



WHAT THE HOST SEES IN THE ZK-CRYPT

TO BE REVISED- NOT COMPLIANT WITH JANUARY 2009 SUBMISSION

A BRIEF GUIDE TO THE INTERFACE, THE CONFIGURATIONS,
THE FUNCTIONS, THE COMMANDS, THE GATE COUNT,
THE CURRENT AND ENERGY CONSUMPTION OF THE ZK-CRYPT
A VERY LOW CURRENT, FAST, COMPACT, COST EFFECTIVE,
UP TO 256 BIT KEYED SYMMETRIC SECURITY DEVICE.

A DOCUMENT FOR THE SILICON FAB DESIGN REVIEW
AND FOR NIST HASH CONTEST* SUBMISSION

ZK-CRYPT-THE 9.5K GATE SYMMETRIC PERIPHERAL FOR BEST OF BREED

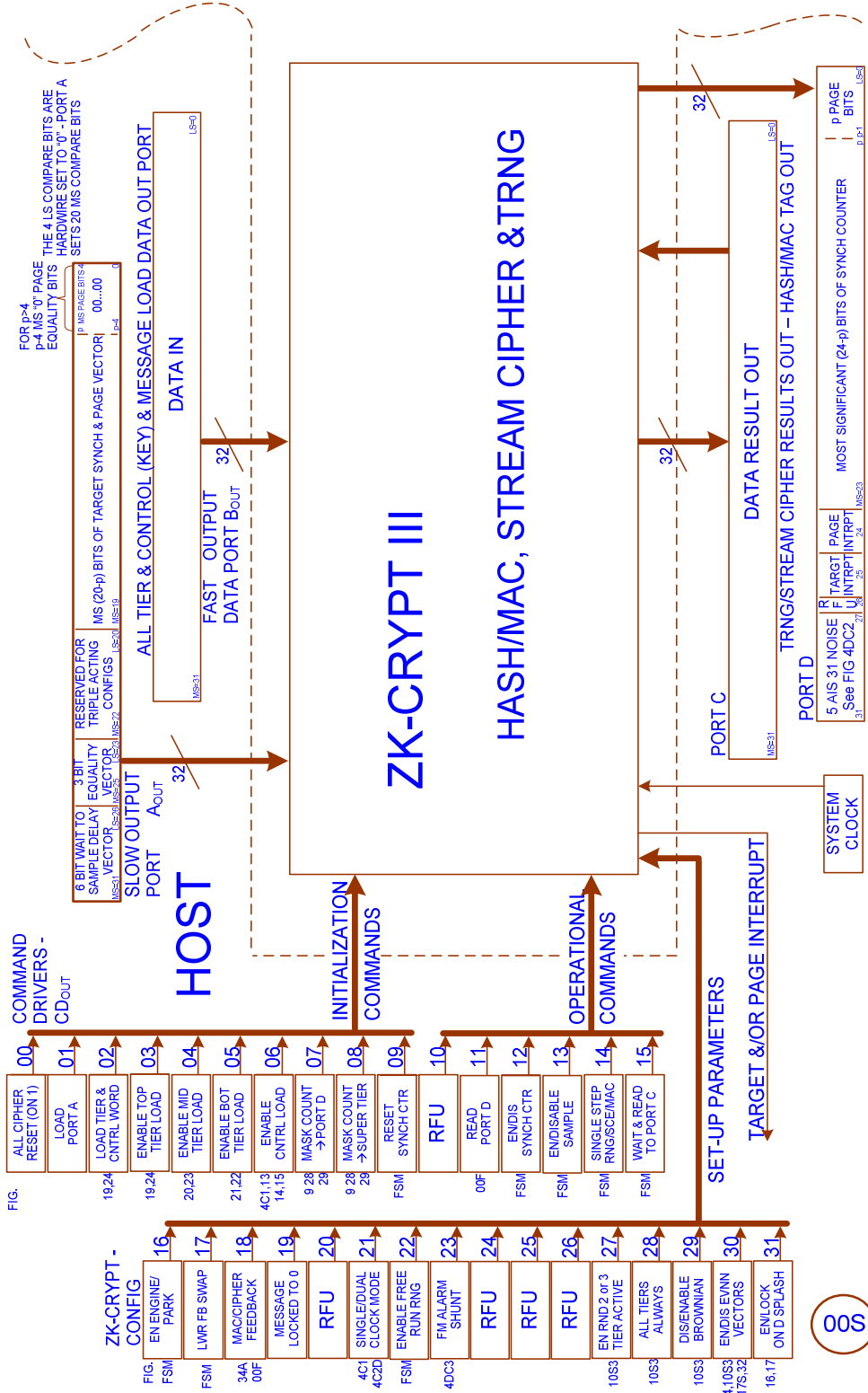
SINGLE STEP 32 BIT STREAM CIPHERING
WITH PAGE SYNCHRONIZATION

DUAL TRACK FEEDBACK HASH*/MAC AUTHENTICATION
WITH THE MAC MIX ANTI-COLLISION PERMUTATION

AIS 31 COMPATIBLE TRUE RANDOM NUMBER GENERATION
WITH A RANDOM FREQUENCY MODULATED CLOCK
AND ON-LINE ENTROPY MONITORING

all with LOW POWER, 32 BIT SINGLE STEP HIGH DIFFUSION
3 GIGA BITS/SECOND at 100 MHz OPERATION

JULY 2008



COMMANDS, INTERRUPTS AND DATA I/O

Command Name signifies Active on 1; XX/YY → XX@1 is active & YY@0 is active
 Explicit explanations found in the following Addendum and the circuit & concept drawings. Tilde (~) suggests "usual, or in the majority of cases" condition.

COMMAND DRIVERS - INITIALIZATION COMMANDS – Preferred Settings

Port Index	Label	SCE	MAC	TRNG	Where Found	Comments
00	Cipher Reset	~0	~0	0	On all variable Flip-flops	The Global Reset to "0" initialization. Active on 1. Certain control bits are set to "1".
	Loading Commands	0	0	0	Figs. 4, 13, 14, 15, 18, 19-24	For 128 bit Secret Key Loading. For maximum uncertainty in the Data Manipulator, extended running keys and IVs are diffused into the ZK-Crypt in MAC mode.
01	Enable Load Port A	0	0	0	Fig. 00S	Used when Mask Counter is used for Page or Target synchronization; used for multi-step highest security functions are used.
02	Load Tier or Control Word	~0	~0	0	Fig. 00S	Active "1" Enables Loading of Top Tier. Must be active before activating "(Delayed) Load Any Tier &/or Control Vector"
03	Enable Top Tier Load	~0	~0	0	Fig. 00S	Active 1 Enables CMD 02
04	Enable Mid Tier Load	~0	~0	0	Fig. 00S	Active 1 Enables CMD 02
05	Enable Bot Tier Load	~0	~0	0	Fig. 00S	Active 1 Enables CMD 02
06	Enable Control Vector Load	~0	~0	0	Fig. 00S	Active 1 Enables CMD 02
07	Mask Count to Port D	0	~1	0	Figs. 00S, 8P	Host Reads to Synchronize Pages
08	Mask Count to Super Tier	0	0	0	Fig. 1C	Enables HAIFA protection of relocation of short sequences.
09	Reset Synch Counter	~0	~0	?	Final Patent in Preparation	For Counting fr pulses in 1/2 Primary Clock Period – AIS 31 Noise Statistics

COMMAND DRIVERS OPERATIONAL COMMANDS-Preferred Embodiments

Port Index	Label	SCE	MAC	RNG	Where Found	Comments
10	RFU	-	-	-	-	
11	Read Port D	~0	~0	0	00S	When Testing- Sampling may be disabled (21).
12	Enable/Disable Synch Counter	~1	~1	~1	Figs. 8, 9	Useful in initializing all functions.
13	Enable Sample Result	~1	~0	1	Figs. 7SEQ, 31HM	Only for Reading Results
14	Single Step RNG/SCE/MAC	1	1	1	FSM	Enables the preferred mode of operation. May Read Message Word &/or output Result.
15	Wait & Sample	0	0	0	FSM	Hi-security -

ZK-CRYPT CONFIGURATIONS- Settings for Preferred Embodiments

Port Index	Function	SCE	MAC	RNG	Where Found	Comments
16	Enable Engine/ Park	1	1	1	FSM	On "0" Disables System Clock.
17	Lower FB to Near Neighbor	*	*	*	Fig. 40SWAP	Chaining Option to Near Neighbor for Multiple Word Acceleration & Security.
18	MAC/Cipher Feedback Mode	~0	1	~1	Figs. 7SEQ 40SWAP	MAC Mode for MAC, Hash and TRNG always for Initializing Stream Cipher
19	Message Locked to Zero	~0	~0	*	Figs. 7SEQ 40SWAP	During "Scrambles" and Reading Hash/MAC Result.
20	RFU	NA	NA	NA	NA	Reserved for Future Use.
21	Single/Dual Clock Mode	1	1	0	Figs. 4xx	Dual Clock for TRNG only- with Free Running Oscillator.
22	Enable Free Running Osc.	0	0	1	Figs. 4xx	Noise Source is based on random Freq Modulated Free Running Oscillator
23	FM Alarm Shunt	0	0	~1	Figs 4DC3 & 4	Active "1" – Lower Base FM Osc Frequency Active "0"- Increases FM Osc Frequency
24	RFU	NA	NA	NA	NA	Reserved for Future Use.
25	RFU	NA	NA	NA	NA	Reserved for Future Use.
26	RFU	NA	NA	NA	NA	Reserved for Future Use.
27	Enable 2or3 Tier Activation	1	1	1	Fig. 10S3	Preferred mode with abt 12% more current consumption than Random Single Tier active.
28	All Tiers Always	1	1	1	Fig. 10S3	" " " "
29	Dis\En Brownian Permutation	0	0	0	Fig. 10S3	XORing rotated tier images randomly is a valuable permutation. Disable for testing only.
30	Enable EVNN Vectors	1	1	1	Figs. 4, 10S3	A valuable permutation. Assures equiprobable odd and even number of ones in output words.
31	Enable Lock on D Splash Vector	~0	~0	0	Figs. 16BSM & 17TSM	Recommended for Legacy Software only- Lengthy displacement in Software

PORT A-TARGET, PAGE &MULTI-STEP COUNT PARAMETERS

100	Synch Target Address Figs. 00S PORT A BITS 0-19 THE 4 LS PAGE BITS ARE HARDWIRED TO ZERO	<p>The Synch & Page Target value in Port A Fig. 00S, is the 20 MS bit portion of the Target value, the LS 4 bits are hardwired zeroes. The 24 bit Target Address value is typically the address of the first word to be decrypted from a long file. Using one of the Synch to Target Operation commands, 12 or 13, the programmer prepares the mask for the start word of the decryption sequence.</p> <p>The p LS address bits (of 2^p word sized page) are all zeroes. The four LS bits of the Target Address are always (hardwired) zeroes; so that the smallest addressable page consists of 16 32 bit words (see Page Equality Fig. 8).</p>
124	Page Equality Figs. 00S, 8 & 9 Page Equality Vector PORT A BITS 23, 24 & 25 Target Number values in PORT A include the MS 20 Bit portion of T which resides in locations 19 to 0	<p>A three bit number operative to regulate an output interrupt to the host, to signify the beginning of a new page. The Synch Comparator triggers the interrupt when the "Page Equality" designated number of Least Significant bits in the Target Register equals the same Least Significant bits of the Synch Counter.</p> <p>The all zero (000) MUX Page Equality Address input deactivates the Page Interrupt. The Synch Counter is hardwired to Port D in the Host, such that at each page end an Interrupt is optionally generated.</p> <p>The defined page MUX sizes for flagging or interrupting are:</p> <p>000 No Page Flag or Target Interrupt (Interrupt Disable)</p> <p>001 4 bit page equality → 16 32 bit words 512 bits of data p=4 010 5 bit page equality → 32 32 bit words 1024 bits of data p=5 011 6 bit page equality → 64 32 bit words 2048 bits of data p=6 100 7 bit page equality → 128 32 bit words 4096 bits of data p=7 101 8 bit page equality → 256 32 bit words 8K bits of data p=8 110 9 bit page equality → 512 32 bit words 16K bits of data p=9 111 10 bit page equality →1024 32 bit words 32K bits of data p=10 where for p>4, the p-4 LS page bits of the target value in PORT A are zeroes.</p>
126	Sample Delay Vector Figs. 00S & 3 PORT A BITS 26 to 31	<p>A 6 bit input, n, constant – in Port A specifying n-1 Primary Clocks which activate the Register Bank prior to the automatically activated Read Sample Command - used only with the Wait and Read Sample to Port C command. 1<n<64. For n=1 use Single Step Mode.</p> <p>Single Step RNG/SCE/MAC activation of the ZK-Crypt is the more resource conserving mode of operation and is unaffected by the Sample Delay Vector.</p>

PORT B DATA IN MESSAGES & INITIALIZATION LOADED CONSTANTS

200	Crypto-Message In Figs. 00F, 00S PORT B	<p>A 32 bit Message Word. In a typical SCE or MAC hardware implementation the Message Word resides in the Host's Port B prior to positive edge of a Sample Command, i.e., Single Step RNG/SCE/MAC, Wait & Read Sample, or Sample Result (Only) Operational Commands. In preferred initialization procedures, keys (secret and IV) are also loaded as MAC Mode Messages.</p>
-----	--	---

PORT C RNG/SCE DATA RESULT & HASH/MAC SIGNATURE OUT

<p>300</p>	<p>Data Result Store</p> <p>Figs. 00F PORT C</p>	<p>In Single Step RNG/SCE/MAC and multi-step Wait & Sample RNG/SCE/MAC operations the Host reads the relevant results after the Sample Step. The sampled result value resides in the ZK-Crypt RESULT Store. The Result Store is not read during SCE or MAC Initialization, and during MAC Message input.</p> <p>In the MAC Feedback mode, the Result Store Outputs the Previous Result to be XORed to the Present Result in the Feedback Stream, during the Message input process. At the end of the MAC data input, the MAC/Hash result is read from the Result Store.</p>
-------------------	---	---

PORT D SYNCH COUNTER WITH INTERRUPTS, & AIS 31 TEST BITS

<p>400</p>	<p>Synch Num Out</p> <p>Figs. 00S, 8 & 9 PORT D COUNTER BITS 0-23</p>	<p>All 24 bits of the Synch Counter output are hardwired to the Host Port D.</p>
<p>424</p>	<p>Page & Target Interrupt</p> <p>Figs. 00S, 8 & 9 PORT D BITS 24 & 25</p>	<p>The Equality Logic Array regulates the number of zero LS bits of the Synch and Page Target Address operative to trigger a Page interrupt. The Page Equality denotes one of the seven page lengths. At the start of a page a Page Interrupt may be generated. See Page Equality.</p> <p>Preferably, reading Port D should Acknowledge Interrupt (lower flag).</p>
<p>426</p>	<p>RFU</p>	<p>Reserved for Future Use</p>
<p>427</p>	<p>AIS 31 Test Bits</p> <p>Figs. 4x PORT D BITS 27-31</p>	<p>AIS 31 specifies running Statistical testing on the output bits of the Noise Source. The four MS bits are all unbiased binary bits which may be read by the Host. to assemble 512 or longer bit streams. FortressGB suggests using the proprietary counter method for testing.</p> <ul style="list-style-type: none"> Bit 27 Current Compensator – Relates to (P)Random Clock Bit 28 Juggle Splash Toggle Bit 29 4th Toggle Bit 30 das L/R Slip Toggle Bit 31 fr – Oscillator Clock

EXTERNAL HOST DRIVEN CLOCK

<p>500</p>	<p>System Clock</p> <p>Figs. 00S, FSM HOST SUPPLIED</p>	<p>The System Clock is a derivative of the Host clock, input into the ZK-Crypt. The System Clock is the sole synchronizer/clock driver of the ZK-Crypt (with the exception of the (P)Random Clock generator operating in the Dual Clock Mode). The Primary Clock is derived from the System Clock, but is active only when commanded by the Host.</p>
-------------------	--	---

Commands, Interrupts and Data I/O

The following describes the I/O signals of the first tape-out version of the ZK-Crypt. As graphically illustrated in the referenced "ZK-Crypt Circuit & Concept Drawings", the following commands, interrupts and data I/O are operative to execute the variety of modes of True Random Number Generation, Stream Ciphering and Message Authentication Coding, TRNG, SCE and MAC, respectively.

This document does not describe the Fortress proprietary methods or circuits that assure safe tamperproof encapsulation.

<p>All Tiers Always</p> <p>Figs. 10P & 10S3</p> <p>CONFIG COMMAND 28</p>	<p>The Command that Enables the Enable Random 2 of 3 Tiers.</p>
<p>Cipher Reset</p> <p>Global</p> <p>INIT COMMAND 00</p>	<p>An asynchronous command used prior to loading the Initial Condition variables for Stream Ciphering or Message Authentication. All variables must be Set to the initial nil condition. This may be the initial condition for Unkeyed Data Authentication.</p>
<p>Crypto-Message In</p> <p>Figs. 00F, 00S</p> <p>PORT B</p>	<p>A 32 bit message word. In a typical SCE or MAC hardware implementation the Message Word resides in the Host's Port B prior to positive edge of a Sample Command, i.e., Single Step RNG/SCE/MAC, Wait & Sample, or Sample Result (Only) Oper Commands.</p>
<p>Data Result Store</p> <p>Figs. 00F</p> <p>PORT C</p>	<p>In Single Step RNG/SCE/MAC and multi-step Wait & Read Sample RNG/SCE/MAC operations the Host reads the relevant results after the Sample Step. The sampled result value resides in the ZK-Crypt RESULT Store. In the MAC Feedback configuration, the Result Store Outputs the Previous Result to be XORed Present Result in the Feedback Stream, during the Message input process. At the end of the MAC/Hash data input, the Hash/MAC signature is read from the Result Store.</p>
<p>Disable Brownian/ Enable Brownian</p> <p>Figs. 10P,10S3</p> <p>CONFIG 29</p>	<p>The test option to disable the Rotated displacement image vector XOR permutations in the Top, Middle and Bottom Tiers, only. Disabling is not advisable, especially as the Rotated Vector is randomly enabled and disabled, to increase "local entropy". (Historically, because of legacy systems where the implementation will be in software, the Brownian vectors have been replaced by the Rotate image vectors, which are more amenable to S/W applications, hence the names Brownian, Brown, and BRN in the circuit drawings.)</p>
<p>Enable EVNN Input to MAJ Vectors</p> <p>Figs. 4,10S3, 17S</p> <p>CONFIG 30</p>	<p>Enables the output of the TOP, MID, BOT, & FOURTH interspersed "MAJ Select EVNN input to the Hybrid Filter preceding the Intermediate Store & XOR.</p>
<p>Enable Free Run RNG</p> <p>FSM</p>	<p>Enabling the Free Run RNG couples the Primary Clock Directly to the System Clock, thereby activating (stepping) the chosen Tiers of the Register Bank and the Random Controls for the duration of the Enable Free Run configuration.</p>

	<p>CONFIG 22</p>	<p>When the ZK-Crypt is in Dual Mode, the Random Clock is Free Running, and its output and configuration are seemingly unpredictable, assuming that the phase difference between the rise and falls of the fr and Primary clock are unpredictable. Maximum unpredictability can be achieved, if the unit is set to constantly Sample for the number of sample steps Loaded in the Synch Target, with Feedback set in MAC mode, and Messages Loaded in randomly into the Message input Port B.</p> <p>When the device is in a non-deterministic random number generation mode, particularly when initializing the ZK-Crypt to a random unpredictable initial condition, exercising the Register Bank and the controls for random intervals, uncontrolled by other Host commands is recommended. Single Tier activation for separate seemingly random intervals is recommended for lowest power initialization.</p>
	<p>Enable Splash/Lock on D Fig. 16, 17 & 18</p> <p>CONFIG 31</p>	<p>A Config that enables random Splashing for normal use, and alternately locks the Splash Matrix onto Vector D, whence the output is a straight through of the input. Locking the Splash Matrix is valuable for S/W applications and testing.</p>
	<p>Enable/Park Fig. 3</p> <p>CONFIG 16</p>	<p>The command that enables the System Clock, and hence the plurality of ZK-Crypt functions.</p> <p>In most implementations, the Park Mode minimizes current consumption during intervals when the ZK-Crypt is not operating. Park does not automatically change volatile variable values. All Cipher Reset is a global initialization function.</p>
	<p>Enable Random 2 or 3 Tier Activation/Single Tier Random Activate Fig. 10S3</p> <p>CONFIG 27</p>	<p>A mode of tier activation which increases current consumption on a Sample Command by an estimated less than 15%, but may more than square the complexity of analysis of the 32 Bit Manipulator. In this mode, randomly, with a probability of less than 0.5, only one of the three tiers is <u>not</u> activated at each Primary Clock cycle. (When the (P)Random clock misses a pulse, the Current Balance Compensator assures that all 3 Tiers and a portion of the Ring Oscillator control are activated, causing a normal range of current consumption. Compare this with the energy conservative strategy of randomly activating only one tier at each Primary Clock; see the Single Step RNG/SCE/MAC command. This is the preferred mode</p> <p>In this configuration "All Tiers Always" Config flag 28 must be set to "1".</p> <p>For Single Tier Activation "All Tiers Always" and Enable Random 2 of 3 Tiers are Active "0".</p>
	<p>Enable Sample Fig. 00F</p> <p>INIT COMMAND 13</p>	<p>The Enable Sample command connects the Result Store to the Host. Typically, the FSM will block the Result Store output during processes where the Result is not read by the Host; e.g., during Hash processing.</p>
	<p>Enable Splash/Lock on D Fig. 16, 17 & 18</p> <p>CONFIG 31</p>	<p>A Config that enables random Splashing for normal use, and alternately locks the Splash Matrix onto Vector D, whence the output is a straight through of the input. Locking the Splash Matrix is valuable for S/W applications and testing.</p>
	<p>Enable Synch Counter Figs. 3, 9C</p> <p>OPERATIONAL CMD 12</p>	<p>In SCE or MAC (Single Clock) configurations, the Synch Counter is operative to receive a count increment pulse at each instant that a Sample pulse is generated. When the Synch Counter is disabled, the Equality Comparator and the Synch Counters may be in an energy saving mode. Typically, the Synch Counter is disabled during initialization.</p> <p>In the Dual Clock configuration, the Synch Counter MUX selects the fr FM oscillator signal for Fortress Proprietary FM Clock on line analysis.</p>

		In the AIS 31 compatible Dual Clock configuration, the Synch Counter is preferably activated to prove that the FM oscillator is driving the Random Clock, and to prove that in short intervals, one or two Primary Clocks, that the phase between the Primary Clock and the fr frequency are uncorrelated.
	<p>En/Load Commands</p> <p>Fig. 00S Signals 02 -09 & Figs. 19 to 24</p> <p>INITIAL LOADING COMMANDS</p> <p>EN TOP TIER LOAD 03</p> <p>LOAD TIERS & CONTROL WORD 02</p> <p>EN MID TIER LOAD 04</p> <p>LOAD TIERS & CONTROL WORD 02</p> <p>EN BOT TIER LOAD 05</p> <p>LOAD TIERS & CONTROL WORD 02</p> <p>EN CNTRL LOAD 06</p> <p>LOAD TIERS & CONTROL WORD 02</p>	<p>The Init Commands for Loading the 3 Tier Register Bank, and the Controls are Host activated in a proper sequence.</p> <p>In the native up to 128 bit key mode, all secret I.C. variables are loaded directly, followed by a 4 step internal digest; followed by IV loading in MAC mode via the Message Port, typically followed by and additional 16 step MAC digest.</p> <p>All variables, native and obscure are initially set to default values, generally zero, by the global Cipher Reset Command, prior to conventional native loading.</p> <p>The native 128 bit I.C. variables consist of the 3 tiers of the Register Bank, and the Cipher Control word, which are each loaded separately, after Cipher Reset.</p>
	<p>FM Alarm Shunt</p> <p>Fig. 4C3, 4C4 & 4CVCO</p> <p>CONFIG COMMAND 23</p>	The Alarm Shunt on "0" shortens the Basic Frequency delay thereby increasing FM Ring Oscillator Frequency. Useful in those circumstances where using the proprietary test, Demerit Figure approaches or passes 65.
	<p>MAC/Cipher Feedback</p> <p>Figs.00FB & 34DBFB</p> <p>CONFIG COMMAND 18</p>	<p>In the ZK-Crypt there are two modes of 32 bit feedback.</p> <p>MAC Feedback is used to diffuse Message Words into the Data Manipulator, useful for loading extended secret keys and initial values, in both SCE and Hash/MAC functions. In Hash/MAC functions this mode is used for the Hash compression process. It is also used, Message Word = 0, for intermediary scrambling of internal variables and for maximum complexity generation of the Hash/MAC Hash Value/Tag.</p> <p>The Cipher Feedback mode is used exclusively for ciphering Messages, as the Cipher Mask is not a function of the input data.</p>
	<p>Page Equality</p> <p>Figs. 00S, 8 & 9</p> <p>Page Equality Vector</p> <p>PORT A</p>	<p>A three bit number operative to regulate an output interrupt to the host, to signify the beginning of a new page. The Synch Comparator triggers the interrupt when the "Page Equality" designated number of Least Significant bits (all zeroes) in the Target Register equals the same Least Significant bits of the Synch Counter.</p> <p>The all zero (000) MUX Page Equality Address input deactivates the Page</p>

	<p>BITS 24, 25 & 26</p> <p>Target Number values in PORT A include the MS 20 Bit portion of T which resides in locations 19 to 0</p>	<p>Interrupt. The Synch Counter is hardwired to Port D in the Host, such that at each page end an Interrupt is generated.</p> <p>The defined page MUX sizes for flagging or interrupting are:</p> <p>000 No page flag or interrupt</p> <p>001 4 bit page equality → 16 32 bit words 512 bits of data p=4 010 5 bit page equality → 32 32 bit words 1024 bits of data p=5 011 6 bit page equality → 64 32 bit words 2048 bits of data p=6 100 7 bit page equality → 128 32 bit words 4096 bits of data p=7 101 8 bit page equality → 256 32 bit words 8K bits of data p=8 110 9 bit page equality → 512 32 bit words 16K bits of data p=9 111 10 bit page equality → 1024 32 bit words 32K bits of data p=10</p> <p>where for p>4, the p-4 LS page bits of the target value in PORT A are zeroes.</p>
	<p>Page Interrupt Figs. 00S, 8 & 9 PORT D BIT 24</p>	<p>The Equality Logic Array regulates the number of zero LS bits of the Synch and Page Target Address operative to trigger a Page interrupt. The Page Equality denotes one of the seven page lengths. At the start of a page a Page Interrupt may be generated. See Page Equality.</p>
	<p>Process to Target FSM Figs. 3</p> <p>OPER COMMAND 11</p> <p>SINGLE STEP 14 WAIT & READ SAMPLE 15</p>	<p>When decrypting parts from a file, starting at any page which is not the beginning of the file, the decryption mask must first be activated to the "offset" distance from the beginning of the encrypted text, in order to output the starting and subsequent mask words. Stated differently, the procedure generates all unused masks, up to the Synch Target Address, whence an interrupt flag may be transmitted to the Host and to Port D, Bit 25.</p> <p>The procedure operates in both Single Step and Multi-Step configurations. Clients will use this command for automatic single and double DMA procedures; e.g., Message In, Previous Result out in a single clock.</p> <p>The p Least Significant bits (all zero) of the 24 bit Target Number are used to define the beginning of a new page, whence a Page Interrupt may be emitted.</p>
	<p>Result Store (Data) Figs. 00S, 00F</p> <p>Relates to- DATA PORT C</p>	<p>In Single and Multi-Step RNG and SCE operations the Host reads the relevant results after the Sample Step. Data is stable in the Result store immediately following the rising edge of the Primary Clock This value resides in the ZK-Crypt RESULT Store. During many operations, e.g., initializing the SCE and/or processing a Hash message, the output of the Result store should not be readable by the Host. (CMD 13 Enable Sample = 0).</p> <p>In MAC mode during data processing, the data in the Result store is part of the secret running key variable, and should not be readable by the Host. The final Hash/MAC signature/Tag is read from the Result store.</p>
	<p>Sample (Read) Delay Vector Figs. 00S & 3</p> <p>PORT A</p> <p>BITS 26 to 31</p>	<p>A 6 bit input, n, constant – in Port A specifying n-1 Primary Clocks which activates the ZK-Crypt Engine wherein the Result prior to the automatically activated Sample Command - used only with the Wait and Read Sample command. 1<n<64. For n=1 use Single Step Mode.</p> <p>Single Step RNG/SCE/MAC activation of the ZK-Crypt is the more resource conserving mode of operation and is unaffected by the Sample Delay Vector. This six bit number is not a part of the running secret key.</p>
	<p>Single/Dual Clock Mode</p>	<p>In the so called True Random Number Generation, TRNG, implementation of the ZK-Crypt; the constantly changing phases of the interacting uncorrelated Primary and random FM ring oscillators are the ultimate physical random source driving</p>

	<p>Figs. 4P, 4C1, 4C2D, 4C3, 4C4 & 4CVCO</p> <p>CONFIG 21</p>	<p>the True Random Controller components of the ZK-Crypt.</p> <p>Obviously, an unpredictable clock source precludes deterministic number generation, therefore, SCE and MAC are configured to Single Clock mode, and the Random Clock module is activated by the Primary Clock (derived from the System Clock not using the Free Running random FM oscillator and without random delayed data signals, see Figs. 4xx).</p> <p>The ETSI specifications for wireless devices preclude the use of a frequency source which is not derived from the system clock. Mobile phone and chip manufacturers often disregard this edict. The ZK-Crypt engine is a Deterministic Random Number Generator. When loaded with a random seed, the Engine is the equivalent of a real RNG.</p> <p>The AIS 31 device specifically addresses the separation of generation, loading and storing compressed entropy in a deterministic Random Number Generator. This storage process of generating redundant entropy in the very fast ZK-Crypt can be accomplished during a few milliseconds in parallel with the normal power up sequence of a wireless communication device, prior to activating over the air communications, when quality random strings can be generated in the Single Clock Mode. We estimate that manufacturers will find either that the very restricted area of oscillations does not generate harmful radiation, or that a 5 or 10 millisecond burst of noise will not interfere with audio transmissions.</p> <p>The Dual Clock mode enables applications that must "prove" on line unpredictability. The autonomous FM oscillator is activated when the Primary Clock is configured to "Free Run". Typically, the autonomous clock is only activated for random string generation for establishing initial random string conditions, or for extended use while generating concatenated strings of random numbers.</p> <p>The missed pulse and the 4 unbiased output signals of the Random Clock are-</p> <ul style="list-style-type: none"> a) the (P)Random Clock which is an "occasional" missed pulse clock stream (average about 1/12 missed pulses). It drives the Top/Mid/Bot Control Units. The clock stream is synched to the Primary Clock; b) the unbiased fr signal active only in Dual Clock mode is the autonomous random FM clock signal; c) the Juggle Splash Toggle regulates the Top and Bottom Splash displacement vectors; d) the 4th Toggle (EVNN) affects the MAJ function in every fourth interspersed hybrid filter which combines 4 near neighbor outputs of the Splash Matrices; and, e) the das, (digitized analog signal) determines if a Control Unit Slip signal output affects the Left or Right hand nLFSRs of the Top, Middle or Bottom Tier. <p>Signals a, c, d and e are active in the SCE, MAC and Hash functions, wherein the output is deterministic. In an AIS 31 application, preliminary to sampling random number strings, the device must determine if the TRNG shows signs of random activity. The simplest test is to determine if the fr is oscillating. Subsequently, the standard requires statistic nibble tests of the c, d and e entropic signal outputs.</p> <p>In Single Clock mode, unpredictability is provided indirectly by 8 MS signals of random data from the Register Bank, and signals are effectively debiased by the LS bit of a programmable up-counter.</p> <p>Ring oscillators are typically used as random noise sources. In Figures 4C3, 4C4, and 4CVCO, oscillators based on delay lines (typically in FPGAs) and randomly</p>
--	--	---

		<p>generated bits which modulate Digital to Analog voltage sources which drive Voltage Controlled Oscillators respectively are designated. All such devices are typically randomly sensitive to minute changes in supply voltages and in-circuit temperatures, and thus have unstable frequencies. Typical ring oscillator frequencies often vary more than 20% from a prescribed base frequency.</p> <p>The Random Clock in both Dual and Single Clock modes generates equivalently excellent statistical unbiased signals (c, d and e), as prescribed by the BIS AIS-31. Typically, the only constraint in Dual Clock mode is that the Host primary clock sampling frequency is at least consistently 10% slower than the fr frequency. FortressGB has tested and measured outputs both on silicon and the more robust software simulator.</p>
	<p>Single Step (Sample) RNG\SCEMAC</p> <p>Figs. 00S, FSM</p> <p>OPER COMMAND 14</p>	<p>The fastest mode of operation for Random Number Generation (from a high entropy random Initial Condition); stream cipher encryption and decryption; and message authentication. This is the preferred mode of operation producing excellent statistics.</p> <p>A single concurrent Primary Clock pulse and Sample pulse activate the selected tier (or tiers) and store previous outputs into defined Store buffers while activating concurrent permutations.</p> <p>At the Positive Edge of the Sample RNG or SCE command; the "Previous Result" is loaded into the Result Store.</p> <p>When in MAC mode of operation, the stepped digest results are not read by the Host, but are digested, "recycled", into the Register Bank;</p> <p>In MAC mode, after processing of the "Message" Data, the Host reads out the "signature" words, See Fig. 00O.</p>
	<p>Synch Num Out</p> <p>Figs. 00S, 8 & 9</p> <p>PORT D</p> <p>COUNTER BITS 0-23</p>	<p>The 24 bits of the Synch Counter output are hardwired to the Host Port D.</p>
	<p>Synch Target Address</p> <p>Figs. 00S</p> <p>PORT A BITS 0-19</p> <p>THE 4 LS PAGE BITS ARE HARDWIRED TO ZERO</p>	<p>The Synch & Page Target value in Port A Fig. 00S, is the 20 MS bit portion of the Target value, the LS 4 bits are hardwired zeroes. The 24 bit Target Address value is typically the address of the first word to be decrypted from a long file. Using one of the Synch to Target Operation commands, 12 or 13, the programmer prepares the mask for the start word of the decryption sequence.</p> <p>The p LS address bits (of 2^p word sized page) are all typically zeroes. The four LS bits of the Target Address are always (hardwired) zeroes; so that the smallest addressable page consists of 16 32 bit words (see Page Equality).</p>
	<p>System Clock</p> <p>Figs. 00S, 3</p> <p>HOST SUPPLIED</p>	<p>The System Clock is a derivative of the Host clock, input into the ZK-Crypt. The System Clock is the sole synchronizer/clock driver of the ZK-Crypt (with the exception of the (P)Random Clock generator operating in the Dual Clock Mode). The Primary Clock is derived from the System Clock, but is active only when commanded by the Host.</p>
	<p>Target Interrupt</p> <p>Figs. 00S, 8 & 9</p>	<p>An interrupt flag is activated by the Equality Comparator when the Synch Counter value is equal to the Synch Target Address value.</p>

	PORT D BIT 25	
	Wait and Read Sample FSM OPER COMMAND 15	The asynchronous command operative to activate the Register Bank, a fixed number of steps wherein at the last step designated Stores latch-in relevant Data.

Summary of Silicon Resources & Estimated Gate Activity of ZK-Crypt Configs*

Itemization of Modules in Pages 15-16 – To be revised to accommodate Dual Track Feedback.

Functional Module	Gates for Config
Control Mechanisms without FSM and Synch/TRNG	945
Data Manipulator (Register Bank & Data Churn)	6200
Bare Bones Stream Cipher & MAC	7145
Synch, Current Balancing & TRNG Ancillaries	695
Finite State Machine - Est Old Fig3	300
Ancillaries for full Implementation	995
Super Tiered Doubled MAC & Cipher Feedback SCE/MAC/TRNG with Transmission Synchronizing Current Balancing & TRNG	8140

The Final Gate Count is dependent upon the fab technology and the silicon compiler's minimization. The above estimate includes abt 5% overhead for non-minimized implementation with estimated gate activity, 66%.

The addition of almost 3000 gates over the original less than 5000 gates was made to increase running key lengths in Stream Ciphering and Data Authentication, according to the eSTREAM norms, and to assure satisfactory statistics in single step Software Legacy applications. The present architecture supports and length secret key.

True Random Number Generation AIS 31 additions added less than 400 gate equivalents, which are used for enhanced DPA current balancing. MAC feedbacks are used for TRNG and SCE initialization; and a Cipher and MAC Feedback functions have been added for increased crypto-complexity. With a pipeline implementation driven at 100 MHz clock, the throughput is 3.2 GBits/sec in all three modes of operation, Stream Cipher, Data Authentication, and TRNG; 2.5 faster than AES 128 published implementations.

For first cut cost benchmarking, we chose the bits/gate at 100 MHz. The ZK-Crypt decrypts/encrypts about 400K bits/gate at 100 MHz, at least an order of magnitude better than compared designs. We note that ETH has implemented the basic algorithm on silicon, using 25 μ technology while operating the device at 203 MHz. For low power applications, battery and mobile applications, where total energy consumption per word processed is important.

The popular benchmark is Megabit/ (mW•second). Here with the 0.09 μ technology, at 1.8 volts, we anticipate about 1,000 [MBit/mWatt Sec] against AES (without second order current countermeasures) at 13 [MBit/mWatt Sec] (or less than 4 [MBit/mWatt Sec] with countermeasures) or A/51 with about 273 [MBit/mWatt Sec].

The addition of the Synchronizer, and current balancing flip flops, adapted to TRNG processing, was necessary for full compliance to the AIS 31 standard for True Random Number Generators, with full online testing, and for FM Modulation of the Random Oscillator.

Itemization of Silicon Resources and Gate Activation

Gate Equivalents (Standard Gate is a 2 input NAND gate)

2in NAND equiv	1 Gate	D-Flip Flop without Reset	5 Gates
3in NAND	2 Gates	D-Flip Flop with Reset	6 Gates
2in XOR/NXOR	3 Gates	D-FF with Clock En & Rst	7 Gates
3in XOx/NXOR	6 Gates	4 Bit Expandable Counter	51Gates
4in MUX nonInvert	8 Gates	8in MUX	15 Gates
3 in MAJority	3 Gates (Fab Implementations 3 Gates)		

The (P)Random Controller

Cipher Control Modules	Gates	Equiv x #	Total
Top Control Unit Fig. 13	2NAND 2XOR 3XOR DFF+S Total	20x1 10x3 4x6 8x7	135
Middle Control Unit Fig. 14	2NAND 2XOR 3XORx DFF +S Total	23x1 10x3 4x6 10x7	150
Bottom Control Unit Fig. 15	2NAND 2XOR 3XORx DFF +S Total	24x1 10x3 4x6 11x7	160
Splash Random Stepper Fig. 18	2NAND 2XOR DFF Other Total	7x1 3x3 2x7 5	40
(P)Random Clock with Dual Clock Switching without Delays and without Random FM Ring Oscillator Figs. 4x See TRNG	2NAND 2XOR 3XOR DFF Total	38x1 13x3 15x6 20x7	350
Tier Selects (Controls) Figs. 4x	2NAND 2XOR 3XOR 8 MUX Total	55x1 6x3 3x6 1x15	120
Control Mechanisms Total Resources			955

Resources for the Data Manipulator (Register Bank and Data Churn)

Data Manipulation Modules	Gates	Equiv x #	Total
Super Tier nLFSR cells– Fig. 28 & 29	2NAND 2XOR DFF Total	5x2 18x3 32x6	265
Super Tier Rotated & Image XORed & XORed to Register Bank Fig. 30	2XOR Total	64x3	200
TOP Tier nLFSR cells with Load and Feedback Fig. 19	2NAND 2XOR DFF Total	64x1 86x3 32x6	530
MID & BOT Tiers nLFSR cells – with Load and Feedback Fig. 20	2NAND 2XOR DFF Total	64x2x1 86x2x3 32x2x6	1100
3 Tiers Rotated & Random XORed Tier Collection Fig. 25	2NAND 2NXOR Total	32x1x3 32x3x3	400
3 Tier MAJ Combiner, NXOR & 5 RROT Image Combiner Fig. 11S2	MAJ 2XOR Total	32x3 32x3	230
Top+Intmdt Store & XOR + 13 & 7 LROT FB Fig. 33	2XOR DFF Total	64x3x2 32x6x2	810
Top+Bot Splash Matrix & Hybrid EVNN MAJ/XOR Filter Fig. 17	4MUX MAJ 3XOR Total	32x6x2 32x3x2 32x6x2	1050
Bot & Result Store & XOR Fig. 33	2XOR DFF Total	32x3x2 32x6x2	620
Mask & Message XOR Fig. 11	2XOR Total	32x3	105
Super & Lower Feedback Stores & Lower Feedback Output Switch Fig. 34	2NAND DFF Total	128x1 64x7	600
Cipher Feedback Combining Logic Fig. 34	3NAND 2XOR Others Total	32x2 32x3 20	190
MAC/SCE Multiplexer Fig. 34	2NAND	96x1	100
Data Enhanced Manipulator Total Resources			6200

Circuitry for Synched Transmissions & TRNG Testing & Random FM Oscillator

TRNG & Synch Transmission Control Modules	Gates	Equip x #	Total
FM Ring Oscillator with Phase Delay Circuitry Figs. 4x	2NAND 3NAND DFF DELays Total	10x1 5x2 10x5 ~ 95	195
Synch Target & Page Comparator with Counter Figs. 8 & 9	2NAND 2XOR 8 MUX 4Bit Cnt Total	65x1 32x3 1x15 51x6	500
Synching & TRNG Ancillary Resources			695

Estimated FSM operative to Arbitrate & Accelerate Pipe Lined/DMA Operation

	Gates	Equip x #	Total
Finite State Machine for DMA FSM	2NAND 2XOR DFF Total	38x1 7x3 30x7	300
Est Resources for FSM	Total		300