RFID101

An Introduction to RFID Hacking



Ege F
ege@physsec.org

Andrew M
andrew@physsec.org


Pay Fare • Paiement
PRESTO
Tap Card Here
Présentez votre carte ici
PRESTO

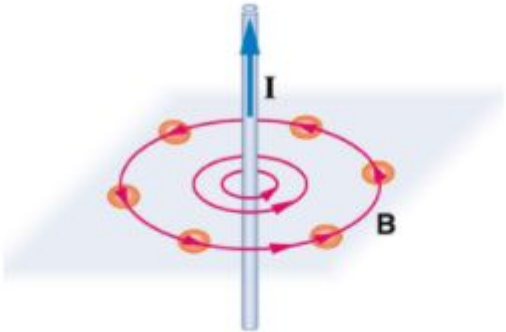



CREDIT CARD

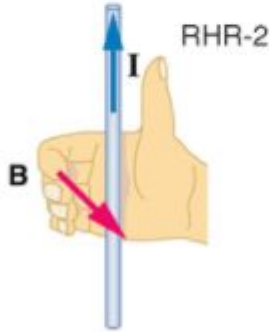
ΦSV

But how does it work?





(a)



(b)

IC: openstax College Physics Textbook

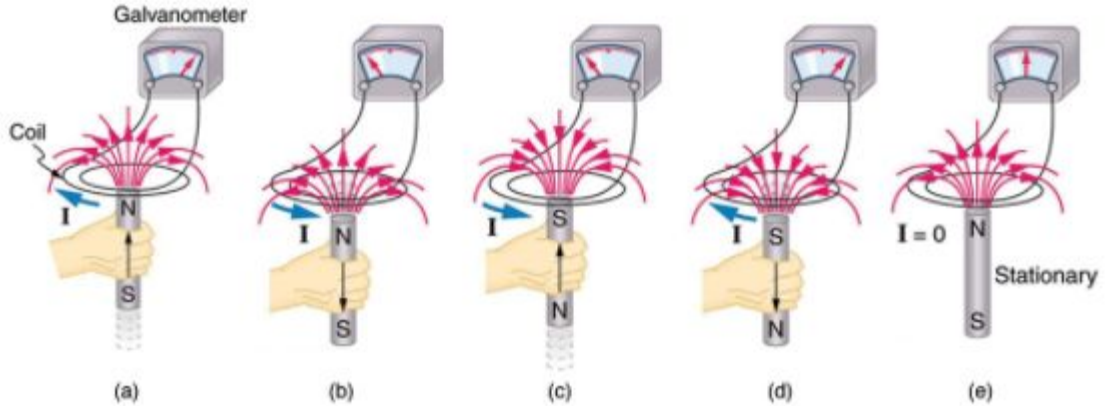
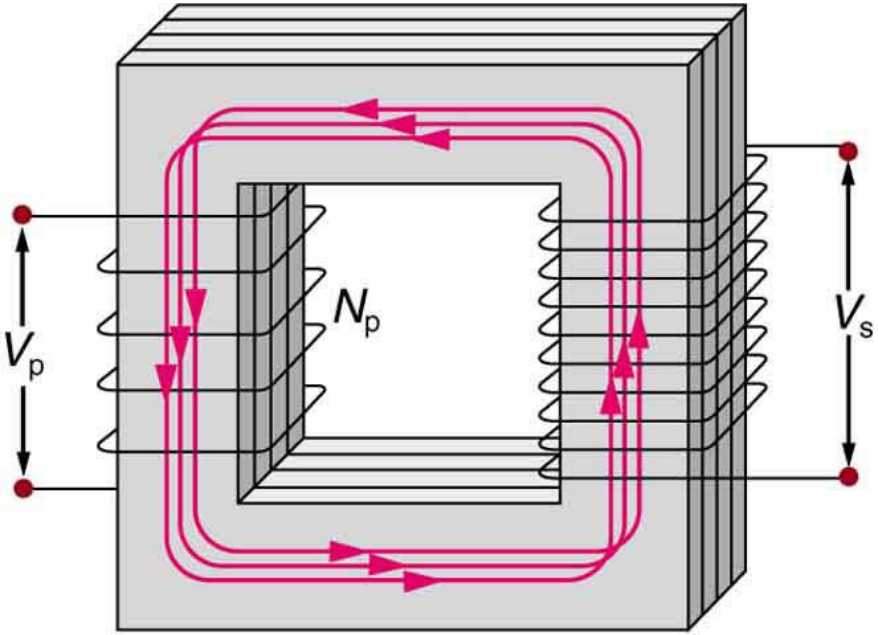
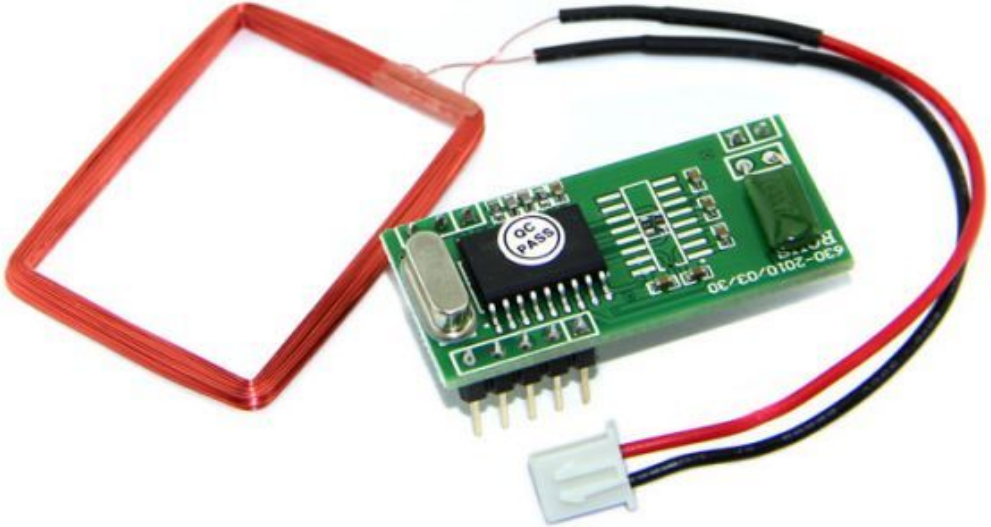


Figure 23.4 Movement of a magnet relative to a coil produces emfs as shown. The same emfs are produced if the coil is moved relative to the magnet. The greater the speed, the greater the magnitude of the emf, and the emf is zero when there is no motion.

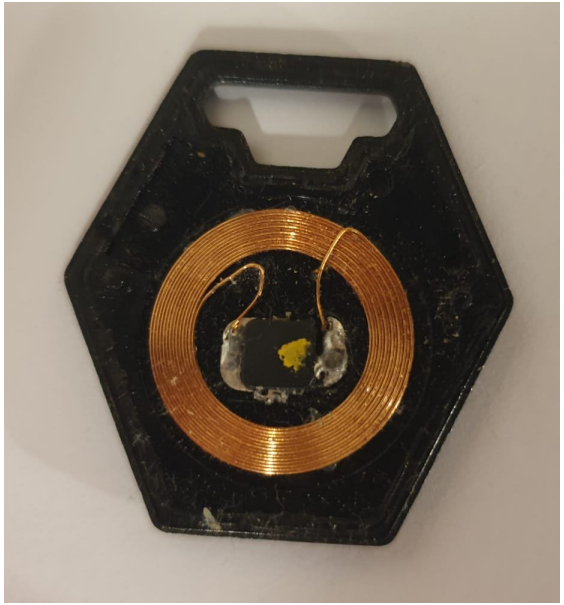
IC: openstax College Physics Textbook

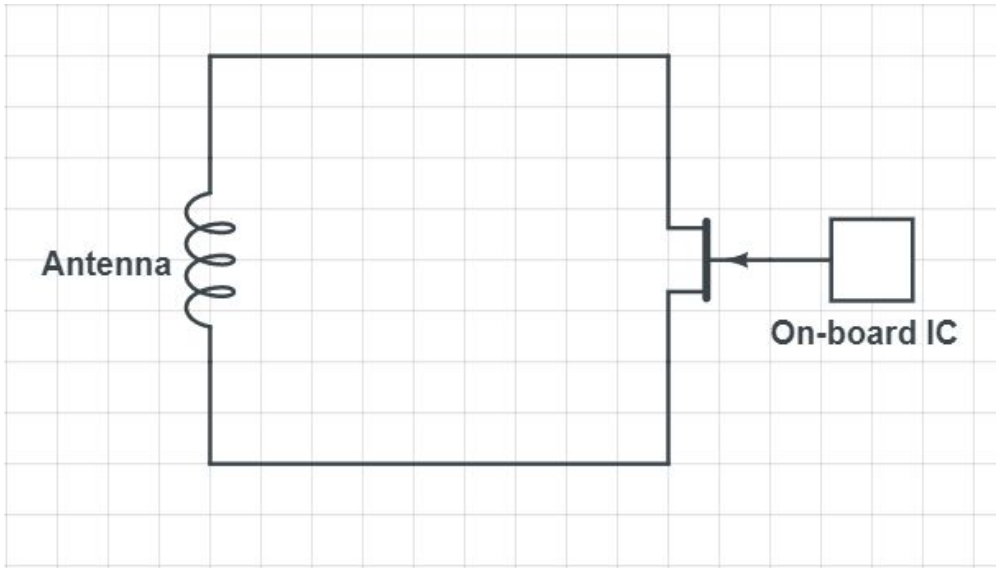


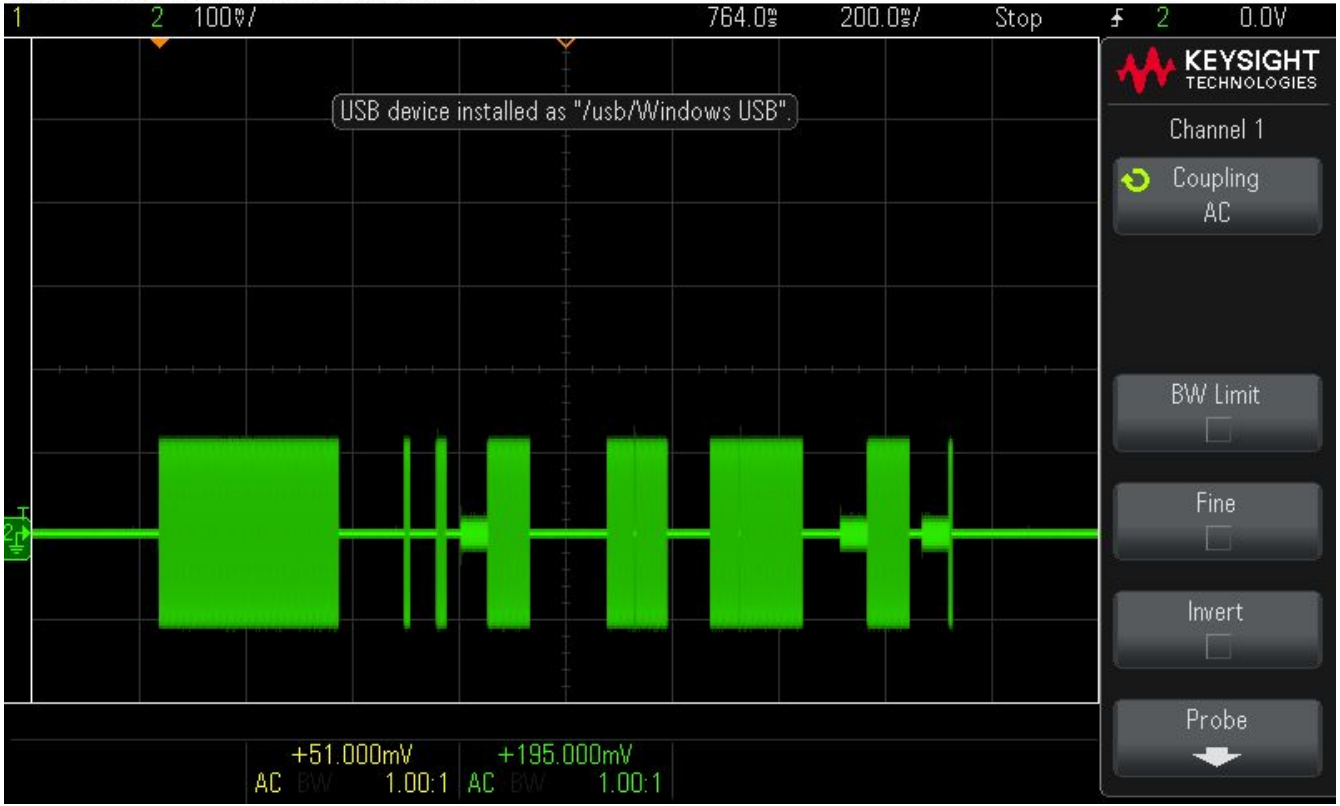
IC: openstax College Physics Textbook

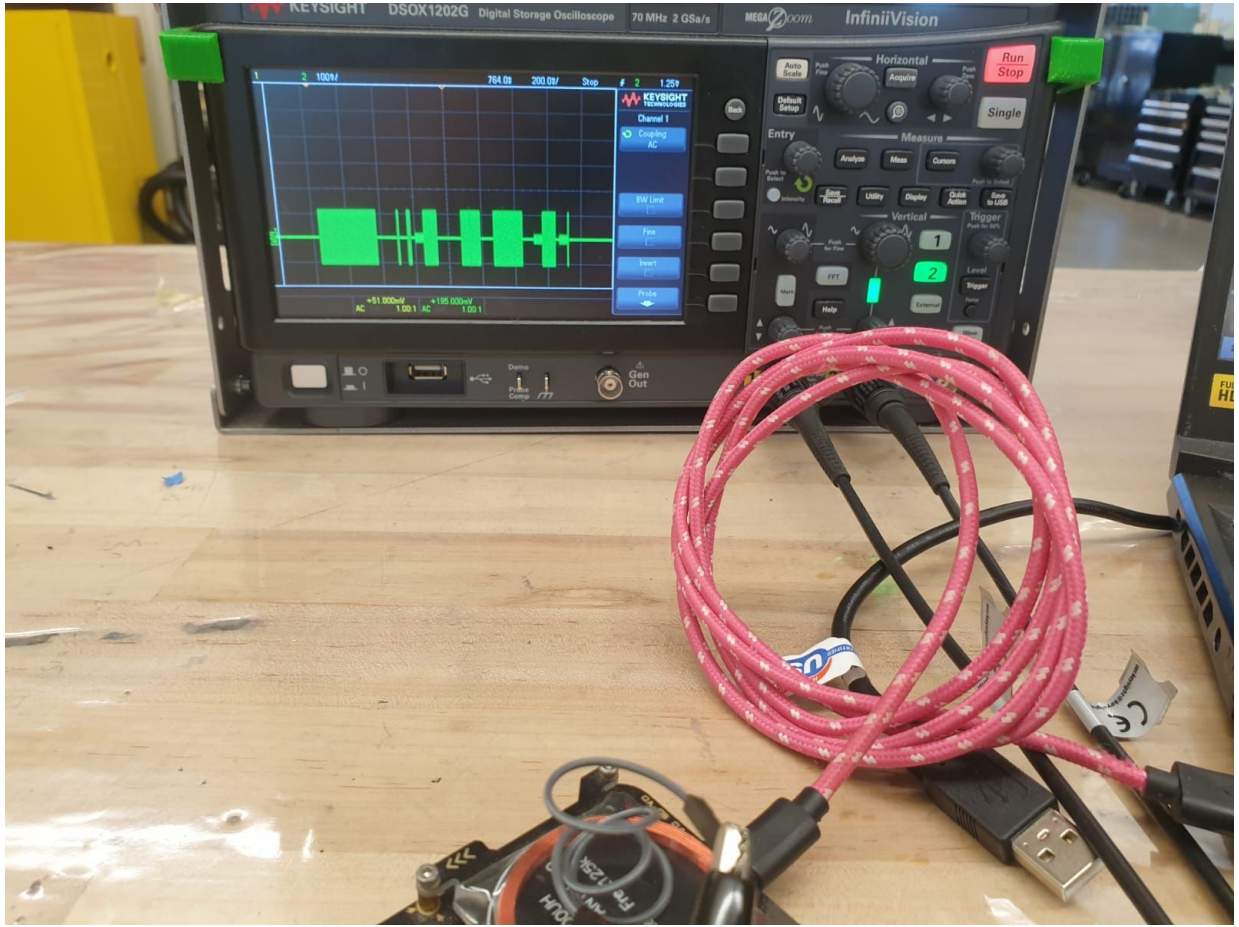

QC
PASS


CHUBB
KLASS




Antenna
On-board IC


DSOX1202G, CN60194206: Sat Aug 27 04:55:51 2022
1
2 100mV/
764.0ns
200.0ns/
Stop
2 0.0V
USB device installed as "/usb/Windows USB".
KEYSIGHT TECHNOLOGIES
Channel 1
Coupling
AC
BW Limit
Fine
Invert
Probe
+51.000mV
AC BW 1.00:1
+195.000mV
AC BW 1.00:1


KEYSIGHT
DSOX1202G
Digital Storage Oscilloscope
70 MHz 2 GSa/s
InfiniiVision
Horizontal
Run
Stop
Single
Entry
Measure
Vertical
Trigger
Channel 1
Gen
Out



How can we solve this problem?

Encryption







Hi! Encrypt this random number please

Sure! Here you go, please encrypt this different random number

Here you go!

Thanks! Now that we know we both know the key, let's use that to communicate encrypted.

ΦSV

Heart of Darkness - exploring the uncharted backwaters of HID iCLASS™ security

Milosch Meriac, *meriac@OpenPCD.de*

***Abstract*—This paper provides detailed information on *iCLASS*™ reader and key security. It explains the security problems found without revealing the extracted secret keys (DES authentication Key and the 3DES data encryption key for *iCLASS*™ Standard Security cards).**

The chosen approach of not releasing the encryption and authentication keys gives iCLASS vendors and customers an important headstart to update readers and cards to High Security mode in order to stop attackers from forging, reading and cloning iCLASS Standard Security cards.

This paper also explains, how Standard Security and High Security keys were extracted from a RW400 reader without leaving visible traces.

I. Introduction

Hunters for gold or pursuers of fame,
they all had gone out on that stream,
bearing the sword, and often the torch ...

– Joseph Conrad: Heart of Darkness

Most existing RFID card systems like Mifare Classic[1] and Legic Prime[2] are already well researched. The lack of security found in these systems increased my attention on other undocumented RFID systems.

This year my interest was caught by HID's iCLASS system. The iCLASS protocol is not documented publicly and sales channels for cards, keys, readers and writers seem to be tightly controlled.

After some intitial research I discovered that CP400 programmers for iCLASS cards are not available on sale, but are only available for leasing under tight contracts and high costs. Non-configured, non-programmed iCLASS cards are no longer available from HID - this made me curious enough to order some second hand RW400 writers from Ebay and some cards. Interestingly I was able to buy unprogrammed cards, which allowed me to do some research on the protocol side as well.

Chapter II gives a brief overview of iCLASS Security. The physical reader security is evaluated in chapter III and shows how the lack of attention to CPU data sheets leads to vulnerabilities that result in leaking of firmware images and key material.

Detailed suggestions to improve system security can be found in chapter IX.

The protocol security aspects of the iCLASS RFID protocol will be presented separately at the public 27C3 talk and thus will not be duplicated here in this paper.

II. iCLASS Security

Do you want the convenience
of receiving preprogrammed cards
that are ready for use? No problem -
trust HID to manage your keys! -

– N. Cummings, HID: iCLASS Levels of Security

iCLASS cards come in two flavors: "Standard Security" and "High Security". In Standard Security mode the customer buys preprogrammed cards from HID that contain a unique combination of card number and facility ID.

Each individual card is initialized with a diversified key. The reader key is hashed with the card serial number to create a unique key[3].

When a card is presented to a reader, the card ID is read, the card key is diversified and the card authentication process is started based on the diversified per-card key. Every successful card read results in a "beep-n-blink" of the reader and a transmission of the data payload to the backend system.

A. Standard Security

Standard Security mode means that two common secret keys are shared across all HID readers in that Mode. The supplied cards contain a unique combination of a card ID and a per-facility ID. A reader in a Standard Security mode will therefore successfully authenticate all Standard Security iCLASS cards and will send the stored card ID and facility ID, usually in Wiegand format, to the upstream system.

The upstream system decides based on the transmitted data if the card is part of the system and determines the access level.

B. High Security

High Security essentially means, that each system uses a system specific key. This system specific key is already used during authentication phase. As authentication fails when presenting a Standard Security or High Security card from another High Security system, no "beep-n-blink" will occur on the reader.

This paper is meant as supplementary information to my joint talk *Analyzing a modern cryptographic RFID system* with Henryk Plötz at the 27th Chaos Communication Congress in Berlin, December 2010. Please visit http://openpcd.org/HID_iClass_demystified for updated information.

[1] 24C3 - Mifare Classic, Little security despite obscurity: http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html

[2] 26C3 - Legic Prime, Obscurity in Depth: http://events.ccc.de/congress/2009/Fahrplan/events/3709.en.html

[3] *iCLASS*™ Levels of Security: http://goo.gl/AUWOP

A. Standard Security

Standard Security mode means that two common secret keys are shared across all HID readers in that Mode. The supplied cards contain a unique combination of a card ID and a per-facility ID. A reader in a Standard Security mode will therefore successfully authenticate all Standard Security iCLASS cards and will send the stored card ID and facility ID, usually in Wiegand format, to the upstream system.

The upstream system decides based on the transmitted data if the card is part of the system and determines the access level.

***Abstract*—This paper provides detailed information on *iCLASS*™ reader and key security. It explains the security problems found without revealing the extracted secret keys (DES authentication Key and the 3DES data encryption key for *iCLASS*™ Standard Security cards).**

The chosen approach of not releasing the encryption and authentication keys gives iCLASS vendors and customers an important headstart to update readers and cards to High Security mode in order to stop attackers from forging, reading and cloning iCLASS Standard Security cards.

This paper also explains, how Standard Security and High Security keys were extracted from a RW400 reader without leaving visible traces.

master ▾ hid-iclass-key / key

Go to file ···

ss23 Add global HID iClass key — Latest commit 5d46cda on Nov 17, 2016 — History

1 contributor

1 lines (1 sloc) | 17 Bytes — Raw | Blame

```
1  3F[redacted]
```

ΦSV

Demo!



Questions?

Ege F
ege@physsec.org

Andrew M
andrew@physsec.org



Where to find a Proxmark:
dangerousthings.com

Where to find the software:
proxmarkbuilds.org

Where to find tutorials:
Iceman on YouTube

(Not affiliated.)