一种基于 RSA 非对称加密的 NFC QSL 卡片设计思路

DE BG2FFJ

2023.12.10

摘　　要

本文中，作者提出了一种基于 NFC 卡片的业余无线电 QSL 卡片。该项目设计并制作了一个 PCB 板，预先在 PCB 内部埋入线圈，并焊接 NFC 芯片和 LED 灯。PCB 丝印部分参考了传统的 QSL 卡片内容，留下了书写空间。将精简后的 QSL 信息写入 NFC 芯片，并使用 RSA 私钥进行加密。加密后的内容和公钥同时写入 NFC 卡片，并设置卡片为不可写入，以确保电子卡片的不可篡改性。这种基于 NFC 的 QSL 卡片不仅继承了传统 QSL 卡片的形式，还增加了电子化、信息化的元素，为业余无线电的确认通联提供了新的可能性。

关键词：业余无线电，近场通信，QSL 卡片

ABSTRACT

In this article, the author proposes an amateur radio QSL card based on NFC card. They designed and produced a PCB board, embedded coils inside the PCB in advance, and soldered the NFC chip and LED lights by themselves. The PCB silk screen part refers to the traditional QSL card content and leaves space for writing. They write the streamlined QSL information to the NFC chip and encrypt it using an RSA private key. The encrypted content and public key are written to the NFC card at the same time, and the card is set to be unwritable to ensure that the electronic card cannot be tampered with. This NFC-based QSL card not only inherits the form of the traditional QSL card, but also adds electronic and information elements, providing new possibilities for amateur radio to confirm communications.

KEY WORDS:Amateur radio, Near Field Communication, QSL Card

目　　录

第一章 引言

1.1 该项目的背景和意义

业余无线电，也被称为 Amateur Radio，是一种全球广泛参与的无线电通信方式。它允许业余无线电爱好者通过各种频率和模式进行全球通信，从而提供了一种独特的社交手段，同时也为紧急通信提供了重要的参考价值。业余无线电不仅是一种娱乐方式，也是一种技术和科学的实践，它鼓励无线电爱好者进行无线电设备的自我建造和实验。

QSL 卡片在业余无线电中起着至关重要的作用。它是无线电爱好者之间确认通联的一种方式。每张 QSL 卡片都包含了一次特定通联的详细信息，如日期、时间、频率、模式和信号报告。这些卡片不仅是一种友好的交流方式，也是无线电爱好者收集和展示他们 QSO 的一种方式。因此，QSL 卡片在业余无线电社区中具有重要的历史和文化价值。

1.2 研究现状

在过去的几十年里，业余无线电和 QSL 卡片的使用一直在全球范围内广泛流行。然而，随着数字技术的发展，传统的 QSL 卡片在某些方面已经无法满足现代通信的需求。例如，传统的 QSL 卡片无法存储大量的信息，也无法保证信息的安全性和不可篡改性。

近年来，有一些研究开始探索如何将现代技术应用到 QSL 卡片中。例如，有些研究者尝试使用二维码、条形码或电子邮件来存储和分享无线电联系的信息。然而，这些方法仍然存在一些问题，如信息容量有限，需要专门的设备扫描，以及信息的安全性和不可篡改性无法得到保证。

此外，还有一些在线确认方式，如 ARRL 的 LOTW（Logbook Of The World）、eqsl.cc 和 qrz 日志簿等，它们提供了一种更加便捷的方式来确认 QSO。然而，这些在线服务通常非常难以操作，界面复古，需要繁琐的验证，且无法提供实体的 QSL 卡片留作纪念。

NFC 技术作为一种新兴的无线通信技术，已经在许多领域得到了广泛的应用，如移动支付、门禁系统和物联网。然而，到目前为止，还没有研究将 NFC 技术应用到 QSL 卡片中。因此，该项目填补了这一空白，提出了一种基于 NFC 的 QSL 卡片的概念，为业余无线电通信提供了一种新的可能性。

1.3 本文研究内容

在这项研究中，提出了一种基于 NFC（近场通信）的 QSL 卡的创新概念。这种新型 QSL 卡将传统 QSL 卡的物理形式与现代 NFC 技术的数字功能相结合，为业余无线电通

信提供了一种新的卡片制作方式。

NFC 技术的引入使 QSL 卡可以存储和传输大量数字信息，从而大大增强了 QSL 卡的功能。例如，NFC QSL 卡可以存储无线电联络的详细信息，包括日期、时间、频率、模式和信号报告。这些信息可以通过任何配备 NFC 的设备（如智能手机）方便快捷地读取和共享，大大提高了信息交流的效率。

此外，该研究还利用 RSA 私钥对存储在 NFC QSL 卡中的信息进行加密，以确保信息的安全性和防篡改性。这是传统 QSL 卡无法实现的功能，它为业余无线电通信提供了一种更安全、更可靠的确认方法。这种方法不仅能防止信息被篡改，还能防止未经授权的访问，从而保护无线电通信的安全。

总之，基于 NFC 的 QSL 卡不仅继承了传统 QSL 卡的形式，还增加了电子和信息元素。这种新型 QSL 卡有望成为业余无线电通信的新朋友，为无线电爱好者提供一种新的、更有效的通联确认方式。

第二章 NFC 技术简介

2.1 NFC 技术简介

NFC（近场通信）技术是一种基于无线射频识别（RFID）的通信技术，利用磁感应和电感耦合的原理进行数据传输。其工作原理基于设备间感应线圈产生的磁场，并通过电感耦合实现信息的传输。这种通信方式具有近场特性，通信的两个设备之间通常保持在几厘米的距离，确保数据传输的高效性和安全性。

它的通信距离通常在 1 至 10 厘米之间，这一特点使得 NFC 在需要安全性的场景中得到广泛应用。短距离通信的限制也为用户提供了更好的控制，确保设备只在非常近距离内进行通信，从而降低了意外数据泄露的风险。且芯片的设计注重短距离通信，通过调整线圈的设计和通信频率，实现了设备之间的高效、稳定的无线通信。数据传输速率相对较低，适用于小型数据交换，如标签读取或简单文件传输。NFC 的数据传输速度可以达到 424 Kbit/秒，虽然这比 Wi-Fi 和蓝牙的速度慢，但对于大多数 NFC 的应用来说已经足够了。

所有的 NFC 卡片工作频率都为 13.56MHz，这是一个全球通用的无线电频率，不需要获得许可就可以使用。NFC 的通信距离通常在 20 厘米以内，确保了通信的安全性，攻击者很难在这么近的距离内进行攻击而不被发现。

总体而言，NFC 技术通过其独特的近场通信原理，为各种应用提供了一种安全、高效的无线通信手段，而这一技术在业余无线电中的应用展现出创新的潜力。

2.2 NFC 在各种应用中的使用

NFC 技术在各种领域中得到了广泛的应用，其灵活性和安全性使其成为许多领域的理想选择。在支付系统中，NFC 技术被广泛应用于无接触支付，用户只需将设备靠近 POS 终端即可完成支付（如 ApplePay，MiPay，HuaWeiPay 等手机钱包），这种便捷的支付方式提高了支付的效率，同时确保了安全性。在物联网（IoT）领域，NFC 技术使得设备之间能够方便快捷地建立连接，智能家居设备、智能标签和可穿戴设备可以通过 NFC 实现简单的配置和数据传输。在身份验证方面，NFC 技术为安全身份验证提供了一种有效的解决方案，用户可以通过将其设备靠近读卡器完成身份验证过程。在电子卡片和身份识别领域，NFC 技术具有显著的重要性，通过将 NFC 芯片整合到卡片中，可以实现信息的安全存储和传输。因此，QSL 卡片项目中采用 NFC 技术是合理的，这不仅具有创新性，也契合了 NFC 在电子卡片和身份识别领域的成功应用。

第三章 设计与制造

3.1 PCB 板设计

该项目的 PCB 板采用了通用卡片的尺寸，长 73mm，宽 46mm，和常见的证件大小相似，便于收纳和携带。在 PCB 板设计上，采用了双层板，正反面各绕了三圈铜线作为 NFC 天线，在一面的天线旁留出 NFC 芯片的位置进行焊接。此外，考虑到卡片的实际使用需求（一目了然的记录通联信息），在 PCB 板上加入了传统 QSL 卡片内容，以便书写或添加其他信息（图 3-1）。

图 3-1 在 PCB 丝印上加入了传统 QSL 卡片内容

考虑到卡片的美观性和易用性，在芯片旁单独引出了一条线路驱动 LED 灯，在刷卡的时候可以通过观察 LED 灯来检测是否刷卡成功。该电路采用一个 100 Ω 的贴片电阻与一个白色贴片 LED 灯，均为 0603 封装。

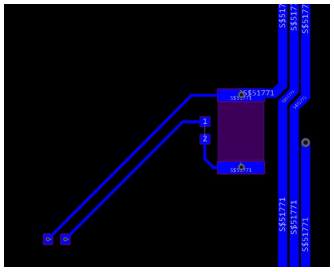

图 3-2 LED 及分压电阻电路

3.2 NFC 芯片选型与连接

在选择 NFC 芯片时，需要考虑多个因素，包括芯片的功能、存储容量和成本等。常用的 NFC 芯片有 NTAG213、NTAG215、NTAG216 和复旦 M1 等。

NTAG213、NTAG215 和 NTAG216 是 NXP（恩智浦）半导体开发的标准 NFC 标签 IC，与 NFC 设备或符合 NFC 标准的近距离耦合设备相结合，可用于零售、游戏和消费电子产品等大众市场应用。这三种芯片在功能上并没有区别，但在存储容量上有着较大的差距。NTAG213 的内存大小为 137 字节，NTAG215 的内存大小为 492 字节，而 NTAG216 的内存大小为 868 字节。

复旦 M1 卡片是一种常见的非接触 IC 卡，广泛应用于各种系统中，如门禁控制、考勤、消费、停车等。然而，复旦 M1 卡片的存储容量相对较小，且价格相对较高，因此在成本和存储量方面并不适合我们的需求。

在该项目中，我需要存储 QSL 信息、加密后的内容以及解密后的公钥。综合考虑成本和存储量，我选择了 NTAG216 作为我们的 NFC 芯片。NTAG216 不仅具有足够的存储容量来满足我的需求，而且其成本相对较低，更符合预算。

第四章 不可篡改性

4.1 RSA 加密概述

RSA 加密算法是一种非对称加密算法，广泛应用于公开密钥加密和电子商务。RSA 算法由罗纳德·李维斯特（Ron Rivest）、阿迪·薩莫爾（Adi Shamir）和倫納德·阿德曼（Leonard Adleman）在 1977 年共同提出。

RSA 算法的安全性基于大数因数分解的难度。换言之，对一个极大整数进行因数分解越困难，RSA 算法就越可靠。如果有人找到一种快速因数分解的算法，那么用 RSA 加密的信息的可靠性就会极度下降。但找到这样的算法的可能性非常小。今天只有短的 RSA 密钥才可能被强力方式破解。到 2020 年为止，世界上还没有任何可靠的攻击 RSA 算法的方式。只要其密钥的长度足够长，用 RSA 加密的信息实际上是不能被破解的。

在 RSA 加密方案中，选定了两个大质数 p 和 q，计算出 N=pq，再在小于φ(N)的正整数中选一个和它互素的 e 作为公钥，它模φ(N)的乘法逆元 d 则为私钥。公开 e，保留 d。

公钥 e 用来加密，私钥 d 用来解密。具体来说，如果乙方想给甲方发送一个加密消息，他可以获取甲方的公钥，然后用它对信息进行加密。甲方收到加密后的信息后，可以使用自己的私钥进行解密。

总的来说，RSA 的公钥和私钥在理论上是可以互换的，但在实际应用中，公钥和私钥有完全不同的要求，这些要求保证了 RSA 加密方案尽可能地更安全高效。在这种情况下，公钥用来公开并加密，私钥用来保留解密，且不可互换。

4.2 防止信息被篡改或伪造

该设计通过使用 RSA 私钥加密，有效地防止了信息被篡改或伪造。由于私钥是保密的，因此无法伪造加密后的信息。此外，由于 RSA 加密是一种不可逆的过程，因此无法从加密后的信息中恢复原始的信息，除非知道对应的公钥。这意味着，即使有人可以访问 NFC 芯片并读取加密后的信息，他们也无法修改或篡改这些信息，除非他们知道私钥。然而，私钥是保密的，因此这在实际中是不可能的。且卡片一旦被写入完成检查无误便会被设置成只读。这种设计有效地防止了信息被篡改或伪造，从而确保了信息的安全性和不可篡改性。

第五章 写入 QSL 信息和加密

5.1 QSL 信息的结构及精简

QSL 信息通常包含以下字段：TORADIO（对方呼号）、TIME（时间）、BAMD MHZ（频率）、MODE（模式）、RST（信号报告）、RIG（设备）、POWER（功率）、ANT（天线）和 PSE/TNKQSL（QSL 状态），每个字段都有其特定的含义和格式。

在将 QSL 信息电子化时要尽可能精简，但是同时还要保证和卡面上写的内容完全一致，即原本的信息不变。以如下的卡片内容为例（图 5-1）：

图 5-1 一张写了通联信息的 QSL 卡片

TO RADIO 字段在考虑精简的情况下，可以更换为 TOCALL，相比之下节省了一个英文字符的空间；DATE 和 TIME 字段都是时间，可以精简为 BJT/UTC；BAND MHZ 精简为 MHZ。其余的内容依次抄写下来，最后得到的用来表示该 QSL 内容的文本为：

“ TOCALL:BG2FFJ/BJT:202305161919/MHZ:439.850MHZ/MODE:EYEBALL/RST:59+20/RIG:XIEGU-G90S/POWER:100W/ANT:20MEND-FED/TNKQSL”

这样就用一串文本电子化了卡片上所表示的 QSL 信息。

5.2 RSA 私钥加密的详细步骤

首先，我们需要生成一对 RSA 公钥和私钥。这可以通过许多编程语言的内置库或第三方库来实现，以及 Openssl。本文使用简易的 Python 代码来进行，我们可以使用 rsa 库来生成 RSA 公钥和私钥：

```
import rsa

# 生成公钥和私钥

public_key, private_key = rsa.newkeys(1024)

//此处为密钥长度 分为 512 位，1024，2048

# 打印公钥和私钥

print(public_key)

print(private_key)
```

接下来，我们使用生成的私钥对 QSL 信息进行加密。我们可以使用 rsa 库的 rsa.encrypt 函数来实现：

```
# QSL 信息

message =
"TOCALL:BG2FFJ/BJT:202305161919/MHZ:439.850MHZ/MODE:EYEBALL/RST:59+20/RIG:XIEG
U-G90S/POWER:100W/ANT:20MEND-FED/TNKQSL"

# 使用私钥加密信息

encrypted_message = rsa.encrypt(message.encode(), private_key)

# 打印加密后的信息

print(encrypted_message)
```

最后，我们需要提供公钥，以便其他人可以使用公钥对加密后的内容进行解密，从而获取原始的 QSL 信息。在 Python 中，我们可以使用 rsa 库的 rsa.PublicKey.save_pkcs1 函数来获取公钥的字符串表示：

```
# 获取公钥的字符串表示

public_key_str = public_key.save_pkcs1().decode()



# 打印公钥

print(public_key_str)
```

接下来我们需要保存上文生成的 原始的 QSL 信息，生成的加密内容，RSA 公钥 准备写入卡片。

5.3 QSL 信息写入

有很多方法可以将文本写入到卡片内部，本文只使用最简单的一种方式：使用用户友好的安卓 App 写入（文中为 NFC Tools Plus）。当然您完全可以使用其他方式，比如自己编写脚本或使用其他卡片读写硬件比如变色龙等。

首先，您需要在 Google Play 商店中搜索并下载 NFC Tools Pro 应用。安装完成后，打开应用，您将看到一个很直白的界面，提供了多种 NFC 相关的功能。

在 NFC Tools Pro 应用中，选择“写入”选项，然后选择“添加记录”。在弹出的菜单中，选择“文本”，然后在文本字段中输入或粘贴您的 QSL 信息。点击“确定”后，您将看到 QSL 信息已被添加到待写入记录列表中。

图 5-3 准备写入界面

接下来，将您的 NFC 芯片放在设备的 NFC 感应区域（通常位于设备的背面中部）。点击上方的“写入”按钮，应用会自动检测到 NFC 芯片，并将待写入记录列表中的所有记录写入芯片。

写入完成后，您可以使用 NFC Tools Pro 应用的“读取”功能来验证写入结果。只需将 NFC 芯片再次放在设备的 NFC 感应区域，应用会自动读取芯片中的数据，并显示在屏幕上。

检查无误后，在标签信息页面，滚动到底部，找到“设置为只读”选项，点击它。这将使 NFC 卡片设置为只读，也就是不可写入。

再次贴卡，应用出现提示信息即为设置成功。

第六章 结论

6.1 主要发现

在该研究中，成功地将 QSL 信息写入 NFC 芯片，并使用 RSA 私钥加密来确保信息的安全性和不可篡改性。通过使用 NFC 技术和 RSA 加密，可以有效地防止信息被未授权的人篡改或窃取。此外，这种方法对于业余无线电爱好者来说非常方便，因为他们可以使用他们的智能手机来读取和写入 NFC 芯片，而无需任何专门的设备。

6.2 研究贡献

该研究对业余无线电领域提出了一种新的 QSL 卡片设计思路。首先，它提供了一种新的、安全的方式来交换 QSL 信息。这对于业余无线电爱好者来说是非常重要的，因为 HAM 群体经常需要交换 QSL 信息，以确认他们的通联信息。其次，该项目还展示了如何使用现代的无线通信技术和加密技术来提高业余无线电通信的安全性和可靠性。这对于业余无线电社区来说是非常有价值的，因为它不同于在线确认，可以帮助防止线下发送的信息被手动篡改或窃取。

6.3 对未来研究的建议

尽管该研究取得了一些发现，但我们认为还有许多有待探索的问题。例如，我们可以进一步研究如何优化信息的存储和传输，以使其更加高效和可靠。此外，我们还可以探索其他类型的加密算法，以看看它们是否可以提供更高级别的安全性。我们还可以研究如何将我们的方法应用到其他类型的无线电通信中，如不通过递送 PCB 卡片，直接在纸质卡片上贴 NFC 芯片和线圈帮助确认信息。我们希望该研究能够激发更多的研究，以进一步提高业余无线电通信的安全性和可靠性。