doi:10.11959/j.issn.1000-436x.2017125

基于 PUF 和 IPI 的可穿戴设备双因子认证协议

王俊[1,2]，刘树波[1,2]，梁才[1,2]，李永凯[1,2]
（1. 武汉大学空天信息安全与可信计算教育部重点实验室，湖北 武汉 430072；2. 武汉大学计算机学院，湖北 武汉 430072）

摘 要：可穿戴设备正推进着移动医疗的快速发展，但无线体域网的开放式结构也给用户数据安全带来了更多威胁。为了数据安全，基于物理不可克隆函数和脉搏间隔，提出一种设备节点和数据中心之间的双因子认证协议。此协议利用设备物理特征和用户生物特征双重唯一性，有效地阻止了妥协和假冒等攻击，且适用于体域网环境下资源受限的医疗设备。与现有方案相比，增强了认证协议安全性。FPGA 平台上实验证明了所提协议的实用性和有效性。

关键词：认证协议；双因子；物理不可克隆函数；脉搏间隔
中图分类号：TP309.2 **文献标识码**：A

Two-factor wearable device authentication protocol based on PUF and IPI

WANG Jun[1,2], LIU Shu-bo[1,2], LIANG Cai[1,2], LI Yong-kai[1,2]
(1. Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China
2. School of Computer, Wuhan University, Wuhan 430072, China)

Abstract: Wearable device is pushing the rapid development of mobile health, however, the open architecture of wireless body area network has brought challenges for the security of user data. In order to protect the security of user data, a two-factor authentication protocol between device note and data hub was proposed based on physically unclonable function and interpulse interval. Using dual uniqueness of device physical characteristic and user biometric trait, the protocol can resist compromise and impersonation attacks and was specially suitable for resource constrained wearable devices under body area network. Compared with the existing authentication schemes, the security of the proposed protocol was enhanced. The practicability and effectiveness of the protocol are confirmed by hardware implementation on FPGA.

Key words: authentication protocol, two-factor, physically unclonable function, interpulse interval

1 引言

可穿戴设备是置于用户体外或体内的智能化微型设备，能提供长期的医疗监控或支持[1]。移动医疗系统利用无线通信技术处理医疗数据，并为用户提供健康服务[2]。然而，由于可穿戴设备涉及用户隐私和数据安全，在无线体域网开放式结构下，系统必须为节点设备和数据中心之间提供一种安全认证机制[3,4]。

针对可穿戴设备，安全认证协议在保护用户隐私和数据安全上起着重要作用。在体域网中，医疗信息非常敏感，除授权用户外，非授权用户不能访问，否则，恶意者可能篡改医疗信息、药物剂量和设备工作程序，会威胁用户数据安全甚至生命[5]。已有基于可信平台模块（TPM, trusted platform module）或高级加密标准（AES, advanced encryption standard）的方法过于复杂，不适应于资源受限的可穿戴设备[6]。为了解决此问题，提出了基于物理不

收稿日期：2016-10-27；**修回日期**：2017-04-24
基金项目：国家自然科学基金资助项目（No.41371402, No.41671443）；中央高校基本科研业务费专项基金资助项目（No.2015211020201, No.2042017gf0038）
Foundation Items: The National Natural Science Foundation of China (No.41371402, No.41671443), Fundamental Research Funds for the Central Universities (No.2015211020201, No.2042017gf0038)

可克隆函数（PUF, physically unclonable function）的认证协议[7]。

PUF 利用硅器件固有的不可克隆物理特性提供了激励（输入）到响应（输出）的唯一映射[7]。基于 PUF 的认证协议具有易实现和低能耗的优点，多应用于资源受限的嵌入式系统中设备身份认证[8]。

早期，基于 PUF 的认证协议利用存储的激励响应对（CRP, challenge response pair）实现[9]。首先，从设备节点获取 CRP 并存储于后台数据库。然后，认证节点根据数据库中某条 CRP 记录的激励，生成对应响应。如果生成响应与 CRP 记录中响应一致，节点认证成功，否则失败。为抵抗重放攻击，每条 CRP 记录仅使用一次，认证完成后即删除。然而，此方法需要在后台存储 CRP，不利于应用程序扩展。在射频识别（RFID, radio frequency identification）系统中，文献[10~12]提出了基于 PUF 的 RFID 认证协议，这些协议同样需要存储 CRP 或密钥。Rostami 等[13]提出一种基于多 PUF 模型的轻量级认证协议，此协议不需要在数据库中存储 CRP，然而，协议中基于线性反馈移位寄存器的伪随机数发生器存在安全隐患[14]。

上述文献考虑了设备物理特征的唯一性，然而，用到可穿戴设备上却忽略了用户生物特征的唯一性，使这些协议易受妥协攻击。如果用户体域网中某节点对敌手妥协，用户隐私与安全将面临威胁。如敌手能通过妥协节点发送错误信息干扰设备正常工作。

文献[15~20]提出多种基于生物特征的认证协议和密钥协商方案。生物传感器收集的数据能同时应用于移动医疗和节点认证，降低了设备的资源开销和计算代价。由于可穿戴设备普遍含有脉搏传感器，用户脉搏间隔（IPI, interpulse interval）被用于体域网中节点认证和密钥生成[5,15~19]。其中，文献[15]利用光电容积脉搏波（PPG，physiological photoplethysmogram）信号获取 IPI，文献[16,17]利用心电图（ECG, electrocardiogram）信号获取 IPI。针对移动医疗，基于 IPI 生物特征的认证协议，开销小，适用于无线体域网中节点认证。然而，这些方案仅考虑了用户生物特征的唯一性，忽略了设备物理特征的唯一性，使这些协议易受假冒攻击。如用户体域网外某节点窃取用户生物特征，侵入用户体域网，进而威胁用户数据与健康安全。

针对上述问题，利用设备物理特征和用户生物特征双重唯一性，本文提出一种基于 PUF 和 IPI 的轻量级双因子认证协议（TFAP, two factor authentication protocol），并采用异或操作确保协议秘密参数的有用信息在信息通道中不被泄露和抵御建模攻击。此外，认证双方利用同步 IPI 作为随机数种子，不需额外的随机数发生器。与现有方案相比，本协议能有效阻止妥协和假冒等攻击，增强了认证协议安全性。

2 预备知识

2.1 物理不可克隆函数

根据文献[21]对 PUF 的分类，本文采用的强 PUF 属于 PUF 分类下子集。强 PUF 拥有海量 CRP，其数量远大于物理设备数量，为多种应用提供了硬件系统身份认证等服务[21]，能防止敌手通过历史 CRP 进行重放攻击。强 PUF 能为生产芯片提供身份验证机制，也可生成密钥[22~24]。

基于延迟的 PUF 适用于资源受限环境下应用，如可穿戴设备[9]，其电路原理如图 1 所示[25]。此电路主要由 n 个延迟单元和一个 D-触发器仲裁器（arbiter）组成。每个延迟单元包含 2 个数据选择器，有上下 2 条延迟路线。脉冲信号从左边输入，然后在上下 2 条路径上竞争通过。利用器件自身内部制造的差异性，得到一个从输入激励到输出响应的映射[26]。

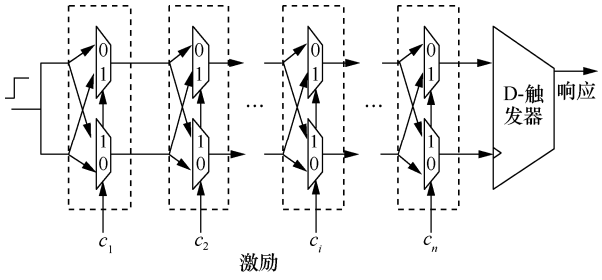


图 1 基于延迟的 PUF 电路

给定激励 $c_i \in \{0,1\}$, i = 1, 2, …, n, 信号在竞争路径中的相对延迟决定了仲裁器的输出结果。如图 1 中虚线框所示，在每个延迟单元中，c_i 作为数据选择器的选择信号，决定了脉冲信号的路径走向。如果 c_i=0，信号在延迟单元中并行通过，否则，信号在延迟单元中交叉通过。脉冲信号通过 n 个延迟单元后，到达电路右边的 D-触发器仲裁器，仲裁器根据信号竞争通过的快慢，得到不同输出结果。如果信号先到达时钟引脚 *Clk*，则

输出结果为 1，否则，输出结果为 0。D-触发器输出结果如图 2 所示。

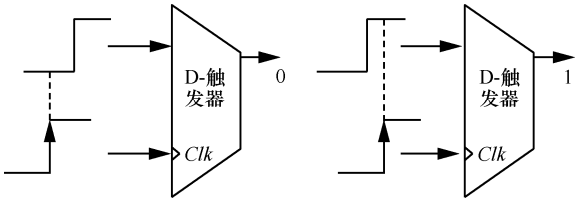


图 2　D-触发器输出

基于延迟的PUF结构简单，易遭受建模攻击[21]。为阻止此类攻击，可采用多 PUF 并联的方式得到经过异或操作的输出结果。多 PUF 拥有更好的雪崩效应，即输入激励一位数据的翻转将导致输出响应50%位数据的变化。并联 PUF 数越多，建模复杂度越高，建模时间跨度越大（大于一年）[7,13]，然而也导致输出结果正确率降低。为了平衡复杂度与正确率，本文采用 4-异或 PUF 电路。如图 3 所示，4 个 PUF 电路的输出结果经过异或操作之后输出，从而保护 PUF 免受敌手建模攻击[23]。

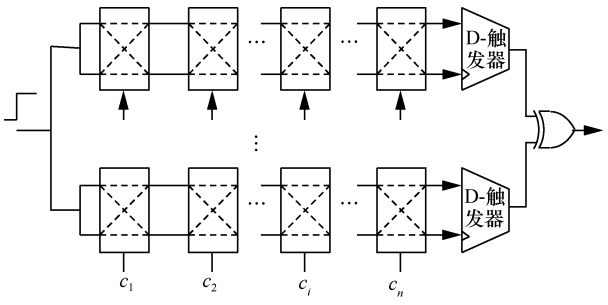


图 3　4-异或 PUF 电路

4-异或 PUF 的多项式模型只能被可信实体建立，如可穿戴设备制造商。设备节点拥有一个 PUF 物理访问接口，可信实体能通过此接口获取设备节点的 CRP，并建立 PUF 模型。模型建立后，诚实认证方能通过此 PUF 模型对节点进行认证[7]。建模完成之后，设备节点中的 PUF 访问接口将被物理毁坏，以防止敌手通过此接口获取 CRP 进行建模攻击。

图 1 中基于延迟的 PUF 可通过线性不等式表达[7,23]，如式(1)所示。

$$r = Sign\left(\vec{\Delta}\cdot\vec{\Theta}\right) \tag{1}$$

其中，$\vec{\Delta}=(\delta_1,\cdots,\delta_i,\ \cdots,\delta_{n+1})$表示信号在上下 2 条路径中延迟，$\delta_1=\dfrac{\delta_1^0-\delta_1^1}{2}$，$\delta_i=\dfrac{\delta_{i-1}^0+\delta_{i-1}^1+\delta_i^0-\delta_i^1}{2}$，$i=2,\cdots,n$，$\delta_{n+1}=\dfrac{\delta_n^0+\delta_n^1}{2}$，$\delta_i^{0/1}$ 为数据选择器 i 中选择信号分别为 0 和 1 时的路径延迟，$\vec{\Theta}=((-1)^{\gamma_1},(-1)^{\gamma_2},\cdots,(-1)^{\gamma_n},1)$，$\gamma_i=c_i\oplus c_{i+1}\oplus\cdots\oplus c_n$，$c_i\in\{0,1\}$，“$\cdot$”为点积运算，$Sign$ 为符号函数。

本文采用文献[7]中基于延迟的 PUF 实现方案，删除了真/伪随机数生成模块，因为此模块需要较多额外资源[14]。通过在协议中引入生物特征 IPI，采用 IPI 二进制编码序列作为 PUF 的输入激励，取消随机数生成模块的同时，增强了认证协议的安全性。

2.2　脉搏间隔

心脏每次的收缩与舒张形成脉搏信号波，而 IPI 则指信号波的脉搏间隔[19]。IPI 可以通过不同的心血管信号获得，如 ECG 和 PPG。ECG 利用置于体表的测量电极记录心电图，PPG 利用脉动血液对一定波长光敏感的特性得到容积脉搏血流的变化[15]。本文认证协议中采用了 PPG 信号。

基于 IPI 生成的二进制序列具有良好的随机性，已被双尾检测和熵测试证明[5,16]。二进制序列的随机性与认证协议安全性紧密相关，序列的随机性越高，协议的安全性越强。敌手通过历史或将来 IPI 实现认证不可行，因为历史或将来 IPI 与实时 IPI 之间差异性过大，详见第 4.3 节。

每次心博周期，仅利用一个 IPI 编码生成位数足够长的二进制序列，时间需要超过 1 min[5]。为克服时间过长的问题，文献[18]采用多 IPI 编码的方式生成最终二进制序列。

PPG 信号中的 IPI 编码过程如图 4 所示，左边的 PPG 信号通过右边的二进制编码器（BE，binary encoder）编码生成一个二进制序列。为了提高 IPI 数据精度，一个 IPI 通过一个脉搏传感器在多次心博周期中的脉搏间隔均值计算，易于编程和硬件实现。同时，IPI 选择格雷编码，此编码方式具有错误最小化特性，减少了相邻 IPI 二进制编码序列间的变化。对 IPI 进行编码时，一个 IPI 被编码为 6 位格雷码，则 11 个 IPI 可编码为 64 位长二进制序列，最高 2 位已删除。编码规则如下：给定 IPI，首先通过整除运算对 IPI 进行无量纲化，以消除 2 个 IPI 间的差异，无量纲化后的值 $val=\left\lfloor\dfrac{IPI}{scale}+0.5\right\rfloor$，其中 $scale$ 为量化尺度参数，量化尺度参数决定了消除 IPI 间差异的程度，本文取

scale=25 000 μs；然后得到 *val* 对应 6 位 ASCII 码 *bin*，高位补零；最后将此 ASCII 码 *bin* 转换为格雷码 *gray*，算式为

$$\begin{cases} gray_i = bin_i, i = 5 \\ gray_i = bin_i \oplus bin_{i+1}, 0 \leqslant i < 5 \end{cases} \tag{2}$$

如对脉搏间隔 975 000 μs，其 $val=\left\lfloor \frac{975\,000}{25\,000}+0.5 \right\rfloor$ =39，*bin*=100111，*gray*=110100。

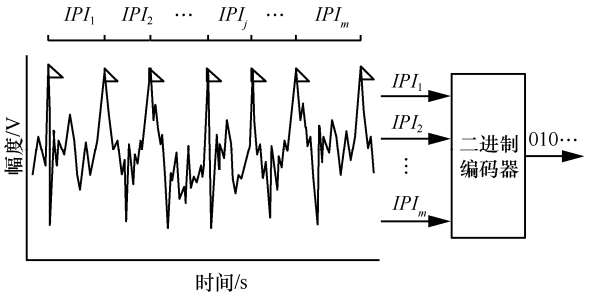


图 4 IPI 二进制编码

上述 IPI 编码方案确保用户同步 IPI 二进制编码序列间具有良好的匹配度。给定一个 64 位二进制编码序列 U，其熵可以通过 $H(U)=-(P_0\text{lb}P_0+P_1\text{lb}P_1)$计算，其中，$P_0$ 和 P_1 分别为二进制序列 U 中“0”和“1”的概率。测试时，二进制序列 U 的数目从 1 开始，数量逐渐增加到 105。熵测试结果表明本文 64 位 IPI 二进制序列的熵值大于 0.93，随机性良好，如图 5 所示，横坐标为二进制序列 U 的数目，纵坐标为熵值。

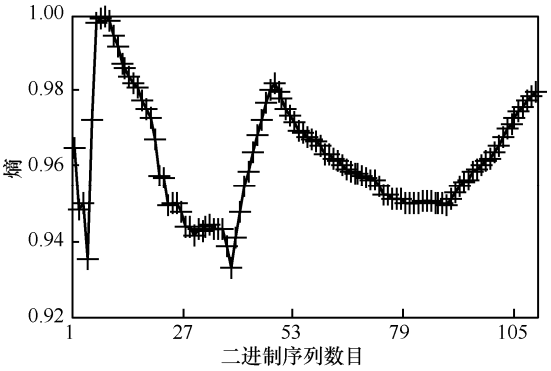


图 5 64 位二进制序列熵分布

可穿戴设备认证协议的研究现主要集中在设备物理特征或用户生物特征上。本文为增强认证协议安全，同时将设备物理特征和生物传感器自身的 PPG 信号引入到协议中，提出了基于 PUF 和 IPI 的双因子认证协议 TFAP。

3 TFAP 双因子认证协议

本节详细介绍了双因子认证协议 TFAP。不同于 PUF 或 IPI 的认证协议，TFAP 保证了设备物理特征和用户生物特征的双重唯一性。

TFAP 应用 PUF 和 IPI 双因子认证的原理如图 6 所示，用户身上数据中心（如手持仪）和认证节点组成一个体域网，协议参与双方分别为数据中心和认证节点。每个传感器节点都是被认证方认证，数据中心为认证方。假设节点 A 要向中心认证，节点 A 和中心首先利用同步 IPI 二进制序列作为 PUF 和 PUF 模型的输入，然后分别得到对应的输出结果。最后，中心通过比较输出结果间的汉明距离（HD, Hamming distance），判断节点 A 认证是否成功。

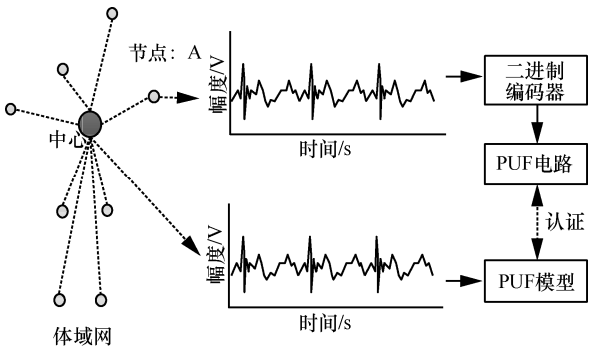


图 6 TFAP 认证原理

认证时，假设数据中心为一个诚实认证方，能对传感器节点进行认证。同时，只有可信实体能将 PUF 模型授权给其他诚实的认证方。TFAP 中的初始化和认证流程如图 7 所示，认证协议中主要参数如表 1 所示。

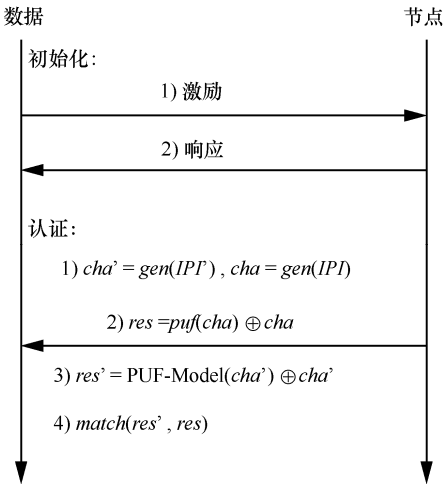


图 7 TFAP 流程

表 1　TFAP 中参数符号

参数符号	描述
IPI’	数据中心记录的用户脉搏间隔，如 969 813 μs
IPI	认证节点记录的用户脉搏间隔
cha’	*IPI*’生成激励，为 64 位二进制编码序列
cha	*IPI* 生成激励，为 64 位二进制编码序列
res’	数据中心输出结果，为 64 位二进制序列
res	认证节点输出结果，为 64 位二进制序列
T	汉明距离阈值，为协议是否认证成功的判断参数

TFAP 的第一阶段为初始化。数据中心向传感器节点发送激励，传感器节点将收到的激励作为 PUF 输入，得到响应，并把响应结果返回数据中心。数据中心根据收集到的 CRP 完成 PUF 建模，最后物理毁坏 PUF 访问接口，防止敌手获取 CRP。

TFAP 的第二阶段为认证。认证时，数据中心和认证节点不需预先存储协商密钥，利用同步 IPI 二进制编码序列作为双方秘密种子，避免信息泄露。

协议认证具体流程如下所示。

Step1　数据中心和认证节点利用同步采集的脉搏间隔 *IPI*’和 *IPI* 作为二进制编码器 BE 生成函数 *gen*()的输入，得到 64 位激励 *cha*’和 *cha*。

Step2　认证节点用 *cha* 作为 PUF 的输入得到输出，此输出进一步与 *cha* 异或，得到最后输出结果 *res*，并发送给数据中心。

Step3　数据中心用 *cha*’作为 PUF 模型的输入得到输出，此输出进一步与 *cha*’异或，得到最后输出结果 *res*’。

Step4　数据中心比较 *res*’与接收到的 *res*，若两者间汉明距离小于给定阈值 *T*，认证成功，否则认证失败。

4　性能评估

本节对 TFAP 的性能和安全性进行分析。设备节点端的协议基于 Altera 公司 Cyclone 开发板实现，硬件描述语言为 Verilog HDL。数据中心端的协议基于软件实现，编程语言为 Java。脉搏传感器为即插即用的光电容积型，可从用户手指或耳垂捕获 PPG 信号。

4.1　度量参数

本文主要通过拒真率（FRR, false rejection rate）和认假率（FAR, false acceptance rate）来对实验结果进行评估。

FRR：使用同一用户同步 IPI 二进制编码序列作为 PUF 和 PUF 模型的输入，得到输出结果，两者间汉明距离大于等于阈值 *T* 的概率。

FAR：使用同一/不同用户异步 IPI 二进制编码序列作为 PUF 和 PUF 模型的输入，得到输出结果，两者间汉明距离小于阈值 *T* 的概率。

FRR 和 FAR 都用到了汉明距离，2 个二进制序列间汉明距离定义如下[7,13]。

$$HD(C_x,C_y)=\sum_{i=1}^{n}(\,|C_x[i]-C_y[i]|\,) \tag{3}$$

其中，C_x 和 C_y 为二进制序列，$C_x[i], C_y[i]\in\{0,1\}$为序列中第 i 位的值。如序列“01001000”和“00101000”间汉明距离为 2。$HD(C_x,C_y)$越大，2 个二进制序列间的差异性越大。

4.2　性能对比

脉搏间隔 *IPI* 和 *IPI*’通过 2 个传感器分别在左手和右手食指上测得，经过二进制编码器 BE 编码后得到二进制序列 *cha* 和 *cha*’，两者间汉明距离在不同情形下的累积分布函数不同。若不同 *cha* 和 *cha*’间汉明距离 *sample*=[1,12,6,12,10]，本文可通过 Matlab 函数 *cdf*(*sample*)得到 *sample* 的累积分布函数。实验中，分别对 100 组数据进行测试。

可以看出，同一用户同步 IPI 二进制编码序列间差异最小，基准时间、间隔 2 h 和 4 h 下，同步二进制序列间汉明距离 90%以上小于 5，如图 8 所示。将不同用户分成甲、乙、丙 3 组，不同用户异步 IPI 二进制编码序列间差异最大，甲、乙和丙组对应二进制序列与基准时间二进制序列间汉明距离 90%以上大于 15，如图 9 所示。同一用户异步 IPI 二进制编码序列间差异居于上述两者之间，间隔 2 h、4 h 和 6 h，二进制序列与基准时间二进制序列间汉明距离 90%以上大于 10，如图 10 所示。

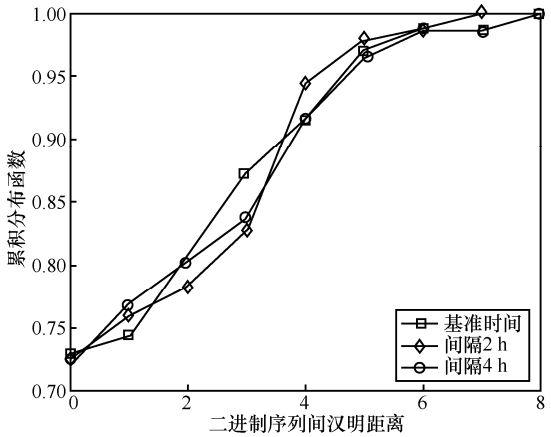


图 8　同一用户同步 IPI 二进制序列间汉明距离的累积分布函数

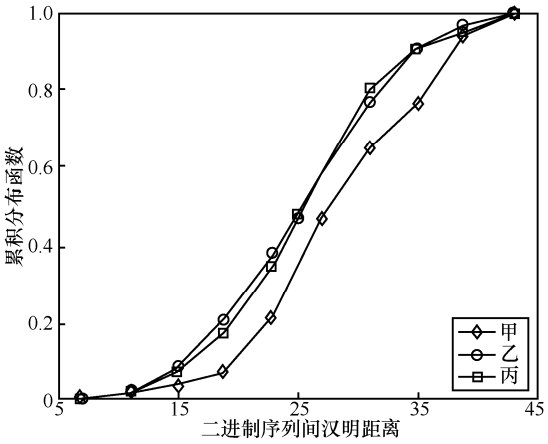


图 9　不同用户异步 IPI 二进制序列间汉明距离的累积分布函数

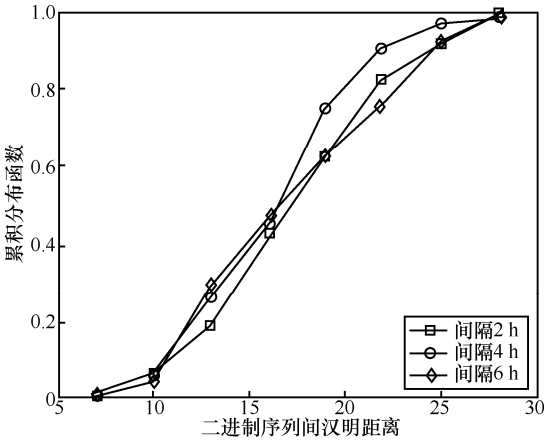


图 10　同一用户异步 IPI 二进制序列间汉明距离的累积分布函数

获得 IPI 二进制序列 *cha* 和 *cha*'之后，比较输出结果 *res* 和 *res*'间汉明距离是否小于给定阈值 *T*，现通过拒真率和认假率对协议进行评估。

假设 PUF 模型准确率为 100%，若 *cha* 和 *cha*'为同一用户同步 IPI 二进制编码序列，协议的 *FRR* 如图 11 所示。可看出，*FRR* 随着阈值 *T* 的变小而升高。

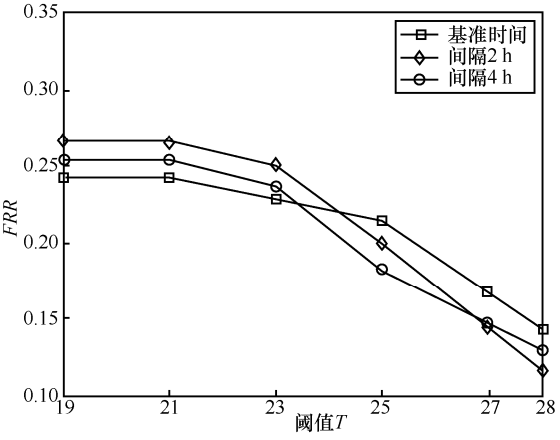


图 11　同一用户同步 IPI 情形中不同阈值 *T* 下的拒真率

例如，当 *T*=28 时，*FRR* 均值为 12.8%，*T*=25 时，*FRR* 均值为 19.8%。注意，当阈值 *T* 小于 21 时，*FRR* 固定不变，这表明 74.6%的同一用户同步 IPI 二进制编码序列具有高度相似性。

若 *cha* 和 *cha*'为同一/不同用户异步 IPI 二进制编码序列，协议的 *FAR* 如图 12 和图 13 所示。可看出，*FAR* 随着阈值 *T* 的变小而快速降低。例如，当 *T*=21 时，同一/不同用户情况下，其 *FAR* 接近于 0 或等于 0。这表明当阈值 *T* 小于 21 时，*FAR* 基本不受阈值 *T* 的影响。

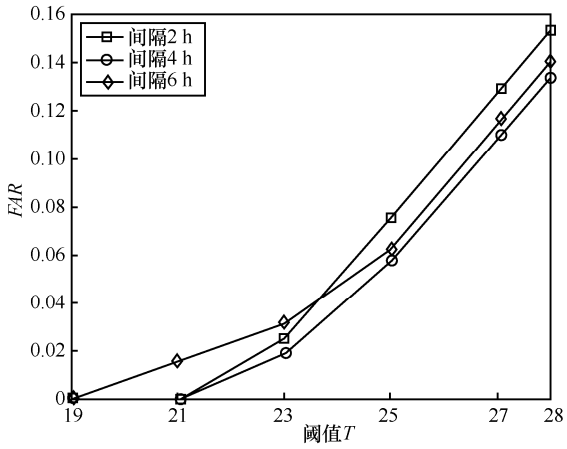


图 12　同一用户异步 IPI 情形中不同阈值 *T* 下的认假率

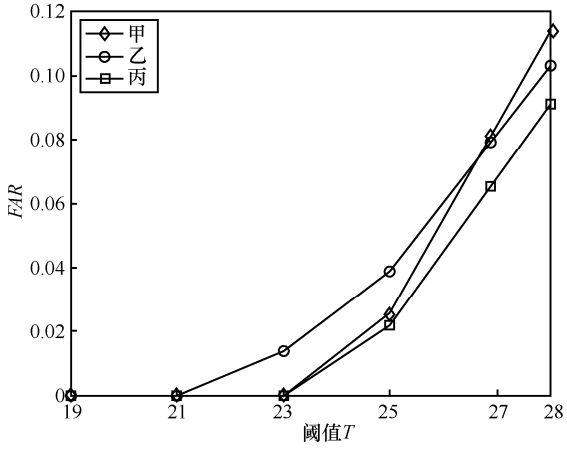


图 13　不同用户异步 IPI 情形中不同阈值 *T* 下的认假率

当阈值 *T*=28 时，拒真率 *FRR* 最小，认假率 *FAR* 最大，当阈值 *T*=19 时，拒真率 *FRR* 最大，认假率 *FAR* 最小。*T* 正比于 *FAR*，反比于 *FRR*。为均衡 *FRR* 和 *FAR*，可取 *T*=21，此时拒真率为 25.4%，平均 *FAR* 为 0.25%，总误差近似为 25.65%，详细实验结果如表 2 所示。

为降低 *FAR*，可以直接减小阈值 *T*。然而根据上述实验结果，*T* 减小，*FAR* 减小的同时 *FRR* 升高。

如何减小 *FAR* 的同时降低 *FRR* 是需要进一步考虑的问题。事实上，IPI 不可避免地含有噪声，含噪 IPI 二进制编码序列对 *FRR* 影响较大。为降低 *FRR*，一方面需适当地对编码前 IPI 降噪，另一方面可通过多个脉搏传感器在一次心博周期中的脉搏间隔均值计算 IPI。

表 2　　实验结果

T	*FRR*	*FAR* (同一用户)	*FAR*(不同用户)
28	12.8%	14.2%	10.2%
25	19.8%	6.4%	2.8%
23	23.8%	2.5%	0.4%
21	25.4%	0.5%	0
19	25.4%	0	0

4.3　安全性分析

本文设定阈值 T=21，脉搏间隔生成激励 *cha*、*cha*’和输出结果 *res*、*res*’码长为 64。现对 TFAP 安全性进行分析，主要包括建模攻击，妥协攻击，假冒攻击和重放攻击。

建模攻击是基于延迟 PUF 面临的一种主要威胁。可利用散列函数[27]、轻量级加密[28]和多 PUF 异或[7]的方式来克服此攻击。给定一个含 n 个延迟单元的 PUF，建立一个误判率为 ε 的 PUF 模型，CRP 的最小数量 Num_{m} 必须满足[23]

$$Num_{\mathrm{m}}=O\left(\frac{n}{\varepsilon}\right) \tag{4}$$

其中，n 为 PUF 电路中延迟单元个数，ε 为误判率。

为增加建模复杂度，本文采用 4-异或 PUF，同时引入了用户生物特征 IPI 来阻止建模攻击。一方面，4-异或 PUF 模型所需 CRP 数量远大于单一 PUF 模型所需 Num_{m}[23] 。另一方面，采取 *puf*(*cha*)与 *cha* 异或操作，使协议传输值 *res* 仅暴露最少有用信息。敌手需要面临 2^n 次判断才能获取到“原始”响应值，即敌手需要进行 2^n Num_{m} 轮认证才能获取到 PUF 建模所需最小数量的 CRP，其最小数量必须满足达到

$$O(2^n Num_{\mathrm{m}}) \tag{5}$$

式(5)为 2^n 指数增长。

妥协攻击利用体域网中妥协节点向数据中心发送错误信息，将危及用户安全[29]。在 TFAP 中，采取双因子进行认证，认证节点必须基于 PUF 和实时 IPI 才能认证成功。假设体域网中某节点对敌手妥协，如某个丢失传感器被敌手获得，然而敌手发起的认证将会失败，因为妥协节点不能获取实时 IPI。

假冒攻击利用体域网外部节点假冒正常节点，从而窃取用户生物特征，欺骗数据中心。一个非法节点潜入用户体域网并假冒成一个合法节点，在这种情况下，非法节点只能提供实时 IPI，而不能提供有效的设备物理特征，最终认证失败。

重放攻击利用一个有效数据重复传输以欺骗系统[30]。利用重复信息，敌手试图非法进入应用系统。在 TFAP 中，IPI 为实时数据，不同时刻的数据都不相同，历史或将来数据不同于实时数据。同时，IPI 二进制编码序列 *cha* 和 *cha*’间细小的差异将导致输出结果 *res* 和 *res*’间巨大的变化，二进制序列间汉明距离与输出结果转换概率之间的关系如图 14 所示。例如，输入二进制序列间 1 位的差异可能带来输出结果 50%位数据的变化。因此，利用重复信息认证失败。

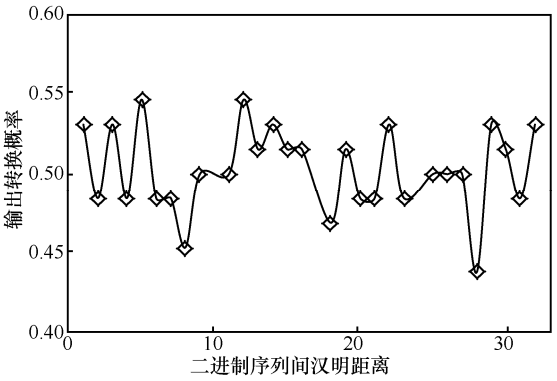


图 14　二进制序列 *cha* 和 *cha*’间不同汉明距离下的输出转换概率

表 3 列出本文提出协议 TFAP 与其他几种典型认证协议之间的安全性比较。其中，T 表示能抵抗此攻击，F 表示不能抵抗此攻击，×表示协议没有此攻击。

表 3　　安全性比较

安全性比较	文献[5]	文献[7]	文献[13]	文献[15]	TFAP
建模攻击	×	T	T	×	T
妥协攻击	T	F	F	T	T
假冒攻击	F	T	T	F	T
重放攻击	T	T	T	T	T

4.4　实现分析

TFAP 采用多 PUF 并联和多 IPI 编码的方式实现。与基于 PUF[7,13]或 IPI[5,15]的认证协议相比，借助体域网自身脉搏传感器，TFAP 在实现上无需随

机数发生器模块，只需将传感器自身 IPI 通过二进制编码器模块(binary encoder)转换为对应格雷码。注意，binary encoder 包含 2 个子模块，ASCII encoder 和 Gray encoder。ASCII encoder 将 IPI 转换为自然二进制，可通过基本的与非门实现，Gray encoder 将二进制转换为对应格雷码，可采用基本的异或门实现。总体上来说，TFAP 比上述 2 类认证协议多了一个 Gray encoder 模块，主要是为了利用格雷码的可靠性，使编码错误最小化。认证协议相关实现模块如表 4 所示。

表 4 实现模块

协议	脉搏传感器	ASCII encoder	Gray encoder	PUF 电路/模型	随机数发生器
文献[7,13]	×	√	×	√	√
文献[5,15]	√	√	×	×	×
TFAP	√	√	√	√	×

若 IPI 数据已经缓存，在运算时间上，TFAP 主要包含 2 个部分。一部分是 binary encoder 模块消耗时间 $time_b$，为 11 个 IPI 数据编码成一个 64 位激励 *cha* 消耗时间。此模块通过 Java 编程实现，$time_b$=112 ms，通过硬件实现可优化其运算速度。另一部分是 PUF 电路消耗时间 $time_p$，主要为 64 个脉冲信号通过 PUF 电路的时间。实验中，晶振为 25 MHz，为了更好采集脉冲信号，经过倍频，使时钟周期为 1 ms，则 $time_p$=64×1ms=64 ms，协议总运算时间约为 176 ms。

5 结束语

针对移动医疗中可穿戴设备，本文提出一种基于 PUF 和 IPI 的双因子认证协议 TFAP。与其他基于 PUF 或 IPI 的认证协议相比，TFAP 具有较高安全性。在 Altera 公司 FPGA 开发板上，通过 3 组不同数据，验证了所提协议的实用性和有效性。

今后在这个研究领域的工作，可以进一步优化 IPI 编码噪声带来的差异；同时也可以改进 D-触发器亚稳态导致的不可预测性。

参考文献：

[1] METIN A. Wiley encyclopedia of biomedical engineering, 6-volume set[M]. United States: John Wiley and Sons, Inc press, 2006.

[2] ALAA A, AMR M, TAREK E. Energy-cost distortion optimization for delay-sensitive m-health applications[C]// Wireless Telecommunications Symposium(WTS). 2015:1-5.

[3] SAXENA D, RAYCHOUDHURY V, NALLURI S. Smarthealth-NDNoT: named data network of things for healthcare services[C]// Proc 2015 Workshop on Pervasive Wireless Healthcare Mobilehealth. 2015:45-50.

[4] FRANCIS T, MADIAJAGAN M, KUMAR V. Privacy issues and techniques in e-health systems[C]//2015 ACM SIGMIS Conference on Computers and People Research. 2015: 113-115.

[5] POON C C Y, ZHANG Y T, BAO S D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health[J]. IEEE Communications Magazine, 2006, 44(4): 73-81.

[6] KONG J, KOUSHANFAR F, PENDYALA P, et al. PUFatt: embedded platform attestation based on novel processor-based PUFs[C]//51st Annual Design Automation Conference. 2014:1-6.

[7] MAJZOOBI M, ROSTAMI M, KOUSHANFAR F, et al. Slender PUF protocol: a lightweight, robust, and secure authentication by substring matching[C]//2012 IEEE Symposium on Security and Privacy Workshops. 2012: 33-44.

[8] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030.

[9] SUH G E, DEVADAS S. Physical unclonable functions for device authentication and secret key generation[C]//44th Annual Design Automation Conference. 2007: 9-14.

[10] BASSIL R, EL-BEAINO W, KAYSSI A, et al. A PUF-based ultra-lightweight mutual authentication RFID protocol[C]//Internet Technology and Secured Transactions. 2011: 495-499.

[11] JIN Y M, XIN W, SUN H P, et al. PUF-based RFID authentication protocol against secret key leakage[C]//14th Asia-Pacific Web Conference. 2012: 318-329.

[12] AKGÜN M, CAGLAYAN M U. Providing destructive privacy and scalability in RFID systems using PUFs[J]. Ad Hoc Networks, 2015, 32: 32-42.

[13] ROSTAMI M, MAJZOOBI M, KOUSHANFAR F, et al. Robust and reverse engineering resilient PUF authentication and key exchange by substring matching[J]. IEEE Transactions on Emerging Topics in Computing, 2014, 2(1): 37-49.

[14] DELVAUX J, PEETERS R, GU D, et al. A survey on lightweight entity authentication with strong PUFs[J]. ACM Computing Surveys, 2015, 48(2): 1-42.

[15] BAO S D, ZHANG Y T, SHEN L F. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems[C]//27th Annual International Conference of the Engineering in Medicine and Biology Society (EMBS). 2005: 2455-2458.

[16] ZHENG G L, FANG G F, SHANKARAN R, et al. An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices[C]//2014 International Symposium on Wireless Personal Multimedia Communications(WPMC). 2014: 624-628.

[17] ZHENG G L, FANG G F, SHANKARAN R, et al. A non-key based security scheme supporting emergency treatment of wireless implants[C]//2014 IEEE International Conference on Communications(ICC). 2014: 647-652.

[18] ZHANG G H, POON C C, ZHANG Y T. A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health[C]//Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS). 2010: 2034-2036.

[19] ZHANG G H, POON C C, ZHANG Y T. Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for

securing wireless body sensor networks[J]. IEEE Transactions on Information Technology in Biomedicine, 2012, 16(1): 176-182.

[20] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. EKG- based key agreement in body sensor networks[C]// IEEE INFOCOM Workshops. 2008:1-6.

[21] TEHRANIPOOR M, WANG C. Introduction to hardware security and trust[M]. New York: Springer press, 2012.

[22] LIM D, LEE J W, GASSEND B, et al. Extracting secret keys from integrated circuits[J]. IEEE Transactions on Very Large Scale Intergration (VLSI) Systems, 2005, 13(10): 1200-1205.

[23] RÜHRMAIR U, SEHNKE F, SÖLTER J, et al. Modeling attacks on physical unclonable functions[C]//17th ACM Conference on Computer and Communications Security(CCS). 2010: 237-249.

[24] BHARGAVA M, MAI K. An efficient reliable PUF-based cryptographic key generator in 65nm CMOS[C]//Design, Automation and Test in Europe Conference and Exhibition(DATE). 2014: 1-6.

[25] CAPOVILLA J, CORTES M, ARAUJO G. Improving the statistical variability of delay-based physical unclonable functions[C]//28th Symposium on Integrated Circuits and Systems Design(SBCCI). 2015:1-7.

[26] DELVAUX J, VERBAUWHEDE I. Fault injection modeling attacks on 65 nm arbiter and RO sum PUFs via environmental changes[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2014, 61(6): 1701-1713.

[27] CHE W J, SAQIB F, PLUSQUELLIC J. PUF-based authentication[C]//2015 IEEE/ACM International Conference on Computer-Aided Design(ICCAD). 2015: 337-344.

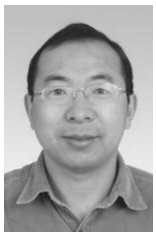
[28] CHERIF Z, DANGER J L, LOZAC H F, et al. Evaluation of delay PUFs on CMOS 65 nm technology: ASIC vs FPGA[C]//2nd International Workshop on Hardware and Architectural Support for Security and Privacy(HASP). 2013:1-8.

[29] DAS M L. Two-factor user authentication in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1086-1090.

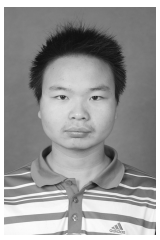
[30] SHELTON J, JENKINS J, ROY K, et al. Genetic based local ternary pattern feature extraction for mitigating replay attacks[C]// SoutheastCon 2016. 2016: 1-2.

作者简介：

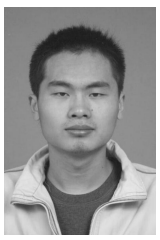
王俊（1983-），男，湖北潜江人，武汉大学博士生，主要研究方向为信息安全、隐私保护等。



刘树波（1970-），男，蒙古族，黑龙江齐齐哈尔人，博士，武汉大学教授、博士生导师，主要研究方向为信息安全、隐私保护、嵌入式系统等。



梁才（1993-），男，湖北仙桃人，武汉大学硕士生，主要研究方向为隐私保护。



李永凯（1988-），男，山东临沂人，武汉大学博士生，主要研究方向为信息安全、隐私保护等。