CHAMELEON By Proxgrind

B. Quick Crash Course

You are here: Home / B. Quick Crash Course

Quick Crash Course

1.Detect keys and upload card files

(1) Prepare the computer GUI or Android APP.

Computer GUI download address: http://www.icesql.se/download/ChameleonMiniGUI/publish.htm

Source: https://github.com/iceman1001/ChameleonMini-rebootedGUI

Android APP download address:

Google Store: https://play.google.com/store/apps/details?id=com.proxgrind.chameleon

(2) Connect the Chameleon MINI or TINY using the Android APP.

USB port direct connection: Both the Chameleon MINI and TINY support direct connection to the mobile phone USB port. For the MINI, an additional OTG adapter needs to be purchased. TINY uses its own dual-headed TYPEC data cable to connect directly to TYPEC mobile phones.

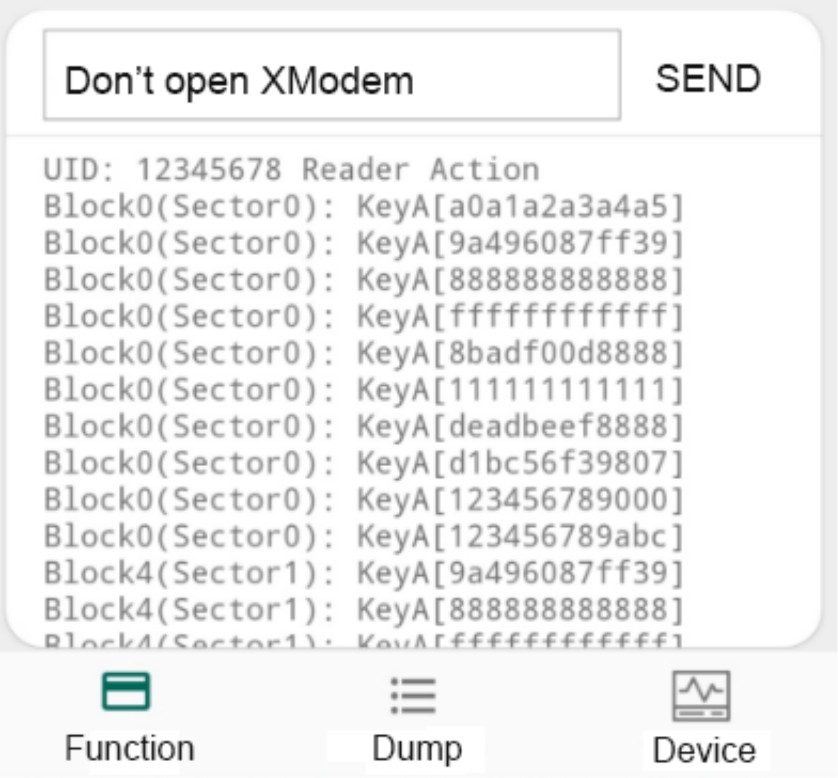
Bluetooth connection: Chameleon MINI has built-in Bluetooth BLE4.0. Press any button first to wake up Bluetooth. Turn on Bluetooth on your Android phone and the app will automatically connect.

(3) Use Android APP to enable detection mode.

After connecting, click on a single card slot and select DETECTION_1K or 4K in the “card slot mode”. This card slot has the detection mode turned on. Write the original card number in the “UID Card Number” column. Click “Write.” If you don’t know the UID number, you can fill in it at will. Then click the “Clear” button below to clear the last detection record.

(4) Use Android APP to get keys.

. At this time, connect back to the mobile phone and click the “crack” button. After few seconds, the app will automatically solve and list the results, as shown in the figure below:



```
UID: 12345678 Reader Action
Block0(Sector0): KeyA[a0a1a2a3a4a5]
Block0(Sector0): KeyA[9a496087ff39]
Block0(Sector0): KeyA[888888888888]
Block0(Sector0): KeyA[ffffffffffff]
Block0(Sector0): KeyA[8badf00d8888]
Block0(Sector0): KeyA[111111111111]
Block0(Sector0): KeyA[deadbeef8888]
Block0(Sector0): KeyA[d1bc56f39807]
Block0(Sector0): KeyA[123456789000]
Block0(Sector0): KeyA[123456789abc]
Block4(Sector1): KeyA[9a496087ff39]
Block4(Sector1): KeyA[888888888888]
Block4(Sector1): KeyA[ffffffffffff]
```

The list shows which blocks the read head just visited, and what password was used for each access.

At this point, click the “History” button, the APP will automatically list the keys separately and copy it automatically for easy copying to other software for next use.

If your mobile phone comes with NFC function, you can directly put the original card on the mobile phone NFC at this time, the APP will automatically use the key in the list to read the entire card, and after successful, it will automatically save the entire card data file on the mobile phone. .

Note: Multiple red LEDs are on at the same time during detection, which means the memory is full, just clear the memory.

(5) Use Android APP to import existing card data files in batches.

Use QQ to send the card data file to the mobile phone QQ, or connect the mobile phone to the computer and transfer the file to any directory on the mobile phone.

Open the app, click the “DUMP” column below, click the “SCanner” in the “plus sign” in the upper right corner, click the three horizontal line buttons in the upper left corner, and select this phone. Then select the root directory of the QQ receiving file or the previously copied directory, and click Allow Access. All card data files will be automatically scanned into the “DUMP file” interface, which can be uploaded or edited at will.

Click the card data file in the “DUM” column below, and click “Upload” below to upload to the card slot corresponding to the chameleon.

Introduction to UID mode and SAK mode

(1) UID mode

After the UID mode is turned on, the card simulated by Chameleon will become a GEN1a card, commonly known as a UID card, Chinese magic card.

Global card slot takes effect.

How to open: Click the button “UID Changeable (GEN1a)” in the APP or directly send the command “UIDMODE = 1” to turn it on, and “UIDMODE = 0” to turn it off.

(2) SAK mode

After the SAK mode is turned on, the card will feedback the real SAK value when it is being found. The SAK value is determined by the 0 sector and 0 block, and the position is the position of the sixth byte immediately after the UID number. If the SAK mode is not turned on, the SAK is a fixed value of 08, and 0 blocks of data are ignored.

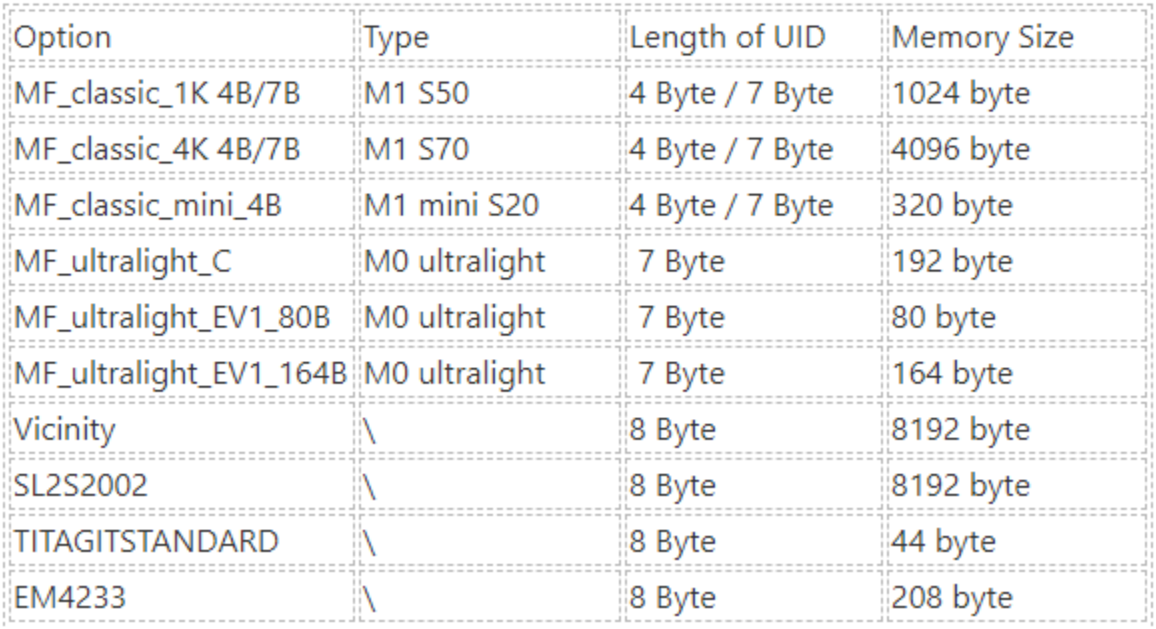
This function is used to meet the situation that some cards with special SAK values cannot be used normally after being copied, and can achieve better compatibility.

The current card slot takes effect.

How to open: Click the “SAK Mode” button in the APP or directly send the command “SAKMODE = 1” to turn it on, and “SAKMODE = 0” to turn it off.

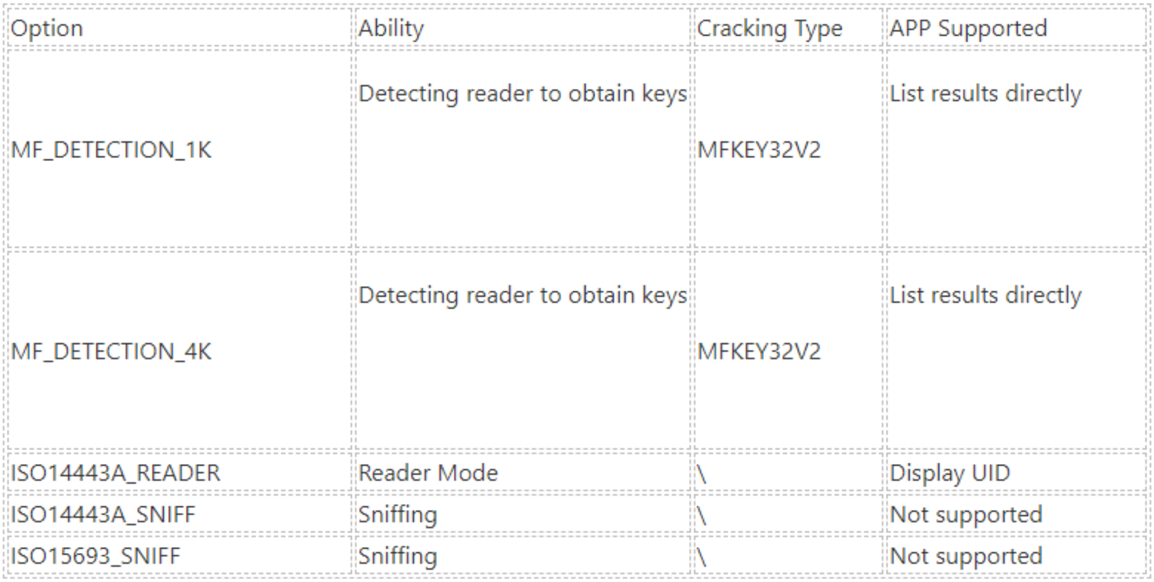
3. Card slot function introduction

UID Card Function Class



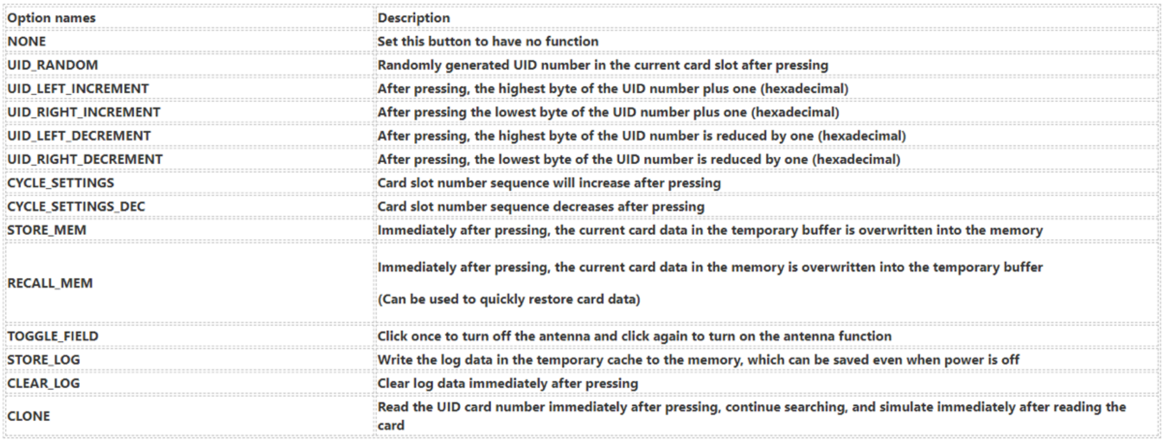
Option	Type	Length of UID	Memory Size
MF_classic_1K 4B/7B	M1 S50	4 Byte / 7 Byte	1024 byte
MF_classic_4K 4B/7B	M1 S70	4 Byte / 7 Byte	4096 byte
MF_classic_mini_4B	M1 mini S20	4 Byte / 7 Byte	320 byte
MF_ultralight_C	M0 ultralight	7 Byte	192 byte
MF_ultralight_EV1_80B	M0 ultralight	7 Byte	80 byte
MF_ultralight_EV1_164B	M0 ultralight	7 Byte	164 byte
Vicinity	\	8 Byte	8192 byte
SL2S2002	\	8 Byte	8192 byte
TITAGITSTANDARD	\	8 Byte	44 byte
EM4233	\	8 Byte	208 byte

Cracking and card reading functions



Option	Ability	Cracking Type	APP Supported
MF_DETECTION_1K	Detecting reader to obtain keys	MFKEY32V2	List results directly
MF_DETECTION_4K	Detecting reader to obtain keys	MFKEY32V2	List results directly
ISO14443A_READER	Reader Mode	\	Display UID
ISO14443A_SNIFF	Sniffing	\	Not supported
ISO15693_SNIFF	Sniffing	\	Not supported

4. Button Custom Function Introduction



Option names	Description
NONE	Set this button to have no function
UID_RANDOM	Randomly generated UID number in the current card slot after pressing
UID_LEFT_INCREMENT	After pressing, the highest byte of the UID number plus one (hexadecimal)
UID_RIGHT_INCREMENT	After pressing the lowest byte of the UID number plus one (hexadecimal)
UID_LEFT_DECREMENT	After pressing, the highest byte of the UID number is reduced by one (hexadecimal)
UID_RIGHT_DECREMENT	After pressing, the lowest byte of the UID number is reduced by one (hexadecimal)
CYCLE_SETTINGS	Card slot number sequence will increase after pressing
CYCLE_SETTINGS_DEC	Card slot number sequence decreases after pressing
STORE_MEM	Immediately after pressing, the current card data in the temporary buffer is overwritten into the memory
RECALL_MEM	Immediately after pressing, the current card data in the memory is overwritten into the temporary buffer (Can be used to quickly restore card data)
TOGGLE_FIELD	Click once to turn off the antenna and click again to turn on the antenna function
STORE_LOG	Write the log data in the temporary cache to the memory, which can be saved even when power is off
CLEAR_LOG	Clear log data immediately after pressing
CLONE	Read the UID card number immediately after pressing, continue searching, and simulate immediately after reading the card