



ALGEBRAIC ERASER™ EMBEDDED PUBLIC KEY ENGINE

Product Brief

SecureRF's foundational Algebraic Eraser™ addresses the critical security needs of resource-constrained embedded devices that require strong, but light-weight, encryption and irrefutable authentication. This security algorithm is thousands of times more efficient than other commercial solutions with ULTRA low power requirements.

Until now, existing security algorithms could not provide strong authentication and data protection on resource constrained devices. That is because these algorithms, many of them over 20 years old, rely on large complex computations that multiply large numbers and requires more computing resources than are available in embedded systems.

The patent-pending Algebraic Eraser uses small primes and a compact computational algorithm, making it uniquely suited for small processing platforms. Plus, the Algebraic Eraser uniquely combines abstract algebraic methods with number theoretic techniques that first "cloak" then "erase" components of our process making it very hard to attack.

Key Features:

- Self contained public key engine.
- Entropy levels orders of magnitude lower than the RSA or Elliptic Curve public key algorithms result in the lowest cost of ownership.
- Simultaneously achieves an operational current lower than 10uA, a gate count of less than 2,900 gates and run times shorter than 1ms.
- Scalable through build time options.
- Fully-interleaved operation with handshaking provided.
- SECURED/VIOLATION indicators.
- Test-bench provided.

Applications

- RFID tags: active, passive, semi-passive
For supply chain & cold chain management, logistics, toll systems, payment networks, defense and homeland security
- Wireless phone devices
- Wireless networks
- WiMax applications
- Peer-to-peer mesh networks
- Sensors and other resource constrained devices

Block Diagram

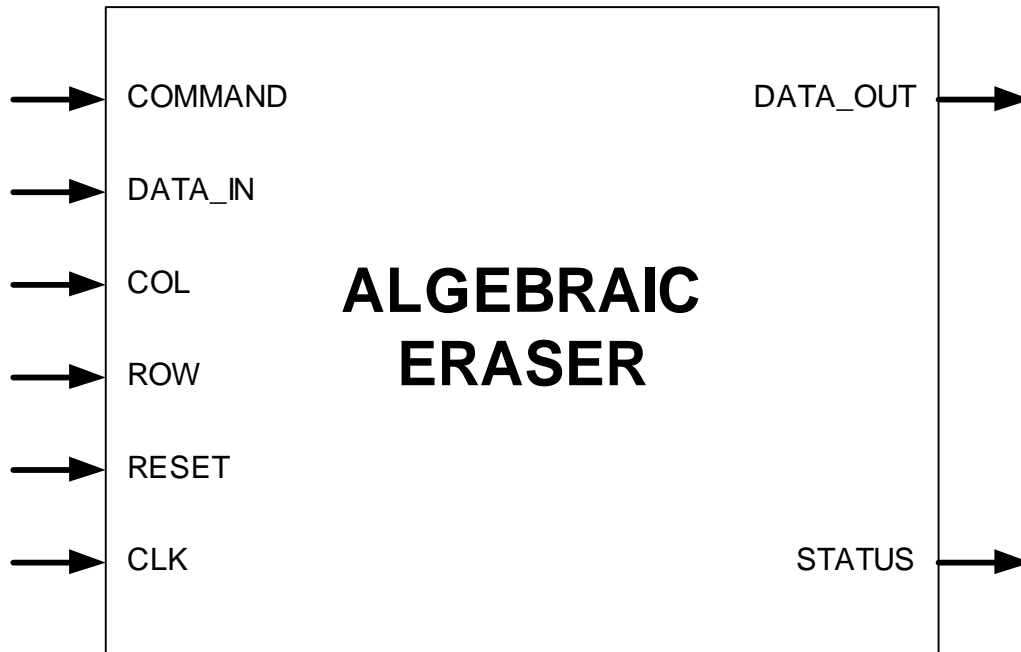


Figure 1 – Algebraic Eraser Block Diagram

Pin Descriptions

NAME	BITS	DESCRIPTION
COMMAND	4	Current AE command, ignored when STATUS is busy
DATA_IN	5	PUBLIC/PRIVATE KEY DATA used to preload the AE before shared secret is computed
COL	4	Column address used for data addressing
ROW	4	Row address, used for data addressing
RESET	1	Asynchronous reset, Active High
CLK	1	Synchronous clock, all signals (except RESET) are referenced to the rising edge
DATA_OUT	5	Computed shared secret
STATUS	4	Current operational status flags {BUSY, DONE, SECURED, VIOLATION}

Table 1: Pin descriptions for block diagram

Algebraic Eraser Hardware Architecture

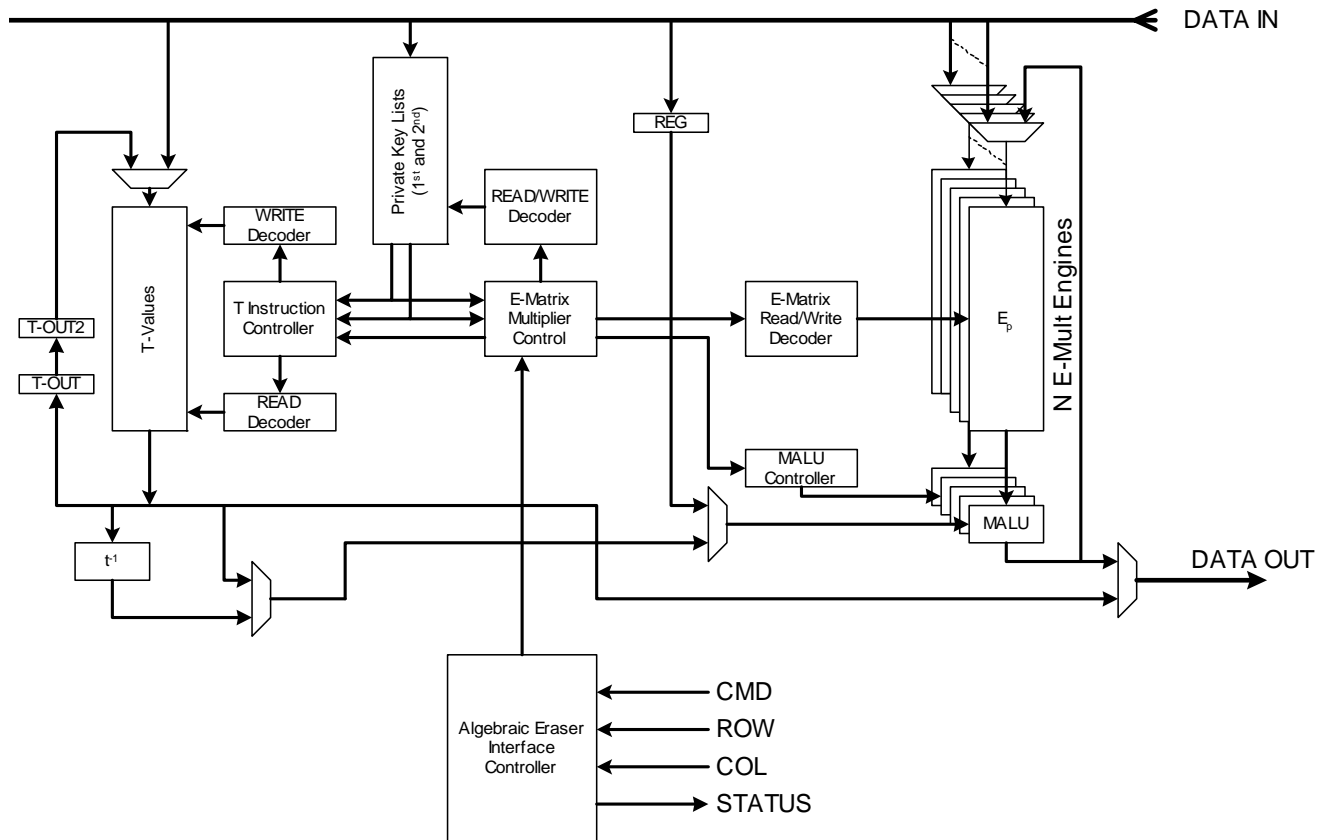


Figure 2: Hardware architecture for Algebraic Eraser

General Description

The Algebraic Eraser, in common with other public key algorithms, relies upon establishing a shared secret that is determined based upon a declared public key and an internal private key. The public key is in the form of a matrix modulo a prime p and a list of initial permutations. To perform a key exchange the public key is passed through a one-way transform in the form of a knot (described using braid group representation via Artin generators) resulting in a shared secret in the same form as the initial public key.

Why is the Algebraic Eraser ideally suited to small embedded systems?

- Small parameter sets – The Algebraic Eraser runs over a very small number system (typically a prime between 13 and 31) resulting in very small datapaths (5 bit or less)
- Small runtimes due to a very efficient computation algorithm.

More About the Algebraic Eraser

How can the Algebraic Eraser security algorithm be so efficient and yet be highly secure at the same time? In part, the answer hinges on attributes of the mathematics of infinite group theory.

A layperson can think of infinite group theory as the mathematics of braids or knots. The quality that makes this desirable for cryptography is akin to the fact that a fishing line can get entangled in a few seconds while it may take hours to untangle. With infinite groups, calculating in one direction is easy, but reversing it is extremely difficult.

Another feature of the algorithm is a cloaking function that erases part of the information as it goes along, hence the name Algebraic Eraser. This increases efficiency because smaller numbers are used. It also increases security, because the Algebraic Eraser process itself effectively erases the data that would be required for the system to be reversed (and hence broken). Traditional cryptographic algorithms do not have an erasing feature and require the multiplication and division of very large numbers thus contributing to the need for large storage and processing resources.

In fact as greater security levels are demanded the more efficient the Algebraic Eraser becomes compared to existing algorithms, see Table 2. Traditional cryptographic functions require computational levels that grow exponentially as the key size increases. The Algebraic Eraser however is the world's first algorithm to have computational requirements that increase in direct proportion (linearly) to the key size, thus running orders of magnitude faster than has been previously seen.

SECURITY LEVEL	RSA	ECC	SECURERF	VERSUS RSA	VERSUS ECC
80 Bit	1,610,000,000	55,800,000	197,000	8,172X	283X
128 Bit	43,500,000,000	143,000,000	329,000	132,218X	435X

Table 2: Number of bit operations to encode a message of length equal to the public key.

Deliverables

- Firmware
- RTL Licenses
 - Verilog RTL
 - Synthesis Script
 - Testbench and Documentation
- Netlist Licenses
 - Post synthesis netlist
 - Simulation Script
 - Testbench and Documentation

Build Options

At compile time the Verilog is parameterized to provide various security levels and latency times. Example configurations are given below.

p (bits)	n	k	Gate Count	RAM	NVM	Run time (mS)		
						1 MHz	4 MHz	200 MHz
4	12	1	2824	624	3776	61.44	15.36	0.307
4	12	2	2920	624	3776	30.72	7.68	0.154
4	12	3	3016	624	3776	20.48	5.12	0.102
4	12	4	3112	624	3776	15.36	3.84	0.077
4	12	6	3304	624	3776	10.24	2.56	0.051
4	12	12	3780	624	3776	5.12	1.28	0.011
5	12	1	2905	780	8400	122.88	30.72	0.614
5	12	2	3025	780	8400	61.44	15.36	0.307
5	12	3	3145	780	8400	40.96	10.24	0.205
5	12	4	3265	780	8400	30.72	7.68	0.154
5	12	6	3505	780	8400	20.48	5.12	0.102
5	12	12	4225	780	8400	10.24	2.56	0.051
5	16	1	2905	1360	8960	163.84	40.96	0.819
5	16	2	3025	1360	8960	81.92	20.48	0.410
5	16	4	3265	1360	8960	40.96	10.24	0.205
5	16	8	3745	1360	8960	20.48	5.12	0.102
5	16	16	4705	1360	8960	10.24	2.56	0.051

Table 3: Run times at various security levels.

Please contact us for more information.

SecureRF Corporation
 175 Post Road West • Westport, Connecticut 06880
 Phone: (203) 227-3151 • Email: info@securerf.com

www.securerf.com

Algebraic Eraser is a trademark of SecureRF Corporation.
 Encryption products are subject to export control regulations and cannot be supplied to some countries.