一种从设备零秘密存储的蓝牙密钥协商方案

李森森 黄一才 郁 滨
(信息工程大学 郑州 450001)

摘 要 针对现有蓝牙配对协议难以抵抗中间人攻击、复制攻击的问题,提出了一种从设备零秘密存储的蓝牙密钥协商方案。该方案利用物理不可克隆函数(Physical Unclonable Functions,PUF),在从设备不存储任何秘密参数的情况下,通过"三次握手"实现主设备与从设备的双向认证及链路密钥协商。理论分析和实验结果表明,该方案不仅具有较高的安全性,而且通信、计算和存储开销均较小。

关键词 蓝牙,PUF,密钥协商,中间人攻击,复制攻击
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.04.024

Bluetooth Key Agreement Scheme with Zero Secret Storage in Slave Device

LI Sen-sen HUANG Yi-cai YU Bin
(Information Engineering University,Zhengzhou 450001,China)

Abstract To solve the problem that the existing bluetooth pairing protocol is difficult to resist the man-in-the-middle attacks and replication attacks,a bluetooth key agreement scheme with zero secret storage in slave device was proposed. By using the Physical Unclonable Functions(PUF),this scheme realized the mutual authentication and link key agreement between the master device and the slave device through "three-time handshake" in the case that the slave device need not store any secret parameters. Theoretical analysis and experimental results show that the proposed scheme not only has high security,but also needs less communication,calculation and storage cost.

Keywords Bluetooth,PUF,Key agreement,Man-in-the-middle attack,Replication attack

1 引言

蓝牙低成本、低复杂度、高可靠性的特点,使其在医疗监护、室内定位、智能家居等领域有广阔的应用前景[1]。随着应用的推广,蓝牙的安全问题也受到国内外学者的广泛关注。

蓝牙规范[2]通过定义安全简单配对(Secure Simple Pair,SSP)协议实现设备间的密钥协商。针对不同的应用需求,SSP协议提供了JW,PE,NC和OOB 4个安全等级的关联模型。文献[3]指出JW模型未提供任何安全机制,不能抵抗中间人攻击;文献[4]提出了一种针对PE模型的攻击方式,并分析了该攻击的实际可行性;文献[5]指出,虽然NC模型和OOB模型具有较高的安全性,但攻击者可以通过篡改IO能力信息迫使蓝牙设备选择安全等级低的关联模型进行配对,从而实施中间人攻击[5]。

针对SSP协议的不足,Perrey等[6]提出一种轻量级方案,利用Merkle谜题实现蓝牙设备间的密钥协商,适用于设备资源受限的应用场景,但该方案耗时较长且只能保证密钥在短期内的安全;黄艺波等[7]利用哈希链的单向性,设计了一种蓝牙双向认证及密钥协商方案,可有效抵抗中间人攻击,但公钥算法的使用增加了方案的计算复杂性。此外,基于传统密码体制的方案需要在设备存储器中保存共享密钥或私钥等秘密参数,文献[8-9]指出该存储方式易遭到复制攻击,攻击者可从存储器中提取秘密信息并复制相似的恶意设备,进而威胁蓝牙通信的安全。

与基于传统密码体制的方案不同,张星昊等[10]利用无线信号强度RSSI实现蓝牙设备间的密钥共享,该方案无需在设备内存储任何密钥参数,可有效抵抗复制攻击,但需要多次发送信道探测序列,且不能实现对设备身份的认证,易受中间人攻击。

PUF[11]是输入挑战与输出响应之间的一种特殊映射关系,该映射建立在设备随机性的物理差异的基础上,其实质反映了设备硬件具有的独特属性,表现为"硬件指纹"。PUF实现简单且具有不可克隆、不可预测等性质[12]。其中,不可克隆性是指对于给定的PUF,无法通过物理或数学方式构造出PUF',使得对任意挑战信号c都有$PUF'(c)=PUF(c)$;不可预测性是指对于给定的PUF和挑战信号c,无法预测其对应的响应信号$PUF(c)$。由PUF的不可克隆性和不可预测性可知,只有拥有该PUF的合法实体才能正确计算出挑战信号

到稿日期:2018-02-17 返修日期:2018-07-13 本文受国防信息保障技术重点实验室开放基金(KJ-15-104)资助。
李森森(1993-),男,硕士,主要研究方向为蓝牙、信息安全,E-mail:lss589@163.com;黄一才(1985-),男,硕士,讲师,主要研究方向为蓝牙、信息安全,E-mail:huangyicai3698@163.com(通信作者);郁 滨(1964-),男,教授,博士生导师,主要研究方向为信息安全、无线通信安全及视觉密码。

c 对应的响应信号 $PUF(c)$。

当前，还未有学者将 PUF 用于蓝牙密钥协商。针对其他应用，文献[11]利用 PUF 的挑战-响应对(Challenge Response Pairs，CRPs)进行设备间的认证和密钥协商，其方案过程简单，但以明文形式传输 CRPs 会造成 PUF 参数泄露，易遭到建模攻击[13]；文献[14]设计的密钥协商方案利用哈希函数隐藏 PUF 的 CRPs，能够抵抗建模攻击，但该方案无法防止服务器发起的身份伪造，即服务器 A 可以伪造成服务器 B 与节点设备通信。

综上所述，本文在蓝牙协议栈的基础上设计安全增强架构，结合蓝牙设备的特点，提出了一种基于 PUF 的蓝牙密钥协商方案，在从设备不存储任何秘密参数的情况下，利用 PUF 的不可克隆性和不可预测性实现主、从设备间的双向认证和链路密钥生成。所提方案能够有效抵抗链路密钥建立过程中存在的安全威胁，同时具有较小的资源开销，满足蓝牙设备的应用需求。

2 系统模型

由一个主设备和多个从设备构成的匹克网是蓝牙通信的基本拓扑。主设备常为用户随身携带的智能设备，具有较高的安全性；从设备则生产成本低、资源受限，容易遭到复制攻击。根据不同设备的特点，提出以下攻击假设。

1)攻击者在蓝牙网络中可以实施窃听、篡改、重放等攻击，也可捕获开放环境中的从设备；

2)若从设备被捕获，攻击者可以获取该设备存储器中的所有信息；

3)主设备拥有可抵抗物理攻击和复制攻击的安全数据库[15]。

本文通过改进蓝牙规范中的密钥建立机制并增加身份认证、入网控制等安全实体，来实现蓝牙设备间安全的密钥协商。在蓝牙协议栈的基础上，设计安全增强架构如图 1 所示。

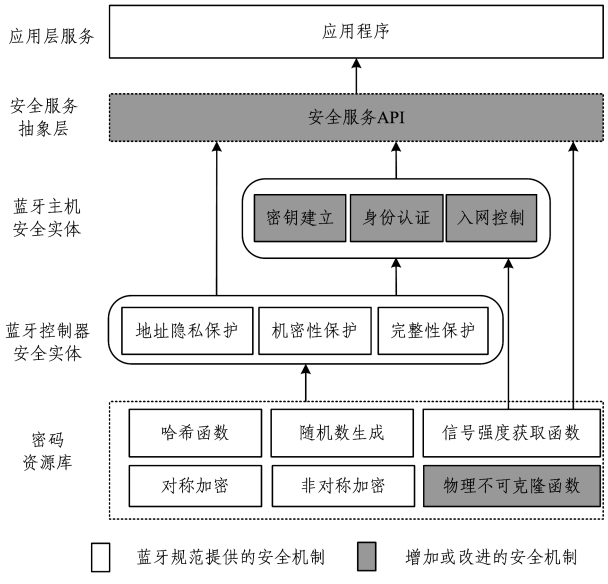

图 1 蓝牙安全增强架构

Fig. 1 Bluetooth security enhancement architecture

其中，密码资源库用于向安全实体提供基本的密码算法，新增的 PUF 利用硬件电路实现；蓝牙控制器安全实体以硬件形式实现，而主机中的安全实体则通过固件代码实现；安全服务抽象层将主机和控制器中的安全实体及部分密码资源以 API 的形式提供给上层应用。

2.1 密钥协商模型

依据安全增强架构，结合蓝牙设备的特点，设计了如图 2 所示的密钥协商模型。在初始化阶段，从设备将其 PUF 参数 P_S 以安全方式发送给主设备，主设备存储 P_S；在密钥协商阶段，主、从设备基于秘密参数 P_S 实现双向认证并产生链路密钥 $Key=F'(nonce_1,nonce_2,P_S)$，同时完成 PUF 参数的更新。其中，$nonce$ 为设备选取的随机值，$F()$ 和 $F'()$ 为哈希函数。

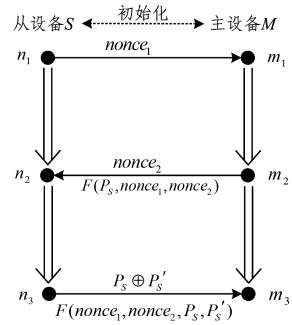

图 2 密钥协商模型

Fig. 2 Key agreement model

2.2 模型安全性证明

串空间[16]是一种基于定理证明的形式化分析方法。首先扩充原有串空间理论的运算符和攻击者串，然后证明密钥协商模型的安全性。

1)串空间理论的扩充

在密钥协商模型中，从设备的 PUF 参数 P_S 可看作双方设备共享的秘密信息，记作 K_{MS}。为便于描述，用 A 表示消息集合，T 表示未经加密或哈希运算的文本项，K 表示密钥集合，K_ρ 表示攻击者已知密钥集合。

定义 1 渗透串空间为(Σ,P)。其中，Σ 由为如下 3 种串组成的串空间；P 为攻击者串集合，满足 $P\in\Sigma$。

①攻击者串 $\rho\in P$。

②发起者串 $t_{init}\in init[nonce_1,nonce_2,K_{MS},K'_{MS}]$，与该串相关联的主体是从设备 S，其迹的形式为：

$\langle +\{nonce_1\},-\{nonce_2,F(K_{MS},nonce_1,nonce_2)\},+\{K_{MS}\oplus K'_{MS},F(nonce_1,nonce_2,K_{MS},K'_{MS})\}\rangle$

③响应者串 $t_{resp}\in resp[nonce_1,nonce_2,K_{MS},K'_{MS}]$，与该串相关联的主体是主设备 M，其迹的形式为：

$\langle -\{nonce_1\},+\{nonce_2,F(K_{MS},nonce_1,nonce_2)\},-\{K_{MS}\oplus K'_{MS},F(nonce_1,nonce_2,K_{MS},K'_{MS})\}\rangle$

在原有串空间理论的基础上，增加哈希、异或运算及相应攻击者串形式，如定义 2 和定义 3 所述。

定义 2 串空间中有如下运算符：①求逆运算 $inv:K\to K$；②哈希运算 $hash:A\times A\to A$；③加密运算 $encr:K\times A\to A$；④连接运算 $join:A\times A\to A$；⑤异或运算 $xor:A\times A\to A$。

定义 3　攻击者串的可能形式包括：①M 串（发送明文消息），$\langle +m\rangle, m\in T$；②C 串（连接消息），$\langle -p,-q,+pq\rangle, p\in A, q\in A$；③S 串（拆分消息），$\langle -pq,+p,+q\rangle, p\in A, q\in A$；④K 串（发送已知密钥），$\langle +k_\rho\rangle, k_\rho\in K_\rho$；⑤E 串（加密），$\langle -k_\rho,-m,+\{m\}_{k_\rho}\rangle, k_\rho\in K_\rho, m\in T$；⑥D 串（解密），$\langle -k_\rho^{-1},-\{m\}_{k_\rho},+m\rangle, k_\rho\in K_\rho, m\in T$；⑦F 串（哈希运算），$\langle -m,-m',+F(m,m')\rangle, m\in A, m'\in A$；⑧X 串（异或运算），其迹为 $\langle -p,-q,+(p\oplus q)\rangle, p\in A, q\in A$。

2）形式化证明

形式化证明的目标包括：主设备认证从设备、从设备认证主设备、链路密钥机密性。

引理 1　$\forall m\in A, k\notin K_\rho$，形如 $F(m,\cdots,k,\cdots)$ 的消息项只起源于合法节点。

证明：采用反证法证明。将形如 $F(m,\cdots,k,\cdots)$ 的消息项记为 $h_{k,m}$，假设 $h_{k,m}$ 起源于攻击者节点 ρ，则 $h_{k,m}\subset term(\rho)$，依次分析攻击者串的可能形式。对于 M 串，其迹 $tr(\rho)$ 具有形式 $\langle +m\rangle, m\in T$，而 $h_{k,m}\notin T$，因此，这种情况不可能。同理可知，C 串、S 串、K 串、E 串、D 串、F 串和 X 串均不满足要求。因此，$h_{k,m}$ 只能起源于合法节点，证毕。

引理 2　$nonce_2$ 唯一起源于节点 m_2。

证明：由 $term(m_2)=+\{nonce_2, F(K_{MS}, nonce_1, nonce_2)\}$ 得，$nonce_2\subset term(m_2)$，因此，要证 $nonce_2$ 唯一起源于节点 m_2，只需证 $nonce_2\not\subset term(m_1)$，这里 m_1 为 m_2 的直接前驱。由于 $term(m_1)=-\{nonce_1\}$，而 $nonce_1\neq nonce_2$，故 $nonce_2\not\subset term(m_1)$。因此，$nonce_2$ 唯一起源于节点 m_2，证毕。

引理 3　$nonce_1$ 唯一起源于节点 n_1。

该引理证明过程与引理 2 相似，不再赘述。

根据串空间理论，主设备认证从设备可转化为证明定理 1 成立，从设备认证主设备可转化为证明定理 2 成立，攻击者无法得到链路密钥 $Key=F'(nonce_1, nonce_2, K_{MS})$ 等价于定理 3。

定理 1　设 C 是串空间 Σ 中的丛，且满足条件：①$nonce_2$ 在 C 中唯一起源；②$nonce_2\neq nonce_1$；③$K_{MS}\notin K_\rho$。若响应者串 $t_{resp}\in resp[nonce_1, nonce_2, K_{MS}, K'_{MS}]$ 且 $C-height(t_{resp})=3$，则 C 中存在发起者串 $t_{init}\in init[nonce_1, nonce_2, K_{MS}, K'_{MS}]$ 且 $C-height(t_{init})=3$。

证明：由引理 2 知，$nonce_2$ 起源于 m_2。设 $t_1=F(nonce_1, nonce_2, K_{MS}, K'_{MS})$，由 $term(m_2)=+\{nonce_2, F(K_{MS}, nonce_1, nonce_2)\}$ 和 $term(m_3)=-\{K_{MS}\oplus K'_{MS}, F(nonce_1, nonce_2, K_{MS}, K'_{MS})\}$ 可得，$t_1\subset term(m_3)$ 且 $t_1\not\subset term(m_2)$。又因为 $nonce_2\subset t_1$ 且 $K_{MS}\notin K_\rho$，所以边 $m_2\Rightarrow^+ m_3$ 是 N_M 的输入认证测试边。由输入认证测试定理可知，丛 C 中存在相应的转换边 $n\Rightarrow^+ n'$，且 n 为正节点，$t_1\subset term(n')$。由引理 1 知，t_1 只能起源于合法节点，又由于 $t_1\not\subset term(m_2)$，故此时 n' 只能为发起者串 $t_{init}\in init[nonce_1, nonce_2, K_{MS}, K'_{MS}]$ 上的节点。通过分析发起者串的迹的形式可知，n' 即为节点 n_3，相应转换边为 $n_2\Rightarrow^+ n_3$，且 $C-height(t_{init})=3$，证毕。

定理 2　设 C 是串空间 Σ 中的丛，且满足条件：①$nonce_1$ 在 C 中唯一起源；②$K_{MS}\notin K_\rho$。如果发起者串 $t_{init}\in init[nonce_1, nonce_2, K_{MS}, K'_{MS}]$ 且 $C-height(t_{init})=3$，则 C 中一定存在响应者串 $t_{resp}\in resp[nonce_1, nonce_2, K_{MS}, K'_{MS}]$ 且 $C-height(t_{resp})$ 至少为 2。

该定理证明过程与定理 1 相似，不再赘述。

定理 3　用于链路密钥生成的 $nonce_1$ 和 $nonce_2$ 是随机的，且对于串空间 Σ 中每个丛 C 的任一结点 $n\in C$，K_{MS} 均非 $term(n)$ 的成分。

证明：由引理 2、引理 3 知，$nonce_1$ 和 $nonce_2$ 均唯一起源于合法节点，故 $nonce_1$ 和 $nonce_2$ 具有随机性。由于 $K_{MS}\notin K_\rho$，对于任意攻击节点 ρ，$K_{MS}\not\subset term(\rho)$。通过分析可知，$K_{MS}$ 不是任何合法节点项的成分。因此，密钥协商模型可以保证链路密钥的机密性，证毕。

3　方案设计

方案分初始化过程和密钥协商过程。为方便描述，方案中用到的符号及其含义如表 1 所列。

表 1　符号定义

Table 1　Symbol definition

符号	含义
A	管理员
M	主设备
S	从设备
K_{AM}	管理员与主设备的共享密钥
AU	设备认证因子
r, N_S, N_M	随机数
$ADDR$	蓝牙设备地址
ID	设备的身份标识
$H(m)$	消息 m 的哈希值
$PUF(c)$	挑战值 c 对应的 PUF 输出响应
$E_K(m)$	利用密钥 K 对消息 m 加密
P	PUF 的响应值
$m_1 \parallel m_2$	消息 m_1 与 m_2 连接
$m_1 \oplus m_2$	消息 m_1 与 m_2 异或

3.1　初始化

1）参数配置

在参数配置过程中进行设备认证因子预置和 PUF 参数提取，其在设备出厂时的安全环境下完成。

该阶段，管理员 A 产生随机数 r_0，并为从设备 S 选取身份标识 ID_S，利用 K_{AM} 计算 $AU_S=H(K_{AM}\parallel ID_S)$，然后将 (ID_S, r_0, AU_S) 传递给 S；S 收到消息后，计算 $c_0=H(r_0\parallel ADDR_M\parallel ADDR_S)$，并利用 PUF 得到 $P_0=PUF(c_0)$，然后将 (ID_S, r_0, P_0, AU_S) 保存于设备存储器中。设备初始化的具体过程如图 3 所示。

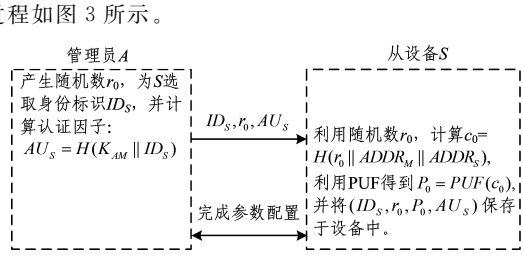

图 3　参数配置过程

Fig. 3　Parameter configuration process

2)设备入网

从设备入网过程中,管理员与主设备无需进行任何交互,该过程主设备处于开放环境而从设备处于受控环境。此时,攻击者可对蓝牙信道实施窃听、篡改、重放等攻击,但不能捕获从设备。该过程利用无线信号特征建立临时链路密钥,并基于认证因子进行设备间的身份认证及参数信息传递。设备入网完成后,从设备进入开放环境,并删除其存储的认证因子和 PUF 参数,即开放环境中的从设备不存储任何秘密信息。

设备入网过程如图 4 所示。

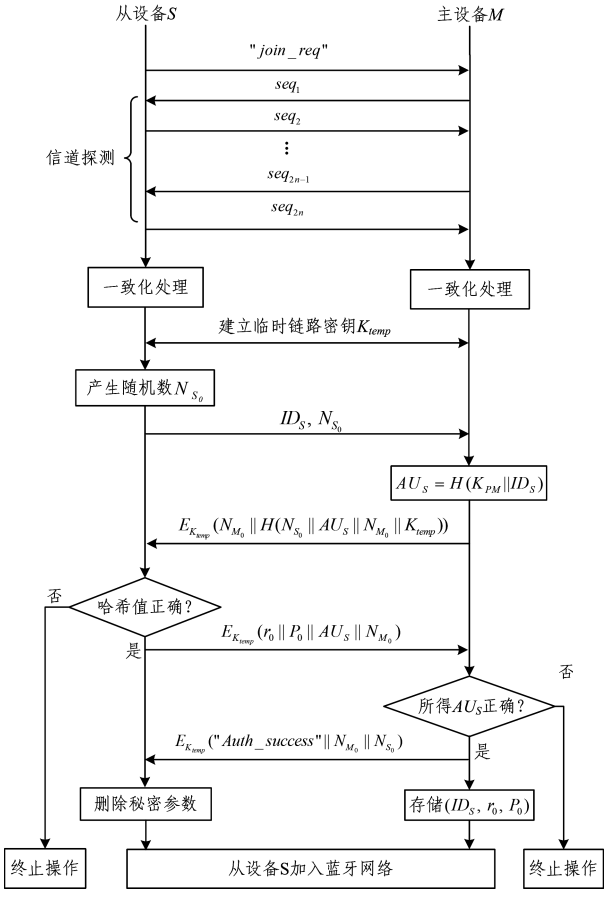

图 4 设备入网过程

Fig. 4 Device access process

设备入网的具体过程如下。

①从设备 S 向主设备 M 发送入网请求"$join\_req$",M 收到请求后,双方基于无线信号强度建立共享的临时链路密钥 K_{temp},该过程分为信道探测和一致化处理,具体见文献[10]。

②S 产生随机数 N_{S_0},向 M 发送消息 $message_1=\{ID_S, N_{S_0}\}$;$M$ 收到 $message_1$ 后,计算 $AU_S=H(K_{AM} \| ID_S)$,产生随机数 N_{M_0},并回复消息 $message_2=E_{K_{temp}}(N_{M_0} \| H(N_{S_0} \| AU_S \| N_{M_0} \| K_{temp}))$;$S$ 收到 $message_2$ 后,利用 K_{temp} 解密得到 N_{M_0} 和哈希值 $H(N_{S_0} \| AU_S \| N_{M_0} \| K_{temp})$,然后验证该哈希值的正确性。若正确,则说明 M 同时拥有 K_{temp} 和 AU_S,即 S 实现对 M 的认证;反之,S 终止操作。

③S 向 M 发送消息 $message_3=E_{K_{temp}}(r_0 \| P_0 \| AU_S \| N_{M_0})$;$M$ 收到 $message_3$ 后,验证解密所得 AU_S 的正确性。若正确,则 M 实现对 S 的认证;反之,M 终止操作。

④M 向 S 回复认证成功消息 $message_4=E_{K_{temp}}("Auth\_success" \| N_{M_0} \| N_{S_0})$,并存储($ID_S$, r_0, P_0);S 收到该消息后,删除存储的认证因子 AU_S 及 PUF 参数(r_0, P_0),完成设备入网。

3.2 密钥协商

密钥协商过程需在每次通信前执行,从设备和主设备完成双向认证并协商链路密钥。链路密钥建立后,主设备对相关参数进行更新。

第 i 次双向认证及密钥协商的流程如图 5 所示。

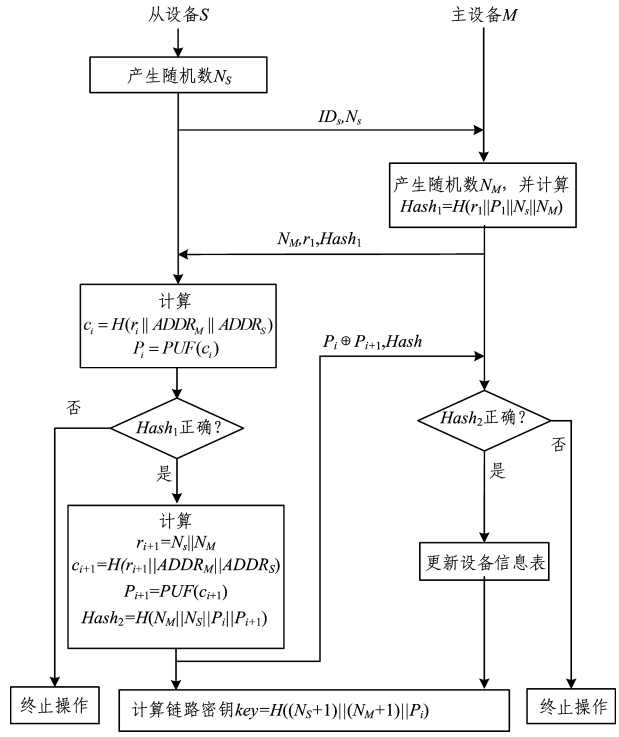

图 5 第 i 次双向认证及密钥协商流程

Fig. 5 i-th mutual authentication and key agreement process

其具体步骤如下。

①设备信息及密钥参数交换。

从设备 S 产生随机数 N_S,向主设备 M 发送消息 $message_1=\{ID_S, N_S\}$,作为密钥协商请求;M 收到 $message_1$ 后,利用 ID_S 找到 S 对应的(r_i, P_i),并产生随机数 N_M,计算 $Hash_1=H(r_i \| P_i \| N_S \| N_M)$,然后向 S 回复消息 $message_2=\{N_M, r_i, Hash_1\}$。

②从设备 S 完成对主设备 M 的认证。

S 收到 $message_2$ 后,利用 PUF 得到 $P_i=PUF(H(r_i \| ADDR_M \| ADDR_S))$,再验证 $Hash_1$ 的正确性。若 $Hash_1$ 正确,则 S 完成对 M 的认证;反之,认证失败,S 终止操作。

③主设备 M 完成对从设备 S 的认证。

S 计算 $P_{i+1}=PUF(H((N_S \| N_M) \| ADDR_M \| ADDR_S))$和 $Hash_2=H(N_M \| N_S \| P_i \| P_{i+1})$,然后向 M 发送消息 $message_3=\{P_i \oplus P_{i+1}, Hash_2\}$;$M$ 收到 $message_3$ 后,计算出 P_{i+1}并对 $Hash_2$ 进行验证。若 $Hash_2$ 正确,则 M 完成对 S 的认证;反之,认证失败,M 终止操作。

④双方计算链路密钥,完成密钥协商及设备信息更新。

双向认证成功后,双方计算共享的链路密钥 $Key=H((N_S+1) \| (N_M+1) \| P_i)$,完成密钥协商。$M$ 计算 $r_{i+1}=$

$N_S \| N_M$，并将 S 对应的信息更新为（ID_S，r_{i+1}，P_{i+1}）。

4　方案安全性分析

参数配置过程在安全环境下进行，设备入网过程通过临时链路密钥加密的安全信道实现，因而本节主要分析密钥协商过程的安全性。本文方案在密钥协商模型的基础上提出，继承了模型的以下安全性。

1）防止从设备发起的身份伪造

由定理 1 知，主设备可确认从设备的合法性。方案将从设备的身份标识与特定的 PUF 信息相关联，可以防止从设备发起的身份伪造。

2）防止主设备发起的身份伪造

由定理 2 知，从设备可确认主设备的合法性。方案中主设备 M 存储从设备 S 的 PUF 信息（ID_S，r，P），并以 $c=H(r \| ADDR_M \| ADDR_S)$ 作为 PUF 的挑战信号，通过哈希算法将 PUF 参数与特定的主设备地址相关联，可以有效防止主设备 M 利用信息（ID_S，r，P）来伪造主设备 M'。若直接将 r 作为 PUF 的输入，则不能防止 M 伪造设备 M' 的身份。

3）抗窃听攻击

由定理 3 知，攻击者无法利用监听信道得到的信息计算出链路密钥。又由于 PUF 具有不可克隆性和不可预测性，攻击者不能得到挑战 c 对应的响应信号 P，因而，方案可抵抗窃听攻击。

4）抗重放攻击

方案中引入随机数作为新鲜因子，可防止攻击者用以前的消息进行重放。此外，方案在设计过程中，避免了关键消息格式的一致性，防止了攻击者发起反射形式的重放攻击。

5）密钥前向和后向安全性

方案在密钥协商完成后对 PUF 参数信息进行更新，链路密钥利用哈希算法计算，并引入随机因子。攻击者不能根据一次通信的链路密钥推测其他密钥，因而方案可保证密钥前向和后向安全性。

6）抗物理攻击

由攻击假设知，主设备可抵抗物理攻击。从设备 PUF 集成于蓝牙芯片中，攻击者只能得到方案交互过程产生的数据，无法直接获取 PUF 挑战-响应对，且对蓝牙芯片的拆解将改变 PUF 映射关系[11]，因而攻击者不能通过物理攻击获取秘密信息。

7）抗复制攻击

由攻击假设知，主设备具有防复制攻击的能力。方案中从设备无需存储任何秘密参数，并且 PUF 具有不可克隆的特性[11]，因此，方案可以抵抗复制攻击。

本文方案与其他方案的安全性对比如表 2 所列。

表 2　安全性对比

Table 2　Security Comparison

	窃听攻击	重放攻击	中间人攻击	物理攻击	复制攻击	身份伪造	
						主设备	从设备
文献[7]	√	√	√	×	×	√	√
文献[10]	√	√	×	√	√	×	×
文献[14]	√	√	√	√	√	×	√
本文方案	√	√	√	√	√	√	√

注："√"表示可抵抗，"×"表示不能抵抗

5　实验及结果分析

方案初始化过程只需执行一次，密钥协商过程则需在主、从设备每次通信前执行，因而本节主要设计实验来分析密钥协商过程的性能。在蓝牙协议栈的基础上实现所提方案，PUF 电路利用 Altera 公司的 EP4CE115F29C7N FPGA 板实现，哈希函数采用 MD5 算法。实验所用参数长度及符号如表 3 所列。

表 3　参数长度及符号表示

Table 3　Parameter length and symbol representation

参数	长度/bit	长度符号
设备标识 ID	48	L_{ID}
哈希值	128	L_H
随机数	128	L_r
PUF 挑战信号	128	L_c
PUF 响应信号	128	L_P
A 和 M 的共享密钥	128	L_{KAM}
链路加密密钥	128	L_{Key}

5.1　实验方案

将支持蓝牙功能的小米 5 手机作为主设备，通过 Android Studio 开发工具实现具有主设备安全功能的手机 app；从设备采用搭载有 CC2541 蓝牙芯片的 SmartRF 开发板作为硬件平台，安全固件利用 IAR 软件编程实现，并通过 USB 转 SPI 线从 PC 烧录至 CC2541 芯片。从设备通过串口与实现 PUF 的 FPGA 相连接。为实现对通信过程的观察，将连接 USB Dongle 抓包工具的 PC 作为监测设备，通过 Packet Sniffer 软件记录的数据包中的时间字段，计算完成密钥协商所需的时间。实验环境如图 6 所示。

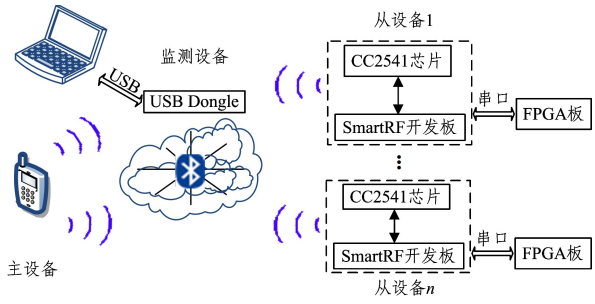

图 6　实验环境

Fig. 6　Experiment environment

为直观反映方案的性能，设置了对比实验，实验配置如表 4 所列。

表 4　实验配置

Table 4　Experiment configuration

组别	软件/固件配置	
	主设备	从设备
1	蓝牙规范 JW 模型软件	蓝牙规范 JW 模型固件
2	文献[7]方案的软件	文献[7]方案的固件
3	本文安全方案的软件	本文安全方案的固件

5.2　实验结果

在开放环境下进行 20 次实验，结果如图 7 所示，横坐标表示实验轮次，纵坐标表示完成密钥协商所需的时间。

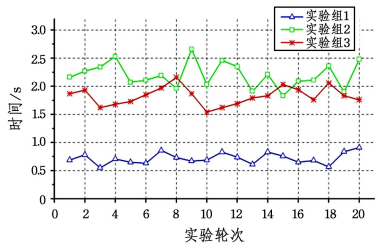

图 7 密钥协商时延

Fig. 7 Latency time of key agreement

从实验结果可以看出，本文方案的密钥协商时延略高于蓝牙规范 JW 模型的时延，但整体低于文献[7]方案的时延。利用 20 轮实验结果可计算出本文方案的密钥协商时延的平均值为 1.82 s，在用户可接受的范围内。

5.3 性能分析

密钥协商所需时间主要受设备间信息交互次数和方案计算复杂度的影响。本节分别从通信开销、计算开销和存储开销 3 个方面对方案的性能进行分析，并与同类的密钥协商方案进行对比。

1)通信开销

本文方案通过“三次握手”实现，主设备发送消息 1 次，从设备发送消息 2 次。在执行过程中，主设备发送的消息总长度为 384 bit，从设备发送的消息总长度为 432 bit。按同样的参数长度可计算得到同类密钥协商方案中主设备和从设备发送消息的轮数和发送消息的总长度。各方案通信开销的对比如表 5 所列。

表 5 通信开销

Table 5 Communication overhead

	发送消息的轮数		发送消息的长度/bit	
	主设备	从设备	主设备	从设备
本文方案	1	2	384	432
文献[7]方案	2	1	608	432
文献[17]方案	2	2	384	224
文献[18]方案	2	2	384	256

由表 5 可知，本文方案与文献[7]方案的主设备和从设备发送消息的总轮数相同，但本文方案发送消息的长度更小；相较于文献[17]和文献[18]的方案，本文方案虽然发送消息的长度略大，但发送消息的轮数更少。

2)计算开销

计算开销可利用高复杂度密码算法的执行时间来衡量。分别采用 T_H，T_{SE}，T_{AE}，T_{MUL} 代表执行哈希运算、对称加/解密运算、非对称加/解密运算和模乘运算所需的时间。在本文方案中，主设备需要执行 3 次哈希运算，从设备需要执行 5 次哈希运算，无需其他复杂的运算。因而，主设备和从设备的计算开销分别为 $3T_H$ 和 $5T_H$。按照同样方法可以计算出同类方案的计算开销，如表 6 所列。

表 6 计算开销

Table 6 Computation overhead

方案	主设备	从设备
本文方案	$3T_H$	$5T_H$
文献[7]方案	$3T_H+T_{AE}+T_{SE}$	$4T_H+T_{AE}+T_{SE}$
文献[17]方案	$2T_{AE}+3T_{SE}$	$2T_{AE}+T_{SE}$
文献[18]方案	$2T_H+2T_{AE}+2T_{SE}$	$2T_H+2T_{AE}+2T_{SE}$

在计算开销方面，由文献[7]可知，$T_{SYM}\approx 2T_{MUL}$，$T_{ASYM}\approx 160T_{MUL}$，$T_H\approx 0.23T_{MUL}$。因此，从各类方案的计算开销对比结果可以看出，本文方案的主设备和从设备只需要进行哈希运算，其计算开销明显优于同类方案。

3)存储开销

将匹克网中从设备的数量记为 m，本文方案主设备 M 需存储每个从设备的身份标识 ID、随机数 r、PUF 的响应值 P 及密钥 KAM，从设备只需存储其身份标识 ID。由此可得本文方案主设备的存储开销为 $(L_{ID}+L_r+L_P)\times m+L_{KAM}$ bit，所有从设备的总存储开销为 $L_{ID}\times m$ bit。

各类方案的存储开销对比如表 7 表示。其中，L_{ADDR}，L_{PIN}，L_{KAE} 分别表示设备地址、PIN 码和非对称密钥的长度，其余符号含义与表 3 一致。

表 7 存储开销

Table 7 Storage overhead

方案	主设备	从设备
本文方案	$(L_{ID}+L_r+L_P)\times m+L_{KAM}$	$L_{ID}\times m$
文献[7]方案	$(L_{id}+L_H+L_{KAE})\times m+L_{KAE}$	$(L_H+2L_{KAE})\times m$
文献[17]方案	$(L_{id}+L_{pwd}+L_{KAE})\times m$	$(L_{pwd}+2L_{KAE})\times m$
文献[18]方案	$(L_{ADDR}+L_{KAE}+L_{PIN})\times m+L_{ADDR}+L_{KAE}$	$(2L_{ADDR}+L_{KAE}+L_{PIN})\times m$

由表 7 可知，4 种方案的主设备的存储开销相差不大，而本文方案的从设备仅需要存储身份标识 ID，其存储开销明显优于其他方案。

结束语 本文提出了一种从设备零秘密存储的蓝牙密钥协商方案，利用 PUF 的不可克隆性和不可预测性实现了设备间的双向认证、链路密钥协商及参数更新。基于串空间理论的形式化证明和安全性分析表明，所提方案能够有效抵抗窃听攻击、中间人攻击、复制攻击等安全威胁。实验结果显示，该方案可以高效地实现设备间的密钥协商且所需计算和存储开销较小，能够满足蓝牙设备需求，对于增强蓝牙安全性，促进其在军事、医疗等高安全要求领域的应用和发展具有重要意义。

参 考 文 献

[1] RAZA S, MISRA P, HE Z, et al. Building the Internet of Things with Bluetooth smart[J]. Ad Hoc Networks, 2017, 57: 19-31.

[2] Bluetooth SIG. Specification of the Bluetooth system: core package version 4.0[EB/OL]. http://www.bluetooth.org, 2009.

[3] PHAN R C W, MINGARD P. Analyzing the secure simple pairing in Bluetooth v4.0[J]. Wireless Personal Communications, 2012, 64(4): 719-737.

[4] BARNICKEL J, WANG J, MEYER U. Implementing an attack on bluetooth 2.1+ secure simple pairing in passkey entry mode [C]// IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool: IEEE Press, 2012: 17-24.

[5] HAATAJA K, TOIVANEN P. Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures [J]. IEEE Transactions on Wireless Communications, 2010, 9(1): 384-392.

[6] PERREY H, UGUS O, WESTHOFF D. WiSec'2011 poster: se-

curity enhancement for bluetooth low energy with Merkle's puzzle[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2011, 15(3): 45-46.

[7] HUANG Y B, HUANG Y C, YU B. Design of BLE Key Agreement Scheme Based on Hash Chain[J]. Journal of System Simulation, 2016, 28(6): 1412-1418. (in Chinese)
黄艺波，黄一才，郁滨. 基于哈希链的 BLE 密钥协商方案设计[J]. 系统仿真学报，2016，28(6)：1412-1418.

[8] SKOROBOGATOV S. Flash memory 'bumping' attacks[C]// Cryptographic Hardware and Embedded Systems, CHES 2010. 2010: 158-172.

[9] MARCHAND C, BOSSUET L, MUREDDU U, et al. Implementation and characterization of a physical unclonable function for IoT: a case study with the TERO-PUF[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 37(1): 97-109.

[10] ZHANG X H, HUANG Y C, YU B. BLE Key Agreement Scheme Based on RSSI Variation Trend[J]. Journal of System Simulation, 2017, 29(4): 873-879. (in Chinese)
张星昊，黄一才，郁滨. 基于 RSSI 变化趋势的 BLE 密钥协商方案[J]. 系统仿真学报，2017，29(4)：873-879.

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

[12] ZHANG Z N, GUO Y B. Survery of physical unclonable function[J]. Journal of Computer Applications, 2012, 32(11): 3115-3120. (in Chinese)
张紫楠，郭渊博. 物理不可克隆函数综述[J]. 计算机应用，2012，32(11)：3115-3120.

[13] NGUYEN P H, SAHOO D P. An Efficient and Scalable Modeling Attack on Lightweight Secure Physically Unclonable Function[J]. IACR Cryptology ePrint Archive, 2016, 2016: 428.

[14] AMAN M N, CHUA K C, SIKDAR B. Position Paper: Physical Unclonable Functions for IoT Security[C]// Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. Xi'an, China, 2016: 10-13.

[15] MUTTI S, BACIS E, and PARABOSCHI S. Sesqlite: Security enhanced sqlite: Mandatory access control for android databases [C]// Proceedings of the 31st Annual Computer Security Applications Conference. Los Angeles, USA, 2015: 411-420.

[16] 王亚弟，束妮娜，韩继红，等. 密码协议形式化分析[M]. 北京：机械工业出版设，2006：126-139.

[17] DIALLO A S, AL-KHATEEB W F M, OLANREWAJU R F, et al. A Secure Authentication Scheme for Bluetooth Connection [C]// International Conference on Computer and Communication Engineering. IEEE Press, 2015: 60-63.

[18] LALIS J T, GERARDO B D, BYUN Y. Securing Bluetooth Communication with Hybrid Pairing Protocol[J]. International Journal of Security & Its Applications, 2014, 8(4): 219-228.