Warning – Bug in AEZ v4 Specification – Correction Pending – 2017.03.08

The authors of AEZ gratefully acknowledge Xavier Bonnetain, Patrick Derbez, Sébastien Duval, Jérémy Jean, Gaëtan Leurent, Brice Minaud, and Valentin Suder for noticing a serious bug in our specification of AEZ (the current version of it, v4). The problem concerns our careless choice of offsets when computing the underlying tweakable blockcipher (TBC). It is crucial that distinct tweaks (our tweak is a pair of numbers i, j) give rise to distinct offsets Δ, but the overly-complex way we defined the offsets for our TBC gives rise to trivial collisions that we failed to notice.

The mistake is major in the sense that it is easy to exploit the error in the spec to destroy the claimed authenticity (and probably the privacy, too). It is minor in the sense that there are lots of easy ways to define offsets so as to not get collisions. We will issue a tweak to our spec in the next few days, after we decide which way to go and have revised all code.

Many thanks again to Gaëtan and all his colleagues for noticing this bug.

Viet Tung Hoang
Ted Krovetz
Phillip Rogaway