

The ZK-Crypt Data Authenticator/Stream Cipher/True Random Number Generator

FortressGB's 9.5K gate ZK-Crypt Hash/Stream Cipher is 2.5 times faster and stronger than AES 128 devices with inherent DPA resistance, & uses less than 1/5th of the Current Consumption per processed bit. It's Green and your solutions will "smell like roses". The engine is tailored to 8, 32 & 64 bit CPUs.

The ZK-Crypt is 1 Best of Breed Solution for 4 Burning IT Security Dilemmas-

Hash (Unkeyed) Data Authentication- The ZK-Crypt Hash was designed to augment or replace the NIST Family of SHAx Secured Hash Devices for Transparent, Faster, Stronger, Lowest Energy, Proof of Authenticity of Safe Boots, Pictures, Text, Financial Transactions, No-Fiddling of Automotive Parameters, etc. The device is herd-collision proof for the first 2^{61} 32 bit frames, and provably immune to Message modification. (Moving a decimal point is the fraudsters' Holy Grail.)

MAC (Secret Keyed) Data Authentication- The ZK-Crypt MAC provides strongest assurance of origin. The MAC is the ZK-Crypt Hash with a Secret Key.

Stream Cipher- The ZK-Crypt cipher is a well reviewed solution for Hi-Security, Low Cost & Hi-Speed Encryption for Internet Servers, Mobile Phones, Satellites, Pay TV, & Smart Cards with small, 128 bit, & up to 512 bit secret keys. The ZK-Crypt I tested on silicon by the ETH, proved to be the outstanding device compared to seven other worthy contestants. The new direction cipher was based on prized hash features; e.g., a hybrid non-linear algebraically intractable expansion PRF with dual orthogonal feedbacks for maximum diffusion and for proactive hashing in secret keys and IVs.

True Random Number Generation- The ZK-Crypt TRNG (True Random Number Generator) a green AIS 31 FM Noise Source, meeting requirements for BIS, Visa/MasterCard/Europay & Common Criteria Specs for "On Lie Provable Randomality". On the real estate of a TRNG, vendors will get all 4 Vital Symmetric Crypto-Devices. We are there with the lowest cost quadruple function.

Parallelization & Concatenation- The massively diffusive dual track orthogonal feedback precludes Message or Key/IV modification. Working in Tandem, being fed the same Message one engine set can de/encrypt while the second engine set can authenticate; e.g., for fast booting encrypted data. Concatenating two or more units with swapped or rotated feedback streams linearly increases speed to meet the emerging 10 Gb/s communication systems with lowest cost, and exponentially increased cryptocomplexity.

David Naccache, a Very Respected Industrial/Academic Cryptographer wrote- "The characteristics of the ZK-Crypt Data Authenticator/Stream Cipher/RNG fit the requirements of future generation smart cards: low power, reduced critical paths, only $8K^1$ gates - where all this boils down to is a secure 3 Gb/s throughput when clocked at 100 MHz. Being AIS 31 compliant paves the way to a valuable cheap True Random Number Generator." ¹(Preliminary Version without the Mersenne Prime Counters and Dual Feedback Tracks.)

The Green ZK-Crypt is strong, fast, & compact – it fits every peripheral & every budget.