AN12265

MIFARE Ultralight C security design and its impact on chip performance

Rev. 1.2 — 5 May 2021
183612

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	Authentication, communication distance, MIFARE Ultralight C, resonance frequency, power consumption, side channel attack, secure crypto implementation, 3DES.
Abstract	This document addresses the reason behind the higher power consumption of MIFARE Ultralight C over MIFARE Ultralight, and highlights other security relevant topics and best practices.

1 Revision history

Revision history

Rev	Date	Description
1.2	20210505	AN number changed to AN12265, security status changed into company public
1.1	20210223	Update recommended implementation of anti-tearing supported features(Counter, OTP and Lock bytes)
1.0	20091116	Initial version

2 Introduction

MIFARE Ultralight C [1] is functionally compatible to MIFARE Ultralight EV1 [2][1]. The IC offers 3-pass mutual authentication between the terminal and the chip itself. The authentication is based on Triple DES crypto (3DES) with a 112-bit key length (2k3DES).

Nevertheless, due to increased security requirements implied by the protection of the 3DES key, the MIFARE Ultralight C design shows some differences compared to MIFARE Ultralight design. In order to minimize the impact of chip differences for the customer designs and ease the transition from existing MIFARE Ultralight systems to MIFARE Ultralight C systems, this document highlights the differences between the two products.

2.1 Organization of the document

Chapter 3 addresses the consequence of secure design on energy performance of the chip, and the system design implications of such secure designs. **Chapter 4** addresses recommendations on the usage of anti-tearing supported memory elements. In **Chapter 5**, general recommendations about adding confidentiality and integrity on data stored in the memory are shown.

This application note does not replace any other relevant application note or functional specification wherever it applies.

2.2 Disclaimer

Note that whenever terms are used like locking, read-only, fraud protection, security feature and the like, this does not imply that there would never be any attack possible to circumvent the feature.

MIFARE Ultralight C is not a security certified product. Depending on the value of the assets that need to be protected, one may consider using Common Criteria certified products with security features that have been demonstrated to resist certain attack potential during certification (e.g. MIFARE Plus and MIFARE DESFire have CC high attack potential profile and MIFARE DESFire Light has CC enhanced-basic attack potential profile)

2.3 References

[1] Product data sheet MIFARE Ultralight C (MF0ICU2), DocStore number 1376xx.

[2] Product data sheet MF0ULX1- MIFARE Ultralight EV1 - contactless ticket IC, DocStore number 2355xx

[3] Kocher P., Jaffe J., Jun B., Differential power analysis, CRYPTO'99, Lecture Notes in Computer Science 1666. Springer-Verlag, 388{397, also: Introduction to differential power analysis and related attacks, http://www.cryptography.com/dpa/

[4] Thomas S. Messerges, Ezzy A. Dabbish, Robert H. Sloan1: Investigations of Power Analysis Attacks on Smartcards, USENIX Technical Program - Paper - Smartcard 99, https://www.usenix.org/legacy/events/smartcard99/full_papers/messerges/messerges_html/

[1] Footnote: Initial first version of MIFARE Ultralight is EOL (End of Life) since 2017. Successor product is MIFARE Ultralight EV1.

[5] SINCE Project, Security and Threat Evaluation Relating to Contactless Cards, eESC Common Specification v2, volume 6, part 2, November 2002. https://www.eurosmart.com/

[6] CMAC specification: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

2.4 Symbol and abbreviated terms

Table 1. Abbreviations

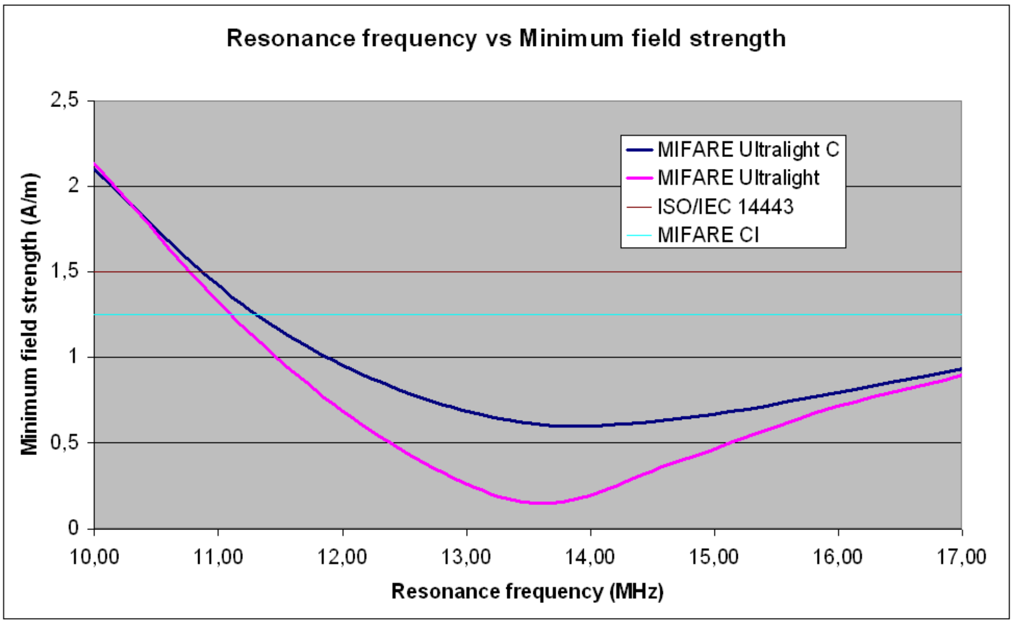
Acronym	Description
3DES	Three times DES, it is also known as TDES
ACK	Positive ACKnowledgement
ATQA	Answer To reQuest, Type A
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
FDT	Frame Delay Time
HLTA	HALT Command, Type A
LSB	Lowest Significant Byte
LSb	Lowest Significant bit
NAK	Negative AcKnowledgement
PCD	Proximity Coupling Device
PICC	Proximity Card
REQA	REQuest Command, Type A
SPA	Simple Power analysis
DPA	Differential Power analysis
HODPA	High order DPA

3 Consequence of security features on energy performance of the chip

If we compare the initial version of MIFARE Ultralight (no cryptographic algorithm) and MIFARE Ultralight C (implemented 2kTDES) on same antenna design, differences can be observed.

In every case the required field strength is according to ISO/IEC 14443, < 1.5 A/m.

Figure 1 shows the dependency between minimum operating field strength and the resonance frequency of the card.



1. Based on ID-1 size PICC antenna. The analysis shows clearly, it is possible to improve the communication distance by well tuned card antenna.

Figure 1. MIFARE Ultralight and Ultralight C minimum field strength over resonance frequency

3.1 Implications on system design

If same physics is applied for MIFARE Ultralight and MIFARE Ultralight C inlay (card, coin, key fobs, and ticket) design and presented in the same reader (terminal), reading distance is decreased for MIFARE Ultralight C. The percentage of reduction of reading distance depends on the reader and inlay physics.

There are different options available to compensate this security feature related effects. In the following, some options are given.

- The antenna size can be made as big as possible within the inlay. May be more to the outer side of the card/ticket as possible.
- The loaded threshold frequency can be defined as close as possible to operating frequency (13.56 MHz).
- Increasing the quality factor of the card antenna as much as possible by keeping the resonance frequency as described in [6].

- Inserting capacitor (in parallel or series depends on the reader/application) may help to increase the communication distance. Refer to the antenna design guide [6] and/or contact the NXP technical support team.
- The reader or terminal can be adapted to emit more power, if possible.

3.2 Conclusion

If applying the same antenna as for the initial version of MIFARE Ultralight on MIFARE Ultralight C, the decrease in performance can be expected. In order to avoid any system relevant degradation of the card performance, the antenna design used has to be reviewed under aspects shown in this document.

The higher energy consumption of MIFARE Ultralight C could have more influence on smaller antenna formats, where energy is already scarcely available. Furthermore, many readers in the field are, and this is especially relevant as antenna size decreases, limited in their output power. Here the matching between the reader and card antenna size also plays a role, therefore the complete system should be evaluated for any implications before assuming that MIFARE Ultralight C can be a replacement of existing MIFARE Ultralight designs.

4 MIFARE Ultralight C anti-tearing implementation

The MIFARE Ultralight C implements anti-tearing for 16-bit counter, OTP and lock bits (see [1]). This means that in case of a tear-off event either the old value or the new (just written) value is present. This section describes what measures a MIFARE Ultralight C application needs to implement in order to ensure the best tear-off support for the user data pages.

For the tearing application implementation, 2 memory areas having the same size are needed see Figure 2.

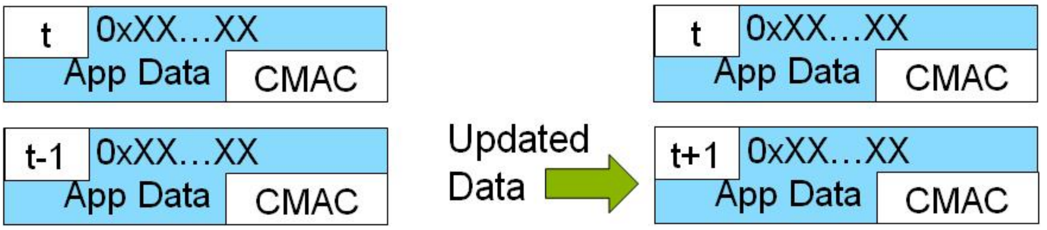


Figure 2. possible anti tearing implementation

The application data is stored in 2 memory locations. The application data also contains a timestamp indicated in white and a CMAC (that can be calculated as indicated in [6]). Every time a new update is needed i.e. new data has to be written, only the set of data with the older timestamp is updated. The CMAC is added to guarantee the integrity of the written application data.

In particular, the Figure 2 shows a typical update of the Application Data done on the older Application Data set (timestamp = t-1). As soon as the new application data is written, the timestamp is updated (timestamp = t+1) and the CMAC is also written.

If the update operation fails due to a tearing event and the application data becomes corrupted, this can be recognized based on the failure of the CMAC validation. In any case, the MIFARE Ultralight C either contains the latest updated application data (timestamp = t+1) or the previous one (timestamp = t).

4.1 Recommended system implementations of tearing supported features

MIFARE Ultralight C supports anti-tearing mechanisms for counter, OTP bits and Lock bits for tearing events that may occur during normal operation in the field. Security researches continuously advise the industry by publishing new attack vectors to advocate for higher secure products and implementation of system level countermeasures. Additional measures should be considered depending on the configuration and use case.

Table 2. System level countermeasures

Tearing supported features of MIFARE Ultralight C	Product and system level recommendation
16-bit counter	1. Protect counter by DES authentication 2. Use Backend fraud detection e.g. deny listing of suspicious tickets based on UID. Once an unexpected counter decrease is seen on a specific UID, the card can be deny listed in the backend and will not be accepted anymore. 3. Disable the tickets when the maximum value of counter is reached. 4. Start counting from high value, e.g. 0xFFF5 = 10 trips. Also make sure to apply recommendation 3) in this case. If migration from an old to a new system is to be done, then make sure that the system can reliable differentiate between cards in the old and the new situation in a way that cannot be misused by adversaries.
OTP bits *(One-Time-Programmable bits)*	1. Protect OTP by DES authentication 2. In case OTP is used as counter, see below. Use a structure in programming of the bits (e.g. from left to right), and reject tickets not following this scheme. When counter is depleted then set all OTP bits (0xFFFFFFFF) **twice** [1] . If a depleted counter should be different from 0xFFFFFFFF, then set the the OTP lock bit **twice** once the counter has reached its target. 3. In case OTP does not need to be changed anymore then lock it. To do so, set the OTP lock bit and all block-locking bits and write this **twice**
Lock bits *(represent the field programmable read-only locking mechanism)*	1. Protect lock bits by DES authentication 2. Set all block-locking bits **twice**

[1] Writing those bits twice makes sure that the value is also written in the internal backup page

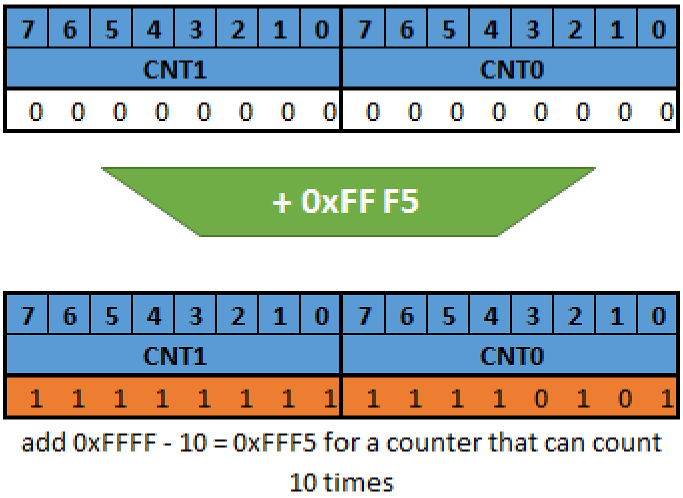
The proposed countermeasures can be applied on the IC by setting all block-locking bits and use of DES authentication. Of importance is also, that the programming of the block-locking bits and the OTP area is done twice to ensure a permanent lock. The reason for this is, that it makes sure the internal backup page is also updated correctly.

System level countermeasures in general have an impact on the infrastructure (reader and backend system) and can require the storage of some extra information in the contactless card to increase the system security overall. In general these countermeasures, e.g. calculation of a CMAC over protected data can be implemented on any contactless card type, unless the storage capacity of the card is too limited to store all extra data. (see Section 4)

4.2 Recommended 16-bit one-way counter implementation including countermeasures

To decrease the possibility for data manipulation in applications and to allow for the detection of manipulated counter values on the three independent anti-tearing supported 16-bit one-way counters following implementations and countermeasures shall be considered:

- Define the start value of the three independent 16-bit one-way counters at the highest possible counter value during personalization, by considering the required counts in application. That can be applied, by setting the counter value to the maximum 0xFF FF minus the number of counts allowed in the system, e.g. set the counter value to 0xFF F5. The counter value of 0xFF F5 allows 10 trips by increase of the value to 0xFF FF (max). (see Figure 3)



7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
CNT1								CNT0							
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
CNT1								CNT0							
1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1

add 0xFFFF - 10 = 0xFFF5 for a counter that can count 10 times

Figure 3. Example of a max. 10 times counter

- Once the counter is at the maximum value (0xFF FF), it is recommended to disable it by issuing an additional INCR_CNT by zero to ensure the maximum value is programmed in both pages. Also if the maximum value in an application is not 0xFF FF, it is recommended to still disable a counter by incrementing to 0xFF FF followed by an additional INCR_CNT by zero.
- Implementation of a data integrity protection on the counter value. The MAC which has been calculated outside the ticket is stored in the user memory on the ticket to give the possibility to detect if there is a malicious change on the counter value.
- Tickets with a low start counter value e.g. 0x 00 00 shall be, if possible, migrated to a high start value e.g. 0x FF F5 as recommended in the first bullet point. It must be made sure that the system can recognize both variants for the transition phase.
- It is recommended to implement countermeasures outside the ticket to support a backend fraud detection mechanism in the infrastructure. It shall give the possibility to detect, based on the UID of MIFARE Ultralight C, if the counter value linked to the ticket (UID) is as expected. If not, the card with this UID shall be immediately rejected in case of online detection. If only offline detection is possible, the card shall be deny-listed for further operations once an inconsistency has been observed.

See also Table 2

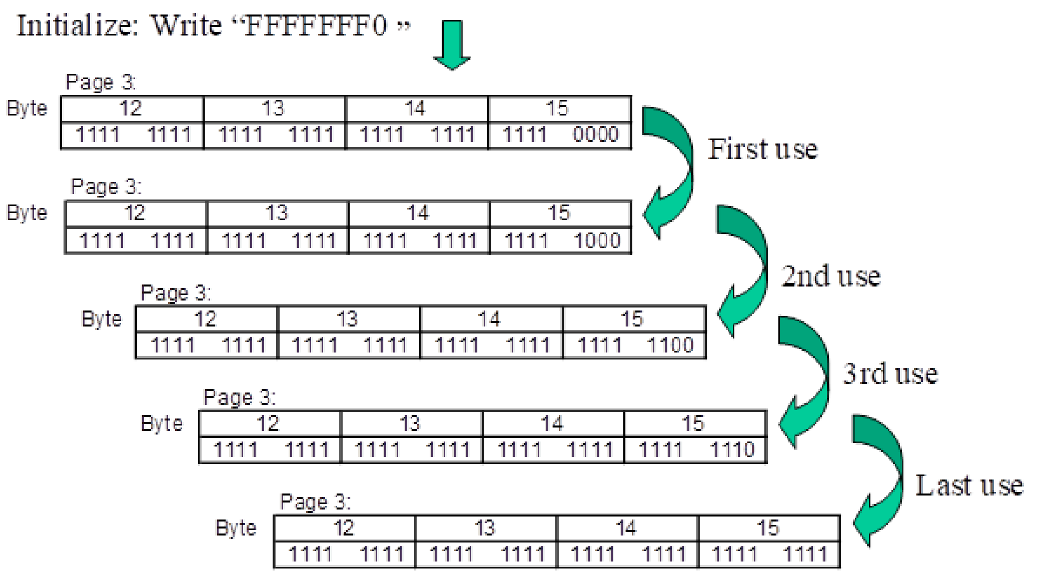
4.3 Recommended implementation of One-Time Programmable bits as counter

The MIFARE Ultralight C offers the possibility to use the OTP bytes in page 03h as counter. All bits of the OTP bytes are pre-set to “0” at the delivery. These bits can be set one time to “1”. This gives the possibility to interpret them as a counter e.g. in a public transport use case to count the number of trips. Therefore, the number of “1” in OTP area of page 03h can be considered as counter value, beside the 16-bit counters on MIFARE Ultralight C. Meaning, the OTP bytes of page 03h offer a number of 32 states that could be used to allow a certain number of passings through a turnstile.

There are different ways the One-Time Programmable bits can be used as counter, but there is one recommended way to implement the counter to identify unintended OTP values. The defined start value of the counter in the OTP area, page 03h is recommended to define at a high value during personalization. That can be applied by setting the counter value to the highest possible value with the remaining trips allowed trips allowed in the system. e.g. set the page 03h of the OTP area to 0xFF FF FF F0. Now, the OTP is pre-set for 4 trips by increase of the value from 0xFF FF FF F0 to 0xFF FF FF FF (max). To disable the counter at the max value of 0xFF FF FF FF, the WRITE or COMPATIBILITY_WRITE command must be applied twice to set the value in both the valid page and the internal backup page to the maximum. (see also Table 2)

4.3.1 Example of the OTP bytes as counter

An example of a 4 trips ticket is shown in Figure 4. For this application, a ticket issuing the OTP memory of the MIFARE Ultralight C has to be pre-set to 0xFFFFFFF0.



Page 3:

Byte	12	13	14	15
	1111 1111	1111 1111	1111 1111	1111 0000

Page 3:

Byte	12	13	14	15
	1111 1111	1111 1111	1111 1111	1111 1000

Page 3:

Byte	12	13	14	15
	1111 1111	1111 1111	1111 1111	1111 1100

Page 3:

Byte	12	13	14	15
	1111 1111	1111 1111	1111 1111	1111 1110

Page 3:

Byte	12	13	14	15
	1111 1111	1111 1111	1111 1111	1111 1111

Figure 4. Example of a four rides ticket

For every access, the 4-byte OTP (page 3) has to be checked and updated (as shown in Figure 4 to ensure the validity of the tickets. The structure of programmed “1” shall be either from left to right or vice versa, to enable the possibility to identify non-compliant counter values. A ticket with OTP value not following this structure, must be rejected.

Additionally, to reduce the chance of fraud on the OTP bytes, it is recommended to support a data integrity protection of the OTP bytes by a CMAC calculated outside the ticket that is stored in the DES protected user memory on the ticket to allow the possibility to identify at a read, if there is an unintended change in the OTP bytes. A CMAC calculation of data including the UID introduces an additional level of data integrity checks against unintended manipulations.

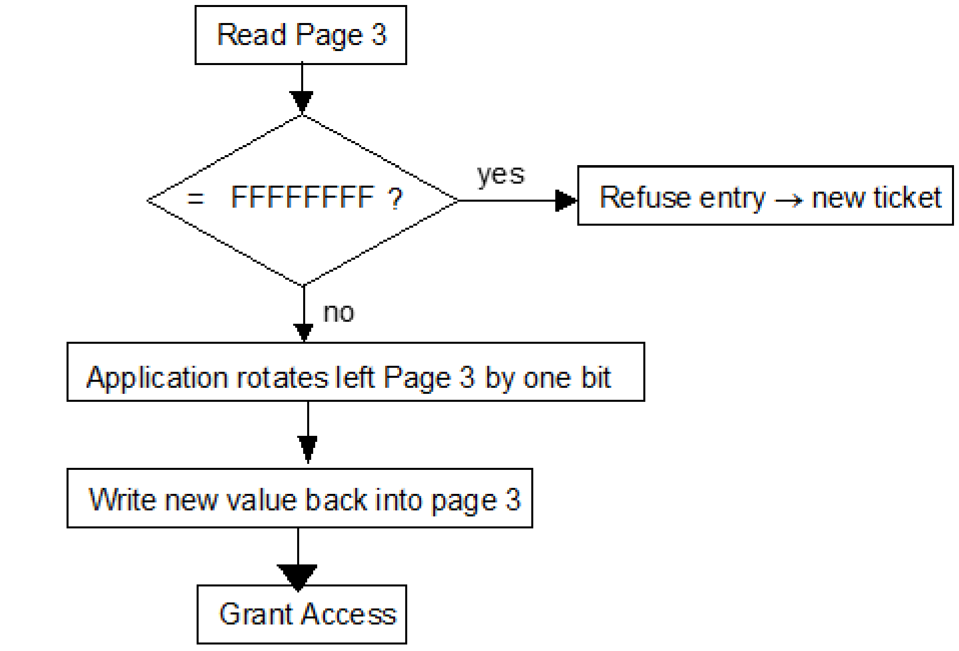

Read Page 3
= FFFFFFFF ?
yes
Refuse entry → new ticket
no
Application rotates left Page 3 by one bit
Write new value back into page 3
Grant Access

Figure 5. Ticket Counter Command flow using left rotation of the value

The example in Table 3 implements a counter that will be filled "from the right side". The current value in page 3 is read and checked, if the counter is not full (not all bits set, e.g. value is not equal to 0xFFFFFFFF). If there are still unset bits, the value is rotated left by one bit and written back to page 3. This will set the next bit left to the current set bits, regardless of the current value[2]. All other bits are kept untouched (existing ones stay ones, as they cannot be reprogrammed, zeros stay zeros). This corresponds to a logic OR of the previous and the rotated value.

Table 3. Left rotation example explained

Step	Comment	Value hex	Value bin
1	Value read from MIFARE Ultralight C page 3	0x0000007F	00000000000000000000000001111111
2	Rotate left by one bit	0x000000FE	00000000000000000000000011111110
3	After writing value of step 2 to page 3 of the MIFARE Ultralight C, one additional bit will be set	0x000000FF	00000000000000000000000011111111

When a maximum of 16 rides need to be possible on one ticket, then some extra protection is possible by introducing some redundancy as is shown in the next example. For a ten times counter, the OTP would be to set to FC00FC00. For each count,

[2] With the initial value “00000000” for 32 times counter, the rotate left at the very first access check after selling the ticket has to be exchanged into another initial WRITE command in order to get the first "1" programmed

two bits should be set (e.g. after first count, the counter value should be FD00FD00, corresponding to the first examples, but with right-rotation, i.e. filling from the left), ideally in one write command (this ensures that a card does not become invalid if a genuine tear-off event happens). Both, the upper and lower half of the 4 bytes always need to be equal. By rejecting OTP values that do not adhere to the expected structure, an additional layer of integrity protection is offered.

5 Confidentiality and Integrity of stored data

Even though MIFARE Ultralight C offers DES authentication, the integrity and confidentiality of the data in the protected part of the memory is not ensured. A so called MitM attack (Man in the Middle) can be used to take over the session after authentication, as the MIFARE Ultralight C does not offer secure messaging based on the authentication. This means, that, depending on the value that a system wants to protect, additional integrity/confidentiality measures may be needed.

5.1 Integrity of stored data

The content of the MIFARE Ultralight C memory lacks guaranteed integrity. To avoid this inconvenience, we propose a MAC to be calculated and appended to the protected data. For this purpose, a CMAC (Cipher-based Message Authentication Code) according to the [NIST SP800-38B] may be a good choice. The complete scheme is shown in Figure 6.

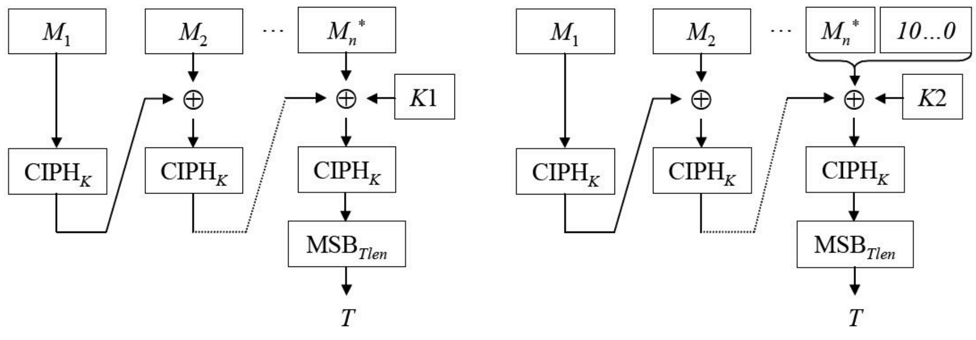


Figure 6. CMAC calculation according to NIST SP800-38. Left side shows input data as a multiple of 16 bytes, right shows padded input data

- The recommended cipher (CIPH) is AES-128.
- Use a secret key (K), which is only known by the reader infrastructure and/or backend.
- The input (M_1 … M_n) is the data to be protected concatenated with the UID, e.g. UID || Data.
- Input data blocks (M_n) need to have a size of 16 bytes. If the number of input data bytes is not a multiple of 16, padding is added acc. NIST SP800-38B (80h following by 00s). This will typically be the case with the UID being 7 bytes and a data page being 4 pages.
- The result of the CMAC calculation is a block of 16 bytes length, which can be truncated to a shorter size as well. Refer to [NIST SP800-38B] for recommendation on the truncation size, but in general, a size below 8 bytes is not recommended for general applications.

By storing the (truncated) CMAC together with the protected user data in the MIFARE Ultralight C user memory, the data is protected against manipulation, as long as the key is kept secret. Including the UID in the MAC calculation, ensures a different MAC is required for each card, even if the protected data is the same. This supports detecting that data has been copied from one MIFARE Ultralight C to another. Alternatively, the UID can also be included via a key diversification step, as outlined in Section 5.2.

Note that this method does not protect against recording the combination of old content and a valid MAC, and writing it back to the card at a later point of time (i.e. a so-called replay attack). Additional measures can be taken by e.g. including a monotonically increasing counter in the user data and maintaining and checking this in the reader and/or back-end infrastructure. There may also remain residual risks of integrity protected data being copied to a clone or emulator. If more high-level security features, like card-integrated cryptographic support are required, other members of the MIFARE card IC family can be used in the application, e.g. the MIFARE Plus EV2 or the MIFARE DESFire EV3.

5.2 Confidentiality of stored data

MIFARE Ultralight C supports a DES authentication to protect the user memory and special memory elements as well, but once authenticated, the session could potentially be taken over by a "Man in the Middle" attack, as no secure messaging is available. This means, that data can be freely available even if it is protected by DES authentication.

If the MIFARE Ultralight C pages can be read without any authentication, anyone can read the pages using any standard reader. But if the stored data is encrypted with a secured key then these are just some bytes to one who does not have the secret key and information regarding the encryption method. Therefore, by storing the encrypted data in MIFARE Ultralight C memory, one can add confidentiality to the data itself.

In general, encryption does not provide integrity protection. Therefore, it is recommended to combine encryption still with a MAC, to also avoid manipulation of the data as also discussed in Section 5.1. The recommended cipher is AES-128. This leads to the following function, composed of the steps described below.

$$Data_{stored} = f\left(Mk, data_{origin}, UID\right)$$

A 16-byte Master Key (Mk) has to be defined by the application provider. For each card, two card keys are derived from the Master Key (Mk):

- Ck_{MAC} for MACing
- CK_{ENC} for encryption

This can be done using the key diversification of [AN10922] including the UID. Including the UID in the key diversification is another method of ensuring unique MACs for each different card (even if the protected data is the same), compared to appending the UID to the input data as described in Section 5.1. For the encryption, this also ensures different ciphertext is generated for different cards, i.e. not disclosing potentially the same plaintext data is stored. Note that including the UID in the encryption, in a similar way as done for the integrity protection method of the previous section, would result in a bigger ciphertext, consuming more storage space on the card. Therefore, key diversification is proposed here.

The steps to be followed for the key diversification are indicated in [AN10922] section 2.2 “AES-128 key” where the inputs to the 128-bit AES key diversification are:

- M: the concatenation of a constant with the 7 bytes UID, i.e. respectively:
  - "$CONST_{MAC}$ || UID" for Ck_{MAC}
  - "$CONST_{ENC}$ || UID" for Ck_{ENC}
- K, the 16 bytes AES-128 Master Key (Mk)

And the output is:

- Diversification Key, respectively the 16 bytes AES-128 bits Ck_{MAC} or Ck_{ENC}

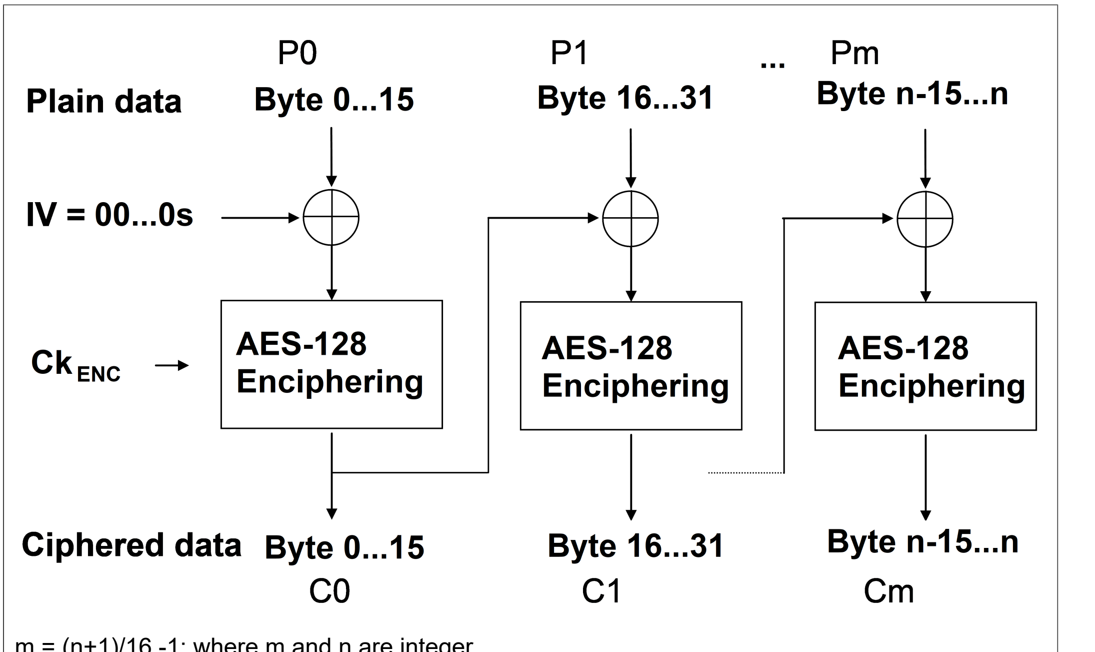
After this step, the plain data is encrypted using the encryption Card Key (Ck_{ENC}) in CBC mode according [NIST SP800-38A].

- Use 16 bytes initial vector (IV) of all ‘00’s, IV= “00...00” (also a random IV can be used. This has the advantage that identical plaintexts would result in a different ciphertext. The drawback is, that the IV needs to be then stored on the ticket as well)
- As AES 128 works with 16-byte block wise, organize the data in multiple of 16 by adding one of the padding schemes of [ISO/IEC 9797-1], e.g. Padding Method 1 which results in padding with all zeros ‘00’. As example (‘xx’ is the data bytes):

```
10 padding bytes: xxxxxxxx xxxx0000 00000000 00000000

15 padding bytes: xx000000 00000000 00000000 00000000
```

The complete CBC encryption scheme is shown in the following figures (Figure 7 for encryption and Figure 8 for decryption):



m = (n+1)/16 -1; where m and n are integer

P = plain 16-byte block

C = ciphered 16-byte block

Figure 7. Data encryption scheme

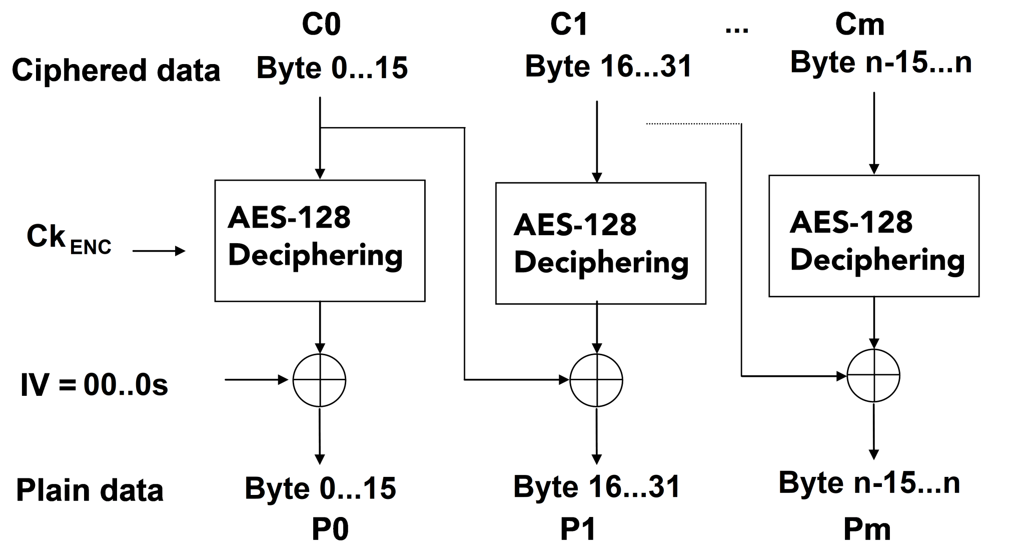


Figure 8. Data decryption scheme

As a final step, a MAC is calculated over the ciphertext. This can be done by applying the CMAC algorithm according [NIST SP800-38B], similar as also used in the previous section, see Figure 6. In this case, Ck_{MAC} is to be applied as the key K, and the ciphertext "C0 … Cn" is the input message M.

Both the ciphertext and the calculated (and eventually truncated) MAC are to be stored on the card.

6 Legal information

6.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

6.3 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

6.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

MIFARE — is a trademark of NXP B.V.

MIFARE Ultralight — is a trademark of NXP B.V.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 5 May 2021
Document identifier: AN12265
Document number: 183612