

ZK-Crypt –Crypto Engines for a Long Secure Future

The ZK-Crypt engines are compact hardware modules which can be used in SOC designs to efficiently encrypt, decrypt and authenticate clear and cipher text; or spawn unpredictable on-line provable true random numbers.

The triple function ZK-Crypt configurable engines are designed to operate at from 0.5 to 200MHz; where an engine processes 32 bits on every clock cycle.

The ZK-Crypt engine and protocol have achieved highest marks in the most rigorous crypto-tests: NIST, Maurer, DieHard, Repeated Word, Binary Differentials, Distinguishing & Impossible Features, and demonstrate immunity to Differential and other known Cryptanalytic attack strategies. ZK-Crypt's mathematical complexity precludes attacks on future quantum or conventional computation platforms.

Compare to the Industry's Standards:

AES family

- at least 2.5 faster and far stronger
- about 1/20 AES's μ Watt/sec per processed bit
- multipermutation vs. Feistel-like architecture
- ZK-Crypt is inherently immune to algebraic attacks
- ZK-Crypt replaces pricey & non AIS 31 RNGs

NIST HMAC Compliance - ZK-ENMAC is Best

The ZK-Crypt efficiently performs NIST HMAC FIPS 198 and 198a Authentication.

The ZK-ENMAC protocol operating on encrypted data is stronger and more efficient.

Patents on Architecture, Orthogonal Feedback and Random & Deterministic Noise Generator.

ZK Crypt – Highlights:

- Hybrid non-Linear Filters Maximize Diffusion
- Multipermutation with only 9.5 K gates
- Portable– using the same block for Servers & Smart Cards
- Highly Diffusive- 1 bit Affects 144 bits
- Inherent Side Channel Attack (DPA) Immunity
- Hi-throughput: 5 Giga bit/sec @ 160 MHz
- ZK-ENMAC- Fastest Robust Authenticator
- AIS 31 All Digital True Noise Generator
- Fastest Strongest Password Authentication
- Precludes Message Modification

The ZK Crypt Target Applications:

- Secure Wireless & Mobile Communicators
- Fast Secure Communication & Emerging 10 Gb/s Protocols; e.g., (EPON, GBE)
- True Random Number Generation for Crypto, CPU simulators & SED generators
- Secure Download of Content from Anywhere using (FTP, HTTPS, VPN)
- De/Encrypts Mass Storage and Video/Multimedia Broadband On the Fly (Pay TV)
- Personal Portable Storage (USB, Memory Stick, Unsecured Hard Drives, Smart Cards)
- Secured Boot (Servers, Home PCs, Embedded Systems & Military Applications)
- Tamper Proof Automotive Motor Controllers



The ZK-Crypt Multipermutation Architecture

The Register Bank- a Leak-Proof Secret Vault consists of 4 pairs of concatenated unique pseudoLinear Feedback Shift Registers- nLFSRs in 4 tiers. FSRs and tiers are clocked and permutation controlled by the Random Controller, and fed dense and LFSR feedbacks. Tiers are filtered and non-linear combined to output a 32 bit word to the Data Churn.

Random Controller- Multiplies Multipermutation deterministically (and randomly) regulates clocks and permutations in the Register Bank and Churn.

The Data Churn- 8 Layers of Multipermutation consists of tiers of hybrid linear/non-linear combiners with memory, and 2 four rule displacement matrices. The Data Churn inputs two versions of the Lower Feedback and outputs five uncorrelated 32 bit words to the Result/Dual Feedback Processor. The stand alone Churn possesses intractable Algebraic Complexity.

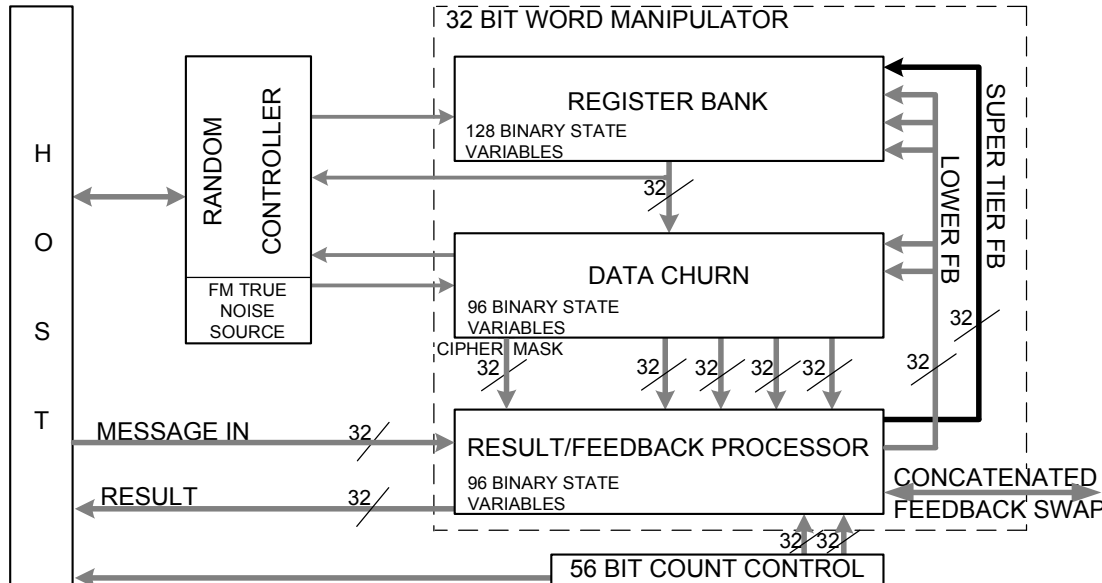
Configurations: Used in tandem, twin engines simultaneously encrypt/decrypt input data whilst authenticating same input data and validating the source of said data.

With concatenated engine configuration, twin engines work on a 64 bit bus, robustly granting doubled speed with "better than military" cryptocomplexity with same low per-processed-bit current consumption.

Result/Feedback Processor- Precludes Fraud consists of one Result and 2 Feedback Registers with random logic to generate two dense orthogonal Feedback streams, provably precluding hostile Message modification.

The all digital AIS 31 Noise Generator breeds hi-entropy true random permuting signals thousands of times faster than expensive popular mixed signal analog noise sources.

ZK Crypt Block Diagram:



Acronyms:

Table with 2 columns: Acronym and Definition. Includes entries for SOC, RNG, NIST, AES, HMAC, DPA, FIPS, and AIS 31.