LOTUS and LOCUS AEAD: Hardware Benchmarking and Security

A.Chakraborti, N.Datta*, A.Jha*, C. Mancillas Lopez**, M.Nandi*, Y. Sasaki

NTT Secure Platform Laboratories, Japan
*Indian Statistical Institute, Kolkata, India
**CINVESTAV, Mexico

NIST Lightweight Workshop Nov 06, 2019

Motivation

Designing Lightweight AEAD with high performance

- Parallel.
- High Security (preferable full security).
- Small block size and state size.
- Integrity under RUP setting.
- Versatility.

Design Choice

Parallel

Begin with popular parallel modes such as OTR, OCB.

High Security

Use nonce-based rekeying and masking to get high security.

Small Block and State size

The high security inturn ensures use of smaller block size (and hence smaller state size).

Integrity under RUP Setting

Use Two layers of encryptions and generate intermediate checksum from the hidden layer.

LOTUS and LOCUS AEAD

LOTUS

- Lightweight OTR with RUP Security
- Inverse-free
- Suitable for encryption-decryption implementation.

LOCUS

- Lightweight OCB with RUP Security
- Smaller state size
- Suitable for encryption only implementation.

AD Processing of LOTUS and LOCUS

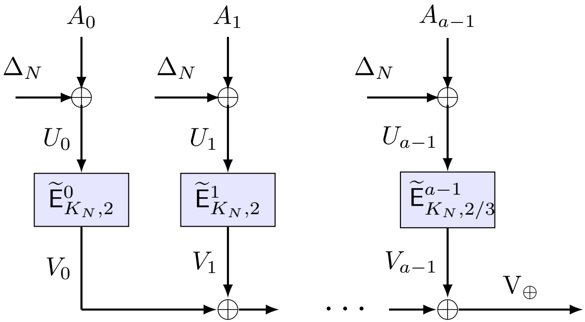
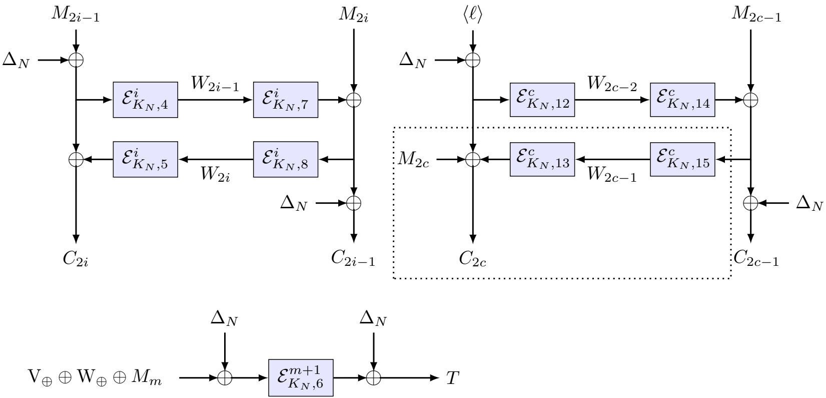
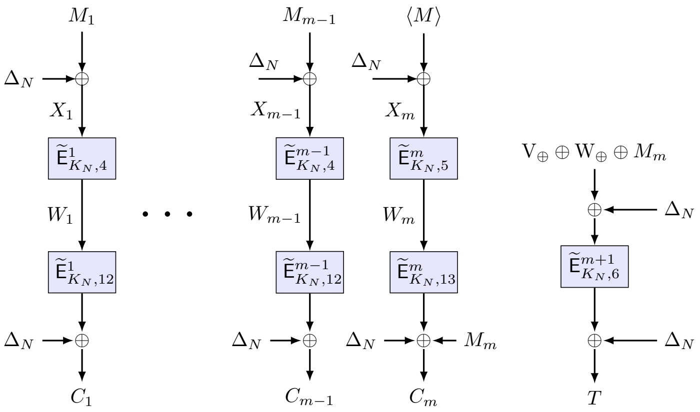


Figure: Here $\tilde{E}^i_{K_N,2}$ denotes E with key $\alpha^i K_N$ and tweak 2.

Message Processing of LOTUS



Message Processing of LOCUS



Why Tweakable Block Cipher?

- Use for domain separation.
- Require small (4-bit) tweaks.
- Use short tweak Tweakable Block Cipher (tBC).

Choice of tBC

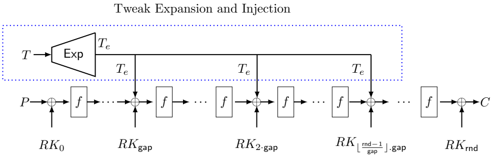


Figure: Elastic-Tweak Framework.

- BC to tBC: BC[t, t_e, tic, gap]
- Expand Tweak with high distance encoding
- Inject Tweak
- Recommendation: GIFT-64[4, 16, 16, 4]

Where Does LOTUS-LOCUS Stand?

Mode	State size	Primitive	Single Pass	Parallel	Rate	Inv-free	INT-RUP
OCB	512	128 (BC)	✓	✓	1	×	×
OTR	640	128 (BC)	✓	✓	1	✓	×
OCB-IC	512	128 (TBC)	✓	✓	1/2	×	✓
COFB	320	128 (BC)	✓	×	1	✓	×
SAEB	256	128 (BC)	✓	×	1/2	✓	–
SUNDAE	256	128 (BC)	×	×	1/2	✓	–
Beetle[Secure+]	256	256 (PP)	✓	×	1/2	✓	–
LOCUS	336	64 (tBC)	✓	✓	1/2	×	✓
LOTUS	400	64 (tBC)	✓	✓	1/2	✓	✓

Architecture of tweGIFT

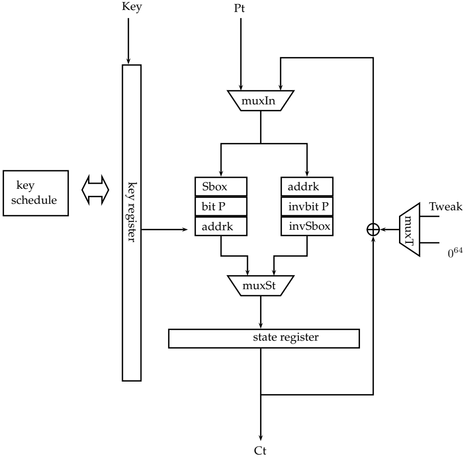


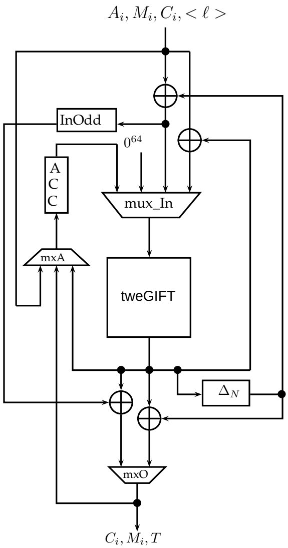
Figure: Architecture for tweGIFT.

How Efficient is tweGIFT?

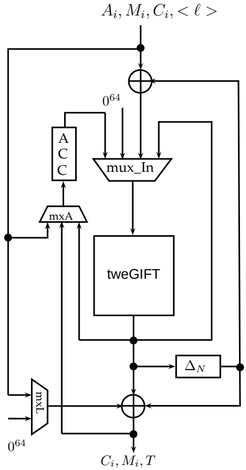
Table: Benchmark for several GIFT-128 based E_K^ts

tBC or TBC	LUTs	FF	Slices	Frequency	Clock	Throughput
GIFT-64-ED	615	277	236	455.17	29	1004.51
tweGIFT-64-ED[4,16,16,4]	617	277	234	430.29	29	946.60
GIFT-64-E	449	275	153	596.66	29	1316.77
tweGIFT-64-E[4,16,16,4]	479	275	179	595.09	29	1313.30
GIFT-128-ED	1113	408	432	447.83	41	1398.10
tweGIFT-128-ED[4,32,32,5]	1158	408	419	416.50	41	1300.29
tweGIFT-128-ED[16,32,32,4]	1223	408	428	429.32	41	1340.31
GIFT-128-E	763	403	330	596.30	41	1861.62
tweGIFT-128-E[4,32,32,5]	796	403	332	597.59	41	1865.65
tweGIFT-128-E[16,32,32,4]	805	403	377	598.78	41	1869.36

Architecture for LOTUS



Architecture for LOCUS



FPGA Results for LOTUS-LOCUS

Platform	Scheme	# Slice Registers	# LUTs	# Slices	Frequency (MHZ)	Throughput (Gbps)	Mbps/ LUT	Mbps/ Slice
Virtex 6	LOCUS	444	695	272	352.77	0.57	0.81	2.08
Virtex 7	LOCUS	446	690	257	420.56	0.67	0.97	2.62
Virtex 6	LOTUS	464	708	260	380.63	0.61	0.86	2.34
Virtex 7	LOTUS	460	664	255	435.58	0.69	1.05	2.74

Benchmarking LOTUS-LOCUS

Scheme	Underlying Primitive	# LUTs	# Slices	Gbps	Mbps/ LUT	Mbps/ Slice
LOCUS	BC (non AES)	695	272	0.57	0.81	2.08
LOTUS	BC (non AES)	708	260	0.61	0.86	2.34
AES-OTR	BC	5102	1385	2.741	0.537	1.979
AES-OCB	BC	4249	1348	3.122	0.735	2.316
AES-OCB	BC	4249	1348	1.56	0.37	1.16
AES-GCM	BC	3175	1053	3.239	1.020	3.076
AES-COPA	BC	7754	2358	2.500	0.322	1.060
CLOC-AES	BC	3145	891	2.996	0.488	1.724
CLOC-TWINE	BC (non-AES)	1689	532	0.343	0.203	0.645
ELmD	BC	4302	1584	3.168	0.736	2.091
JAMBU-AES	BC	1836	652	1.999	1.089	3.067
JAMBU-SIMON	BC (non-AES)	1222	453	0.363	0.297	0.801
SILC-AES	BC	3066	921	4.040	1.318	4.387
SILC-LED	BC (non-AES)	1685	579	0.245	0.145	0.422
SILC-PRESENT	BC (non-AES)	1514	548	0.407	0.269	0.743
COFB-AES	BC	1075	442	2.850	2.240	6.450
AEGIS	BC-RF	7592	2028	70.927	9.342	34.974
DEOXYS	TBC	3143	951	2.793	0.889	2.937
Beetle[Light+]	Sponge	616	252	1.879	3.050	7.369
Beetle[Secure+]	Sponge	998	434	2.520	2.525	5.806
ASCON-128	Sponge	1271	413	3.172	2.496	7.680
Ketje-Jr	Sponge	1236	412	2.832	2.292	6.875
NORX	Sponge	2964	1016	11.029	3.721	10.855
PRIMATES-HANUMAN	Sponge	1012	390	0.964	0.953	2.472
ACORN	SC	455	135	3.112	6.840	23.052
TriviA-ck	SC	2118	687	15.374	7.259	22.378

Security Statement for INT-RUP

- NAEAD* security is sufficient
- $\mathcal{R} = (\phi.enc, \phi.dec, \phi.ver)$, $\mathcal{I} = (\$_{enc}, \$_{dec}, \perp)$
- $\mathrm{Adv}_{\phi}^{int-rup} \leq 2\mathrm{Adv}_{\phi}^{naead*}$
- Find $\mathrm{Adv}_{\phi}^{naead*}$

Theorem

For any nonce-respecting $(q_e, q_d, q_v, q_p, \sigma_e, \sigma_d, \sigma_v)$*-adversary* $\mathcal{A}$*, we have*

$$\mathbf{Adv}^{\mathrm{naead}^\star}_{LOCUS[\widetilde{E}]}(\mathcal{A}) \leq \frac{q_p + \sigma}{2^{n+\kappa}} + \frac{6q_p\sigma}{2^{n+\kappa}} + \frac{\sigma^2}{2^{n+\kappa}} + \frac{2q_v}{2^n},$$

where $\sigma = \sigma_e + \sigma_d + \sigma_v$.

On the Security (RUP) of LOCUS

- Tweak values properly differentiates the domains.
- Nonce based keys
- Intermediate checksum (hidden to the adversary) instead of the plaintext checksum
- This gives an INT-RUP bound of the form $O(\sigma^2/2^{n+k} + 2q_v/2^n)$, where
  - $O(\sigma^2/2^n)$ is due to the TSPRP advantage of $\widetilde{E}$, and
  - $O(q_v/2^n)$ is due to the forgery attempt where q_v denotes the number of forgery attempts.

Security of the Recommended Instantiations

- We consider nonce-misuse adversaries.
- We claim integrity security even under the INT-RUP model.

Table: Summary of security claims for recommended instantiations.

Submissions	**Privacy (DT $\approx 2^{192}$)**		**Integrity (DT $\approx 2^{192}$)**	
	Time	Data (in bytes)	Time	Data (in bytes)
LOTUS	2^{128}	2^{64}	2^{128}	2^{64}
LOCUS	2^{128}	2^{64}	2^{128}	2^{64}

Features

High Security: Both LOTUS and LOCUSachieve optimal security. $DT = O(2^{n+\kappa})$. Here $D < 2^n$, and $T < 2^\kappa$ are obvious conditions.

Lightweight: 64-bit tweakable block ciphers with short tweaks.

High Performance: Both of them are single pass and fully parallelizable. LOTUS is inverse-free.

INT-RUP Secure

Thank you