Practical Forgery attacks on Limdolen and HERN

Raghvendra Rohit and Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo, Canada

NIST Lightweight Cryptography Workshop 2019

Limdolen [Mehner] and HERN [Ye et.al]

- NIST LWC round 1 candidates

Limdolen

- Two variants: Limdolen-n, $n \in \{128, 256\}\leftarrow$
- Key size = Nonce size = Tag size = n
- A combination of PMAC and counter mode of operation
- Integrity claims: n-bit $\times\leftarrow$

HERN

- Key size = Nonce size = Tag size = 128
- High level design similar to CAESAR finalist Acorn [Wu]
- Integrity claims: 128-bit $\times\leftarrow$

This work

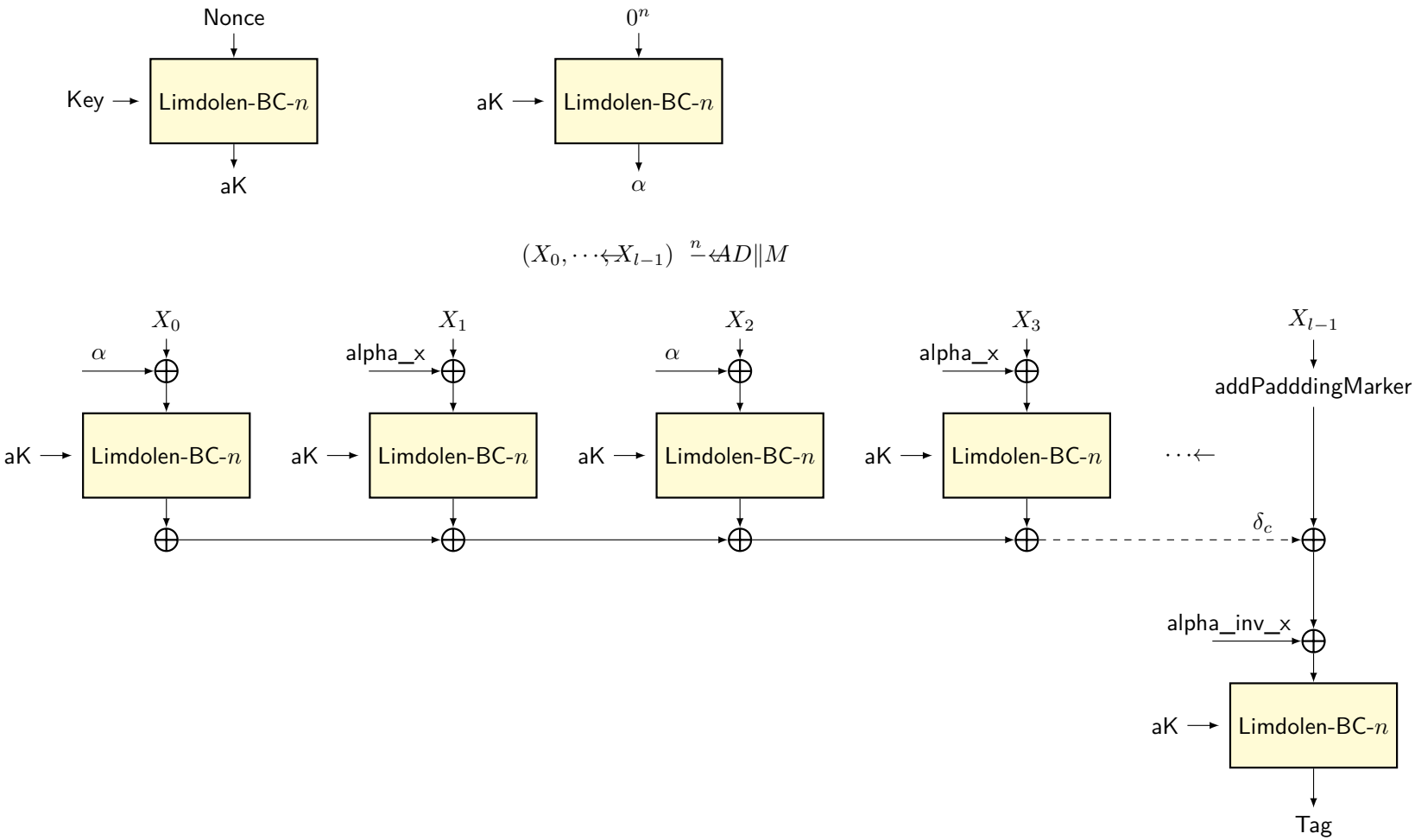
- Practical forgeries on both Limdolen and HERN in a nonce-respecting setting.

Algorithm	**Forgery type**	# Enc. queries	# Dec. queries	Success prob.	# blocks
Limdolen-128	associated data only	1	1	1	$\geq$~~1~~
	ciphertext only	1	1	1	$\geq$~~4~~
	associated data and ciphertext	1	1	1	$\geq$~~1~~
Limdolen-256	associated data only	1	1	1	$\geq$~~1~~
	ciphertext only	1	1	1	$\geq$~~4~~
	associated data and ciphertext	1	1	1	$\geq$~~1~~
HERN	associated data only	2	2	1	$-\leftarrow$
	ciphertext only	4	2	1	$-\leftarrow$
	associated data and ciphertext	2	1	1	$-\leftarrow$

Limdolen

Limdolen: Tag generation

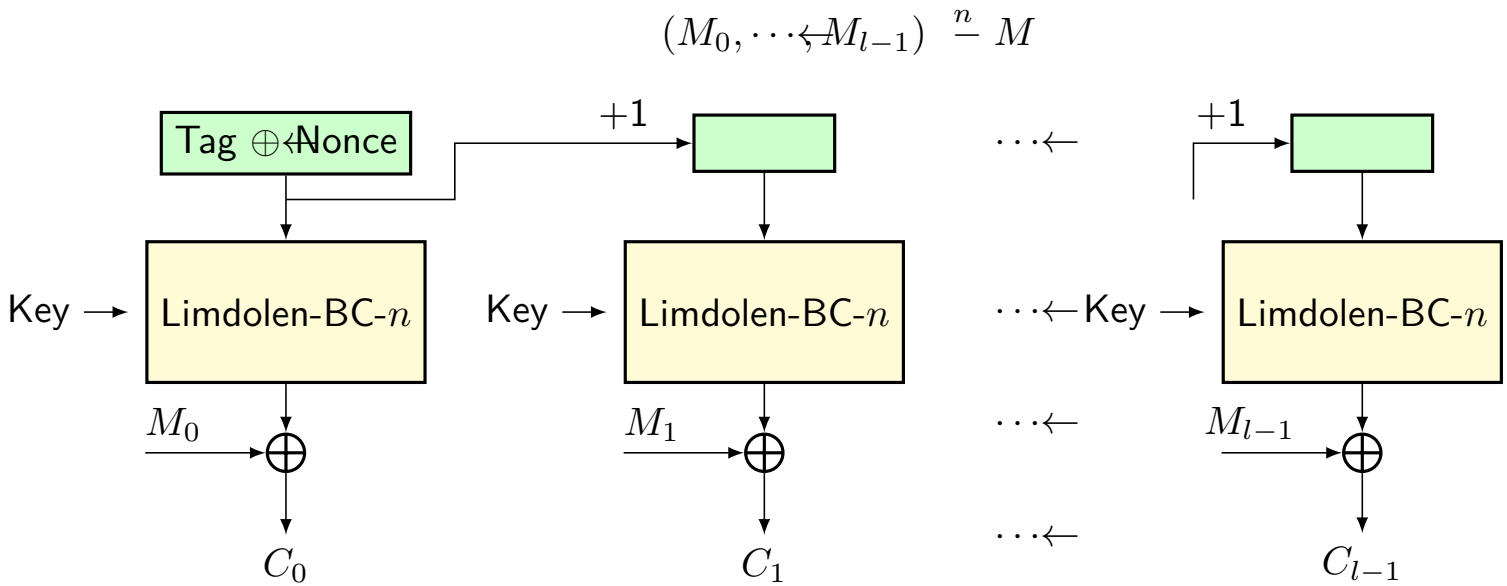
- Variant of PMAC [Black & Rogaway, 2002]



"*Due to Limdolen's target of constrained environments, rather than a series of calculations, we will alternate between* $i = 0$ *and* $i = 1$*, the two most common values of* i *in* $\gamma^i L$."

Limdolen: Encryption

- Similar to the counter mode of operation
- Initial counter: Tag $\oplus\!\!\leftarrow$Nonce

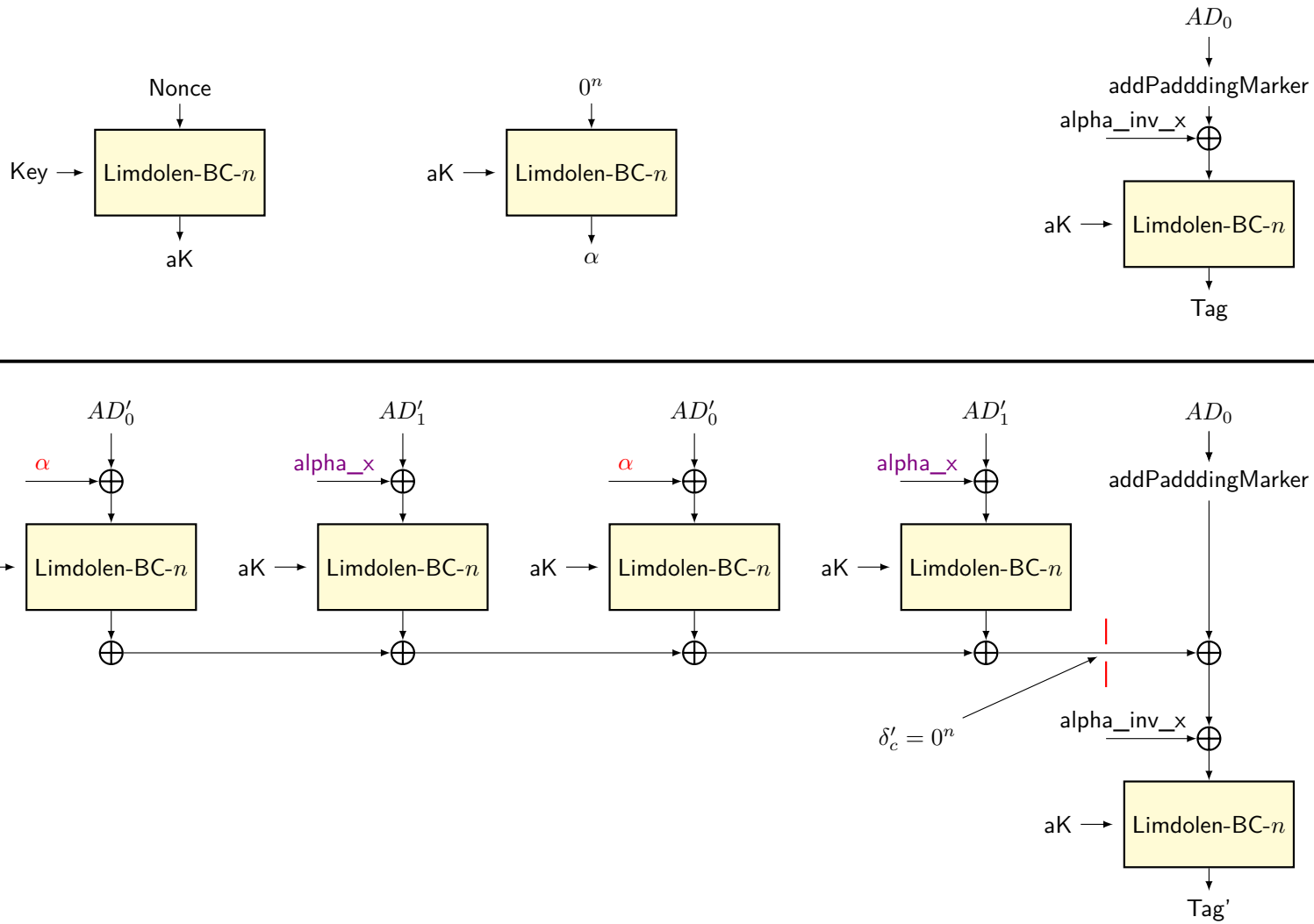


Limdolen: Distinguisher and our attack

- Differential distinguisher for full round block cipher that holds with probability 2^{-16} [Neves]. Not directly exploitable to Limdolen-n.

- Our attack exploits the structural weakness in the operating mode of Limdolen and is independent of the underlying block cipher.

Structural weakness and core idea of forgery



- Only two alternating masks α and alpha_x
- For forgery, ensure that δ'_c is a constant value

Example of associated data only forgery

	Encryption query	Decryption query
Key	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
Nonce	6B22729F7CEA8F9E1EDFB968365BF23B	6B22729F7CEA8F9E1EDFB968365BF23B
AD	BE0A1CDB4142106B5F2BB5BC8911E75E	A5687AF34938ED433536D8AB281FED78 5D1808F6DDD8D60B23EE9E0E061A5B93 A5687AF34938ED433536D8AB281FED78 5D1808F6DDD8D60B23EE9E0E061A5B93 BE0A1CDB4142106B5F2BB5BC8911E75E
M	Empty string	Empty string
C	Empty string	Empty string
Tag	EF4F60E08694CABB285D3841C433645D	EF4F60E08694CABB285D3841C433645D

- Adding/removing arbitrary number of blocks gives the same tag.

Example of ciphertext only forgery

	Encryption query	Decryption query
Key	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
Nonce	92C2A61831DCDE2EF3DB6060DF03DD0A	92C2A61831DCDE2EF3DB6060DF03DD0A
AD	Empty string	Empty string
M	ACCC9952DBB1CC0C8FA8106D463F483A BF23441F82A4BC61D2BF42AF6E4C1F1A 19B86CF46A3800F9E01066264FAF600E D2A42D5449E9B51BA9F8CB1744EA315D	19B86CF46A3800F9E01066264FAF600E BF23441F82A4BC61D2BF42AF6E4C1F1A ACCC9952DBB1CC0C8FA8106D463F483A D2A42D5449E9B51BA9F8CB1744EA315D
C	07AC6C25FAF2BA41F3B808502BA15F66 13237F247E2777389835C8C5B88BC655 E5EB9286DF5EE3FB8140B3588BC18C11 FBF38906197E5B6E069E50E4D8FABF45	B2D899834B7B76B49C007E1B22317752 13237F247E2777389835C8C5B88BC655 509F67206ED72F0EEEF8C5138251A425 FBF38906197E5B6E069E50E4D8FABF45
Tag	EDFDDE9B652A0FB16A7BFF22FD3B44D8	EDFDDE9B652A0FB16A7BFF22FD3B44D8

- Permutating 1) odd or even, 2) odd and even blocks gives the same tag.

Example of associated data and ciphertext forgery

	Encryption query	Decryption query
Key	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
Nonce	2B2CC56156A6ACF4D3B1CCE369F4C934	2B2CC56156A6ACF4D3B1CCE369F4C934
AD	0C558F14C1E88FED	0C558F14C1E88FED60D1B7E5BA6EDC
M	60D1B7E5BA6EDC62	62
C	93C6C56CBBF3B39D	91
Tag	C248D7D75062DE6163AFC13CADEBC55B	C248D7D75062DE6163AFC13CADEBC55B

Note:

- Large degrees of freedom for constructing forgeries (see our paper).
- Forgeries for Limdolen-256 can be constructed in a similar way.

HERN

HERN: Encryption and tag generation

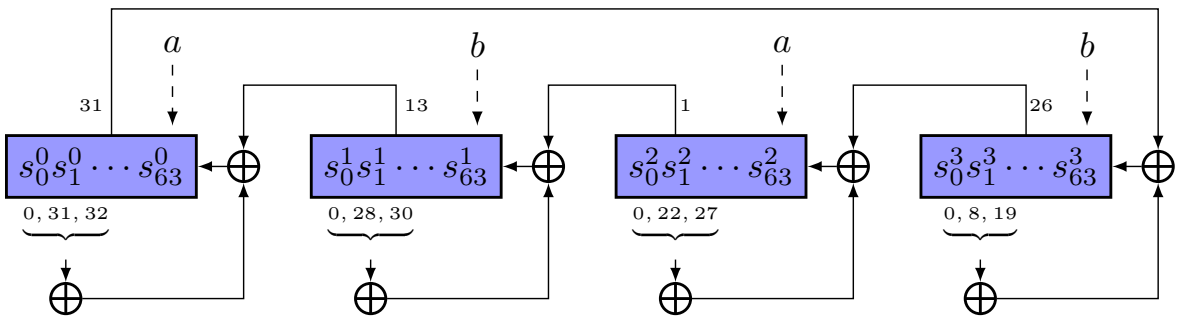


Figure: Schematic of HERN state update function

- Compute nonlinear bits a and b
- a $a \oplus x$ where x is nonce, AD or M bit
- b is used as keystream bit for encryption and tag bit, and not feedback to state during these phases

HERN: Encryption and tag generation (cont.)

1: **function** H_core_step:
2: $a \leftarrow \mathsf{SB}(s^0_{30}, s^0_{29}, s^1_{32}, s^1_{24}, s^2_{31}, s^2_4, s^3_{15}, s^3_{14})$
3: $b \leftarrow \mathsf{SB'}(s^0_{30}, s^0_{29}, s^1_{32}, s^1_{24}, s^2_{31}, s^2_4, s^3_{15}, s^3_{14}) \oplus s^0_{32}$
4: $f^0 \leftarrow s^0_0 \oplus s^0_{31} \oplus s^0_{32} \oplus s^1_{13}$
5: $f^1 \leftarrow s^1_0 \oplus s^1_{28} \oplus s^1_{30} \oplus s^2_1$
6: $f^2 \leftarrow s^2_0 \oplus s^2_{22} \oplus s^2_{27} \oplus s^3_{26}$
7: $f^3 \leftarrow s^3_0 \oplus s^3_8 \oplus s^3_{19} \oplus s^0_{31}$
8: $s^i \leftarrow s^i \ll 1$, for $i = 0, 1, 2, 3$
9: $s^i_{63} \leftarrow f^i$, for $i = 0, 1, 2, 3$

10: **function** $\mathsf{SB}(x_0, y_0, x_1, y_1, x_2, y_2, x_3, y_3)$:
11: **return** $1 \oplus x_0y_0 \oplus x_1y_1 \oplus x_2y_2 \oplus x_3y_3$

12: **function** $\mathsf{SB'}(x_0, y_0, x_1, y_1, x_2, y_2, x_3, y_3)$:
13: **return** $x_0y_2 \oplus y_0y_3 \oplus x_1x_3 \oplus y_1x_2$

1: **function** Adda:
2: $s^0_{63} \leftarrow s^0_{63} \oplus a$
3: $s^2_{63} \leftarrow s^2_{63} \oplus a$

4: **function** Addb:
5: $s^1_{63} \leftarrow s^1_{63} \oplus b$
6: $s^3_{63} \leftarrow s^3_{63} \oplus b$

7: **function** H_if_step(x):
8: H_core_step
9: $a \leftarrow a \oplus x$
10: Adda
11: Addb

12: **function** H_enc_step(m):
13: H_core_step
14: $a \leftarrow a \oplus m$
15: Adda
16: $c \leftarrow b \oplus m$
17: **return** c

- 512 blank rounds with H_if_step(0) during phase changes

Associated data only forgery

	Encryption query	Decryption query
Key	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
Nonce	D8A4ADC965EECE56330E5CC01A53C928	D8A4ADC965EECE56330E5CC01A53C928
AD	CA5F	CA5F00
M	Empty string	Empty string
CT	Empty string	Empty string
T	00FC40BF26954B37993E9C56C6C49ACA	FC40BF26954B37993E9C56C6C49ACAB6

- Complexities: 2^n encryption queries and 2^n decryption queries. In above example $n = 8$ (see our paper for proof).

Ciphertext only forgery

	Encryption query	Decryption query
Key	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
Nonce	3E1327BCC61246AC87901E0922C1A354	3E1327BCC61246AC87901E0922C1A354
AD	9524	9524
M	8500	85
CT	0D00	0D
T	8472B9D92F6AAC22CE3F188CC13D711C	008472B9D92F6AAC22CE3F188CC13D71

- Complexities: 2^{2n} encryption queries and 2^n decryption queries. In above example $n = 8$.

Associated data and ciphertext forgery

	Encryption query	Decryption query
Key	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
Nonce	7B8A185D3B33E4F906E02F291BEF6C06	7B8A185D3B33E4F906E02F291BEF6C06
AD	4328	432800
M	00	Empty string
CT	00	Empty string
T	A72C78D89FAD7A7D785EF13AB2EC085B	A72C78D89FAD7A7D785EF13AB2EC085B

- Complexities: 2^n encryption queries and 1 decryption query. In above example $n = 8$.

- We informed the designers on May 26. Same weaknesses later found by [Schrottenloher, July 11] and [Mege, July 12].

Lessons learned

- Do not use Limdolen and HERN (simple, practical and devastating forgeries).
- Proper handling of masks and domain separation required.
- Most of second round candidates (especially new modes) use LFSR based masks and require further analysis.

Thank You!

https://eprint.iacr.org/2019/907.pdf