Requirements for an Accordion Mode

UK National Cyber Security Centre

The National Cyber Security Centre (NCSC) is the UK National Technical Authority on cryptography. The NCSC is very supportive of NIST's initiative to standardise new modes of operation, and we submit this talk in response to NIST's request for feedback on requirements for a new accordion mode.

NCSC conducts research into cryptographic design, principally for high-threat use cases in which data might require very long-term security, or have some sensitivity to it that warrants a particularly risk-averse approach to its handling. For high-threat use cases we place great value on reducing the likelihood that data is put at risk through misuse of cryptographic algorithms and protocols, since NCSC often does not have direct oversight of the end-users of the cryptography we design. In designing for these use cases we are usually able to make trade-offs to prioritise robustness and simplicity over other important considerations, such as performance.

In this talk we will review some desirable security goals proposed by NIST, by us, and by the community. We observe that it seems challenging to satisfy all of these requirements with a single mode. For example, a mode designed to work with AES cannot demonstrate context commitment with a security proof in the standard model. And yet making an ideal cipher assumption on AES is problematic: AES admits related-key attacks, and proofs that rely on an ideal cipher assumption may not apply to quantum adversaries. As another trade-off, a mode of AES that has multi-user security and permissive per-user usage limits will likely require beyond-birthday security. The most obvious way to achieve this is with nonce-based key derivation, which results in poor performance on short messages. A permutation-based mode, or a mode designed for use with a 256-bit block cipher, would not encounter these issues, but would not meet the requirement to support AES.

We are sure that participants in the workshop will have many views on how to make these trade-offs, and with this talk we hope to encourage discussion around such issues. We view our recent paper and its VIGORNIAN scheme as a contribution towards this process, illustrating how we tried to strike a balance between all our own requirements. The NCSC believes that standardising more than one accordion mode may be necessary in order to provide good solutions for all use cases, but an excessively broad portfolio could hamper deployment or interoperability, and we are interested to discuss this further.