



Chapter 10 Declaration of Inventors/Submitters

Declaration of Inventors/Submitters

We are not only unaware of any algorithmic weaknesses, but we have enlisted external help and a new submitter to prove non-existence of weaknesses. We believe that we have adequately immunized the ZK-Crypt against any known power measurement or radiation attack. We believe that the design is inherently immune to probing the inner workings of the ZK-Crypt hardware. Protecting keys and key loading is out of the scope of the NIST SHA3 contest, and methods for doing so are not included in this document. Note that Fortress mature hardware deployed secured process technology is an intrinsic part of the company's asset, and the source of a company slogan "if you want to keep a secret, don't know it".

We know of no hidden weaknesses in the design of the ZK-Crypt. We have designed the engine in good faith; have opened the design for review by experienced engineers, cryptanalysts and security experts in all phases of digital and cryptographic design. We have not introduced backdoors, Trojan horses or other means that would allow us or anyone who learned the device to use such knowledge advantageously. Should we learn of any weakness, in the hardware or the protocol, we will make prompt amends.

We have enhanced the initialization process and tweaked the hardware to speed up initialization, ciphering and authentication processes. A weak key or no loaded key will not preclude a complete pseudo random dispersion as shown by a manual study in Appendix 3 of the untweaked ZK-Crypt. For effective, accelerated hash initialization the Global (Pre)set command assure a reasonable start for short message authentication.