SECURE RF

Securing the Internet of Things®

A Lightweight, Highly Performant Public Key Exchange

August 18, 2015

SECURE RF
Securing the Internet of Things®

VERIDIFY™

Algebraic Eraser (AEDH)

- Key Agreement Based on Braids, Matrices, Permutations, and Finite Field Arithmetic
- Is NOT "Braid Group Cryptography"
- Hard Problem: Simultaneous Conjugacy Separation Search Problem in the Braid Group
- Performance scales *linearly* with security

Performance in 65nm CMOS

2^{128} Security Level

ECC 283			AE B16F256			Gain
Cycles	Gates	Wtd. Perf.	Cycles	Gates	Wtd. Perf	
164,823	29,458	4,855,355,934	3,352	20,206	67,730,512	71.7x
85,367	77,858	6,646,503,866				98.1x
70,469	195,382	13,768,374,158				203.3x

Wtd. Perf. Is Weighted Performance (clock cycles x gate count) and represents time and power usage.

ECC data taken from *A Flexible Soft IP Core for Standard Implementations of Elliptic Curve Cryptography in Hardware*, B. Ferreira and N. Calazans, 2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS), 12/2013.

SECURE RF
Securing the Internet of Things®

VERIDIFY™

Performance on ARM Cortex M3

Security Level	Algorithm	Language	ROM	RAM	Speed (48MHz)
128	AE	C + Assembly	2065	544	15ms
128	*AE*	*C*	*3339*	*521*	*34ms*
128	ECC(i)	Assembly (M0)	7168	540	233ms
128	ECC (ii)	C (ARM)	(?)	(?)	864ms
128	ECC (iii)	C (WolfSSL)	9780	7456	889ms
310	*AE*	*C*	*656*	*820*	*74ms*

ECC data: (i) *Shades of Elliptic Curve Cryptography on Embedded Processors*, Wenger, Unterluggauer, and Werner, Progress in Cryptology (Indocrypt 2013); (ii) *Crypto Performance on ARM Cortex-M Processors*, H.Tschofenig, M. Pegourie-Gonnard, IETF-92 (March 2015); (iii) SecureRF implementation

Help Review AEDH!

- We want more reviews and analysis
- Papers are available at http://www.securerf.com/

SecureRF Corporation

100 Beard Sawmill Road, Suite 350, Shelton, CT 06484

Derek Atkins
Voice: (203) 227-3151 x1343
Email: datkins@SecureRF.com
http://www.securerf.com/

Member AIM NORTH AMERICA
Association for Automatic Identification and Mobility

RFID SECURITY ALLIANCE

NSF

U.S. AIR FORCE

ALLIANCE PARTNER RENESAS

incits™

RAIN™ RFID CHARTER MEMBER

SECURE RF
Securing the Internet of Things®

VERIDIFY™