Journal of System Simulation

Volume 28 | Issue 6 Article 23

6-8-2020

# Design of BLE Key Agreement Scheme Based on Hash Chain

Yibo Huang
*PLA Information Engineering University, Zhengzhou 450004, China;*

Yicai Huang
*PLA Information Engineering University, Zhengzhou 450004, China;*

Bin Yu
*PLA Information Engineering University, Zhengzhou 450004, China;*

# Design of BLE Key Agreement Scheme Based on Hash Chain


## Abstract

Abstract: Aiming at the problem that BLE Secure Simple Pairing protocol is vulnerable to eavesdropping and man-in-the-middle attacks, a BLE key agreement scheme based on hash chain was proposed. The scheme *realized mutual authentication and link key agreement applying the unidirectivity and crashworthiness of hash chain. Update mechanism of the hash chain was designed to prevent from reuse of hash chain node values.* The security analysis of BAN logic and experiment results show that, the scheme can effectively resist eavesdropping and man-in-the-middle attacks. Meanwhile, it has low storage and computation overheads.



## Keywords

BLE, hash chain, key agreement, eavesdropping attack, man-in-the-middle attack

## Recommended Citation

Huang Yibo, Huang Yicai, Yu Bin. Design of BLE Key Agreement Scheme Based on Hash Chain[J]. Journal of System Simulation, 2016, 28(6): 1412-1419.

第 28 卷第 6 期 系统仿真学报© Vol. 28 No. 6
2016 年 6 月 Journal of System Simulation Jun., 2016

# 基于哈希链的 BLE 密钥协商方案设计

黄艺波，黄一才，郁滨
(解放军信息工程大学，河南 郑州 450004)

**摘要：**针对低功耗蓝牙安全简单配对协议易受到窃听攻击和中间人攻击的问题，将哈希链引入低功耗蓝牙配对过程，提出了一种基于哈希链的低功耗蓝牙密钥协商方案。该方案利用哈希链的单向性和抗碰撞性实现了设备间的双向认证及链路密钥协商，同时设计哈希链更新机制，防止哈希链节点值的重复使用所带来的安全威胁。BAN 逻辑安全性分析和实验结果表明，方案具有较好的安全特性，能够有效抵御窃听、中间人等攻击，同时具有较小的存储和计算开销。

**关键词：**低功耗蓝牙；哈希链；密钥协商；窃听攻击；中间人攻击
中图分类号：TP309.1 文献标识码：A 文章编号：1004-731X (2016) 06-1412-08

## Design of BLE Key Agreement Scheme Based on Hash Chain

*Huang Yibo*, *Huang Yicai*, *Yu Bin*
(PLA Information Engineering University, Zhengzhou 450004, China)

**Abstract:** Aiming at the problem that BLE Secure Simple Pairing protocol is vulnerable to eavesdropping and man-in-the-middle attacks, a BLE key agreement scheme based on hash chain was proposed. The scheme *realized mutual authentication and link key agreement applying the unidirectivity and crashworthiness of hash chain. Update mechanism of the hash chain was designed to prevent from reuse of hash chain node values.* The security analysis of BAN logic and experiment results show that, the scheme can effectively resist eavesdropping and man-in-the-middle attacks. Meanwhile, it has low storage and computation overheads.

**Keywords:** BLE; hash chain; key agreement; eavesdropping attack; man-in-the-middle attack

## 引言

低功耗蓝牙(Bluetooth Low Energy，BLE)由蓝牙技术联盟 SIG 于 2010 年发布，是一种主要面向嵌入式低功耗传感器类应用的短距离无线通信标准[1-2]。BLE 降低了数据传输速率和协议安全等级以减少功耗，极大地推动了可穿戴设备市场的发展，预计 2015 年搭载 BLE 芯片的可穿戴设备及周边产品出货量将达到 4 570 万[3]。

蓝牙规范设计了安全简单配对协议(SSP)来完成安全的密钥协商，其中 ECDH 公钥交换用于抵御窃听攻击，关联模型用于防止中间人攻击。而 BLE 规范 SSP 协议中没有使用公钥交换，因此不能抵御窃听攻击[4]。针对关联模型(恰好工作、带外、口令输入等)的安全性，众多学者进行了较为深入的研究与分析。Iman 等[5]指出恰好工作是安全等级最低的配对方式，容易受到中间人攻击，应尽量避免使用该模型；Haataja 等[6]认为带外模式利用带外信道传输认证关键信息，传输时要保证带外信道处于安全环境中，实现难度较大。Lindell 等[7]提出了一种针对口令输入模式的中间人攻击方案，

收稿日期：2015-05-02 修回日期：2015-07-21;
作者简介：黄艺波(1990-)，男，河南洛阳，硕士生，研究方向为蓝牙、信息安全技术；黄一才(1985-)，男，土家，湖北巴东，硕士，讲师，研究方向为蓝牙、信息安全技术等；郁滨(1964-)，男，河南郑州，博士，教授，博导，研究方向为信息安全、无线网络安全技术、视觉密码等。



 

指出能够运用 DHkey 加密认证过程来增强该关联模型的安全性。Suomalainen 等[8]的研究表明攻击者可以通过篡改配对信息，强迫设备选择使用安全等级较低的关联模型，从而对其实施中间人攻击。因此，由于 SSP 协议中关联模型自身安全性不足，且多种模式共存，使攻击者可以针对关联模型的选择过程进行攻击，威胁 BLE 配对过程的安全性。

李等[9]结合 ECC 和连锁协议设计了一种蓝牙密钥协商方案，有效地防止了中间人攻击并提供了密钥完整性认证，然而此方案针对经典蓝牙协议，其与 BLE 协议层次有明显区别，不适用于低功耗蓝牙。Diallo 等[10]提出的认证模型实现了认证服务器对从设备的认证，然而当 2 个从设备需要进行通信时，必须以认证服务器为中继，系统实现较为复杂、灵活性不佳。

施等[11]提出了一种基于单向哈希链的网络密钥协商协议，该协议利用哈希函数的单向性进行双向身份认证，通过双方各自产生随机数，并利用随机数产生加密密钥。此方案较好地完成了设备的双向认证及密钥协商，但仍存在交互过程复杂、缺乏哈希链更新机制等问题，不适用于低功耗蓝牙的安全认证及链路密钥协商。

综上所述，本文利用哈希函数的单向性，结合低功耗蓝牙数据传输速率小、功耗要求高的特点，提出一种基于哈希链的 BLE 密钥协商方案，设计蓝牙设备双向认证流程及链路密钥生成算法，保证 BLE 设备配对过程的安全，同时降低方案开销，以较小的功耗抵御窃听和中间人等攻击。

# 1 方案设计

由于 BLE 设备计算能力有限，对功耗要求高，故安全协议设计必须考虑交互过程的复杂度、计算开销等问题。基于哈希链的 BLE 密钥协商方案精简交互过程，以减小系统开销，提高方案效率，同时加入哈希链更新机制，对哈希链当前轮次进行判断，及时更新秘密种子，防止因哈希链重复使用而使系统受到已知明文攻击，保证配对过程的安全。

为方便描述，方案所用的符号及其含义如表 1 所示。

表 1 符号含义表

| 符号 | 含义 |
|---|---|
| $a_i$ | 低功耗蓝牙设备 |
| $i,j$ | 设备 $i$ 的秘密种子 |
| $T$ | 设备 $i$ 的标识 |
| $B$ | 用密钥 $R$ 加密信息 $m$ |
| $t_{threshold}$ | 单向哈希函数 |
| $t_{\max}$ | 设备 $i$ 的第 $N$ 轮次单向哈希链值 |
| $t_{\min}$ | 设备 $i$ 生成的随机数 |
| $\Delta t$ | 设备 $i$ 的椭圆曲线域参数 |
| $PK_i$ $SK_i$ | 设备 $i$ 的公、私密钥对 |
| $K_{ij}$ | 设备 $i$ 和设备 $j$ 之间的共享密钥 |
| $D_R(M)$ | 用密钥 $R$ 解密信息 $M$ |
| $N$ | 当前哈希链轮次 |
| $MAC_i$ | 设备 $i$ 的验证关键信息 |
| $\|\|$ | 连接操作符号 |

## 1.1 参数配置

BLE 设备双方 $A$，$B$ 各自选择安全的椭圆曲线域参数 $e_i$，并生成公、私密钥对 $(SK_i, PK_i)$，保存各自的私钥 $SK_i$。设备双方各自选择随机数 $s_i$，生成 $k$ 轮哈希链 $h^k(s_i)$，将各自哈希链的根节点值 $h^k(s_i)$、公钥 $PK_i$ 和蓝牙设备标识 $ID_i$ 发送到对方设备中，完成系统参数配置，此过程在安全环境下进行。具体流程如图 1 所示。

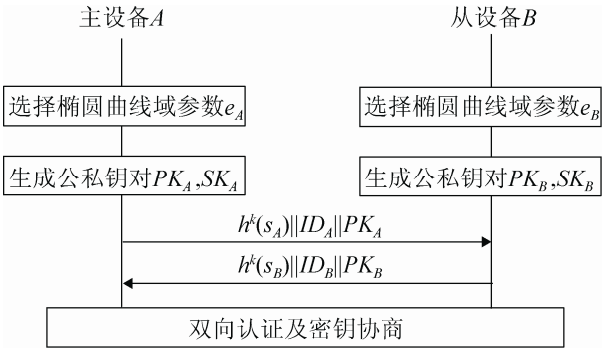


图 1 参数配置流程

## 1.2 双向认证及密钥协商

本文方案在 BLE 设备双向认证的同时，完成密钥协商，具体流程如图 2 所示。



 

第 28 卷第 6 期 系统仿真学报 Vol. 28 No. 6
2016 年 6 月 Journal of System Simulation Jun., 2016

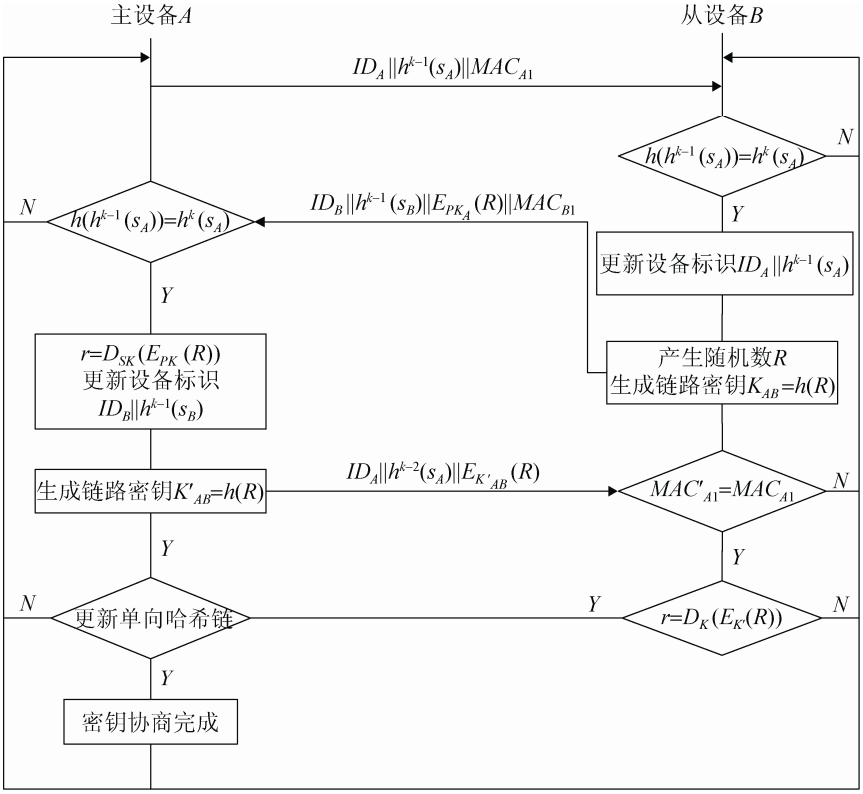


图 2 低功耗蓝牙设备双向认证及密钥协商流程

Step 1：主设备 A 向从设备 B 发起认证请求，请求数据包中包含主设备的蓝牙标识 $ID_A$，$k-1$ 阶哈希链值 $h^{k-1}(s_A)$ 及验证信息 $MAC_{A1}$，其中 $MAC_{A1}=h(ID_A||h^{k-2}(s_A))$。从设备接收到请求信息后，计算 $h(h^{k-1}(s_A))$，验证设备 A 的合法性。如果计算结果与初始化时存储的 $h^k(s_A)$ 相等，则可确认两者为同一条哈希链上的值，从设备 B 通过对 A 的认证，并更新从设备记录中主设备的设备标识为 $\{ID_A||h^{k-1}(s_A)\}$，若不相等，则协议终止。

Step 2：从设备生成随机数 $R$，进而生成链路密钥 $K_{AB}=h(R)$，利用设备 A 的公钥 $PK_A$ 对随机数 $R$ 进行加密，并将 $ID_B||h^{k-1}(s_B)||E_{PK_A}(R)||MAC_{B1}$ 发送给主设备 A。A 判断 $h(h^{k-1}(s_B))$ 与存储的 $h^k(s_B)$ 是否相等，若相等，则更新主设备记录中从设备的设备标识为 $\{ID_B||h^{k-1}(s_B)\}$。主设备 A 使用私钥 $SK_A$ 解密，得到随机数 $R$，并生成链路密钥 $K'_{AB}=h(R)$。若不相等，则协议终止。

Step 3：主设备 A 利用其生成的密钥 $K'_{AB}$ 加密收到的随机数 $E_{K'_{AB}}(r)$，与 $h^{k-2}(s_B)$ 一起发送给从设备 B，B 判断 $h(ID_A||h^{k-2}(s_A))$ 值与先前获得的 $MAC_{A1}$，若不相等，则协议终止；若相等，则从设备使用自身生成的密钥 $K_{AB}$ 解密读取 $r$。若与其产生的 $r$ 相等，则说明主、从设备生成的链路密钥相等，协议执行正常；否则，协议终止。优化后的方案只要求计算一方生成随机数，通过公钥加密并共享该随机数，进而计算出双方的可信链路密钥。

Step 4：链路密钥协商完成后，主设备 A 对当前哈希链轮次进行判断，决定是否更新哈希链。具体过程如图 3 所示。若当前为第 $n$ 次认证，则主设备 A 判断其当前哈希链轮次 $k-2(n-1)$ 是否小于 2(主设备 A 完成一次密钥协商需要使用两轮哈希链)。若当前哈希链节点轮次小于 2，则双方设备更新秘密种子 $r_A$ 为 $s_i||K_{AB}$，形成新的哈希链。到此，密钥协商完成。优化后的方案在当前认证结束后增加对当前使用的哈希链节点轮次的判断，及时更新用于认证的哈希链，避免了哈希链的重复使用。



 

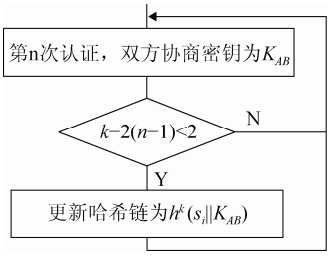


图 3 低功耗蓝牙密钥协商方案哈希链更新流程

## 2 安全性分析

运用 BAN 逻辑方法对本文方案的安全性进行分析。

1、方案初始假设

(1) $B|\equiv \#(R)$：$B$ 相信 $R$ 是新鲜的；

(2) $B|\equiv \xrightarrow{PK} A$：$B$ 相信 $PK_A$ 是 $A$ 的公钥；

(3) $A|\equiv \#(h^{k-1}(s_A))$：$A$ 相信 $A$ 发送的 $h^{k-1}(s_A)$ 是新鲜的；

(4) $B|\equiv \#(h^{k-1}(s_B))$：$B$ 相信 $B$ 发送的 $h^{k-1}(s_B)$ 是新鲜的；

(5) $B|\equiv A\xleftrightarrow{R}B$：$R$ 为 $B$ 生成的随机数，因此可假设 $B$ 相信 $R$ 为 $A$ 和 $B$ 的共享秘密；

(6) $A|\equiv B|\Rightarrow A\xleftrightarrow{R}B$：$A$ 相信 $B$ 对 $R$ 有仲裁权。

2、协议理想化模型

根据 BAN 逻辑对协议的一般分析方法，基于哈希链的低功耗蓝牙密钥协商协议形式化描述如下：

$M1: A\rightarrow B: \{h^k(s_A)\}$：参数配置阶段，系统将 $h^k(s_A)$ 值存储到设备 $B$ 中，可以表示为 $A$ 将 $h^k(s_A)$ 发送给设备 $B$；

$M2: B\rightarrow A: \{h^k(s_B)\}$：参数配置阶段，系统将 $h^k(s_B)$ 值存储到设备 $A$ 中，可以表示为 $B$ 将 $h^k(s_B)$ 发送给设备 $A$；

$M3: A\rightarrow B: \{ID_A, h^{k-1}(s_A), MAC_{A1}\}$：$A$ 将其身份标识 $ID_A$，$k-1$ 阶哈希链值 $h^{k-1}(s_A)$，验证信息 $MAC_{A1}$ 发送给设备 $B$；

$M4: B\rightarrow A: \{ID_B, h^{k-1}(s_B), \{R\}_{PK_A}, MAC_{B1}\}$：$B$ 将其身份标识 $ID_B$，$k-1$ 阶哈希链值 $h^{k-1}(s_B)$，使用 $A$ 的公钥加密的随机数 $R$，验证信息 $MAC_{B1}$ 发送给设备 $A$；

$M5: A\rightarrow B: \{ID_A, h^{k-2}(s_B), \{R\}_K\}$：$A$ 将其身份标识 $ID_A$，$k-2$ 阶哈希链值 $h^{k-2}(s_A)$，使用密钥 $K'_{AB}$ 加密的随机数 $R$ 发送给设备 $B$。

3、协议 BAN 逻辑语言化

基于哈希链的安全密钥协商协议使用 BAN 逻辑语言描述如下：

$M1: B\triangleleft h^k(s_A)$：$B$ 看到过 $h^k(s_A)$，即 $B$ 能读出并重复 $h^k(s_A)$；

$M2: A\triangleleft h^k(s_B)$：$A$ 看到过 $h^k(s_B)$，即 $A$ 能读出并重复 $h^k(s_B)$；

$M3: B\triangleleft h^{k-1}(s_A)$：$B$ 接收到 $A$ 发送的 $k-1$ 阶哈希链值 $h^{k-1}(s_A)$；

$M4: A\triangleleft h^{k-1}(s_B), \{A\xleftrightarrow{R}B\}_{PK_A}$：$A$ 接收到 $B$ 发送的 $k-1$ 阶哈希链值 $h^{k-1}(s_B)$ 和使用 $A$ 的公钥加密的随机数 $R$；

$M5: B\triangleleft h^{k-2}(s_B), \{A\xleftrightarrow{R}B\}_{K'_{AB}}$：$B$ 接收到 $A$ 发送的 $k-2$ 阶哈希链值 $h^{k-2}(s_A)$ 和使用密钥 $K'_{AB}$ 加密的随机数 $R$。

4、安全性证明

基于哈希链的 BLE 密钥协商方案的目的是认证设备双方的身份，并为双方协商链路密钥，本文给出以下证明。

**引理 1**：$A$ 相信 $B$ 发送的 R 是新鲜的，即：$A|\equiv B|\sim \#(R)$。

证明：协议中 $A\triangleleft\{R\}_{SK}$ 同样可表示为 $A\triangleleft R$，由于初始假设中 $B|\equiv\#(R)$，可得 $A\triangleleft\{\#(R)\}_{PK^{-1}}$。

由初始假设 $A|\equiv\xrightarrow{PK}B$ 和公钥规则 $\dfrac{P|\equiv\xrightarrow{K}Q, P\triangleleft\{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$ 得 $\dfrac{A|\equiv\xrightarrow{PK}B, A\triangleleft\{\#(R)\}_{PK^{-1}}}{A|\equiv B|\sim\#(R)}$，从而推出 $A|\equiv B|\sim\#(R)$。

**引理 2**：$B$ 相信 $A$ 接收到了 R 值，即：$B|\equiv A\triangleleft\#(R)$。

证明：由协议可得 $A\triangleleft\{R\}_{PK^{-1}}$，且初始假假定 $A|\equiv\xrightarrow{PK}B$，根据接收规则 $\dfrac{P|\equiv\xrightarrow{K}Q, P\triangleleft\{X\}_{K^{-1}}}{P\triangleleft X}$ 可得 $B|\equiv A\xleftrightarrow{K}B$。

协议BAN语言描述中 $B \lhd R$ 且 $B \mid\equiv \xrightarrow{PK} A$，由公钥规则 $\dfrac{P \mid\equiv \xrightarrow{K} Q, P \lhd \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$ 可得 $\dfrac{B \mid\equiv \xrightarrow{PK} A, B \lhd \{R\}_{PK^{-1}}}{A \mid\equiv B \mid\sim R}$。

又因为 $B \mid\equiv \#(R)$，结合 $A \lhd R$ 和 $\dfrac{B \mid\equiv \xrightarrow{PK} A, B \lhd \{R\}_{PK^{-1}}}{A \mid\equiv B \mid\sim R}$ 可推出 $B \mid\equiv A \lhd \#(R)$。

**定理 1**：$A$ 相信 $B$ 相信 $A$、$B$ 之间的会话密钥是 $K_{AB}$，即：$A \mid\equiv B \mid\equiv A \xleftrightarrow{K_{AB}} B$。

证明：由消息 4 可得到 $A \lhd \{A \xleftrightarrow{K} B\}_{PK}$，设备 $A$ 和 $B$ 使用相同的公、私钥对，所以可得 $A \lhd \{A \xleftrightarrow{K} B\}_{SK}$ 和 $A \lhd A \xleftrightarrow{K} B$。消息 4 可表示为 $A \lhd \{ID_B, h^{k-1}(s_B), A \xleftrightarrow{K} B\}$。

又因为 $A \mid\equiv \xrightarrow{PK} B$，根据公钥推理规则 $\dfrac{P \mid\equiv \xrightarrow{K} Q, P \lhd \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$ 可得 $A \mid\equiv B \mid\sim \{ID_B, h^{k-1}(s_B), A \xleftrightarrow{K} B\}$。

且初始化假设中 $A \mid\equiv \#(h^{k-1}(s_B))$，根据临时值验证规则 $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$ 和新鲜性规则 $\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$ 可得 $A \mid\equiv B \mid\equiv \{ID_B, h^{k-1}(s_B), A \xleftrightarrow{K} B\}$，即 $A \mid\equiv B \mid\equiv A \xleftrightarrow{K} B$。

**定理 2**：$B$ 相信 $A$ 相信 $A$、$B$ 之间的会话密钥是 $K_{AB}$，即：$B \mid\equiv A \mid\equiv A \xleftrightarrow{K_{AB}} B$。

证明：由仲裁规则 $\dfrac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$ 和假设 $A \mid\equiv B \mid\Rightarrow A \xleftrightarrow{K} B$ 可得 $A \mid\equiv A \xleftrightarrow{K} B$。

由消息 5 和共享密钥规则 $\dfrac{P \mid\equiv Q \xleftrightarrow{K} P, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$ 可得 $B \mid\equiv A \mid\sim \{ID_A, h^{k-1}(s_A), A \xleftrightarrow{K} B\}$。

根据 $R$ 可以计算出 $K$，因此 $B \mid\equiv \#(R)$ 可以推出 $B \mid\equiv \#(A \xleftrightarrow{K} B)$。

又根据公钥推理规则 $\dfrac{P \mid\equiv \xrightarrow{K} Q, P \lhd \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$ 得到 $B \mid\equiv A \mid\equiv A \xleftrightarrow{K} B$。

因此，由定理 1 和定理 2 可得，低功耗蓝牙设备 $A$, $B$ 双方成功地共享了加密密钥，实现了安全配对过程，同时分析和证明过程充分说明了该协议是安全的，也是合理的。

## 3 实验及结果分析

针对基于哈希链的 BLE 密钥协商方案，设计并完成实验，记录方案时延，与 SSP 协议的 PE 模型进行比较。同时从存储开销、通信开销和计算开销等方面对本文及文献[9-10]方案进行对比，分析对比结果。

### 3.1 实验方案

为了对方案性能进行实验测试，采用低功耗蓝牙开发平台 Keyfob，配套使用 CSR1010 低功耗蓝牙芯片模块。主机通过 USB 转 SPI 下载线将嵌入密钥协商的固件下载到代表主、从设备的两块 Keyfob 开发板蓝牙芯片中，测试数据由开发板经 USB 转 UART 数据线传送至主机，用于实时显示测试结果。低功耗蓝牙主、从设备开发板之间距离设置为 2 m，实验环境空旷无遮挡，如图 4 所示。

通过截获并分析协商过程的 BLE 数据包来判断协商开始与结束，从而计算得到协商时延。其中无线抓包软件使用 Packet Sniffer，蓝牙 Dongle 使用 CC2540 USB Dongle。在以上环境下，对本文方案独立、反复进行 20 次测试，分析数据包，计算并记录下每次协商所用的时间。并记录 SSP 协议关联模型 PE 运行的时间(不计入口令输入时间)。

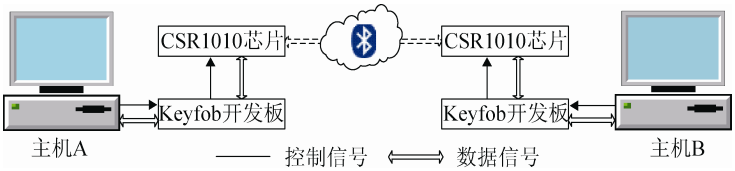


图 4 实验环境

### 3.2 实验结果及分析

得到本文方案与原协议密钥协商时延对比如图 5 所示，横坐标代表实验次数，纵坐标代表方案运行一次所需的时间。

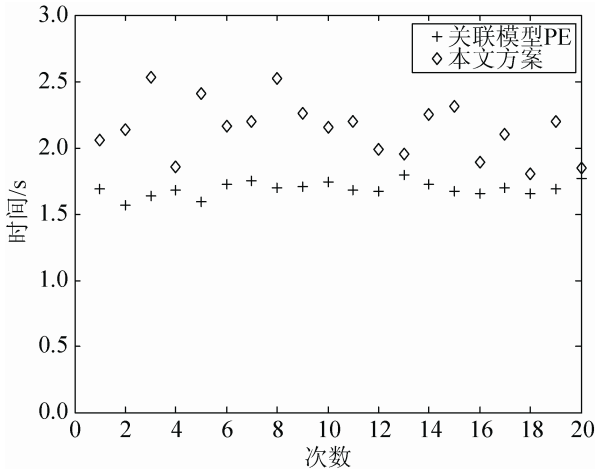


图 5 密钥协商时延对比

方案第 $i$ 次实验测试时延记为 $T_{Hi}$，PE 模型第 $i$ 次实验测试时延记为 $T_{Pi}$。由实验测试可得，基于哈希链的 BLE 密钥协商时延约为 $\frac{1}{20}\sum_{1}^{20}T_{D_{Hi}}=2.1408\ s$，关联模型 PE 的时延约为 $\frac{1}{20}\sum_{1}^{20}T_{D_{Pi}}=1.689\ s$。因此，方案较原协议时延增加较小，仍在用户可接受范围内，适用于对 BLE 设备安全性要求较高的应用场合。

### 3.3 性能分析

为了便于对方案性能进行分析，选定主、从设备 $A$、$B$ 的身份标识 $ID_i$ 的长度 $m$ 为 6 yte，ECC 算法公、私钥长度 $Len(K_{ECC})$ 为 20 Byte，哈希函数采用适合软件实现的 MD5 算法，哈希值长度 $Len(K_{ECC})$ 为 16 Byte。分别使用 $T_{MUL}$，$T_{ASYM}$，$T_{SYM}$，$T_H$ 代表一次模乘运算、非对称加解密运算、对称加密运算和哈希运算的执行时间。

1、存储开销

主设备 $A$ 中需要存储从设备 $B$ 的身份信息标识 $ID_B$、公钥 $PK_B$、$k$ 轮哈希链值 $h^k(s_B)$ 以及自身的身份信息标识 $ID_A$ 和私钥 $SK_A$。从设备 $B$ 需要存储主设备 $A$ 的身份信息标识 $ID_A$、公钥 $PK_A$、哈希链值 $h^k(s_A)$ 及其身份信息标识 $ID_B$ 和私钥 $SK_B$，由此可得主设备 $A$ 和从设备 $B$ 的存储开销均为 $2Len(K_{ECC})+Len(K_{Hash})+2m$ Byte。

2、通信开销

通信开销的衡量可以通过设备发送和接收的报文数量来表示。基于哈希链的密钥协商方案要求主设备 $A$ 发送认证请求数据报文，从设备 $B$ 将加密的随机数发送给主设备 $A$，并接收主设备 $A$ 的确认报文。因此，双方要进行 3 次信息的收发，通信开销均为 3。

3、计算开销

计算开销的衡量可以通过方案中主要运算的执行时间来表示。方案中主设备 $A$ 需要计算认证信息 $MAC_{A1}$，验证 $B$ 的身份，使用私钥解密随机数 $R$，根据随机数计算链路密钥，使用链路密钥加密随机数。因此，主设备 $A$ 需要进行 3 次哈希运算、一次非对称解密运算和一次对称加密运算，计算开销为 $3T_H+T_{ASYM}+T_{SYM}$。从设备 $B$ 需要验证主设备 $A$ 的身份，计算链路密钥，使用公钥加密其生成的随机数 $R$，计算认证信息 $MAC_{B1}$，验证确认信息的可靠性，使用其生成的链路密钥解密随机数。因此，从设备 $B$ 需要进行 4 次哈希运算、一次非对称解密运算和一次对称加密运算，计算开销为 $4T_H+T_{ASYM}+T_{SYM}$。

根据文献[12]可以将对称加密运算、非对称加解密运算和哈希运算的时间开销用模乘运算时间开销来表示，具体如下：$T_{SYM}\approx 2T_{MUL}$；$T_{ASYM}\approx 160T_{MUL}$；$T_H\approx 0.23T_{MUL}$。

针对本文方案，从存储开销、通信开销及计算开销等 3 个方面进行分析对比文献[9]和文献[10]两种蓝牙认证及密钥协商方案，结果如图 6 所示。由上文效率分析可得，本文方案中主、从设备 $A$、$B$ 的存储开销分别为 $2Len(K_{ECC})+Len(K_{Hash})+2m=88$ Byte；通信开销均为 3；主设备 $A$ 的计算开销为



 

$4T_H + T_{ASYM} + T_{SYM} \approx 163T_{MUL}$，从设备 $B$ 的计算开销为 $5T_H + T_{ASYM} + T_{SYM} \approx 163T_{MUL}$。文献[9]中没有指明 ECC 密钥及对称密钥长度，在此假设分别为 20 Byte 和 16 Byte。文献[10]中没有指定从设备的数量 $g$，假设 $g$=1，同时忽略其安全数据库查询所需时间和用户口令输入的时间。

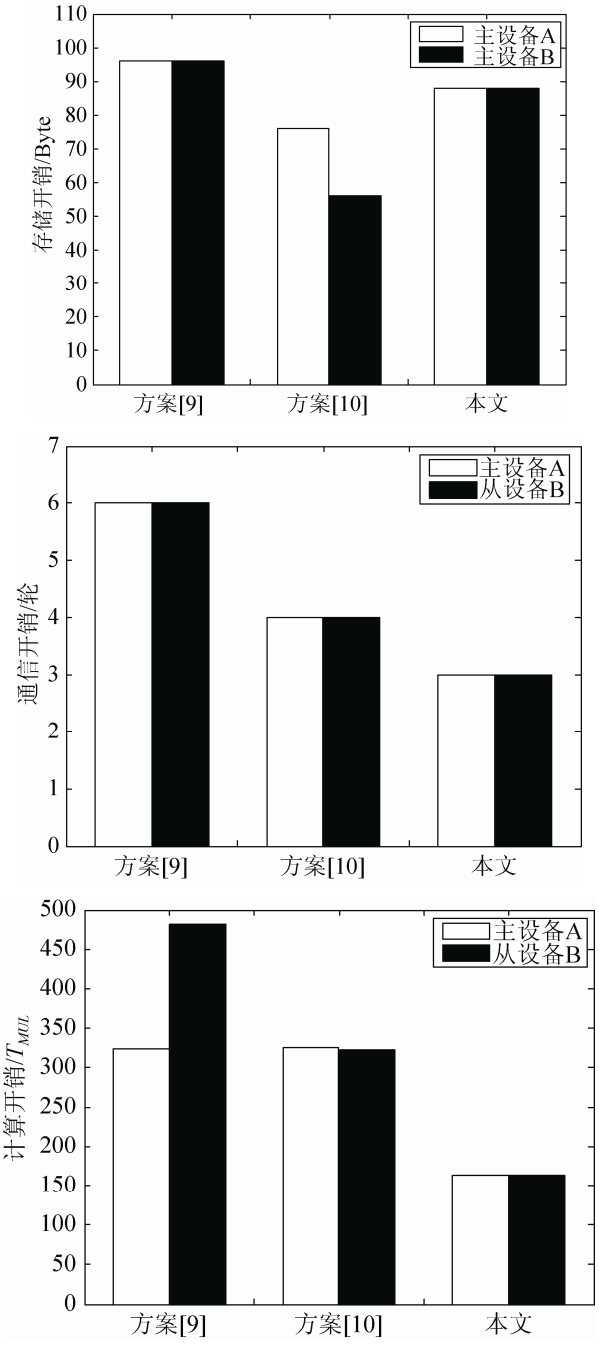


图 6 各方案开销对比

从图 6 可以看出，本文方案所需的计算开销均小于文献[9]和文献[10]，且存储开销小于文献[9]。文献[10]虽然需要的存储开销较小，但其通信开销远大于其他两个方案，且主设备需要维护一个用于从设备存储身份标识和密钥的安全数据库，加大了系统开销和实现难度。本文以较小的开销，实现了低功耗蓝牙设备的安全密钥协商。

## 4 结论

在深入研究 BLE 安全简单配对协议和安全密钥协商机制的基础上，本文提出了一种基于哈希链的 BLE 密钥协商方案。方案利用哈希链的单向性和抗碰撞性等特点，实现了设备的双向认证和链路密钥协商。BAN 逻辑安全性分析表明方案具有较好的安全特性，可有效抵御窃听、中间人等攻击，能够保证低功耗蓝牙安全连接的建立。实验测试结果表明，方案时延在用户可接受范围之内，同时所需的存储和计算开销较小，具有效率高、功耗低的特点，适用于对 BLE 设备功耗及安全性要求较高的场合。

## 参考文献:

[1] 陈灿峰. 低功耗蓝牙技术原理与应用 [M]. 北京: 北京航空航天大学出版社, 2013.

[2] Bluetooth Special Interest Group.Bluetooth SIG Specification of the Bluetooth system: core package version 4.0 [EB/OL]. (2009-07-28) [2015-04-20]. http://www.bluetooth.org. 2009.

[3] 魏德龄. 蓝牙4.2欲让物联网成真, 低功耗成核心优势 [EB/OL]. (2015-01-23) [2015-04-21]. http://www.cctime.com/index.asp. 2015.

[4] Heiner Perrey, Osman Ugus, Dirk Westhoff. Security enhancement for bluetooth low energy with Merkle's puzzle [C]// Proceedings of Mobile Computing and Communications Review. New York: ACM, 2011: 45-46.

[5] Iman Almomani, Mohammed Al-Saruri, Mousa Tawfiq AL-Akhras. Secure public key exchange against man-in-the-middle attack during secure simple pairing (SSP) in Bluetooth4.0 [J]. World Applied Sciences Journal (S1818-4952), 2011, 13(4): 769-780.

（下转第 1444 页）