DOI: 10.13382/j.jemi.B2003215

面向智能家居的生理参数密钥加密方法研究*

陈思伟 高翠云 沈庆伟 唐欢欢
(安徽建筑大学 电子与信息工程学院 电能质量分析及负荷检测技术研究室 合肥 230601)

摘 要:针对健康智能家居系统中数据的隐私与安全性问题、存储和传输效率问题,提出了面向智能家居的生理参数密钥加密方法研究。通过提取脉搏波形数据的主波峰特征和短时傅里叶变换(STFT)频域特征并拼接得到密钥序列,随机性检验表明 2.4 s 原始数据可产生 128 bit 随机性良好的密钥序列,接着将 3 种参数的原始数据分块后先进行数据压缩再利用密钥序列采用 AES 对称加密与 ECC 非对称加密相结合。实验对比了 3 种参数的 CECC、AECC、CAECC 三种加密方法,实验结果表明 CECC 时间和空间开销最大;当参数数据量不大于 64 KB 时,AECC 时间开销约为 CAECC 的 0.8 倍,空间开销约为 CAECC 的 3 倍,AECC 时间开销最小,CAECC 空间开销最小;当数据量大于 64 KB 时,CAECC 时间和空间开销最小。

关键词: 脉搏;多参数;轻量级;密钥序列
中图分类号: TM712;TN98 **文献标识码**: A **国家标准学科分类代码**: 470.40

Research on key encryption method of physiological parameters for smart home

Chen Siwei Gao Cuiyun Shen Qingwei Tang Huanhuan
(Power Quality Analysis and Load Detection Technology Laboratory, School of Electronic and Information Engineering, Anhui Jianzhu University, Hefei 230601, China)

Abstract: Aiming at the issues of data privacy and security, storage and transmission efficiency in the health smart home system, this article proposed a key parameter encryption method for smart home. The key sequence is obtained by extracting the main peak characteristics of the pulse waveform data and the STFT frequency domain characteristics and splicing them together. The randomness test shows that the 2.4 s original data can generate a 128-bit key sequence with good randomness, and then the three parameters of the original data are divided into blocks Compress data first and then use the key sequence to combine AES symmetric encryption and ECC asymmetric encryption. The experiment compares the three encryption methods CECC, AECC and CAECC of the three parameters. The experimental results show that the CECC time and space overhead are the largest; when the parameter data amount is not greater than 64 KB, the AECC time overhead is about 0.8 times CAECC, and the space overhead is about 3 times of CAECC, AECC time overhead is minimum, CAECC space overhead is minimum; when the data volume is greater than 64 KB, CAECC time and space overhead is minimum.

Keywords: pulse; multi-parameter; lightweight; key sequence

0 引 言

智能家居中的传感、网络、服务、云和接口的五层架构[1-2]与物联网解决方案中的射频识别、无线传感器网络、中间件、云计算和应用开发软件五项技术[3]紧密相连。所有的家庭设备都配备了无线通信接口,构成了家庭的无线传感器网络(WSN)。每个家庭都有一个 WSN,来自每个设备的感知数据被转发到一个家庭集线器。所有家庭集线器的数据都在云中积累,云负责管理和共享

收稿日期:2020-06-05 Received Date: 2020-06-05
*基金项目:2019 年安徽省高校自然科学重大项目(KJ2019ZD56)、2018 年度安徽省自然科学基金面上项目(1808085MF192)、2017 年度安徽省高校学科(专业)拔尖人才学术项目(gxbjZD17)、2017 年度安徽省学术和技术带头人后备人选科研活动经费(2017H114)资助项目

分布式的数据[1,4]。而在数据的收集,存储和使用过程中,很容易导致数据的泄露,因此数据加密至关重要[4],本文重点讨论感知设备中原始数据的加密。

目前智能家居的常用加密算法有对称密钥加密和非对称密钥加密两种。Bhanot 等[5]通过分析十种加密算法发现,ECC 和 Blowfish 这两种加密算法所提供的安全级别和加密速度处于领先地位;Singh 等[6]验证了 ECC 优于 RSA 加密算法。无论是私钥加密还是公钥加密,密钥的大小某种程度上决定了加密算法的强度,某些学者研究利用生理特征来产生密钥。虽然外部生物特征很容易模仿和伪造,但内部生物特征识别的方式更加有效。Sandeep 等[7]利用心率变异性(HRV)进行简单的密钥生成以保证人体传感网络(BSN)的安全,但密钥的传输并没有进行加密;Bai 等[8]采用 BAN 系统的生命体征形成初始密钥,利用 LFSR(线性反馈移位寄存器)电路生成密钥流,4 s 产生 16 bits 密钥,但密钥位数较短;Zhang 等[9]利用 ECG 生成 128 bits 的 IPI 密钥种子,再利用 AES 生成随机性更强的密钥,128 bits 密钥种子需要采集 60 s 的 ECG 信号,AES 虽然提高了密钥安全性,但时间开销太长。

针对上述密钥生成时间,密钥加密,以及健康智能家居系统[10]中生理信号、家电信号数据的隐私性问题,在深入研究人体脉搏信号特征的基础上,提出了面向智能家居的生理参数密钥椭圆曲线加密(ECC)方法研究。首先根据采集的人体脉搏数据利用小波去噪和立方插值法去基线漂移,再利用微分法和短时傅里叶变换(SFFT)提取脉搏数据特征值;将脉搏波形特征拼接得到 NIST 中频率和线性复杂度均大于 0.01 要求的密钥序列;将待加密的明文数据按时间周期分块后利用密钥序列,采用对称加密与非对称加密相结合的方式加密,密钥按照时间周期进行更新,确保了数据的安全性。

1　方　法

本文的压缩方法如图 1 所示。基本步骤如下:1)首先将脉搏波形数据进行小波去噪和立方插值法去基线漂移的预处理,然后利用微分法和短时傅里叶变换计算脉搏波形数据的时域和频域特征值;2)按照“时域—频域”的顺序拼接特征值得到加密的密钥序列;3)将当天采集的生理信号、家电信号、环境参数数据按照时间周期分块,利用密钥序列采用对称加密与非对称加密相结合的方式加密数据,增加数据保密性。

1.1　脉搏特征提取

光电容积脉搏波是反映人体组织血液溶剂变化的一种波动信号[11],正常脉搏波波形如图 2 所示。

人体脉搏波一般被认为有 6 个特征点,如图 2 所示,

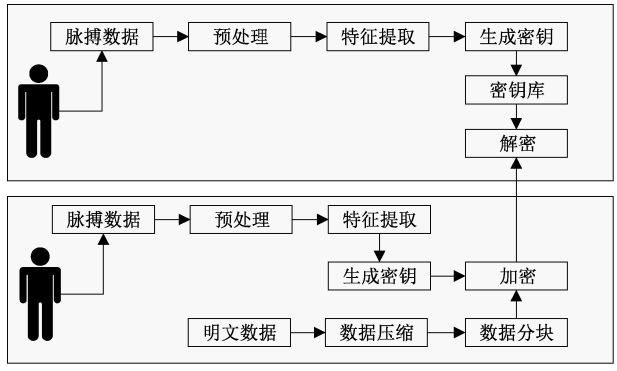


图 1　本文加密方法框图

Fig. 1　Block diagram of encryption method in this paper

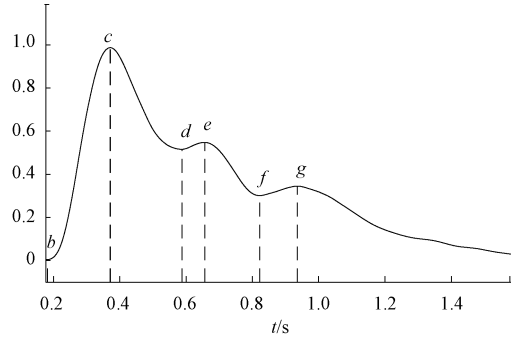


图 2　正常脉搏波波形

Fig. 2　Normal pulse wave waveform

点 *b* 是主动脉瓣开放点,点 *c* 为主波峰、点 *d* 为潮搏波起点、点 *e* 为潮波峰、点 *f* 为重搏波起止点、点 *g* 为重搏波峰。这些特征点分别反映出心血管不同的状态[12]。本文脉搏时域特征提取方法如下。

1)波形去噪,脉搏波形原始数据如图 3(a)所示,根据脉搏信号频率 0~30 Hz,为了更好的保留脉搏波形细节特征,本文频率分辨率为 0.5 Hz,选择 sym8 小波对脉搏波形数据进行 7 层小波分解,各层系数的频带范围如表 1 所示,其中,“*A*”表示低频系数,“*D*”表示高频系数,数字表示第几层。由表 1 可知,大于 30 Hz 的噪声主要分布在第 1~4 层小波细节中,将高频系数 *D*1、*D*2、*D*3、*D*4 置 0,进而小波系数重构得到去噪脉搏波形[13]。

表 1　7 层小波分解的各层系数的频带范围

Table 1　Frequency band of each layer coefficient of 7-layer wavelet decomposition

小波系数	*D*1	*D*2	*D*3	*D*4
频带范围/Hz	128-256	64-128	32-64	16-32
小波系数	*D*5	*D*6	*D*7	*A*7
频带范围/Hz	16-32	8-16	4-8	0-4

2)波形去基线漂移,将去噪的脉搏波数据进行一阶微分,根据峰值点波形陡峭,幅度大的特点,利用区间极

值法寻找峰值点。峰峰值区间为周期/1.5,本文脉搏波采样率为 512 Hz,则极值检测区间为 341 码点值。一阶微分波形极大值的左侧第一个过零点为特征点 b,将特征点 b 作为插值点进行立方插值得到基线曲线,将去噪波形减去基线曲线即得到去极限漂移的波形[14],如图 3(b)所示。

3)特征提取,为了在尽可能短的时间内提取到尽可能多的特征,考虑到文献[8]生成 16 bits 密钥需要采集 4 s 心电信号,文献[9]生成 128 bits 密钥需要采集 60 s 心电信号,另外,人体脉率为 60~100 次/min,选择 2 s 脉搏信号可以满足特征提取需要。因此,本文以 2 s 为时间间隔提取脉搏波特征参数。时域特征为计算 2 s 内所有特征 c 对应的幅值 h_c 和时刻值 t_c,时域特征提取采用微分区间极值法。假设步骤 2)的波形数据为 $x=\{x_1,x_2,\cdots,x_L\}$,L 为 2 s 信号长度,首先根据式(1)计算 x 的一阶微分 u,然后计算 u 的极大值。由于 u 的极大值点过多,本文采用窗宽法来去除无效的极大值点,设置窗宽 W 为周期/1.5,即 $W=341$,比较相邻两个极大值点的间距是否大于 W,若大于则保留两个极大值,否则去掉后一个极大值点。再检测极大值左侧第 1 个过零点即为时域特征 $S=\{(h_{c1},t_{c1}),(h_{c2},t_{c2}),\cdots,(h_{cg},t_{cg})\}$,g 为每 2 s 内的时域特征值个数。

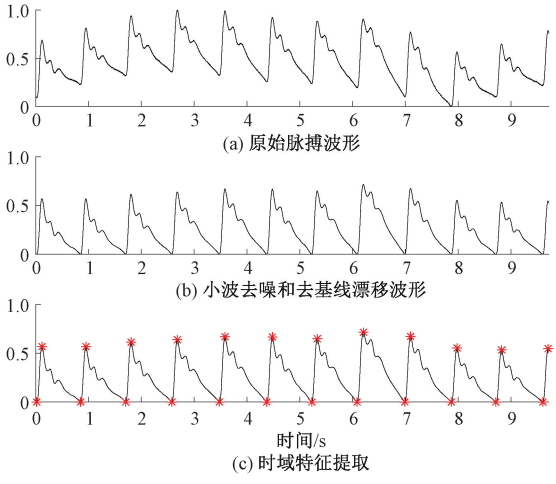


图 3　脉搏波形处理示意图

Fig. 3　Schematic diagram of pulse waveform processing

频域特征为计算 2 s 内脉搏波形的短时傅里叶变换系数的模值[15]。令 2 s 内脉搏波数据长度为 L,利用快速傅里叶变换(FFT)计算长度为 L 的脉搏波数据的频谱,得到频谱系数 $\{(a_1+ib_1),(a_2+ib_2),\cdots,(a_L+ib_L)\}$,然后根据式(2)得到频域特征值 F 序列,根据脉搏信号频率为 0~30 Hz,频率分辨率为 0.5 Hz,频域特征为 F 的前 60 个数值,即 $F=\{F_1,F_2,\cdots,F_{60}\}$。

$$u(i)=x(i+1)-x(i) \tag{1}$$

$$F_k=\sqrt{a_k^2+b_k^2} \tag{2}$$

式中:数组 u 长度为 $L-1$;$k\in[1,L]$。

1.2　生理参数密钥生成

本文利用脉搏信号的综合特征拼接生成密钥,综合特征可以增加不同个体甚至同一个体在不同时间内的密钥的多样性。本文以 2 s 为时间间隔将时域特征 S 和频域特征 F 的结果均保留 4 位小数并乘以 10 000 倍转为正整数,然后将时域和频域特征顺序拼接得到正整数特征密钥序列$\{S,F\}$,将正整数密钥序列的数值按照每个整数实际占用的字节数转为二进制序列后拼接得到$\{\varepsilon_1,\varepsilon_2,\varepsilon_3,\cdots\}$,最后将二进制序列每 8 个 0、1 串转为 1 byte 无符号整数作为密钥 $M=\{m_1,m_2,m_3,\cdots\}$。

本文利用实际采集 3 min 脉搏数据,以证明密钥的多样性,计算不同时间段内同一个人的脉搏信号时域特征 c(图 4(a)),频域特征 F(图 4(b)),密钥 M 特征(图 4(c)),图 4 横坐标为对应特征实际数值,纵坐标 Num 为特征数值出现的次数。由图 4 可知,时域特征数值集中在 0.4 ~0.5,频域特征数值集中在 0~0.08,而本文的特征序列的取值范围遍布整个横坐标区间,因此避免了同一个人的特征值重复。脉搏信号特征值对于不同个体的密钥多样化也有更好的效果。因为与同一个人相比,不同的个人在特征值的分布上有较大的差异。

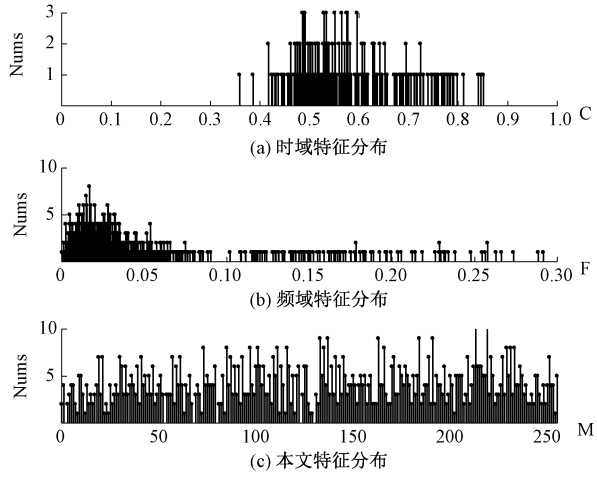


图 4　特征分布直方图

Fig. 4　Histogram of feature distribution

1.3　密钥加密体制

本文采用对称加密与非对称加密相结合的方式保证数据传输的安全性。针对大量的原始数据采用对称加密中的高级加密标准 AES 加密,密钥按照周期进行更新,即使窃取其中一部分数据也无法还原出原始数据。然后利用 ECC 加密 AES 的密钥,最后将 ECC 加密后的密钥和 AES 加密后的原始数据发送给接收方,接收方接收数据后,先 ECC 解密得到 AES 密钥,然后利用 AES 密钥解

密加密数据得到原始数据,加密过程如图5所示。

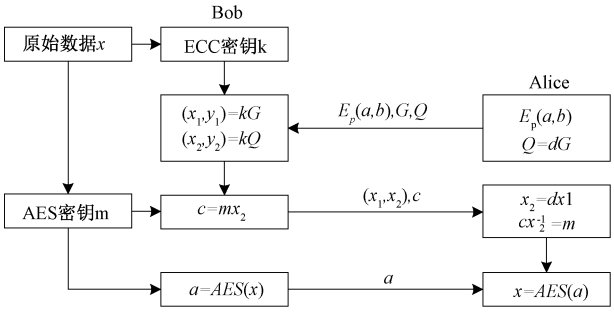


图5　本文加密过程

Fig. 5　The encryption process

参考标准ANSI X9.63-2011(2017),本文采用F_p域ECC,参数六元组$T=(p, a, b, G, n, h)$,由一个指定有限域F的整数p组成,两个元素$a,b\in F$指定由方程定义的椭圆曲线$E(F)$为$y^2=x^3+ax+b(mod\ p)$。一个基点$G=(x, y)$在$E(F)$上,一个质数n是F的阶数,一个整数h是余因子$h=\#E(F)/n$。F_p域的P取值为$[\log_2 p]=\{192, 224, 256, 384, 521\}$,椭圆曲线加密过程如下。

1)首先选取基域F_p,椭圆曲线E,在E上选择阶为素数n的点$P(x_p, y_p)$,公开信息为域F_p,曲线参数a和b,点P及其阶n。椭圆曲线密钥系统建立后,每一个使用的人都要下面的计算:在区间$[1, n-1]$里面任意选取一个整数d,计算$Q=dG$。公开密钥点Q,整数d作为使用人的私钥d。

2)当用户Bob要把消息m发送给Alice时,(1)找到A的公开密钥Q;(2)把消息m表示为一个基域F_p里的元素;(3)在区间$[1, n-1]$内随机选择整数k;(4)计算点$(x_1, y_1)=kG$;(5)计算点$(x_2, x_2)=kQ$,若$x_2=0$,则重新选择k;(6)计算$c=mx_2$;(7)传送加密消息(x_1, y_1, c)发送给Alice。

3)当Alice收到Bob的密文(x_1, y_1, c)后,(1)利用密钥d,计算$d(x_1, y_1)=dkG=k(dG)=kQ=(x_2, y_2)$;(2)再计算$cx_2^{-1}=m$,得到消息$m$。

1.4　评价指标

本文采用生理特征参数作为密钥加密数据,因此密钥序列需要选择随机性大的特征参数,密钥随机性越好在一定程度上决定了数据的安全性[16]。为了更好的评估生理特征生成密钥的随机性,本文对生理特征密钥序列进行频率检验、块内最长游程检验以及累加和检验[17],若3种检验结果的P-value值均大于0.01则密钥序列具有随机性,否则没有随机性。其中,频率检验(FT)目的是确定序列中的1和0的数目是否与真正随机序列所期望的数目大致相同,即1到1/2的分数的接近度;块内最长游程检验(BT)是判断待检验序列的最长"1"游程的长度是否同随机序列的相同;累加和检验(ST)目的是判断序列的累加和的偏移是否在0附近。

评估加密算法的可靠性主要是基于数学问题需要克服解密过程的复杂性,而不是对加密过程的复杂性。本文采用的ECC加密算法在不对称密码算法条件下,相同长度的密钥比RSA算法具有更高的安全性[18],如表2所示。通常在二进制域中,非对称密钥空间大小的ECC约为相应对称密钥空间的两倍。因此,本文采用AES与ECC相结合的方式加密,主要评价在智能家居系统中本文加密方式的时间和空间开销。

表2　加密算法比特级安全性比较分析

Table 2　A comparative analysis based on security bit level

AES	ECC	RSA
80	160	1 024
112	224	2 048
128	256	3 072
192	384	7 680
256	512	15 360

2　实验数据及实验方法

本文所采用的家电的电压、电流数据通过通用自动测试系统平台(GPTS)与含有电压、电流传感器的预处理接口板进行采集,指尖脉搏波信号通过合肥华科电子技术研究所的HKG-07B型红外脉搏传感器与GPTS相组合进行采集,该通用自动测试平台荣获2010年度安徽省科技进步二等奖,具有面向低频信号的通用性。根据ISO-IEEE-11073-10406-2012标准,生理信号数据采集的采样率为512 Hz,实验对象为30人,每个人静态测试3 min,采集3次,共90组数据用于本文的生理信号特征提取。

家电数据采集根据GB/Z 17624.2-2013标准对谐波和功率计算的要求,所有家用电器采集电压、电流两种数据,采样率为12 800 Hz,每秒12 800个数据,每个数据需要4 bytes存储;环境参数包括温度、湿度、CO、PM2.5、NO2、SO2等5种参数,根据GA127-1996和GB/T18883-2002标准可知,可燃气体报警响应时间不小于30 s,空气质量检测平均3~15 min采集一次结果,本文3 s采集一次符合要求,然后根据标准规定的参数范围和参数测量精度模拟出环境参数数据,如温度参数采用数显式温度计要求测量范围0 ℃~60 ℃,最小分辨率为0.1,则模拟数据从0开始,步长0.1增长到60,得到600个数据点,其他参数同理可得。每次5种参数需要30 bytes存储;生理参数主要采集脉搏波数据,每个数据需要4 bytes存储。本文按照24 h参照式(6)计算数据量。表3为智能家居中3种数据类型24 h采集统计表。

$$x = \nu \cdot f_s \cdot T \cdot B \tag{6}$$

式中：x 为总的数据量；f_s 为采样率；T 为采样时间；B 表示一个字节大小；ν 表示每次采集数据点需要的字节存储空间。

表 3　每种类型数据存储空间统计表

Table 3　Statistics table for each type of data storage space

数据类型	采样率/Hz	采集时长/h	原始数据 MB
环境参数	1/3	24	1.65
生理参数	512	24	168.75
家用电器	12 800	24	8 437.50

本文数据处理平台配置为 CentOS7 系统，运行内存 8 GB，酷睿 i5 三代 4 核处理器，实验内容具体如下：1）评估生理特征生成密钥序列 FT、BT 以及 ST；2）本文采用 ZLIB 无损压缩[19]，降低加密前数据的空间开销，进而降低加密的时间开销，分别统计如下 3 种组合方法：1）先对原始数据进行压缩，然后利用 ECC 加密压缩后的数据（CECC）；2）先对原始数据进行 AES 加密，然后对 AES 的密钥进行 ECC 加密（AECC）；3）先对原始数据进行数据压缩，然后利用 AES 加密压缩后的数据，最后利用 ECC 加密 AES 的密钥（CAECC）的时间和空间开销。为了更好的评估本文算法的效率，特征提取采用脉搏波数据，需要压缩和加密的数据用采样率高数据量大的家用电器数据，时间开销还包括生理参数特征提取的时间。

3　实验结果及分析

3.1　生理特征密钥序列的频率和线性复杂度测试

本文特征提取为每次计算 2 s 内脉搏波的时域和频域特征，按照“时域—频域”的顺序拼接后进行测试，密钥序列 key = 128 bits。与文献[9]的 IPI 方法进行对比，利用 3 min 脉搏信号生成密钥序列，文献[9]每个人每组数据可以产生 3 个密钥序列，本文方法每个人每组数据可产生 90 个密钥序列，分别取每个实验对象的 NIST 检测均值，且两种方法每个人 3 组数据的结果再取均值，结果如图 6 和 7 所示，图 8 所示为本文方法每个人 90 组密钥的合格率情况。

由图 6 可知，文献[9]生成密钥序列的方法不同个体之间差异性大，其中 BT 检验结果部分个体的 P-value 值为 0，说明该方法对个体依赖性强；由图 7 可知，本文生成密钥序列的方法不同个体间波动相对平缓，三项检验的 P-value 值均大于 0.01，由此可知本文的密钥序列具有随机性，为加密算法提供了研究基础。由图 8 可知 FT 通过率大于 73.33%，BT 通过率大于 90%，ST 通过率大于 78.89%，整体通过率大于 80.74%，平均 2.4 s 即可产生一个具有随机性的 128 bits 随机数，效率优于文献[9]。

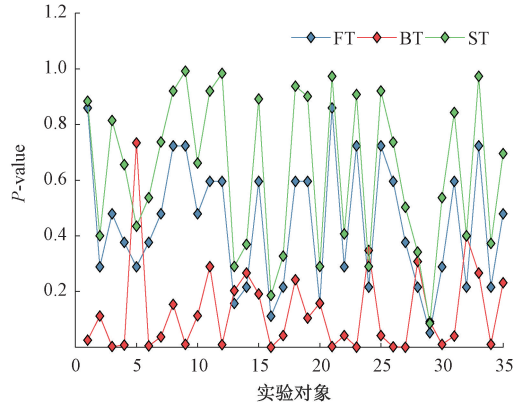


图 6　文献[9]检验结果

Fig. 6　The test results of reference[9]

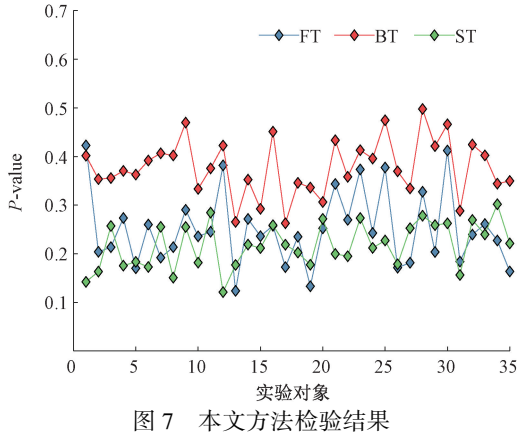


图 7　本文方法检验结果

Fig. 7　The test results of proposed method

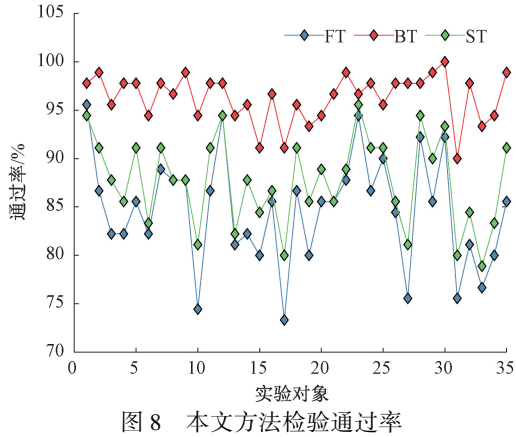


图 8　本文方法检验通过率

Fig. 8　The proportions of proposed method

3.2　CECC、AECC 和 CAECC 的时间和空间开销

根据《密钥建议协议书》NIST SP 800-57 中可比安全性表可知[20]，目前满足安全要求且椭圆曲线有限域 P 最小为 256，因此本文 ECC 取 P = 256，ECC 其他参数按照标准 ANSI X9.63-2011（2017）中 P = 256 的 ECC 参数。AES 密钥位数选择安全性与 ECC-256 相等的 AES-128。根据智能家居系统中对采集数据上传服务器的时

间间隔的不同,本文首先将原始数据分块,分块周期为10、20、30、1、3、5、10、20、30 min,其中生理参数大于3 min的数据利用3 min以内的数据拼接得到。ECC密钥为224 bits,AES密钥为128 bits。加密过程中,用于产生密钥的脉搏波原始数据长度与分块周期对应,ECC和AES密钥各取分块周期内FP和LP值最大的一组作为密钥,ECC密钥和AES密钥按照分块周期一次一密,结果如图9~11所示。

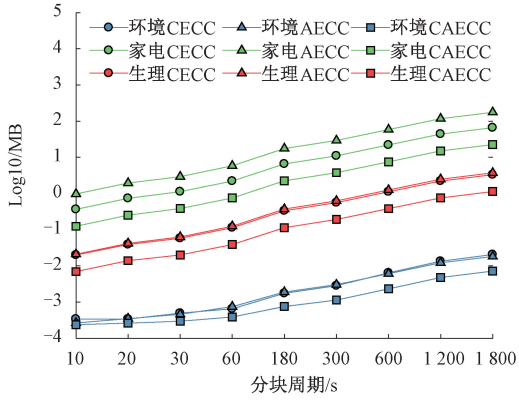


图9　三种参数在三种方法下的空间开销对比

Fig. 9　Comparison of the space cost of the three parameters under the three methods

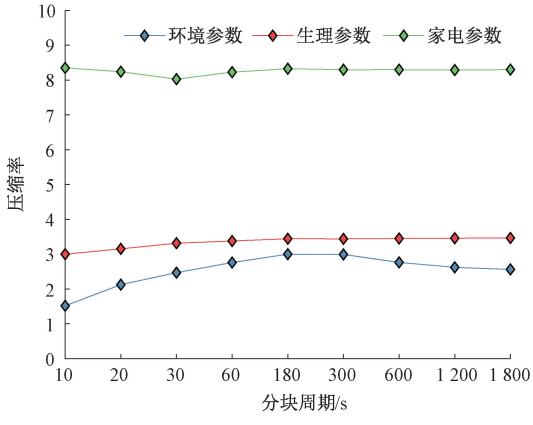


图10　三种参数在三种方法下的压缩率对比

Fig. 10　Comparison of the compression ratios of the three parameters under the three methods

图9为3种参数在3种方法下的空间开销对比图。其中,每个ECC密钥需要28 bytes存储,每个AES密钥需要16 bytes存储,每个AES密钥经ECC加密后需要164 bytes存储;CECC数据量为压缩后的数据和ECC密钥数据;AECC数据量包括AES加密后的数据、AES密钥、ECC密钥、ECC加密AES后的密钥;CAECC的数据量包括了AES加密压缩后的数据、AES密钥、ECC密钥、ECC加密AES密钥的数据。

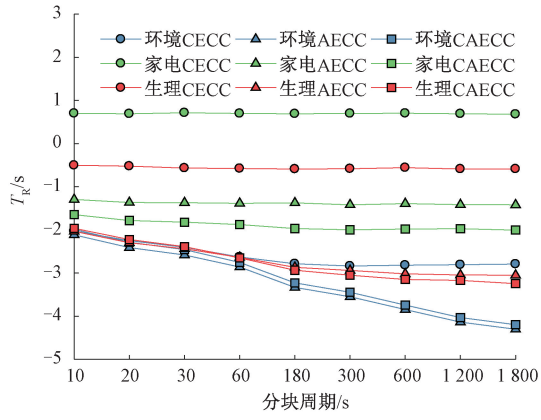


图11　三种参数在三种方法下的时间开销对比

Fig. 11　Comparison of the time cost of the three parameters under the three methods

图10为3种参数的压缩率对比图,压缩率为原始数据与压缩后数据的比值。图11为3种参数在3种方法下的时间开销对比图,纵坐标 T_R 通过将每个时间块的时间开销除以对应的时间周期可得,时间开销包括脉搏波特征提取、随机性测试、数据压缩(C)、AES加密(A)、ECC加密,3种方法的时间开一销所含内容与字母对应。

由图9可知,无论是同种参数的不同加密方法还是不同参数的同一种加密方法,CAECC的空间开销最小,环境参数和生理参数的CECC和AECC空间开销相当,家电参数的CECC空间开销最大,AECC次之。

由图11可知,无论是同种参数的不同加密方法还是不同参数的同一种加密方法,CECC时间开销最大;环境参数作为结果数据,数据量最小,AECC时间开销最小;生理参数以30 s分块周期为界,不大于30 s时AECC时间开销最小,大于30 s时CAECC时间开销最小;家电参数的CAECC时间开销最小。

由图9~11可知,同种参数在3种加密方法下的空间和空间开销随着分块周期的增大而增大;不同参数在同一种加密方法下的时间和空间开销均随着分块周期的增大而增大;数据压缩通过降低空间开销达到了降低时间开销的目的,不同类型的数据压缩率也不相同;当参数数据量不大于64 KB时,AECC的时间开销约为CAECC的0.8倍,空间开销约为CAECC的3倍,考虑时间则选择AECC,考虑空间则选择CAECC;当参数数据量大于64 KB时,CAECC的时间和空间开销最小,优选CAECC作为系统加密算法;而CECC适用于对实时性和空间要求均低的系统。

4　结　论

本文提出的面向智能家居的生理参数密钥加密方法

研究,通过利用微分法和短时傅里叶变换计算脉搏波数据,得到时域和频域特征生成加密的密钥序列,密钥序列的频率检验、块内最长游程检验以及累加和检验的 *P*-value 均大于 0.01,且只需要采集 2 s 的脉搏数据即可生成 128 bits 密钥序列,效率优于同类文献;本文结合对称加密的时间与空间开销小和非对称加密安全性高的优点实现了对健康智能家居系统中的 3 种参数数据的加密,当数据量不大于 64 KB 时,AECC 时间开销最小,CAECC 空间开销最小;当数据量大于 64 KB 时,CAECC 时间和空间开销最优;CECC 适用于时效性要求极低的系统。另外,通过数据压缩降低了数据的空间和时间开销。本文的加密机制具有普遍性,针对不同的健康智能家居系统中对数据处理要求的不同,可以自定义数据分块周期实现系统应用。

参考文献

[1] XU L D, HE W, LI S. Internet of things in industries: A survey[J]. IEEE Transactions on Industrial Informatics, 2014, 10(4):2233-2243.

[2] LEE I, LEE K. The internet of things (IoT): Applications, investments, and challenges for enterprises[J]. Business Horizons, 2015, 58(4):431-440.

[3] STOJKOSKA B L R, TRIVODALIEV K V. A review of internet of things for smart home: Challenges and solutions[J]. Journal of Cleaner Production, 2017, 140: 1454-1464.

[4] POH, GEONG SEN & GOPE, PROSANTA & NING, JIANTING. PrivHome: Privacy-preserving authenticated communication in smart home environment[J]. IEEE Transactions on Dependable and Secure Computing, 2019, PP (99):1-1.

[5] BHANOT, RAJDEEP & HANS, RAHUL. A review and comparative analysis of various encryption algorithms[J]. International Journal of Security and Its Applications, 2015, 9(4): 289-306.

[6] SINGH S R, KHAN A K, SINGH S R. Performance evaluation of RSA and Elliptic Curve Cryptography[C]. International Conference on Contemporary Computing & Informatics. IEEE, 2017.

[7] SANDEEP P, HEYE Z, SUBHAS M, et al. An efficient biometric-based algorithm using heart rate variability for securing body sensor networks[J]. Sensors, 2015, 15(7):15067-15089.

[8] BAI T, LIN J, LI G, et al. A lightweight method of data encryption in BANs using electrocardiogram signal[J]. Future Generation Computer Systems, 2018:S0167739X17310361.

[9] Z. ZHANG, H. WANG, A. V. VASILAKOS, et al. ECG-cryptography and authentication in body area networks[J]. IEEE Transactions on Information Technology in Biomedicine, 2012, 16(6):1070-1078.

[10] 安徽建筑大学. 健康智能家居系统的管理方法:中国, 201510777559. X[P]. 2016-01-27.

[11] HAYDAR A A, COVIC A, COLHOUN H, et al. Coronary artery calcification and aortic pulse wave velocity in chronic kidney disease patients[J]. Kidney International, 2004, 65(5):1790-1794.

[12] 孙薇, 唐宁, 江贵平. 脉搏波信号特征点识别与预处理方法研究[J]. 生物医学工程学杂志, 2015,32(1): 197-201.
SUN W, TANG N, JIANG G P. Study of characteristic point identification and preprocessing method for pulse wave signals[J]. Journal of Biomedical Engineering, 2015, 32 (1): 197-201.

[13] DONOHO D L. De-noising by soft-thresholding[J]. IEEE Transactions on Information Theory, 1995, 41(3): 613-627.

[14] 郭垚垚, 陈兆学. 一种脉搏波和心电信号时域基线漂移消除方法[J]. 中国医学物理学杂志, 2016, 33(2): 65-70.
GUO Y Y, CHEN Z X. A method of eliminating baseline drift of the pulse waves and ECG signals in time domain[J]. Chinese Journal of Medical Physics, 2016, 33 (2): 65-70.

[15] LIU X, JI Z, TANG Y. Recognition of Pulse Wave Feature Points and Non-invasive Blood Pressure Measurement[J]. Journal of Signal Processing Systems, 2017, 87(2):241-248.

[16] DINCA L M, HANCKE G. Behavioral sensor data as randomness source for IoT devices[J]. 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, 2017:2038-2043.

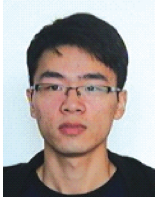
[17] RUKHIN A L, SOTO J, NECHVATAL J R, et al. SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. Applied Physics Letters, 2010, 22(7):1645-179.

[18] DINDAYAL M, DILIP K Y. RSA and ECC: A comparative analysis[J]. International Journal of Applied Engineering Research, 2017, 12(19): 9053-9061.

[19] 陈思伟, 高翠云, 胡翀. 基于相似度分段及重采样的自适应波形数据压缩[J]. 电子测量与仪器学报, 2019,31(4):178-185.
CHEN S W, GAO C Y. Adaptive waveform data compression based on similarity segmentation and Resampling[J]. Journal of Electronic Measurement and Instrumentation, 2019,31(4):178-185.

[20] BARKER E, DAN Q. Recommendation for key management-Part 3: Application-specific key management guidance [EB/OL]. National Institute of Standards and Technology, NIST Special Publication 800-57 Part 3 Revision 1, January 2015.

作者简介



陈思伟,2017年于皖西学院获得学士位,现为安徽建筑大学硕士研究生,主要研究方向为电能质量数据压缩算法研究。
E-mail: 1462202789@qq.com

Chen Siwei received B. Sc. from West Anhui University in 2017. Now he is a M. Sc. candidate in Anhui Jianzhu University. His main research interest includes power quality data compression algorithm.

高翠云,2005年于合肥工业大学获得硕士学位,现为安徽建筑大学教授,主要研究方向为电能质量分析及负荷检测。
E-mail: gaocuiyun@ahjzu.edu.cn

Gao Cuiyun received M. Sc. from Hefei University of Technology in 2005. Now she is a professor of Anhui Jianzhu University. Her main research interests include power quality analysis and load detection.

沈庆伟(通信作者),2013年合肥工业大学获得硕士学位,现为安徽建筑大学教授,主要研究方向网络安全与模式识别。
E-mail: qwshen@ahjzu.edu.cn

Shen Qingwei (Corresponding author) received M. Sc. from Hefei University of Technology in 2013. Now she is a professor of Anhui Jianzhu University. Her main research interests include network safety and pattern recognition.

唐欢欢,2017年于长春理工大学获得学士学位,现为安徽建筑大学硕士研究生,主要研究方向为生理信号的系统设计和算法研究。
E-mail: 2449143591@qq.com

Tang Huanhuan received B. Sc. form Changchun University of Science and Technology in 2017. Now she is a M. Sc. candidate in Anhui Jianzhu University. Her main research interests include system design and algorithm research of physiological signal.