Observation on Weak Keys for AEZ

Bart Mennink

Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and iMinds, Belgium
bart.mennink@esat.kuleuven.be

Abstract. AEZ is one of the submission to the CAESAR competition. In this note, we describe the observation that AEZ has approximately $3 \cdot 2^{256}$ weak keys, namely

$$K \in \{I \| J \| 0^{128}, I \| 0^{128} \| L, 0^{128} \| J \| L\}\,,$$

where $I, J, L \in \{0,1\}^{128}$. If any of these keys is used, AEZ can be broken in two AEZ evaluations. Although the fraction of weak keys seems to be too small to derive an effective attack on AEZ, the observation may entail stronger attacks on AEZ.

1 Introduction

AEZ is an authenticated encryption scheme by Hoang et al. [4]. In this work we focus on AEZ v4, the latest version that has been submitted to CAESAR [3]. The addendum "v4" will be omitted for brevity.

AEZ allows for arbitrarily sized keys, and derives a 384-bit subkey as follows:

$$I \| J \| L \leftarrow \begin{cases} K \text{ if } |K| = 384\,, \\ \text{BLAKE2b}(K) \text{ otherwise.} \end{cases}$$

In other words, if the key is already 384 bits long, it is simply padded into $I \| J \| L$; otherwise, it is first hashed via BLAKE2b [1]. This is done deliberately, as the authors state [3]: "We dispense with calling BLAKE2b if the key K is already $3 \cdot 128$ bits."

Unfortunately, if one of the three subkeys I, J, L equals 0^{128}, AEZ can be distinguished from an ideal AE in at most two evaluations. The observations that these keys are weak follows from explicitly writing out the tweakable blockcipher underlying AEZ, as we have done in Section 2.1. This explicit description may contribute to a better understanding of what is the effective underlying primitive of AEZ, and what is the assumption made on it.

A simple computation shows that the number of weak keys K is at least $3 \cdot 2^{256} - 3 \cdot 2^{128} + 1 \approx 3 \cdot 2^{256}$, not taking into account any weak keys of size differently from 384. If one would opt to *always* hash the key through BLAKE2b, regardless of the size of K, this would at first sight solve above issue. Yet, weak keys still exist: assuming that BLAKE2b is a random oracle (see Guo et al. [2] for the latest analysis of BLAKE2b) this means that approximately 1 out of 2^{128} keys is weak. In general, the fraction of weak keys seems to be too small to derive an effective attack on AEZ, but nevertheless, we think that this observation should be taken into account when considering AEZ.

A high-level description of AEZ is given in Section 2, and its weak keys are discussed in Section 2.3.

2 AEZ

We will describe the tweakable blockcipher used in AEZ in Section 2.1 and give a high-level description of AEZ in Section 2.2.

2.1 Tweakable Blockcipher Design

AEZ internally uses a tweakable blockcipher constructed from the AES round function. In more detail, define the *keyless* AES round function $\mathrm{aesr}(X)$ as

$$\mathrm{aesr}(X) = \mathrm{MixColumns} \circ \mathrm{ShiftRows} \circ \mathrm{SubBytes}(X)\,.$$

AEZ uses the two blockciphers AES4 and AES10, where for $r \in \{4, 10\}$,

$$\mathrm{AES}r_{K_0,K_1,\ldots,K_r}(X) = \mathrm{aesr}(\cdots \mathrm{aesr}(X \oplus K_0) \cdots \oplus K_{r-1}) \oplus K_r\,.$$

The tweakable blockcipher $\widetilde{E}$ takes as input a key $I\|J\|L \in \{0,1\}^{3\cdot 128}$, a tweak $(j,i) \in (\{-1,0\} \times [0..7] \cup \{1,2,3\} \times \mathbb{N})$, and a plaintext X and computes the ciphertext as

tweak	$\widetilde{E}^{j,i}_{I\|J\|L}(X) =$	
$j = -1, i \in [0..7]$	$\mathrm{AES10}_{\mathbf{K}}(X)$	with $\mathbf{K} = (iJ, I, J, L, I, J, L, I, J, L, I)$
$j = 0, \quad i \in [0..7]$	$\mathrm{AES4}_{\mathbf{K}}(X)$	with $\mathbf{K} = (iI, J, I, L, 0^{128})$
$j = 1, \quad i \in \mathbb{N}$	$\mathrm{AES4}_{\mathbf{K}}(X)$	with $\mathbf{K} = \big(\Delta_i I, J, I, L, 0^{128}\big)$
$j = 2, \quad i \in \mathbb{N}$	$\mathrm{AES4}_{\mathbf{K}}(X)$	with $\mathbf{K} = \big(\Delta_i I, L, I, J, L\big)$
$j \geq 3, \quad i = 0$	$\mathrm{AES4}_{\mathbf{K}}(X)$	with $\mathbf{K} = \big(2^{j-3}L, J, I, L, 2^{j-3}L\big)$
$j \geq 3, \quad i \geq 1$	$\mathrm{AES4}_{\mathbf{K}}(X)$	with $\mathbf{K} = \big(2^{j-3}L \oplus \Delta_i J, J, I, L, 2^{j-3}L \oplus \Delta_i J\big)$

where $\Delta_i = (2^{3+\lfloor (i-1)/8 \rfloor} + (i\text{–}1 \bmod 8))$ for brevity. Hoang et al. [3] effectively claim that the AEZ construction is secure as long as $\widetilde{E}$ is a secure tweakable blockcipher. The use of AES4, which theoretically invalidates this condition, is validated using the so-called proof-then-prune approach.

In this work, we will *not* consider any internal properties of AES4, and simply consider both AES4 and AES10 as secure primitives. Instead, the attacks are based on a more structural property, namely that in the case of weak keys, the tweakable blockciphers are not distinct. For instance, if $J = 0^{128}$, then

$$\widetilde{E}^{-1,i}_{I\|0^{128}\|L} = \widetilde{E}^{-1,i'}_{I\|0^{128}\|L}$$

for any i, i'. Hence, different tweaks give the same blockcipher.

2.2 High-Level Description of AEZ

Fundamental to the AEZ authenticated encryption scheme is the key scheduling. In more detail, AEZ takes as input an arbitrarily sized key $K \in \{0,1\}^*$, and performs all of its procedures with three keys $I, J, L \in \{0,1\}^{128}$, where

$$I\|J\|L \leftarrow \begin{cases} K \text{ if } |K| = 384\,, \\ \mathrm{BLAKE2b}(K) \text{ otherwise.} \end{cases} \tag{1}$$

AEZ then evaluates a different algorithm depending on the size of M:[1]

- If $|M| = 0$, it evaluates AEZ-prf$(I\|J\|L, N, A, \tau)$;
- If $|M| < 256 - \tau$, it evaluates Encipher-AEZ-tiny$(I\|J\|L, N, A, \tau, M)$;
- If $|M| \geq 256 - \tau$, it evaluates Encipher-AEZ-core$(I\|J\|L, N, A, \tau, M)$.

[1] The interfaces of the underlying algorithms have been slightly modified for the sake of simplicity.

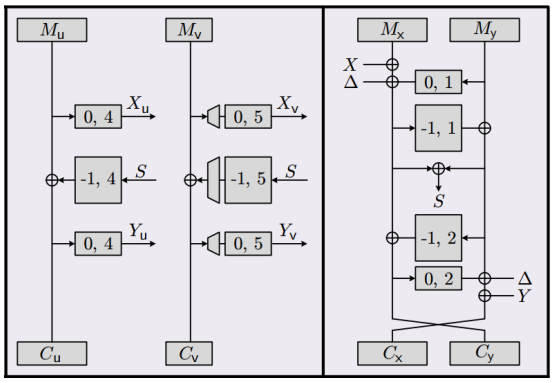

Fig. 1: AEZ for messages such that $384 \leq |M| + \tau < 511$. Here, $I \| J \| L$ are the subkeys. Not depicted are the computation $\Delta \leftarrow \text{AEZ-hash}(I \| J \| L, N, A, \tau)$ and the padding $M_u \| M_v \| M_x \| M_y \leftarrow M \| 0^\tau$ where $|M_u| = |M_x| = |M_y| = 128$ and $0 \leq |M_v| < 127$.

In this work, we are specifically interested in Encipher-AEZ-core. More detailed, for simplicity of presentation we will describe our attacks for a message M such that $384 \leq |M| + \tau < 511$. Encipher-AEZ-core for this case is given in Algorithm 1 and Figure 1. The attack can easily be generalized to any M such that $|M| \geq 256 - \tau$, as well as to $|M| = 0$. We do not immediately see a way to generalize the attack to Encipher-AEZ-tiny (the range $0 < |M| < 256 - \tau$).

Algorithm 1 Encipher-AEZ-core

Input: $(I \| J \| L, N, A, \tau, M)$ with $384 \leq |M| + \tau < 511$
Output: $C \in \{0,1\}^{|M|+\tau}$

1: $\Delta \leftarrow \text{AEZ-hash}(I \| J \| L, N, A, \tau)$ ▷ See [3] for AEZ-hash
2: $M_u \| M_v \| M_x \| M_y \leftarrow M \| 0^\tau$, where $|M_u| = |M_x| = |M_y| = 128$ and $0 \leq |M_v| < 127$
3: $X \leftarrow \widetilde{E}^{0,4}_{I\|J\|L}(M_u) \oplus \widetilde{E}^{0,5}_{I\|J\|L}(M_v 10^*)$
4: $S_x \leftarrow M_x \oplus \Delta \oplus X \oplus \widetilde{E}^{0,1}_{I\|J\|L}(M_y)$; $S_y \leftarrow M_y \oplus \widetilde{E}^{-1,1}_{I\|J\|L}(S_x)$
5: $S \leftarrow S_x \oplus S_y$
6: $C_u \leftarrow M_u \oplus \widetilde{E}^{-1,4}_{I\|J\|L}(S)$; $C_v \leftarrow M_v \oplus \widetilde{E}^{-1,5}_{I\|J\|L}(S)$
7: $Y \leftarrow \widetilde{E}^{0,4}_{I\|J\|L}(C_u) \oplus \widetilde{E}^{0,5}_{I\|J\|L}(C_v 10^*)$
8: $C_y \leftarrow S_x \oplus \widetilde{E}^{-1,2}_{I\|J\|L}(S_y)$; $C_x \leftarrow S_y \oplus \Delta \oplus Y \oplus \widetilde{E}^{0,2}_{I\|J\|L}(C_y)$
9: **return** $C_u \| C_v \| C_x \| C_y$

2.3 Weak Keys for AEZ

Our attacks on AEZ are based on the following observation:

Lemma 1. *The tweakable blockcipher $\widetilde{E}$ satisfies the following properties:*

(i) If $J = 0^{128}$, then $\widetilde{E}^{-1,i}_{I\|0^{128}\|L} = \widetilde{E}^{-1,i'}_{I\|0^{128}\|L}$ for any $i, i' \in [0..7]$;
(ii) If $I = 0^{128}$, then $\widetilde{E}^{0,i}_{0^{128}\|J\|L} = \widetilde{E}^{0,i'}_{0^{128}\|J\|L}$ for any $i, i' \in [0..7]$;
(iii) If $L = 0^{128}$, then $\widetilde{E}^{j,i}_{I\|J\|0^{128}} = \widetilde{E}^{j',i}_{I\|J\|0^{128}}$ for any $j, j' \geq 3$ and $i \in \mathbb{N}$.

More properties can be derived in a similar fashion, but these three relations suffice for the discussion of our attacks.

We will perform two distinguishing attacks on AEZ for the case of $384 \leq |M| + \tau < 511$, one which exploits property (i) and one which exploits property (ii). In these attacks, we consider a distinguisher that has access to either AEZ or an ideal authenticated encryption scheme \$ that on input of a tag size parameter τ and message M responds with a ciphertext $C \xleftarrow{\$} \{0,1\}^{|M|+\tau}$. Finally, we will briefly elaborate on how an attack can be performed that exploits property (iii).

Attack exploiting property (i). Assume that $J = 0^{128}$. Using Lemma 1 property (i), we can perform the following distinguishing attack.

- Let N, A, τ be any nonce, associated data, and tag size;
- Let M be any message such that $384 \leq |M|+\tau < 511$. Write $M\|0^\tau = M_{\mathsf{u}}\|M_{\mathsf{v}}\|M_{\mathsf{x}}\|M_{\mathsf{y}}$, where $|M_{\mathsf{u}}| = |M_{\mathsf{x}}| = |M_{\mathsf{y}}| = 128$ and $|M_{\mathsf{v}}| = |M| + \tau - 384 =: \ell$;
- Query $C = \mathcal{AE}_K(N, A, \tau, M) \in \{0,1\}^{|M|+\tau}$. Write $C = C_{\mathsf{u}}\|C_{\mathsf{v}}\|C_{\mathsf{x}}\|C_{\mathsf{y}}$, where $|C_{\mathsf{u}}| = |C_{\mathsf{x}}| = |C_{\mathsf{y}}| = 128$, and $|C_{\mathsf{v}}| = \ell$;
- If

$$\mathrm{chop}_\ell\big(M_{\mathsf{u}} \oplus C_{\mathsf{u}} \oplus M_{\mathsf{v}} \oplus C_{\mathsf{v}}\big) = 0^\ell\,, \tag{2}$$

  output 0, otherwise output 1.

Note that, if $\mathcal{AE} = \mathrm{AEZ}$, (2) is always satisfied as

$$\mathrm{chop}_\ell\big(M_{\mathsf{u}} \oplus C_{\mathsf{u}} \oplus M_{\mathsf{v}} \oplus C_{\mathsf{v}}\big) = \mathrm{chop}_\ell\left(\widetilde{E}^{-1,4}_{I\|0^{128}\|L}(S) \oplus \widetilde{E}^{-1,5}_{I\|0^{128}\|L}(S)\right) = 0^\ell\,,$$

using that $\widetilde{E}^{-1,4}_{I\|0^{128}\|L} = \widetilde{E}^{-1,5}_{I\|0^{128}\|L}$. Thus, the adversary always outputs 0 in the real world. In the ideal world, this condition is satisfied with probability $1/2^\ell$. Recall that $\ell = |M|+\tau-384$, where M is a freely chosen message. Hence, by taking $|M|+\tau = 511$ the success probability of the attack is $1 - 1/2^{127}$.

Attack exploiting property (ii). Assume that $I = 0^{128}$. Using Lemma 1 property (ii), we can perform the following distinguishing attack.

- Let N, A, τ be any nonce, associated data, and tag size;
- Let $0 \leq \ell < 128$. Let $M_{\mathsf{v}}, M'_{\mathsf{v}} \in \{0,1\}^\ell$ be any two *distinct* message blocks. Let $M_{\mathsf{xy}} \in \{0,1\}^{256-\tau}$ be any message block. Write

$$M = M_{\mathsf{v}}10^*\|M_{\mathsf{v}}\|M_{\mathsf{xy}} \text{ and } M = M'_{\mathsf{v}}10^*\|M'_{\mathsf{v}}\|M_{\mathsf{xy}}\,;$$

- Query $C = \mathcal{AE}_K(N, A, \tau, M) \in \{0,1\}^{|M|+\tau}$ and $C = \mathcal{AE}_K(N, A, \tau, M') \in \{0,1\}^{|M'|+\tau}$. Write $C = C_{\mathsf{u}}\|C_{\mathsf{v}}\|C_{\mathsf{x}}\|C_{\mathsf{y}}$ and $C' = C'_{\mathsf{u}}\|C'_{\mathsf{v}}\|C'_{\mathsf{x}}\|C'_{\mathsf{y}}$, where $|C_{\mathsf{u}}| = |C_{\mathsf{x}}| = |C_{\mathsf{y}}| = |C'_{\mathsf{u}}| = |C'_{\mathsf{x}}| = |C'_{\mathsf{y}}| = 128$, and $|C_{\mathsf{v}}| = |C'_{\mathsf{v}}| = \ell$;
- If

$$M_{\mathsf{u}} \oplus C_{\mathsf{u}} \oplus M'_{\mathsf{u}} \oplus C'_{\mathsf{u}} = 0^{128}\,, \tag{3}$$

  output 0, otherwise output 1.

Note that, if $\mathcal{AE}$ = AEZ, (3) is always satisfied. Indeed, using that $\widetilde{E}^{0,4}_{0^{128}\|J\|L} = \widetilde{E}^{0,5}_{0^{128}\|J\|L}$, we have

$$X_{\mathsf{u}} \oplus X_{\mathsf{v}} = 0^{128} = X'_{\mathsf{u}} \oplus X'_{\mathsf{v}}\,,$$

and thus $S = S'$. Therefore,

$$M_{\mathsf{u}} \oplus C_{\mathsf{u}} \oplus M'_{\mathsf{u}} \oplus C'_{\mathsf{u}} = \widetilde{E}^{-1,4}_{0^{128}\|J\|L}(S) \oplus \widetilde{E}^{-1,4}_{0^{128}\|J\|L}(S') = 0^{128}\,.$$

In the ideal world, this condition is satisfied with probability $1/2^{128}$. Thus, the success probability of the attack is $1 - 1/2^{128}$.

Attack exploiting property (iii). Using similar techniques, one can guarantee that if for an empty message $M = \varepsilon$ and for two nonces $N, N' \in \{0,1\}^{128}$, the two queries $C = \mathcal{AE}_K(N, N', \tau, M)$ and $C = \mathcal{AE}_K(N', N, \tau, M)$ satisfy $C = C'$. We refer to [3] for the specification of the corresponding function AEZ-prf.

Acknowledgments. This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). Bart Mennink is a Postdoctoral Fellow of the Research Foundation – Flanders (FWO). The author would like to thank his COSIC colleagues and the attendees of Dagstuhl Symmetric Cryptography for their comments and suggestions.

References

[1] Aumasson, J., Neves, S., Wilcox-O'Hearn, Z., Winnerlein, C.: BLAKE2: simpler, smaller, fast as MD5. In: Applied Cryptography and Network Security - ACNS 2013. Lecture Notes in Computer Science, vol. 7954, pp. 119–135. Springer, Heidelberg (2013)

[2] Guo, J., Karpman, P., Nikolić, I., Wang, L., Wu, S.: Analysis of BLAKE2. In: CT-RSA 2014. Lecture Notes in Computer Science, vol. 8366, pp. 402–423. Springer, Heidelberg (2014)

[3] Hoang, V.T., Krovetz, T., Rogaway, P.: AEZ v4: Authenticated Encryption by Enciphering (2015), submission to CAESAR competition

[4] Hoang, V., Krovetz, T., Rogaway, P.: Robust authenticated-encryption AEZ and the problem that it solves. In: Advances in Cryptology - EUROCRYPT 2015, Part I. Lecture Notes in Computer Science, vol. 9056, pp. 15–44. Springer, Heidelberg (2015)