The Amendments

The synchronous keystream generator BMGL, [1], has been selected by NESSIE for further evaluation. In response to a call from NESSIE for amendments (tweaks), we would like to submit the following modifications.

Tweak 1: To be able to divide the keystream into segments, that each can be generated in any order, BMGL can use the generalized (re-keying) interface as described in [2].

Rationale: Higher flexibility.

Implementation effect: None.

Security effect: Analyzed in [2].

Tweak 2: The parameters $n$ (key/blocksize of Rijndael) and $m$ (number of output bits per iteration) can be selected by an implementation, rather than being fixed. The previously recommended values, $n = 256$, $m = 40$ are still valid as “defaults”.

Rationale: Higher flexibility, offering speed/security trade-off.

Implementation effect: None, except for some “hard-wired” implementations of Rijndael.
**Security effect:** Can be seen directly from [1] (later improved in [3]).

The final tweak is an alternative “mode of operation” for BMGL.

**Tweak 3:** An existing BMGL implementation should optionally be possible to run in the GGM-mode, as described in [3], §4 (for output length a priori unknown, as in §4.1).

**Rationale:** Higher level of provable security.

**Implementation effect:** A few lines of extra code, existing BMGL implementation remains untouched.

**Security effect:** As determined in [3].

**References**

