How we avoided a second Dual_EC_DRBG fiasco

(Simon and Speck will not be standardized as encryption algorithms in ISO)

Tomer Ashur Atul Luykx and many others

Why?

- The NSA has been constantly and systematically refusing to provide details about their design decisions and parameter choices

Why?

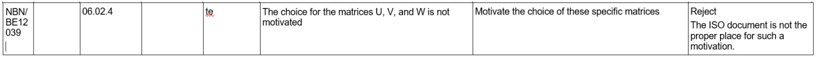
- The NSA has been constantly and systematically refusing to provide details about their design decisions and parameter choices
- After facing strong opposition in ISO, they released ePrint 2017/560, which claims to be a design rationale

Why?

- The NSA has been constantly and systematically refusing to provide details about their design decisions and parameter choices
- After facing strong opposition in ISO, they released ePrint 2017/560, which claims to be a design rationale
- Even in light of ePrint 2017/560, many questions remain open

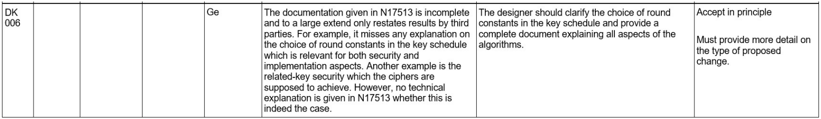
Why?

- The NSA has been constantly and systematically refusing to provide details about their design decisions and parameter choices
- After facing strong opposition in ISO, they released ePrint 2017/560, which claims to be a design rationale
- Even in light of ePrint 2017/560, many questions remain open
  - `https://youtu.be/3d-xruyR89g`



NBN/ BE12 039		06.02.4		te	The choice for the matrices U, V, and W is not motivated	Motivate the choice of these specific matrices	Reject The ISO document is not the proper place for such a motivation.

Figure: NSA's response to technical comments



DK 006				Ge	The documentation given in N17513 is incomplete and to a large extend only restates results by third parties. For example, it misses any explanation on the choice of round constants in the key schedule which is relevant for both security and implementation aspects. Another example is the related-key security which the ciphers are supposed to achieve. However, no technical explanation is given in N17513 whether this is indeed the case.	The designer should clarify the choice of round constants in the key schedule and provide a complete document explaining all aspects of the algorithms.	Accept in principle Must provide more detail on the type of proposed change.

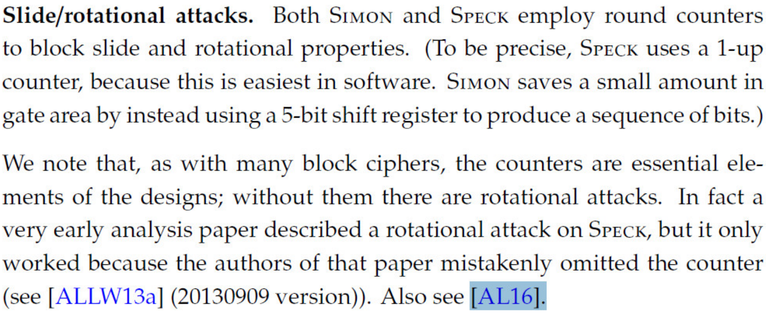
Figure: NSA's response to technical comments

Why?

- This is not about politics

Why?

- Third party analysis does not support the claim that the ciphers are secure



Slide/rotational attacks. Both Simon and Speck employ round counters to block slide and rotational properties. (To be precise, Speck uses a 1-up counter, because this is easiest in software. Simon saves a small amount in gate area by instead using a 5-bit shift register to produce a sequence of bits.)

We note that, as with many block ciphers, the counters are essential elements of the designs; without them there are rotational attacks. In fact a very early analysis paper described a rotational attack on Speck, but it only worked because the authors of that paper mistakenly omitted the counter (see [ALLW13a] (20130909 version)). Also see [AL16].

Figure: From the so-called design rationale

Why?

- The NSA's behavior around this has been very strange and aggressive

To conclude

- It doesn't matter if we think the ciphers are secure, or if a backdoor exists. There is so much doubt and uncertainty around these ciphers that including them would simply undermine ISO's reputation.