Information & Security: An International Journal

Farzaneh Abed, Francesco Berti & Stefan Lucks, vol.37, 2017, 45-53

https://doi.org/10.11610/isij.3704

ATTACKING A LEAKAGE-RESILIENT AUTHENTICATED ENCRYPTION SCHEME WITHOUT LEAKAGE

Farzaneh ABED, Francesco BERTI, and Stefan LUCKS

Abstract: Leakage-resilient authenticated encryption (AE) aims at privacy and authenticity against adversaries with an additional side channel. The first published "leakage resilient" AE scheme is the RCB block cipher mode. As it turns out, RCB is insecure, even if there is no side channel for the adversary. The current paper presents several attacks on RCB.

Keywords: authenticated encryption, leakage-resilience, block cypher, attack

Introduction

Several issues exist for the security of modern cryptosystems that can reveal useful information about the cryptosystem. One of these issues is the security of the cryptosystem against side-channel attacks when implemented physically. Therefore, many countermeasures have been proposed to protect those schemes against these kinds of attacks. [13], [18] and [9] represent different countermeasures, such as masking, shuffling and noise addition, to thwart these sorts of attacks. Yet, such countermeasures are often quite expensive for constraint devices exposed to these kinds of attacks. Therefore, another approach, initiated with high hopes, is to design "leakage-resilient" schemes. The goal is to maintain a certain level of security, even when the implementation leaks some information about internal secrets to the adversary. There have been a handful of proposals for leakage-resilient en encryption, such as [6],[7],[12],[16],[17],[7],[19], and [20]. Yet, few proposals using a block cipher-based leakage-resilient message authentication, such as [15] and [11], exist. To the best of our knowledge, RCB represents the first claim to be a leakage-resilient authenticated encryption scheme [2]. Later, Berti et al. [4] and Dobraunig et al. [5]

proposed DIV and ISAP, in two independent works, as a new leakage-resilient authenticated encryption schemes.

The RCB Mode

The RCB mode [2] is based on the OCB mode [8],[14], a well-known authenticated encryption scheme that has been proven to be secure within the black-box model (i.e. without leakage). Agrawal et al. [2] enhanced the OCB mode using a rekeying scheme g, which is assumed not to leak [10]. Using rekeying assures that the block cipher is never used twice under the same key, and this is where the claimed leakage resilience comes from. To make sure both the sender and the receiver use a single secret key, both parties need to maintain a shared *ctr* value. RCB encrypts a message $M = (m_1,\ldots,m_L)$, where $m_1,\ldots, m_{L-1}$ are b-bit blocks, and the size of m_L is at most b bits, into a ciphertext $C = (c_1,\ldots,c_L)$, with $|c_i| = |m_i|$, and authentication tag $T \in \{0,1\}^\tau$ for some tag size $\tau \leq b$. The value of the internal counter before the start of the encryption, ctr', is also part of the output (see Algorithm 1). For decryption, given ctr', C and T, RCB first computes M, then its own authentication tag T', and returns M if $T' = T$, else it returns $\perp$.

1: **state** long-term key $K*$, counter ctr ($*K^*$ is constant, ctr always increases $*$)
2: **input** message $M = (m_1,\ldots,m_L)$
3: $ctr' \leftarrow ctr$
4: **for** $i \in \{1,\ldots,L-1\}$ **do**
5: $K_i \leftarrow g_{K*}(ctr)$
6: $ctr \leftarrow ctr + 1$
7: $c_i \leftarrow E_{Ki}(m_i)$
8: $ctr \leftarrow ctr + 1$ ($*$ skip one value $*$)
9: $K_L \leftarrow g_{K*}(ctr)$
10: $ctr \leftarrow ctr + 1$
11: $X \leftarrow len(m_L) \oplus ctr'$
12: $Y \leftarrow E_{K_L}(X)$
13: $c_L \leftarrow Y \oplus m_L$
14: $S \leftarrow m_1 \oplus \cdots \oplus m_{L-1} \oplus (c_L 0^{b\tau}) \oplus Y$ ($*$ checksum $*$)
15: $K_{L+1} \leftarrow g_{K*}(ctr)$
16: $ctr \leftarrow ctr + 1$
17: $T \leftarrow E_{K_{L+1}}(S)$[first τ bits]
18: **return** $(ctr', \overbrace{(c_1,\ldots,c_L)}^{C}, T)$

Algorithm 1 RCB Encryption

Our Contribution and Results

In this paper, we analyze the security of RCB. As it turns out, even without leakage, RCB is neither robust against nonce-misuse nor to the release of unverified plaintexts (RUP) [3],[1]. RCB is inherently vulnerable to Denial-of-Service (DoS) attacks, and RCB is insecure when one key is used for full-duplex communication. For the worst, RCB is vulnerable to forgery attacks, thus missing INT-CTXT security. Thus, even within a black-box model (without leakage), RCB is not a secure scheme for authenticated encryption.

Weaknesses of RCB

Below we assume that Alice uses RCB to send authenticated and encrypted messages to Bob. Alice and Bob have shared a secret key $k*$ and a synchronized counter *ctr*. Adversary ***A*** is trying to attack Alice and Bob.

Lack of Nonce-Misuse Resistance

[2] claimed that RCB is nonce-misuse resistant as it does not have the nonce requirement. But actually, the counter *ctr* **is** a nonce ("number used once"). If the same value for *ctr* is reused, security fails:

1. ***A*** knows the current value of Alice is *ctr* and chooses $m^1_1, m^2_1, m^2_2 \in \{0,1\}^b$.
2. Alice encrypts $m^1 = (m^1_1, m^2_1)$ to $(tr,(c^1_1, c^2_1), \tau^1)$.
3. ***A*** resets Alice's counter to *ctr* (nonce-reuse!).
4. ***A*** chooses message $m^2=(m^2_1 [=m^1_1 \oplus e], m^2_2=m^1_2)$ $(e \in \{0,1\}^b, e \neq 0...0)$.
5. Alice encrypts m^2 to $(ctr, (c^2_1, c^2_2), \tau^2)$ (Due to the nonce reuse, the value *ctr* is the same as the one in step 2)
6. if $c^2_1 = c^1_1 \oplus e$, then ***A*** using RCB otherwise the random oracle $(., ., .).

A can distinguish the two oracles RCB from $(., ., .) with probability $1-2^{-b}$.

Vulnerability to Denial-of-Service (DoS) Attacks

By tampering with the counter, ***A*** can deny the service such that Bob will reject a valid ciphertext. Our first DoS attack goes as follows:

1. Alice initializes her counter value to ctr. She then encrypts a message m to (ctr, c, τ). The value of Alice's counter is now $(ctr + a)$ for some $a > 0$. She chooses another message m' to encrypt to $(ctr + a, c', \tau')$. The value of Alice's counter is now $(ctr + a + a')$ for some $a' > 0$.
2. ***A*** forwards $(ctr + a, c', \tau')$ to Bob. If a does not exceed a pre-defined threshold[i], then Bob decrypts $(ctr + a, c', \tau')$ to m'. The value of Bob's new counter is now $(ctr + a + a')$.
3. ***A*** forwards (ctr, c, τ) to Bob. Since $ctr < (ctr + a + a')$, he will abort the decryption of (ctr, c, τ), and will perform a resynchronization, yet he will not obtain the correct m.

Our second DoS attack does not even require Alice to encrypt two messages:

1. Alice initializes her counter value to ctr. She chooses message m to encrypt it to (ctr, c, τ). The value of Alice's new counter is now $(ctr + a)$.
2. ***A*** chooses c' and τ' and sends (ctr, c', τ') to Bob.
3. Bob decrypts (ctr, c', τ') to $\perp$. The value of Bob's new counter is $(ctr + a')$[ii].
4. ***A*** now forwards (ctr, c, τ) to Bob. Since $ctr < (ctr + a')$, therefore he will abort the decryption (ctr, c, τ) and will perform a resynchronization, yet he will not obtain the correct m.

Not Suitable for Full-Duplex Communication

Contrary to most other AE s hemes, bidirectional communication between Alice and Bob using a single key is insecure. If Alice sends a message to Bob using $k*$, and Bob sends a message to Alice using $k*$, then ***A*** can exploit this as follows:

1. Alice and Bob share the same initial counter value ctr.
2. ***A*** chooses $m_1 \neq m_2 \in \{0, 1\}^b$.
3. Alice encrypts (m_1, m_2) to $(ctr, (c_1, c_2), \tau)$ but Bob does not see this message.
4. A now chooses $m_1 = (m_1, m_1)$.
5. As a next, Bob encrypts m_1 to $(ctr, (c'_1, c'_2), \tau')$.
6. Since $c_1 = c'_1$ in the first case, adversary ***A*** can easily distinguish which oracle (RCB or a random) Bob has been used.

To prevent this attack, one needs two independent keys. But a random-nonce

[i] Else, Alice and Bob would perform an interractive resynchronisation [2], Figure 2.

[ii] Bob must increase the counter, even if the message turns out to be invalid. Otherwise, Bob would use the same interval key more than once, thus destroying the main purpose of using RCB, namely its claimed leakage-resilience.

instantiation of, say, OCB [14] neither requires synchronized counters nor two independent keys for bidirectional communication.

No Authenticity: Vulnerable to a Forgery Attack

The idea of the attack is to use one valid ciphertext to produce another valid ciphertext. For this purpose, we need to prevent Bob from receiving this ciphertext with the aim that his counter will not change. We present a forgery attack using only the encryption of a 5-block message, yet the attack can also be generalized. We remind that $\mathcal{E}$ is a block cipher, the block space of which is $\{0, 1\}^b$. Bob must not see the message. We prove that this message will contain all the information required to forge a 2-block message:

1. Initially, Alice and Bob share the same counter value *ctr*.
2. ***A*** hooses five different arbitrary messages: (m_1, m_2) in $\{0, 1\}^b$, $m'^2 \in \{0, 1\}b'$ with $b' \leq b$, $m_3 = |m'^2| \oplus (ctr + 2 + 1)$, m_4 *as* $m_4 = m_1 \oplus (m'_2 0^b)$, and finally m_5 in $\{0, 1\}^{b'}$ with $b' < b$.
3. ***A*** then asks for the encryption of all five messages $(m_1, ..., m_5)$.
4. Alice encrypts this to $(ctr, (c_1, ..., c_5), \tau)$.
5. ***A*** sets c'_2 *to* $(c_2 \oplus m'_2)$.
6. ***A*** sends $(ctr, (c_1, c'_2), \lfloor c_4 \rfloor \tau s)$ to Bob.

In our attack, we suppose that we know the counter value *ctr*. This is not an issue, we just need to see a message sent by Alice and add the length of the message $+2$. Because of the following reasons $(ctr, (c_1, c'_2), \lfloor c_4 \rfloor \tau s)$ is valid encryption of the message (m_1, m'_2) with initial counter *ctr*, which Bob will accept:

1. the message block m_1 is encrypted to c_1.
2. the ciphertext block c_3 is the encryption of $|m'_2| \oplus (ctr + 2 + 1)$ under the key $g_{k*}(ctr + 2)$, and the ciphertext block c'_2 as $(c_3 \oplus m'_2)$, as required by lines 8-13 of Algorithm 1.

1. The message m_4 has been chosen as $(m_1 \oplus m'_2 0^b)$, and the tag is the encryption of $(m_1 \oplus m'_2 0^b)$ under the key $G_{k*}(ctr + 4)$.
2. If the last message block m'_2 of the forged message is a b-bit block, then the ciphertext is valid. Otherwise, it is valid if the last $b - b'$ bits of $y[= \mathcal{E}_{k4}(|m'_2| \oplus (ctr + 2 + 1))]$ are 0, which happens with probability $2^{-b+b'}$. So, in this case, the atta k succeeds with probability $2^{-b+b'}$.

Since RCB does not provide any security for ciphertext integrity, it clearly cannot provide integrity with the release of unverified plaintext.

Conclusion

What went wrong? And can one repair RCB?

RCB has been derived from the well-established OCB mode. OCB is neither leakage-resilient nor robust, but it provides secure authenticated encryption in the black-box model (without leakage). [2] lists the following modifications to turn OCB into RCB:

1. There is no masking for the input and output of the block cipher in the rekeying scheme. (Instead, the keys change.)
2. The starting counter is XORed to the input of block cipher during processing the last block of the message to prevent an adversary from creating a valid pair of a message and a tag. (Note that the starting counter is not a secret. OCB uses a secret mask derived from the key at this point.)
3. One fresh key is omitted before processing the last message block to thwart a forgery attack by the adversary.

The second modification clearly weakens RCB, in contrast to OCB. Apparently, [2] attempted to solve this with the third modification. As our forgery attack shows, the third modification is not sufficient. To thwart this attack, one could propose a modification of the original RCB, which is more in the spirit of the original OCB. For example, the modified RCB could use $K_i = g_{K*}(X + 2i)$ as the ephemeral keys to encrypt the first $L - 1$ message blocks and the checksum. The ephemeral key for the final block m_L could be $g_{K*}(X + 2L + 1)$. We conjecture that this would defend against black-box forgery attacks such as ours. But it would not solve any of the other issues.

Summary

We described several attacks against RCB, a leakage-resilient authenticated encryption scheme. RCB is not robust, neither against nonce-misuse nor against the release of unverified plaintexts. RCB does not resist Denial-of-Service attacks. RCB even fails at providing authenticity, one of the two main goals of every authenticated encryption scheme.

None of the attacks presented here assume the adversary to have access to a side channel. Our ongoing research also considers attack scenarios where the adversary has access to a side channel.

Acknowledgement

Farzaneh Abed was supported by the Simple Scry project with Cisco, and Francesco Berti by the INNOVIRIS project SCAUT.

Endnotes

1. Farzaneh Abed, Scott Fluhrer, John Foley, Christian Forler, Eik List, Stefan Lucks, David McGrew, and Jakob Wenzel, "Pipelineable online encryption (poe)" In: *21st International Workshop on Fast Software Encryption (FSE 2014*), *Lecture Notes in Computer Science (LNCS)* 3 (2014).
2. Megha Agrawal, Tarun Kumar Bansal, Donghoon Chang, Amit Kumar Chauhan, Seokhie Hong, Jinkeon Kang, and Somitra Kumar Sanadhya, "R b: leakage-resilient authenticated encryption via rekeying," *The Journal of Supercomputing* (2016): 1-26.
3. Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda, "How to Securely Release Unverified Plaintext in Authenticated Encryption," In: *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, Proceedings, Part I*, 2014, pp. 105-125.
4. Francesco Berti, François Koeune, Olivier Pereira, Thomas Peters, and François Xavier Standaert, "Leakage-resilient cryptography in practice," *IACR Cryptology ePrint Archive* 2016:996 (2016).
5. Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, and Thomas Unterluggauer, "Isap - authenticated encryption inherently secure against passive side-channel attacks," *IACR Cryptology ePrint Archive* 2016:952 (2016).
6. Stefan Dziembowski and Krzysztof Pietrzak, "Leakage-resilient cryptography," In: *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, Philadelphia, PA, USA, IEEE Computer Society*, 2008, pp. 293-302.
7. Sebastian Faust, Krzysztof Pietrzak, and Joachim Schipper, "Practical leakage-resilient symmetric cryptography," In: Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012, Proceedings*, *Lecture Notes in Computer Science*, vol. 7428 (Springer, 2012), 213-232.
8. Ted Krovetz and Phillip Rogaway, "The software performance of authenticated-encryption modes," In: Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, Revised Selected Papers*, *Lecture Notes in Computer Science*, vol. 6733, (Springer, 2011), 306-327.
9. Stefan Mangard, "Hardware countermeasures against DPA-a a statistical analysis of their effectiveness," In: *Cryptographers' Track at the RSA Conferenc*e, (Springer, 2004), 222-235.
10. Marcel Medwed, Christophe Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert, "Fresh re-keying II: securing multiple parties against side-channel and fault attacks," In: Emmanuel Prouff, editor, *Smart*

Card Research and Advanced Applications - 10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011, Leuven, Belgium, September 14-16, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 7079 (Springer, 2011), 115-132.

11. Olivier Pereira, François-Xavier Standaert, and Srinivas Vivek, "Leakage-resilient authentication and encryption from symmetric cryptographic primitives," In: Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6,* 2015, pp. 96-108.
12. Krzysztof Pietrzak, "A leakage-resilient mode of operation," In: Antoine Joux, editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, Proceedings, Lecture Notes in Computer Science*, vol. 5479 (Springer, 2009), 462-482.
13. Matthieu Rivain and Emmanuel Prouff, "Provably secure higher-order masking of AES," In: *International Workshop on Cryptographic Hardware and Embedded Systems* (Springer, 2010), 413-427.
14. Phillip Rogaway, Mihir Bellare, and John Black, "OCB: A block-cipher mode of operation for efficient authenticated encryption," *ACM Trans. Information Systems Security* 6, no. 3 (2003):365-403.
15. Joachim H. Schipper, "Leakage Resilient Authentication," Master's thesis, Utrecht University, the Netherlands, 2010.
16. François-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald, "Leakage resilient cryptography in practice," *IACR Cryptology ePrint Archive* 2009:341 (2009).
17. François-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald, "Leakage resilient cryptography in practice," In: Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security: Foundations and Practice (Information Security and Cryptography)* (Springer, 2010), 99-134.
18. Nicolas Veyrat-Charvillon, Marcel Medwed, Stéphanie Kerckhof, and François Xavier Standaert, "Shuffling against side-channel attacks: A comprehensive study with a cautionary note," In: *International Conference on the Theory and Application of Cryptology and Information Security*, (Springer, 2012), 740-757.
19. Yu Yu and François-Xavier Standaert, "Practical leakage-resilient pseudorandom objects with minimum public randomness," In: Ed Dawson, editor, *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Tracktat the RSA Conference 2013, San Francisco, CA, USA, February 25 - March 1, Proceedings, Lecture Notes in Computer Science*, vol. 7779, (Springer, 2013), 223-238.
20. Yu Yu, François-Xavier Standaert, Olivier Pereira, and Moti Yung, "Practical leakage-resilient pseudorandom generators," In: Ehab Al-Shaer,

Angelos D. Keromytis, and Vitaly Shmatikov, editors, *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8*, 2010, pp.141-151.

About the Authors

Farzaneh Abed
Farzaneh Abed is a research assistant at the Bauhaus-Universität Weimar. Her field of research revolves around symmetric cryptography, cryptanalysis, media security and networking.

Francesco Berti
Francesco Berti is a researcher at the Department of Electrical Engineering at the Université Catholique de Louvain. He is also a member of the UCL Crypto Group. Francesco Berti's research interests include information security, applied cryptography, and cryptology.

Stefan Lucks
Stefan Lucks' fields of research are cryptology and communication security. He obtained a diploma in Computer Science in 1993 at the University of Dortmund. In 1997, he finished his PhD at the University of Göttingen and went to the University of Mannheim, where he obtained his postdoctoral lecture qualification in 2003 and became a lecturer in 2004, leading the security research team for the Mobile Business Research Group at the University of Mannheim. In 2007, he became a full professor for Media Security at Bauhaus-University, Weimar.