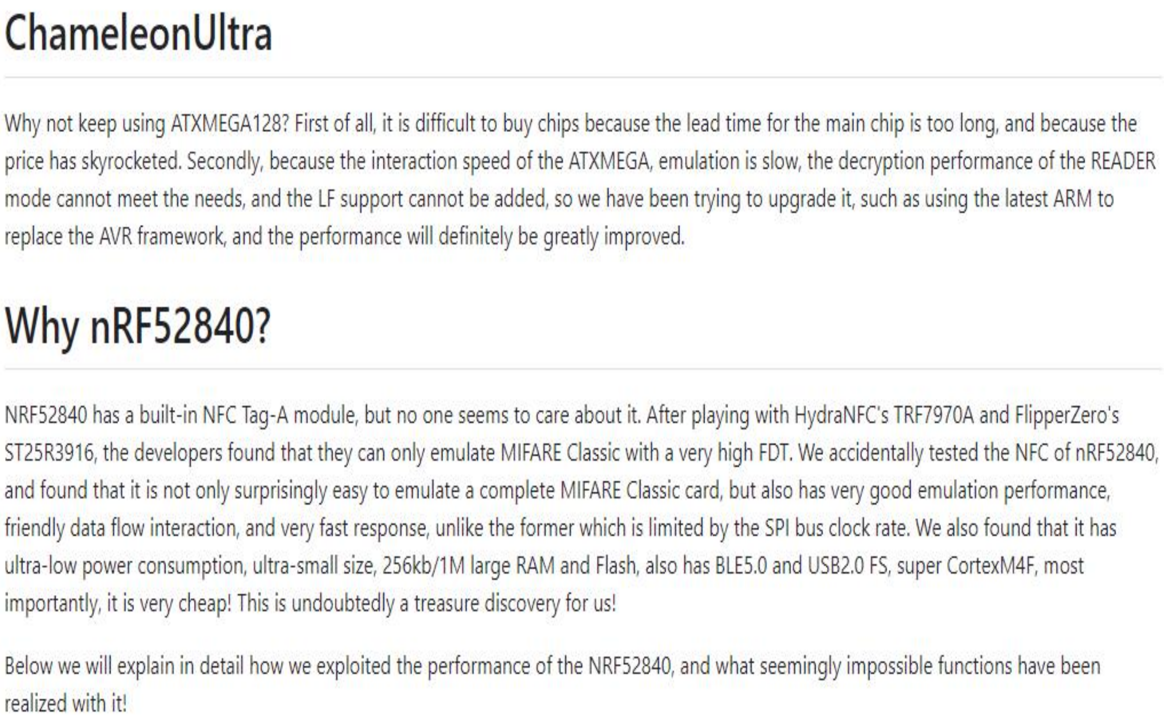


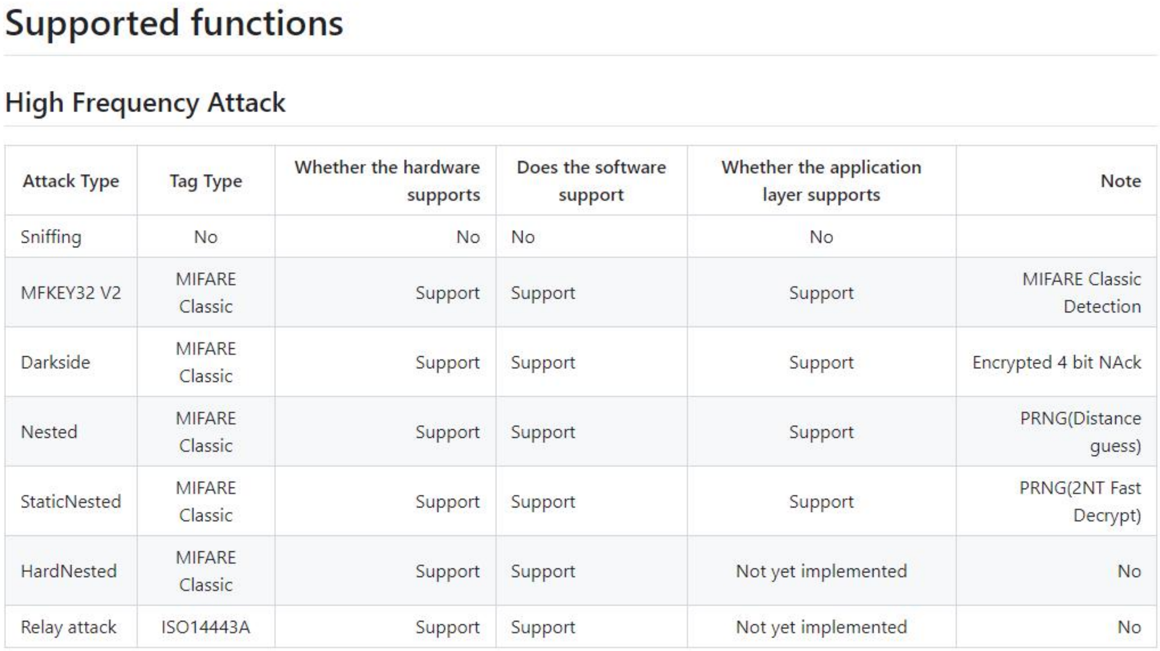
ChameleonUltra

Why not keep using ATXMEGA128? First of all, it is difficult to buy chips because the lead time for the main chip is too long, and because the price has skyrocketed. Secondly, because the interaction speed of the ATXMEGA, emulation is slow, the decryption performance of the READER mode cannot meet the needs, and the LF support cannot be added, so we have been trying to upgrade it, such as using the latest ARM to replace the AVR framework, and the performance will definitely be greatly improved.

Why nRF52840?

NRF52840 has a built-in NFC Tag-A module, but no one seems to care about it. After playing with HydraNFC's TRF7970A and FlipperZero's ST25R3916, the developers found that they can only emulate MIFARE Classic with a very high FDT. We accidentally tested the NFC of nRF52840, and found that it is not only surprisingly easy to emulate a complete MIFARE Classic card, but also has very good emulation performance, friendly data flow interaction, and very fast response, unlike the former which is limited by the SPI bus clock rate. We also found that it has ultra-low power consumption, ultra-small size, 256kb/1M large RAM and Flash, also has BLE5.0 and USB2.0 FS, super CortexM4F, most importantly, it is very cheap! This is undoubtedly a treasure discovery for us!

Below we will explain in detail how we exploited the performance of the NRF52840, and what seemingly impossible functions have been realized with it!



Supported functions

High Frequency Attack

Attack Type	Tag Type	Whether the hardware supports	Does the software support	Whether the application layer supports	Note
Sniffing	No	No	No	No	
MFKEY32 V2	MIFARE Classic	Support	Support	Support	MIFARE Classic Detection
Darkside	MIFARE Classic	Support	Support	Support	Encrypted 4 bit NAck
Nested	MIFARE Classic	Support	Support	Support	PRNG(Distance guess)
StaticNested	MIFARE Classic	Support	Support	Support	PRNG(2NT Fast Decrypt)
HardNested	MIFARE Classic	Support	Support	Not yet implemented	No
Relay attack	ISO14443A	Support	Support	Not yet implemented	No

High Frequency emulation

Card Type	Encoding Type	Whether the hardware supports	Does the software support	Whether the application layer supports	Note
Other than ISO14443A	No	No	No	No	NRF52 NFC Module
NTAG 21x (210-218)	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Ultralight	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Ultralight Ev1	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Ultralight C	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Classic1K/2K/4K (4B/7B)	ISO14443A/106 kbit/s	Support	Support	Support	
MIFARE DESFire	ISO14443A High Rate	Only supported Low rate	Only supported Low rate	Not yet implemented	
MIFARE DESFire EV1	ISO14443A High rate	Only supported Low rate	Only supported Low rate	Not yet implemented	Backward compatible
MIFARE DESFire EV2	ISO14443A High rate	Only supported Low rate	Only supported Low rate	Not yet implemented	
MIFARE Plus	ISO14443A High rate	Only supported Low rate	Only supported Low rate	Not yet implemented	

High Frequency Reader

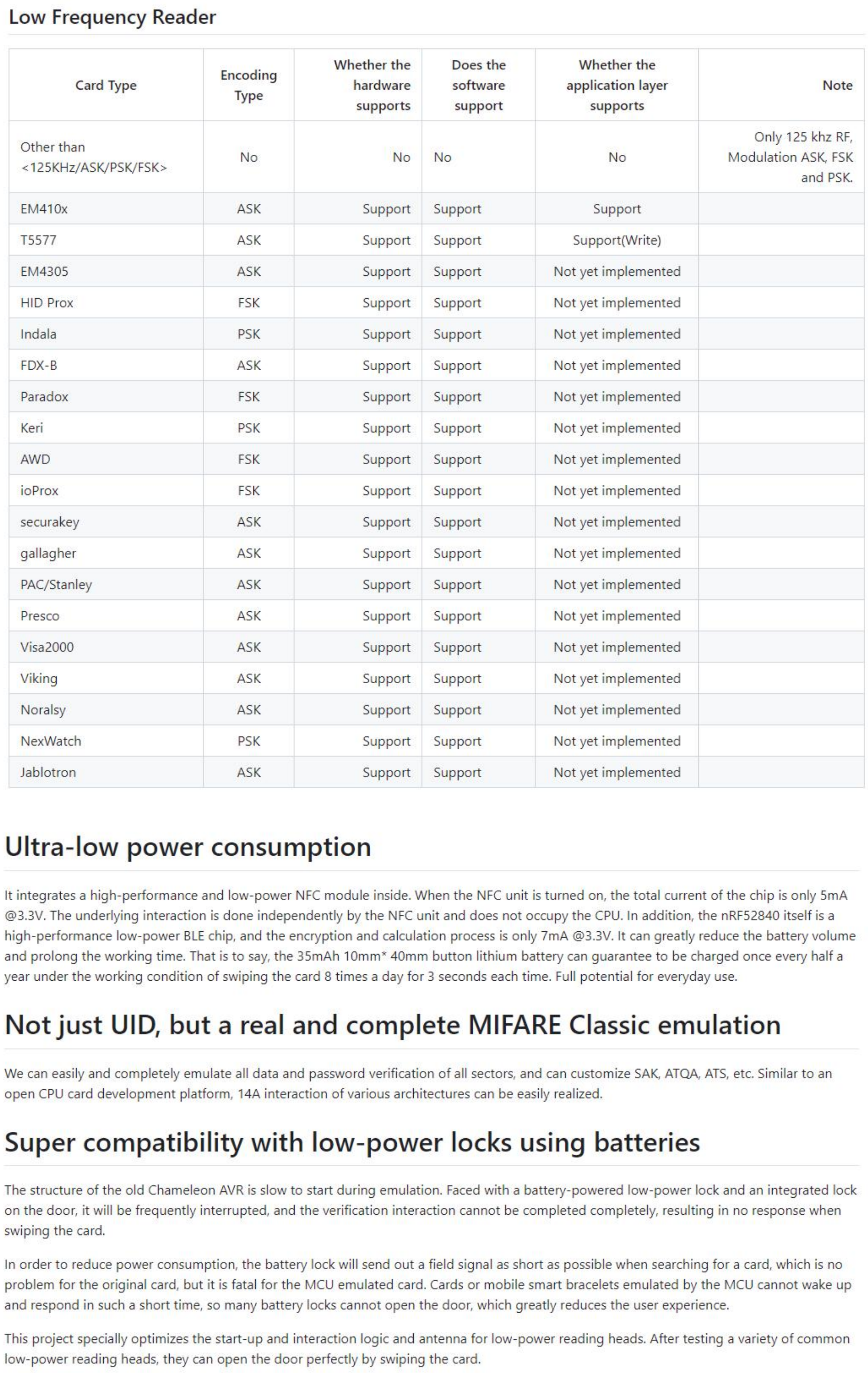
Card Type	Encoding Type	Whether the hardware supports	Does the software support	Whether the application layer supports	Note
Non <13.56MHz or ISO14443A>	No	No	No	No	NXP RC522 Datasheet
NTAG 21x (210-218)	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Ultralight	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Ultralight Ev1	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Ultralight C	ISO14443A/106 kbit/s	Support	Support	Not yet implemented	
MIFARE Classic 1K/2K/4K (4B/7B)	ISO14443A/106 kbit/s	Support	Support	Support	
MIFARE DESFire	ISO14443A High Rate	Supports low rates, or possibly higher rates	Supports low rates, or possibly higher rates	Not yet implemented	
MIFARE DESFire EV1	ISO14443A High rate	Supports low rates, or possibly higher rates	Supports low rates, or possibly higher rates	Not yet implemented	Backward compatible
MIFARE DESFire EV2	ISO14443A High rate	Supports low rates, or possibly higher rates	Supports low rates, or possibly higher rates	Not yet implemented	
MIFARE Plus	ISO14443A High rate	Supports low rates, or possibly higher rates	Supports low rates, or possibly higher rates	Not yet implemented	

Low Frequency Attack

Vulnerability Type	Tag Type	Whether the hardware supports	Does the software support	Whether the application layer supports	Note
Sniffing	125KHz	Support	Support	Not yet implemented	
Brute Force	EM410x ID	Support	Support	Not yet implemented	

Low Frequency emulation

Card Type	Encoding Type	Whether the hardware supports	Does the software support	Whether the application layer supports	Note
Other than <125KHz/ASK/PSK/FSK>	No	No	No	No	Only 125 khz RF, Modulation ASK, FSK and PSK.
EM410x	ASK	Support	Support	Support	EM4100 is support(AD 64bit)
T5577	ASK	Support	Support	Not yet implemented	
EM4305	ASK	Support	Support	Not yet implemented	
HID Prox	FSK	Support	Support	Not yet implemented	
Indala	PSK	Support	Support	Not yet implemented	
FDX-B	ASK	Support	Support	Not yet implemented	
Paradox	FSK	Support	Support	Not yet implemented	
Keri	PSK	Support	Support	Not yet implemented	
AWD	FSK	Support	Support	Not yet implemented	
ioProx	FSK	Support	Support	Not yet implemented	
securakey	ASK	Support	Support	Not yet implemented	
gallagher	ASK	Support	Support	Not yet implemented	
PAC/Stanley	ASK	Support	Support	Not yet implemented	
Presco	ASK	Support	Support	Not yet implemented	
Visa2000	ASK	Support	Support	Not yet implemented	
Viking	ASK	Support	Support	Not yet implemented	
Noralsy	ASK	Support	Support	Not yet implemented	
NexWatch	PSK	Support	Support	Not yet implemented	
Jablotron	ASK	Support	Support	Not yet implemented	



Low Frequency Reader

Card Type	Encoding Type	Whether the hardware supports	Does the software support	Whether the application layer supports	Note
Other than <125KHz/ASK/PSK/FSK>	No	No	No	No	Only 125 khz RF, Modulation ASK, FSK and PSK.
EM410x	ASK	Support	Support	Support	
T5577	ASK	Support	Support	Support(Write)	
EM4305	ASK	Support	Support	Not yet implemented	
HID Prox	FSK	Support	Support	Not yet implemented	
Indala	PSK	Support	Support	Not yet implemented	
FDX-B	ASK	Support	Support	Not yet implemented	
Paradox	FSK	Support	Support	Not yet implemented	
Keri	PSK	Support	Support	Not yet implemented	
AWD	FSK	Support	Support	Not yet implemented	
ioProx	FSK	Support	Support	Not yet implemented	
securakey	ASK	Support	Support	Not yet implemented	
gallagher	ASK	Support	Support	Not yet implemented	
PAC/Stanley	ASK	Support	Support	Not yet implemented	
Presco	ASK	Support	Support	Not yet implemented	
Visa2000	ASK	Support	Support	Not yet implemented	
Viking	ASK	Support	Support	Not yet implemented	
Noralsy	ASK	Support	Support	Not yet implemented	
NexWatch	PSK	Support	Support	Not yet implemented	
Jablotron	ASK	Support	Support	Not yet implemented	

Ultra-low power consumption

It integrates a high-performance and low-power NFC module inside. When the NFC unit is turned on, the total current of the chip is only 5mA @3.3V. The underlying interaction is done independently by the NFC unit and does not occupy the CPU. In addition, the nRF52840 itself is a high-performance low-power BLE chip, and the encryption and calculation process is only 7mA @3.3V. It can greatly reduce the battery volume and prolong the working time. That is to say, the 35mAh 10mm* 40mm button lithium battery can guarantee to be charged once every half a year under the working condition of swiping the card 8 times a day for 3 seconds each time. Full potential for everyday use.

Not just UID, but a real and complete MIFARE Classic emulation

We can easily and completely emulate all data and password verification of all sectors, and can customize SAK, ATQA, ATS, etc. Similar to an open CPU card development platform, 14A interaction of various architectures can be easily realized.

Super compatibility with low-power locks using batteries

The structure of the old Chameleon AVR is slow to start during emulation. Faced with a battery-powered low-power lock and an integrated lock on the door, it will be frequently interrupted, and the verification interaction cannot be completed completely, resulting in no response when swiping the card.

In order to reduce power consumption, the battery lock will send out a field signal as short as possible when searching for a card, which is no problem for the original card, but it is fatal for the MCU emulated card. Cards or mobile smart bracelets emulated by the MCU cannot wake up and respond in such a short time, so many battery locks cannot open the door, which greatly reduces the user experience.

This project specially optimizes the start-up and interaction logic and antenna for low-power reading heads. After testing a variety of common low-power reading heads, they can open the door perfectly by swiping the card.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception,

which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the separation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.

The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction