各行各业以提高人们的工作效率和生活水平。物联网在医疗领域的广泛应用,不仅能方便患者获取医疗服务,同时也能让医生更及时、准确地获取患者的身体状况,从而制定更高效的治疗方案。然而,人们在享受医疗物联网便利的同时,如何保证患者的通信安全和个人隐私也是不容忽视的问题。为了实现用户安全访问网络,提出了一个基于同态加密的高效匿名认证与密钥交换协议,医疗设备与远程医疗服务器之间只需要一个低熵的口令就可以实现相互认证,从而协商出一个高熵的会话密钥。在标准模型下证明了方案的安全性,仿真实验结果表明该方案比现有的同类方案具有更高的效率。

关键词:密码认证;医疗物联网;标准模型;匿名认证
中图法分类号　TP309.2

Anonymous Authentication Protocol for Medical Internet of Things

LIU Yingjun[1],LUO Yang[2],YANG Yujun[2] and LIU Yuanni[3]
1 Industry Development and Promotion Center,Beijing 100846,China
2 School of Computer Science and Technology,Chongqing University of Posts and Telecommunications,Chongqing 400065,China
3 School of Cyber Security and Information Law,Chongqing University of Posts and Telecommunications,Chongqing 400065,China

Abstract　As IoT technology continues to mature,it has been frequently used in various industries to improve people's work efficiency and living standards. The widespread application of IoT in the medical field facilitates patients' access to medical services while also allowing doctors to obtain more timely and accurate information about the patient's physical condition,so that they can develop more efficient treatment plans. However,while people are enjoying the convenience of medical IoT,how to ensure the communication security and personal privacy of patients are issues that cannot be ignored. In order to realize users' secure access to the network,this paper proposes an efficient anonymous authentication and key exchange protocol based on homomorphic encryption. Medical devices and telemedicine servers only need a low-entropy password for mutual authentication,thus negotiating a high-entropy session key. In this paper,the security of the scheme is proved under the standard model,and the simulation experimental results show that the scheme is more efficient than existing similar schemes.

Keywords　Cryptography authentication,Medical Internet of things,Standard model,Anonymous authentication

1　引言

近年来,物联网技术与医疗行业的联系越来越紧密。在医疗物联网给人们的生活带来便利的同时,如何保证医疗物联网中的信息安全也是一个非常重要的问题。目前,为医疗物联网设备提供身份认证的方法有多种,如基于口令的认证密钥交换(PAKE)、公钥基础设施(PKI)等身份认证方法。其中,PAKE 被认为是解决物联网各个领域[1]

到稿日期:2022-07-15　返修日期:2023-06-12
基金项目:重庆市自然科学基金面上项目(cstc2020jcyj-msxmX1021);重庆市教委科学技术研究项目(KJZD-K20200602);网络与交换技术国家重点实验室(北京邮电大学)开放课题资助项目(SKLNST-2021-1-18);重庆市自然科学基金(cstc2020jcyj-msxmX0343)
This work was supported by the General Program of Natural Science Foundation of Chongqing(cstc2020jcyj-msxmX1021),Science and Technology Research Program of Chongqing Municipal Education Commission(KJZD-K20200602),Open Foundation of State key Laboratory of Networking and Switching Technology(Beijing University of Posts and Telecommunications)(SKLNST-2021-1-18) and Natural Science Foundation of Chongqing,China(cstc2020jcyj-msxmX0343).
通信作者:杨钰均(s200231254@stu.cqupt.edu.cn)

安全问题最有前景的解决方案之一。

PAKE通常用于客户端-服务器模式，使用简单易记的低熵口令来完成双向身份认证并协商出一个高熵会话密钥。这是一种非常方便的通信保障方法，它使用户摆脱了PKI，也不必记住一个非常复杂的高熵密钥。1992年Bellovin等[2]提出了第一个PAKE协议EKE。此后，大量的PAKE协议被提出[3-8]。在许多传统的PAKE协议中，客户端发送的消息可以被服务器识别，然后服务器决定应该使用哪个口令参与运算。然而，随着对隐私问题的日益关注，研究人员开始研究匿名口令认证协议(APAKE)来保护用户的隐私[9-11]。服务器只知道与它交互的客户端是合法的，但不知道它的真实身份。由于医疗物联网中部署了各种医疗传感器和设备，网络中包含大量敏感且关键的数据，因此，保护身份认证的鲁棒安全性和私密性变得更加具有挑战性。基于此，本文提出了一种基于同态加密的高效匿名认证与密钥交换协议，形式化证明和实验分析显示，该协议更适用于医疗物联网。

本文第2节对相关工作进行简要介绍；在第3节介绍了协议中涉及的一些密码原语；第4节详细介绍了协议流程；第5节对协议的安全性进行了形式化证明；第6节进行效率分析；最后总结全文并展望未来。

2 相关工作

Viet等[12]提出了第一个APAKE协议，之后Yang等[13]指出该协议无法抵抗离线字典攻击并给出了改进后的新协议。Liu等[14]提出了一个轻量级的认证协议，该协议使用对称加密的方式替换公钥加密，降低了计算开销。为了构造出扩展性更好的APAKE协议，Yang等[15]提供了一种新的思路，客户端不向服务器注册自己的口令，而是使用自己的口令来保护其身份认证凭据。Qian等[16]在协议[15]的基础上做了改进，降低了计算耗费，但却引入了额外的设备用于存储重要的认证凭据。在服务器端存储明文口令，若服务器文件发生泄露，将破坏整个协议的安全性。针对这种问题，学者们提出了不在协议实体两端使用明文口令的方法。Hu等[17]使用一种类似验证元的技术来对明文口令进行计算，在协议的初始化阶段客户端将计算出哈希口令，并以哈希口令向服务器注册并完成后续的协议操作，即使服务器发生泄露事件，敌手也需要进行离线字典攻击才能获得明文口令，大大降低了服务器文件泄露的危害。

为了更好地适应医疗物联网环境，Jiang等[18]使用ECC构建了一个高效的协议，将复杂的操作放在网关上，从而降低了传感器端的计算成本。Zhang等[19]提出了一种利用无线衰落信道的变种PAKE协议(vPAKE)，而Chen等[20]指出该协议[19]效率低，其次不能抵抗伪造攻击。Chang等[21]提出了一个双因子3-PAKE协议，并在ROR模型下证明了其安全性。He等[22]在双因子3-PAKE协议的基础上进行了改进，但未能实现语义安全。Jiang等[23]基于二次剩余定理提出了一种能保证客户端匿名性的端到端协议。Zhao等[24]利用用户口令和智能卡完成与传感器节点的双重身份认证和会话密钥协商，实现双方安全通信并确保只有合法终端用户才能获取节点收集的实时数据。Liu等[25]提出了一种基于双线性对的认证协议来实现医疗物联网设备与远程医疗服务器之间的认证。Li等[26]指出LIU等的协议不能抵御离线字典攻击，并提出了一种更高效的匿名认证协议。

3 密码学原语

3.1 安全模型

我们简要介绍由Bellare等[27]提出的广受认可的形式化安全模型BPR2000。本协议的协议参与者由客户端$C=\{C_1,\cdots,C_k\}$和服务器S组成，客户端和服务器共享了相同的口令，从而完成认证操作协商出共同的高熵会话密钥SK。协议的参与者$U\in C\cup S$可能具有多个实例，称参与者的第i个实例为U^i，也称之为预言机。

长期密钥：BPR2000模型的长期密钥就是口令，每一个客户端C_i都拥有一个自己的口令π_i，服务器端拥有一个口令列表PW。

敌手能力：概率多项式时间敌手A与协议参与者通过各种预言机查询来进行交互，这些预言机查询就是敌手的攻击能力。

$Excute(C_i,\alpha,S,\beta)$查询：这种查询模拟被动攻击，攻击者$A$通过该查询获得客户端实例$C_i^\alpha$和服务器实例$S^\beta$协议执行过程中的所有交互信息。

$Send(U,i,m)$查询：此查询模拟一个主动攻击，敌人给实例U^i发送一个消息m，该实例依据协议规定响应。

$Reveal(U,i)$查询：此查询模拟了会话密钥的泄露。当实例U^i实际持有会话密钥时，它会返回该会话密钥。

$Corrupt(U)$查询：该查询模拟前向安全性。被询问的协议参与者U将返回它拥有的长期密钥或者其所有实例的内部状态。而回答过$Corrupt$查询的参与者的状态称为已腐化。

$Test(U,i)$查询：此查询用于定义会话密钥的语义安全性。敌手只能对一个“新鲜”的实例U^i进行1次$Test$查询，然后获得一个挑战值。U^i随机选择一位比特b，如果$b=1$则返回会话钥sk；如果$b=0$则返回一个等长的随机值。

新鲜性：在协议参与者实例U^α已经成功认证其伙伴实例U^β的情况下，如果U^α没有经历过$Reveal$查询和$Corrupt$查询，则称它具有新鲜性。

语义安全：语义安全意味着敌手不能获得关于会话密钥的任何信息，是一种最基本的安全。我们使用$Succ(A)$来表示敌手A成功猜对Test预言机的值b的概率，那么敌手A攻击协议语义安全的优势即可定义为：

$$Adv_{\text{Apake}}^{\text{AKE}}(A)=|2Pr[Succ(A)]-1|$$

若该值可忽略不计，则表明我们的协议是语义安全的，反之则不安全。

3.2 DDH困难问题

设G是一个q阶有限循环群，q是素数，其生成元为g。给定$g^a,g^b,g^z(a,b,z\in Z_q^*)$，判断是否$g^z=g^{ab}$，即$Succ_G^{DDH}(A)=Pr[A(g^a,g^b,g^z),g^{ab}=g^z]\leqslant\varepsilon$，若其中$\varepsilon$是可忽略的，则称DDH问题是$(t,\varepsilon)$困难的。

3.3 伪随机函数集

设 Λ 是一个概率多项式算法，那么该算法能够成功区分均匀分布函数集 $R=\{R_n\}(n\in N)$ 与伪随机函数集 $F=\{F_n\}(n\in N)$ 的优势可以定义为：

$$Adv^F(\Lambda)=|pr[\Lambda^{F_n}(1^n)=1]-pr[\Lambda^{R_n}(1^n)=1]|$$

若 $Adv^F(\Lambda)$ 的值可忽略，则 F 就是伪随机的。

3.4 公钥加密方案

本协议用到了 CPA 安全的公钥加密体制。$\mathcal{M}=(Gen,Enc,Dec)$ 为一个公钥加密方案，它由密钥生成算法 Gen、加密算法 Enc、解密算法 Dec 组成。密码生成算法 Gen 以一个安全参数 1^k 为输入，输出一对公私钥 (pk,sk)。给定公钥 pk，消息 m 和随机字符串 r，使用加密算法 Enc 可得密文 $C=Enc_{pk}(m;r)$。解密算法 Dec 将私钥 sk 和密文 c 作为输入，并输出明文 m。

如果对于任何知道公钥 pk 的概率多项式敌手 A，它区分两个具有挑战性的消息 m_0 和 m_1 的密文的优势可忽略不计，那么加密方案 $\mathcal{M}$ 就是 CPA 安全的。

本协议最终采用的公钥加密方案为 EIGamal，此方案具有乘同态性质，对于明文空间中的两条任意消息 m_1 和 m_2，以下情况成立：

$$Enc_{pk}(m_1;r_1)2\ Enc_{pk}(m_2;r_2)=Enc_{pk}(m_1 2\ m_2;r_3)$$

4 认证方案

4.1 初始化阶段

设 G 是一个阶为大素数 q 的循环群，g 为随机选择的 G 的生成元。令 $H:G\rightarrow\{0,1\}^n$ 为一个哈希函数，$M=(Gen,Enc,Dec)$ 是一个同态加密方案生成密钥对 (pk,sk)，随机选择辅助参数 $M\in G$。经由安全信道发送 (M,sk) 给服务器。

4.2 注册阶段

客户端 C_i 从口令字典 N 中随机选择口令 pw_i 并把口令发送给服务器，由服务器计算辅助参数 $\gamma_i=Enc_{pk}(M^{-1}\cdot g^{-H(ID_i)\cdot H(pw_i)};r_i)$ 并公开。

4.3 认证阶段

(1)客户端选择一个随机数 x，计算出 $A=g^x$，为了利用 EIGamal 的乘同态性质，将参数 A 秘密地发送至服务器，客户端计算一个伪装参数 $\pi=g^{-H(ID_i)\cdot H(pw_i)}$，最后计算出密文 $\varepsilon=Enc_{pk}(A\cdot\pi;r)\cdot\gamma_i$ 并发送至服务器。

(2)客户端在收到消息 ε 后利用私钥解密，此时根据 EIGamal 的乘同态性质将成功得到参数 A，服务器选择随机数 y，计算出 $B=g^y$，$\sigma=A^y=g^{xy}$，最后利用伪随机数计算出认证参数 $\theta_s=F_\sigma(1)$。服务器将消息 $\langle B,\theta_s\rangle$ 发送至客户端。

(3)客户端在收到来自服务器的消息后，首先计算出 $\sigma=B^x=g^{xy}$，紧接着验证是否 $F_\sigma(1)=\theta_s$，若否，则终止协议。通过了身份认证后，计算认证参数 $\theta_c=F_\sigma(2)$ 并且生成会话密钥 $K=F_\sigma(3)$。最终，客户端将消息 $\langle\theta_c\rangle$ 发送至服务器。

(4)服务器在收到消息 θ_c 后，首先验证是否 $F_\sigma(2)=\theta_c$，若否，则终止协议，最终服务器计算出会话密钥 $K=F_\sigma(3)$。客户端与服务器认证过程如图 1 所示。

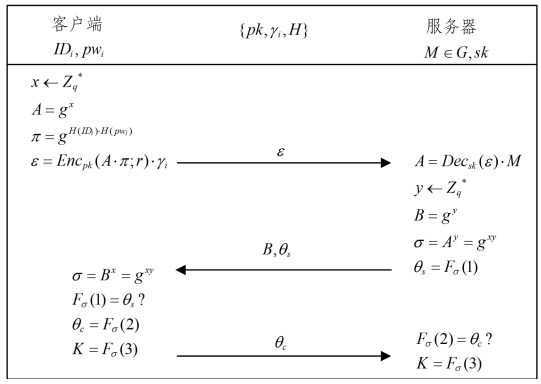

图 1 认证过程

FIg. 1 Process of authentication

5 安全性分析

5.1 正确性

在正常交互的情况下，客户端与服务器会获得相同的迪菲赫尔曼秘密值 σ，从而计算出相同的认证参数，完成认证并且最后协商出相同的会话密钥 K。为了证明方案的正确性，采用 BAN 逻辑证明来实现正确性证明。

(1)目标

goal1：$C|\equiv C\overset{K}{\leftrightarrow}S$

goal2：$S|\equiv C\overset{K}{\leftrightarrow}S$

(2)理想化方案

$C\rightarrow S:(A,\pi,r)_{\mapsto S}^{pk}$

$S\rightarrow C:(A,B)_{C\overset{\sigma}{\rightleftharpoons}S}$

(3)初始化假设

$A1:C|\equiv\#(x)$

$A2:C|\equiv\#(r)$

$A3:S|\equiv\#(y)$

$A4:C|\equiv C\overset{\sigma}{\rightleftharpoons}S$

$A5:S|\equiv C\overset{\sigma}{\rightleftharpoons}S$

$A6:C|\equiv S(C\overset{K}{\leftrightarrow}S)$

$A7:S|\equiv C(C\overset{K}{\leftrightarrow}S)$

(4)证明部分

(1)$S\lhd(A,\pi,r)_{\mapsto S}^{pk}$，应用接受消息规则可以推断出：

$$\frac{S\lhd(A,\pi,r)_{\mapsto S}^{pk}}{S\lhd A}$$

(2)当服务器收到消息 A 之后便可以计算出迪菲赫尔曼秘密值 σ，从而计算出会话密钥 K。故可以推断出：

$$S|\equiv C|\equiv(C\overset{K}{\leftrightarrow}S)$$

(3)由假设 A7、结论(2)应用管辖权规则可推断出：

$$\frac{S|\equiv C(C\overset{K}{\leftrightarrow}S),S|\equiv C|\equiv(C\overset{K}{\leftrightarrow}S)}{S|\equiv(C\overset{K}{\leftrightarrow}S)}(\text{goal2})$$

(4)由假设 A4、$C\lhd(A,B)_{C\overset{\sigma}{\rightleftharpoons}S}$ 应用消息含义规则可以推断出：

$$\frac{C|\equiv C\overset{\sigma}{\rightleftharpoons}S,C\lhd(A,B)_{C\overset{\sigma}{\rightleftharpoons}S}}{C|\equiv S|\sim(A,B)}$$

(5)由假设 A3 应用新鲜性规则可推断出：

$$\frac{C|\equiv\#(y)}{C|\equiv\#(B)}$$

(6)由结论(5)应用新鲜性规则可推断出：

$$\frac{C|\equiv\#(B)}{C|\equiv\#(A,B)}$$

(7)由结论(4)、结论(6)应用临时值校验规则可以推断出：

$$\frac{C|\equiv\#(A,B),C|\equiv S|\sim(A,B)}{C|\equiv S|\equiv(A,B)}$$

(8)由结论(7)应用信念规则可以推断出：

$$\frac{C|\equiv S|\equiv(A,B)}{C|\equiv S|\equiv B}$$

(9)由结论(8)可知客户端得到了消息 B，可以计算出迪菲赫尔曼秘密值 σ，从而计算出会话密钥 K。故可以推断出：

$$C|\equiv S|\equiv(C\overset{K}{\leftrightarrow}S)$$

(10)由假设 $A6$、结论(9)应用管辖权规则可推断出：

$$\frac{C|\equiv S(C\overset{K}{\leftrightarrow}S),C|\equiv S|\equiv(C\overset{K}{\leftrightarrow}S)}{C|\equiv(C\overset{K}{\leftrightarrow}S)}(\text{goal1})$$

由于协议具有对称性，通过相同方式能够证明目标 goal2，因此不再赘述。由此证明了方案的正确性，正常交互情况下服务器端和客户端能够得到相同的会话密钥。

5.2 语义安全性

设 A 是攻击协议语义安全性的敌手。设计一系列的实验，所有的实验中，预言机按协议的描述诚实回答攻击者的查询。逐步修改预言机回应查询的方式使得相邻实验中敌手成功的概率可忽略，从而估算出敌手优势的上界。$Pr[S_i]$ 表示攻击者在实验 Exp_i 中成功攻击协议的概率。

实验 0　这是真实的协议攻击实验。模拟器模拟所有诚实的会话，并且诚实地回答敌手提出的所有查询。敌手优势定义如下：

$$Adv_{\text{Apake}}^{\text{AKE}}(A)=|2Pr[S_0]-1|$$

实验 1　在本次实验中，我们修改预言机回应 $Excute(C_i,\alpha,S,\beta)$ 的方式，用随机值 r 代替 ε。由于 ε 是由 EIGamal 密文相乘得到的一个乘积结果，因此，依靠 EIGamal 方案的 CPA 安全性，敌手将无法区分随机值 r 与密文 ε。可得结论：

$$Pr[S_1]-Pr[S_0]\leqslant q_e\cdot Adv^{\text{CPA}}$$

实验 2　在本次实验中，修改预言机回应 $Excute(C_i,\alpha,S,\beta)$ 的方式，实验 1 与实验 2 的区别在于，用随机值 r 代替消息 B。消息 B 本就是服务器利用随机数计算出的一个随机值，攻击者 A 是感觉不到任何变化的。可得结论：

$$Pr[S_2]=Pr[S_1]$$

实验 3　在本次实验中，修改预言机回应 $Excute(C_i,\alpha,S,\beta)$ 的方式，用随机值 r 替代关键参数 σ。对于攻击者来说，想要成功区分 r 与 σ，就必须解决 DDH 困难问题。可得结论：

$$Pr[S_3]-Pr[S_2]\leqslant q_e\cdot Adv_{g,G}^{\text{DDH}}$$

实验 4　在本次实验中，修改预言机回应 $Excute(C_i,\alpha,S,\beta)$ 的方式，用随机值 r_1 和 r_2 分别替代认证参数 θ_s 和 θ_c。在实验 3 中我们已经知道敌手无法通过得到关键参数 σ 来计算出正确的认证参数 θ_s 和 θ_c，由于这两个认证的参数均是使用伪随机函数计算得到的，那么在敌手能攻破伪随机函数的安全性之前，θ_s 和 θ_c 与随机值是不可区分的。可得结论：

$$Pr[S_4]-Pr[S_3]\leqslant q_e\cdot Adv^{F}$$

我们把交互过程中所使用到的一些关键参数随机化，利用 DDH 困难问题、CPA 安全性和伪随机函数来保证敌手不能通过这些参数攻破我们的协议。现在开始考虑主动攻击，以下是几种 send 查询的方式。让 $Send_0(C_i^{\alpha},\alpha,S)$ 作为发送给客户端实例 C_i^{α} 的协议初始化消息，$Send_1$，$Send_2$，$Send_3$ 分别表示为：

$Send(S,\beta,\langle\varepsilon\rangle)$

$Send(C_i,\alpha,\langle B,\theta_s\rangle)$

$Send(S,\beta,\langle\theta_c\rangle)$

实验 5　在本次实验中，攻击者通过构造消息 ε，来发起 $Send(S,\beta,\langle\varepsilon\rangle)$。攻击者有以下两种攻击方式：

(1)利用重放攻击，与实验 1 的证明方式类似，敌手成功的事实建立在其攻破 CPA 安全性的基础上，那么攻击者成功的概率为 $q_s\cdot Adv^{\text{CPA}}$。

(2)攻击者猜中所使用的辅助参数 γ_i 且伪造出了正确参数 π，这样一来，敌手可以构造出一个能够完成后续认证流程的合法 ε，那么攻击者成功的概率为 $Adv_{g,G}^{\text{DDH}}\cdot\frac{q_s}{N}$（$N$ 是客户端个数）。

可得结论：

$$Pr[S_5]-Pr[S_4]\leqslant q_s\cdot Adv^{\text{CPA}}+Adv_{g,G}^{\text{DDH}}\cdot\frac{q_s}{N}$$

实验 6　在本次实验中，敌手进行 $Send(C_i,\alpha,\langle B,\theta_s\rangle)$ 查询时，预言机将按照协议描述验证 θ_s 的正确性，如果认证成功，则敌手攻击成功，终止协议。敌手用以下方式来进行攻击：

(1)利用重放攻击。很明显，敌手若想要重放出有效的 B 和 θ_s 就必须与上一步的 ε 进行匹配，那么攻击者成功的概率为 $\frac{q_s+q_e}{q}$。

(2)在前面的证明过程中，所有参数的随机化使得敌手无法计算出正确的关键参数 σ，因而无法通过正常计算得出正确的 θ_s。若敌手在这种前提下还能得到正确的 θ_s，说明敌手已攻破了伪随机函数，那么攻击者成功的概率为 $q_s\cdot Adv^{F}$。可得结论：

$$Pr[S_6]-Pr[S_5]\leqslant\frac{q_s+q_e}{q}+q_s\cdot Adv^{F}$$

实验 7　在本次实验中，敌手进行 $Send(C_i,\alpha,\langle\theta_c\rangle)$ 查询时，预言机将按照协议描述验证 θ_c 的正确性，如果认证成功则敌手攻击成功，终止协议。若攻击者在实验 6 中攻击失败，说明交互过程中均为正常的实体，整个交互过程并未泄露任何有用的关键信息。此时敌手能够成功攻击协议的方式只有随机猜测。可得出结论：

$$Pr[S_7]-Pr[S_6]\leqslant\frac{q_s}{2^n}$$

实验 8　在本次实验中，修改预言机回应 $Reveal$ 查询的方式，以随机值 r 替代会话密钥 K。会话密钥 K 由伪随机函数结合关键参数 σ 计算而来，在前面的各个实验中并未泄露

任何方便敌手计算出 σ 的参数，那么敌手想在 *Reveal* 查询中攻击成功就必须建立在其攻破伪随机函数的基础上。可得结论：

$$Pr[S_8]-Pr[S_7]\leqslant q_r \cdot Adv^F$$

通过对 *Excute* 查询进行修改，攻击者不能获得任何有助于后续计算的参数，故敌手在 *Test* 查询中无法区分得到的是真正的会话密钥还是随机数，除非在这之前敌手对通信实体或者实体搭档进行过 *Reveal* 查询，但这是进行 *Test* 查询的前提“新鲜性”所不允许的，因此在实验 8 中敌手成功攻击协议的概率为：$Pr[S_8]=\frac{1}{2}$。

综上所述，敌手成功攻击协议的优势可表示为：

$$\begin{aligned}Adv_{Apake}^{AKE}(A)&=|2Pr[S_0]-1|\\&\leqslant 2\,q_e \cdot (Adv^F+Adv^{CPA}+Adv_{g,G}^{DDH})+2\,q_s \cdot \left(Adv^F+Adv_{g,G}^{DDH}+\frac{1}{2^n}\right)+\frac{2(q_s+q_e)}{q}+\\&\quad 2\,q_r \cdot Adv^F\end{aligned}$$

6 效率分析

本节将展示本协议性能分析的实验结果。所有实验均在搭载 Intel(R) Core(TM) i5-4200H CPU @2.80GHz CPU 的 Windows 10 系统上操作，所使用的工具包为 JPBC(Java Pairing-Based Cryptography Library)。本文选择已有的一些同类型的匿名认证协议[28-31]与本协议进行安全性和计算开销的比较。

对于在随机预言下证明安全的协议来说，由于现实世界中只能以哈希函数来进行模拟，因此这些协议在实际环境中的安全性有待商榷，故本文认为在标准模型下进行安全性证明的协议具有更高的安全性。双向认证也是匿名认证协议的基本安全要求，双向认证意味着，除非正确猜出客户端和服务器事先预享的口令，否则任何人都不能冒充任何合法参与者。协议的安全性对比如表 1 所列。

表 1 安全性对比

Table 1 Safety comparison

协议	模型	双向认证	困难问题
LPAKE[28]	标准模型	是	LWE
YPAKE[29]	随机预言模型	是	LWE
TPAKE[30]	标准模型	是	CDH
SPAKE[31]	随机预言模型	是	CDH
Our Protocol	标准模型	是	DDH

表 2 从通信代价和计算开销两方面来分析协议的效率。本文和对比方案在通信中都交互 3 次，因此在相同的通信环境中，通信代价是相同的。但在计算开销方面，表中列出了各协议最为耗时的模幂运算(Exp)。LPAKE 与 YPAKE 虽然在标准模型下证明了安全性，但是均使用了计算复杂度较高的平滑投射希函数以及 CCA 安全的加密算法，因此整个协议复杂度较高，计算开销较大；TPAKE 为了更方便地将安全性规约到 CDH 困难问题使用了大量模幂运算，导致复杂度较高；SPAKE 计算复杂度较好，但是接受了随机预言机的启示，实际安全性无法保证；本文的协议在标准模型下是可证明安全的，与其他同类型的协议相比，在通信代价相同的情况下，其在计算效率上也具有显著优势。

表 2 计算效率对比

Table 2 Comparison of computational efficiency

协议	交互次数	客户端复杂度	服务器复杂度
LPAKE[28]	3	7 Exp	7 Exp
YPAKE[29]	3	7 Exp	6 Exp
TPAKE[30]	3	5 Exp	6 Exp
SPAKE[31]	3	5 Exp	3 Exp
Ours	3	5 Exp	3 Exp

如图 2 所示，本文将各个协议进行仿真，得到各自的运行时间。结果表明，与标准模型下的协议相比，本文的协议在运行时间上具有显著优势，其在协议构造时未采用过于复杂的密码学组件，这是本文在运行时间上占据优势的主要原因。虽然 SPAKE 随机预言模型下的协议理应具有更高的计算效率，但是该协议过于依赖随机预言机的启示，计算效率并不高。本文的协议在保证安全性的基础上进一步优化了计算效率，减少了协议运行时间。

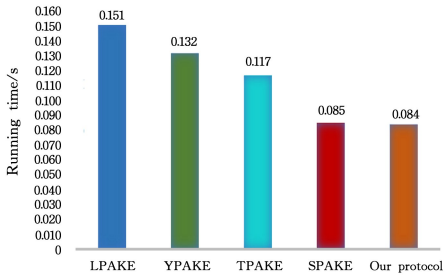

图 2 仿真结果

Fig. 2 Simulation results

结束语 本文介绍了一个利用同态加密方案所构造出的客户端匿名的双向匿名认证协议。该协议属于口令认证类协议，客户端和服务器可以利用一个预享的低熵口令，匿名地完成实体认证，之后协商出一个高熵的会话密钥。首先，本协议达到了单向匿名的效果，即在交互过程中服务器不知道客户端的身份，保证了用户的个人隐私；其次，与现有的同类型认证协议相比，本文协议计算开销大大降低；最后，本文使用了 BAN 逻辑与形式化安全性证明方法分别得出了本文协议的正确性和安全性结论。

参 考 文 献

[1] HAASE B, LABRIQUE B. AuCPace: Efficient verifier-based PAKE protocol tailored for the IIoT[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(2): 1-48.

[2] BELLOVIN S M, MERRITT M. Encrypted key exchange: password-based protocols secure against dictionary attacks[C]// Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, CA, USA, 1992: 72-84.

[3] LI X, NIU J, KHAN M K, et al. An enhanced smart card based remote user password authentication scheme[J]. Journal of Network and Computer Applications, 2013, 36(5): 1365-1371.

[4] KUMARI S, KHAN M K, LI X, et al. Design of a user anonymous password authentication scheme without smart card[J]. International Journal of Communication Systems, 2016, 29(3): 441-458.

[5] SHEN J, FENG M, LIU D, et al. Enhanced Remote Password-

Authenticated Key Agreement Based on Smart Card Supporting Password Changing[C]// International Conference on Information Security Practice and Experience. Cham: Springer, 2017: 454-467.

[6] SHU J, XU C X. Efficient Password-Based Authenticated Key Exchange Protocol under Standard Model[J]. Journal of Electronics & Information Technology, 2009, 31(11): 2716-2719.

[7] JIANG Q, MA J, LI G, et al. Improvement of robust smart-card-based password authentication scheme[J]. International Journal of Communication Systems, 2015, 28(2): 383-393.

[8] JIANG Q, MA J, TIAN Y. Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al[J]. International Journal of Communication Systems, 2015, 28(7): 1340-1351.

[9] WEI F, VIJAYAKUMAR P, SHEN J, et al. A provably secure password-based anonymous authentication scheme for wireless body area networks[J]. Computers & Electrical Engineering, 2018, 65: 322-331.

[10] WANG C, XU G, LI W. A secure and anonymous two-factor authentication protocol in multiserver environment[J]. Security and CommunicationNetworks, 2018, 2018: 1-15.

[11] BANERJEE S, ODELU V, DAS A K, et al. A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment[J]. IEEE Internet of Things Journal, 2019, 6(5): 8739-8752.

[12] VIET D Q, YAMAMURA A, TANAKA H. Anonymous password-based authenticated key exchange[C]// International Conference on Cryptology in India. Berlin: Springer, 2005: 244-257.

[13] YANG J, ZHANG Z. A new anonymous password-based authenticated key exchange protocol[C]// International Conference on Cryptology in India. Berlin: Springer, 2008: 200-212.

[14] LIU F F, LIU Y B. Lightweight smart phone security authentication protocol based on social network [J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2013, 25(1): 132-137.

[15] YANG Y, ZHOU J, WENG J, et al. A new approach for anonymous password authentication[C]// 2009 Annual Computer Security Applications Conference. IEEE, 2009: 199-208.

[16] QIAN H, GONG J, ZHOU Y. Anonymous password-based key exchange with low resources consumption and better user-friendliness[J]. Security and Communication Networks, 2012, 5(12): 1379-1393.

[17] HU X, ZHANG J, ZHANG Z, et al. Anonymous password authenticated key exchange protocol in the standard model[J]. Wireless Personal Communications, 2017, 96(1): 1451-1474.

[18] JIANG Q, MA J, WEI F, et al. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks[J]. Journal of Network and Computer Applications, 2016, 76: 37-48.

[19] ZHANG Y, XIANG Y, WU W, et al. A variant of password authenticated key exchange protocol[J]. Future Generation Computer Systems, 2018, 78: 699-711.

[20] CHEN Y, YUAN J, ZHANG Y. An improved password-authenticated key exchange protocol for VANET[J]. Vehicular Communications, 2021, 27: 100286.

[21] CHANG C C, LE H D. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks[J]. IEEE Transactions on wireless communications, 2015, 15(1): 357-366.

[22] HE J, YANG Z, ZHANG J, et al. On the security ofa provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(1): 1-11.

[23] JIANG Q, MA J, YANG C, et al. Efficient end-to-end authentication protocol forwearable health monitoring systems[J]. Computers & Electrical Engineering, 2017, 63: 182-195.

[24] ZHAO Z Q, GUO X J, YIN M H, et al. Research on authentication method of identity-based higncryption in IoT[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2023, 35(2): 343-351.

[25] LIU C H, CHUNG Y F. Secure user authentication scheme for wireless healthcare sensor networks[J]. Computers & Electrical Engineering, 2017, 59: 250-261.

[26] LI C T, WU T Y, CHEN C L, et al. An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system[J]. Sensors, 2017, 17(7): 1482.

[27] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2000: 139-155.

[28] LI Z P, WANG D. Achieving one-round password-based authenticated key exchange over lattices[J]. IEEE Transactions on Services Computing, 2019, 15(1): 308-321.

[29] YU J X, LIAN H H, ZHAO Z Q, et al. Provably secure verifier-based password authenticated key exchange based on lattices [M]// Advances in Computers. Elsevier, 2021: 121-156.

[30] XIANG S B, XU B, CHEN K. A two-party password-authenticated key exchange protocol with verifier[J]. Journal of Computer and Communications, 2021, 9(4): 102.

[31] SHIN S H, KOBARA K. Simple anonymous password-based authenticated key exchange (sapake), reconsidered [J]. IEIC Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, 100(2): 639-652.

LIU Yingjun, born in 1974, master, senior engineer. His main reaserch interests include cybersecurity data governance and new generation information technology, digital transformation and high quality development of small and medium enterprises, and industrialization of manufacturing innovation achievements.

YANG Yujun, born in 1998, postgraduate. Her main research interests include authentication and key agreement protocol and communication security.

(责任编辑:何杨)