The ISC Int'l Journal of Information Security

ISeCure

July 2023, Volume 15, Number 2 (pp. 254–259)

http://www.isecure-journal.org

Reverse Engineering of Authentication Protocol in DesFire

Mansoureh Labafniya [1,*], Hamed Yusefi [1], and Akram Khalesi [1]

[1] *Research Center on Developing Advanced Technologies, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: November 23, 2022
Revised: February 26, 2023
Accepted: July 1, 2023
Published Online: July 17, 2023

Keywords:
Contactless Smart Card, EV1, EV2, EV3, MIFARE DESFire, Reverse Engineering, Secure Messaging Authentication Protocol

Type: Research Article

doi: 10.22042/isecure.2023.371284.889

dor: 20.1001.1.20082045.2023.15.2.7.6

ABSTRACT

Nowadays, contactless intelligent cards are extensively used in applications that need strong authentication and security feature protection. Among different cards from different companies, MIFARE DESFire cards are one of the most used cases. The hardware and software design and implementation details of MIFARE DESFire cards are kept secret by their manufacturer. One of the essential functions is authentication which usually its procedure is secret in cards. MIFARE DESFire EV3 is the fourth generation of MIFARE DESFire products which supports integrity and confidential, protected communication. DESFire EV3 is the latest addition to the MIFARE DESFire family of intelligent card chipsets from NXP. This type of card is compatible with MIFARE DESFire D40, EV1, and EV2. The details of the authentication protocols in the MIFARE DESFire EV3 cards with three different secure messaging protocols are introduced in this paper. We use ProxMarak4 to obtain the details of the authentication protocol of the DESFire cards as readers and a custom special-purpose board as a card.

1 Introduction

Over the last few years, more systems based on contactless smart cards are used like personal identification, access control, loyalty, micropayments, and transport systems. Contactless smart cards consist of a small piece of a chip with memory(volatile and non-volatile for processing and storage) and can communicate wirelessly. Most of these cards implement some sort of simple symmetric-key ciphers in hardware or software, making them suitable for applications that require access control to the smart card's memory like smart health cards, membership cards, employee cards, or credit cards [1–3]. There are many parties in smartcards, including a cardholder, terminal, data owner, card manufacturer, card issuer, and software manufacturer [4].

There are different types of cards on the market from different companies. These cards are different in physical size, cost, size of memory, security features, and computational capabilities. One of the most used cases is MIFARE cards from NXP company. According to NXP's report, there are about 200 million MIFARE cards worldwide covering 85 percent of the contactless smartcard market[5]. The MIFARE name covers four families of contactless cards: MIFARE Classic, MIFARE Plus, MIFARE Ultralight, and MIFARE DESFire. MIFARE DESFires contactless cards are adapted to parts 3 and 4 of ISO/IEC 14443 Type A with an operating system from NXP. The DES in the name refers to the use of a DES/3DES and AES encryption; while Fire is an acronym for fast, innovative, reliable, and enhanced with four subtypes:

* Corresponding author.
**This article is an extended/revised version of an ISCISC'18 paper.
Email addresses: Labafnia@rcdat.ac.ir, h.yusefi@rcdat.ac.ir, khalesi@rcdat.ac.ir
ISSN: 2008-2045

MIFARE DESFire D40, MIFARE DESFire EV1, MIFARE DESFire EV2, and MIFARE DESFire EV3. MIFARE DESFire EV3 is the fourth generation of the MIFARE DESFire products family succeeding MIFARE DESFire EV2. It is functionally backward compatible with all previous MIFARE DESFire generations, namely MIFARE DESFire EV2, MIFARE DESFire EV1, and MIFARE DESFire D40 [6].

In this paper, we focus on MIFARE DESFire EV3. We reverse engineer the authentication protocol of MIFARE DESFire EV3, which consists of the authentication protocols of MIFARE DESFire D40, EV1, and EV2 as three different secure messaging.

2 Related Work

Some papers can break algorithms such as AES or Triple-DES (3DES) by side-channel analysis. non-invasive side-channel attacks on the Mifare DESFire MF3ICD40 contactless smartcard, recover the complete 112-bit secret key of the employed 3DES algorithm, using non-invasive power analysis and template attacks[7, 8]. Some other papers do a non-invasive attack like brute-force attacks to discover secret keys[9, 10]. Different non-invasive attacks are also used to discover the procedure of an algorithm, for example, authentication algorithms.

Once a card has been put in the reader's field, the command and response of anti-collision will be sent and received between the card and reader. After successful anti-collision, the command of selecting a particular application will be issued. An authentication procedure must be carried out after selecting the application successfully. This procedure authenticates both the reader and card as possessing a particular key. During authentication, a unique session key is generated, which will be used to either encrypt complete communications or generate a MAC for MAC-type communication.

Authentication protocols are one of the hidden parts of smart cards, although their overall scheme is obvious. D. Garcia *et al.* in [5] reverse-engineered the authentication protocol of the MIFARE Classic chip. Figure 1 shows the details of this communication protocol. They used the ProxMark3 and a custom device for tag emulation and eavesdropping, called Ghost. Authentication protocol in the MIFARE DESFire version is reverse-engineered by [11]. To examine the authentication protocol, they log the data transfer between the DESFire card and the card reader. The procedure of the DESFire communication protocol is presented in Figure 2.

In [12] the DESFire EV1 authentication protocol using AES-128 key type is reverse-engineered, by eavesdropping on genuine protocol runs. They developed a custom, freely programmable device, termed "Chameleon", which can emulate contactless smartcards compliant with the ISO 14443 standard in a stand-alone manner. Figure 3 shows the Procedure of EV1 authentication protocol with AES-128 key type.

3 Authentication Protocol

In this paper, the goal is to discover the details of the MIFARE DESFire EV3 authentication protocol. For implementation and reverse engineering, we use a freely programmable device, which can emulate contactless smartcards with the ISO 14443 standard as a card and ProxMark4 as a reader. In addition, we have a genuine MIFARE DESFire EV3 card.

To have proper communication with ProxMark, we implement anti-collision and select-application commands which are primary commands before starting the authentication procedure on the emulator board.

The anti-collision protocol starts as soon as the card enters the magnetic field of the reader after it is powered up. Select-application is the next command which is sent from reader to card as defined in ISO 14443A. The selected application is represented by its Application Identifier (AID). After that, the authentication protocol starts.

We reverse-engineered the response of ProxMark and genuine MIFARE DESFire EV3 cards in D40, EV1, and EV2 secure messaging modes. In addition, we logged the responses between the emulator board as a MIFARE DESFire EV3 card and the ProxMark4 as a reader to authentication commands. Using these two send and receive responses, we could illustrate the details of the authentication procedure in MIFARE DESFire D40, EV1 with DES key-type and MIFARE DESFire EV2 compatible mode in Figure 4, Figure 5 and Figure 6.

The method we used to reverse-engineer is like a brute-force attack with less sample input data. We check different sample inputs and their output responses during communication for authentication between genuine EV3 cards, and Proxmark. In the next step, we checked the AES or DES algorithm input and output with considering the gathered responses. In addition to some guesses based on the usual authentication algorithm, we could define the exact authentication algorithm.

A MIFARE DESFire EV3 card responds to the authentication command in D40 secure messaging with an encrypted 128-bit random nonce nC with DES algorithm, as illustrated in Figure 4. The reader decrypts the received 64-bit long b0 and rotates it one byte to the left. In the reader, likewise, a 128-bit random nonce nR is produced. The decrypted

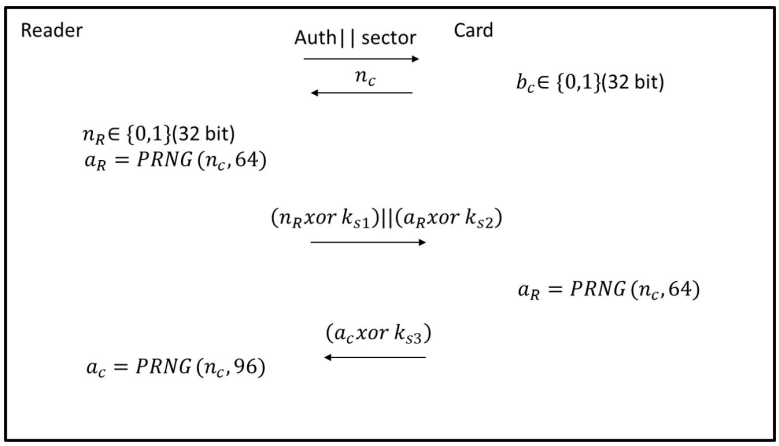

Figure 1. MIFARE classic authentication protocol[5]

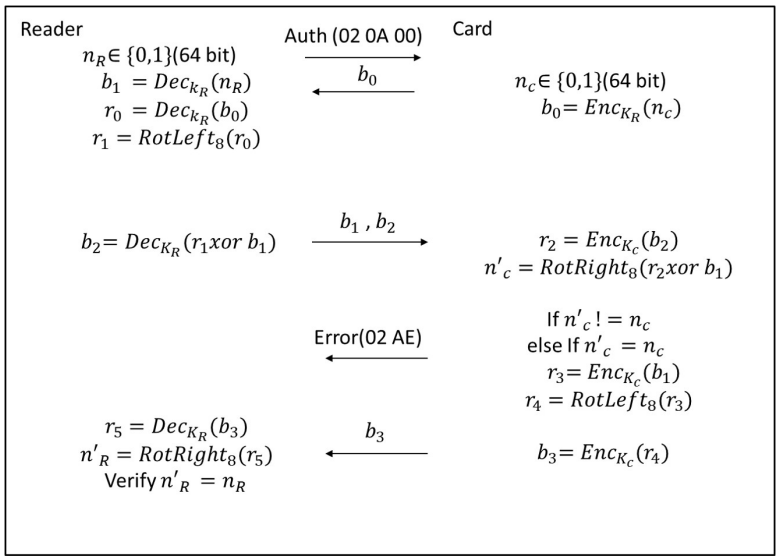

Figure 2. DESFire authentication protocol[11]

result of the concatenation of nR and r1 with the DES algorithm is sent from reader to card. In the next step, the card verifies the received b1 by decrypting and rotating the second part, one byte, to the right. If the result n'C is not equal to nC, an error response will be sent to the reader else, the result of rotating one byte to the left and encryption will be sent. In the last step, the reader verifies b3 by decrypting and rotating r5 one byte to the right.

If EV1 secure messaging with DES key type is selected as the authentication command in the MIFARE DESFire EV3 card, different commands and responses from Figure 3 will be exchanged between the card and reader. Figure 3 shows the EV2 authentication command with the AES key type, but we illustrate it with DES key type. In response to the authentication command from the reader, a 128-bit random nonce nC encrypted with the DES algorithm is sent from card to reader as illustrated in Figure 5. The reader decrypts the received b0 and then rotates the result. In the reader likewise, a 128-bit random nonce nR is produced. The encrypted form of the upper eight bytes of nR XORed with the lower eight bytes of b0 concatenated lower eight bytes of nR, is named b1. The encrypted form of the upper eight bytes of the r1 XORed lo bytes eight bytes of the b1 which is bytes concatenated with the lower eight bytes of r1 is named b2. b1 and b2 in the next step are received by cards. The card verifies the received b1 and b2. In the first step, the card decrypts b1 and b2. In the next step, the upper eight bytes of r3 XORed with the lower eight bytes of b1 in concatenation with the second eight bytes of r3 must be rotated one byte to the right. If the result n'C is not equal to nC, an error response will be sent to the reader else the result of rotating one byte to the left of the upper eight bytes of r2 XORed with the second part b0, concatenated with the lower eight bytes of r2 calculated. By encrypting the upper eight bytes of r4 XORed the lower eight bytes of b2,

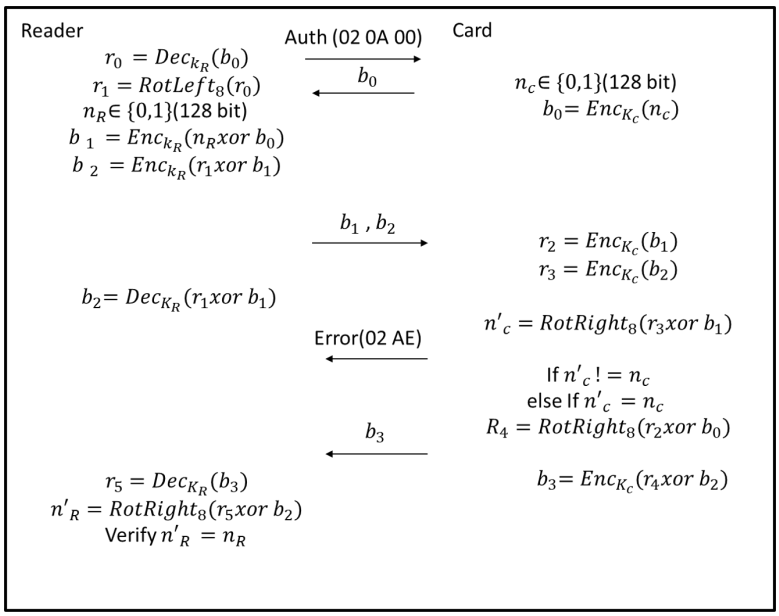

Figure 3. EV1 authentication protocol[12]

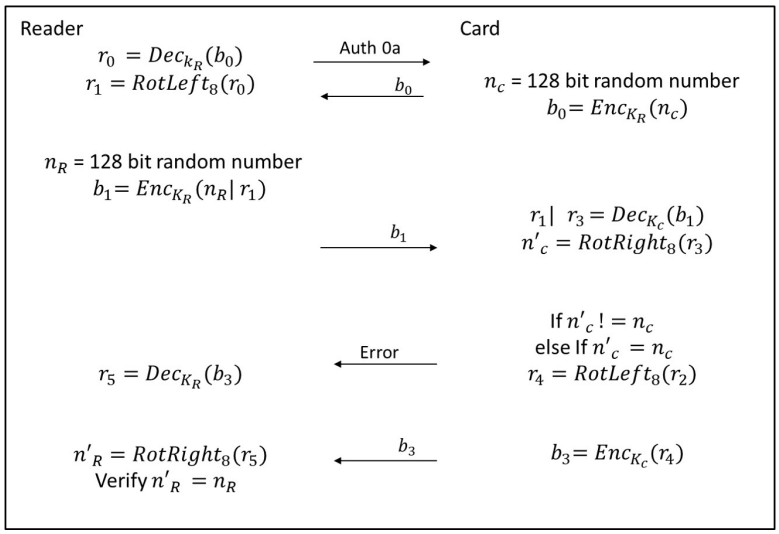

Figure 4. D40 authentication protocol

which are concatenated with the lower eight bytes of r4 and b3 are produced and sent to the reader. In the last step, the reader verifies b3 by decrypting and rotating r5 one byte to the right.

During the authentication protocol, if EV2 secure messaging is selected in the DESFire EV3 card, an encrypted 128-bit random nonce nC with AES algorithm is received by the reader as illustrated in Figure 6. Figure 5 shows that The reader decrypts the received 128-bit long b0 and rotates it one byte to the left. In the reader likewise, a 128-bit random nonce nR is produced. The encrypted form of nR XORed with r1. The result is encrypted with the AES algorithm. b1 and b2 in the next step are received by card. The card verifies the received b1 and b2 by decrypting them and rotating r3 XORed with b1, one byte to the right. If the result n'C is not equal to nC, an error response will be sent to the reader else the result of rotating one byte to the left of r2 and encrypting r4 will be sent. In the last step, the reader verifies b3 by decrypting and rotating r5 one byte to the right.

We evaluated the correctness of the results and calculated algorithms for authentications by implementing them on our evaluation board as an EV3 card. Our emulated card worked correctly in communication with Proxmark4 which indicates the algorithm for authentication is correct.

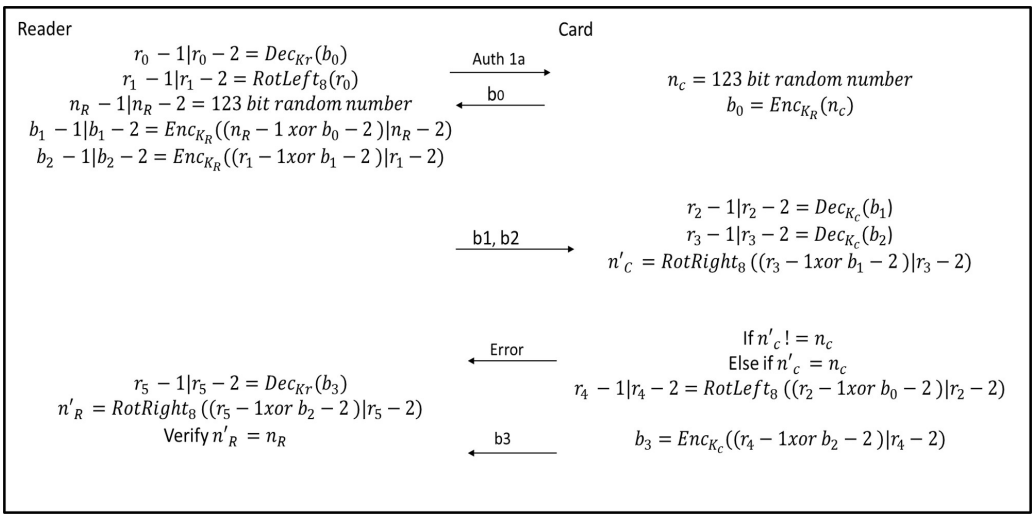

Figure 5. EV1 authentication protocol with DES key-type

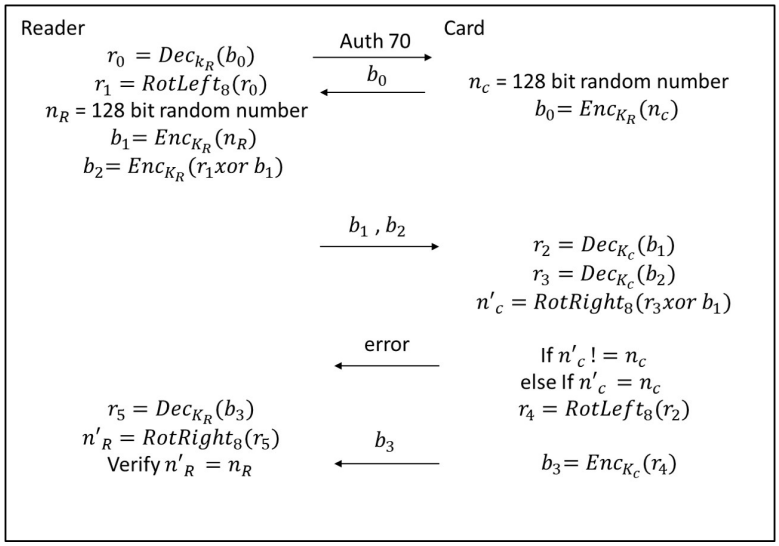

Figure 6. EV2 authentication protocol

4 Conclusion

We have reverse-engineered the authentication protocol of MIFARE DESFire EV3 cards, which consists of D40, EV1, and EV2 secure messaging. AES and DES algorithms were implemented on the evaluation board to emulate a MIFARE DESFire card successfully to communicate with ProxMarak4. We could illustrate the details of the authentication procedure by Logging and analyzing the transmitted authentication commands and responses between the card and reader.

References

[1] Adoption of smart cards in the medical sector:: the canadian experience. *Social Science & Medicine*, 53(7):879–894, 2001.

[2] Brij B Gupta and Shaifali Narayan. A survey on contactless smart cards and payment system: technologies, policies, attacks and countermeasures. *Journal of Global Information Management (JGIM)*, 28(4):135–159, 2020.

[3] Shi Chen. Trust management for a smart card based private eid manager. Master's thesis, NTNU, 2016.

[4] Bruce Schneier, Adam Shostack, *et al.* Breaking up is hard to do: modeling security threats for smart cards. In *USENIX Symposium on Smart Cards*, 1999.

[5] Flavio D Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling mifare classic. In *European symposium on research in computer security*, pages 97–114. Springer, 2008.

[6] NXP SemiConductors. Mifare desfire ev1 contactless multi-application ic. *Product short data*

sheet.[online] Available at:, 2010.

[7] David F. Oswald and Christof Paar. Breaking mifare desfire mf3icd40: Power analysis and templates in the real world. In *Workshop on Cryptographic Hardware and Embedded Systems*, 2011.

[8] Petr Socha, Vojtěch Miškovskỳ, and Martin Novotnỳ. A comprehensive survey on the non-invasive passive side-channel analysis. *Sensors*, 22(21):8096, 2022.

[9] Oleksiy Lisovets, David Knichel, Thorben Moos, and Amir Moradi. Let's take it offline: Boosting brute-force attacks on iphone's user authentication through sca. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 496–519, 2021.

[10] Jung-Sik Cho, Sang-Soo Yeo, and Sung Kwon Kim. Securing against brute-force attack: A hash-based rfid mutual authentication protocol using a secret value. *Computer communications*, 34(3):391–397, 2011.

[11] Dario Carluccio. Electromagnetic side channel analysis for embedded crypto devices. *Master's thesis, Ruhr Universität Bochum*, 2005.

[12] Timo Kasper, Ingo von Maurich, David Oswald, and Christof Paar. Chameleon: A versatile emulator for contactless smartcards. In *International Conference on Information Security and Cryptology*, pages 189–206. Springer, 2010.

Mansoureh Labafniya received her B.Sc. in hardware computer engineering in 2008. Her first M.Sc. degree is in computer architecture from Islamic Azad University, Science and Research Branch, Tehran, Iran. Her second M.Sc. degree is in mechatronic Engineering from the Sharif University of Technology, Tehran, Iran in 2012. She was a visiting researcher at KU Leuven for six months in 2018 and 2019. She got her Ph.D. degree in Computer Architecture Engineering at the University of Isfahan, Iran in 2020. She is currently a researcher at the Research Center for Development of Advanced Technologies (RCDAT). Her research interests include Hardware security and Digital system design.

Hamed Yusefi received his B.Sc. degree in 2009 from Shahrekord University, Iran, in Electrical Engineering and M.Sc. degree in 2012 from Imam Hossein University, Tehran, Iran, both in Communication Engineering. He is currently a Ph.D. candidate in Electrical Engineering at Shahed University, Tehran, Iran, and a researcher at the Research Center for Development of Advanced Technologies (RCDAT), Tehran, Iran. His research area includes hardware security and the root of trusts.

Akram Khalesi received her B.Sc. degree in 2011 from Kashan University, Isfahan, Iran, and her M.Sc. degree in 2014 from Malek-Ashtar University, Tehran, Iran, both in Electrical Engineering. She is currently a Ph.D. candidate in Electrical Engineering at Shahid Beheshti University, Tehran, Iran, and a researcher at the Research Center for Development of Advanced Technologies, Tehran, Iran. Her research area includes cryptology with an emphasis on symmetric designs and applied cryptography.