# WAGE: An Authenticated Encryption with a Twist

Riham AlTawy*, Guang Gong, Kalikinkar Mandal[1],
and **Raghvendra Rohit**[2]

* University of Victoria

University of Waterloo
Faculty of Engineering
Department of Electrical & Computer Engineering

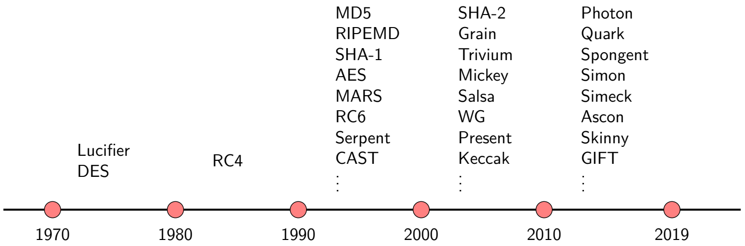
IACR FSE 2020

[1] Currently with University of New Brunswick, Canada

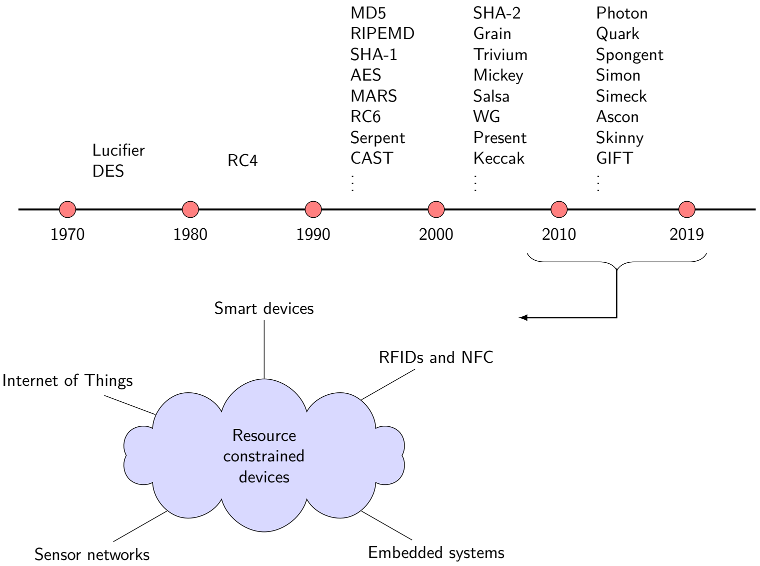
[2] Currently with University of Rennes 1, CNRS, IRISA, France

# Outline

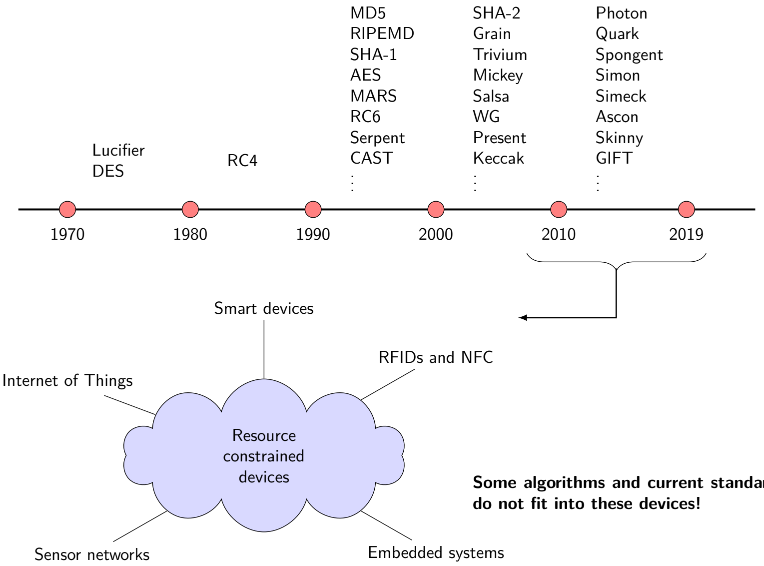
# Developments in symmetric key cryptography



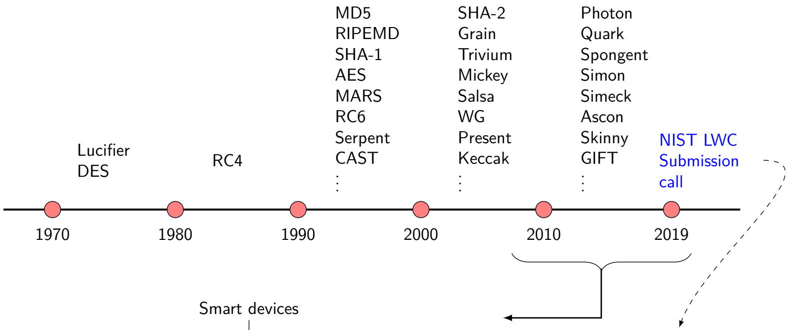
# Developments in symmetric key cryptography



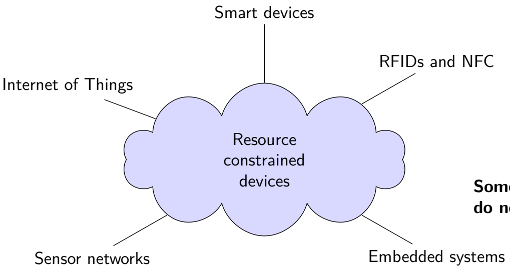
# Developments in symmetric key cryptography




**Some algorithms and current standards do not fit into these devices!**

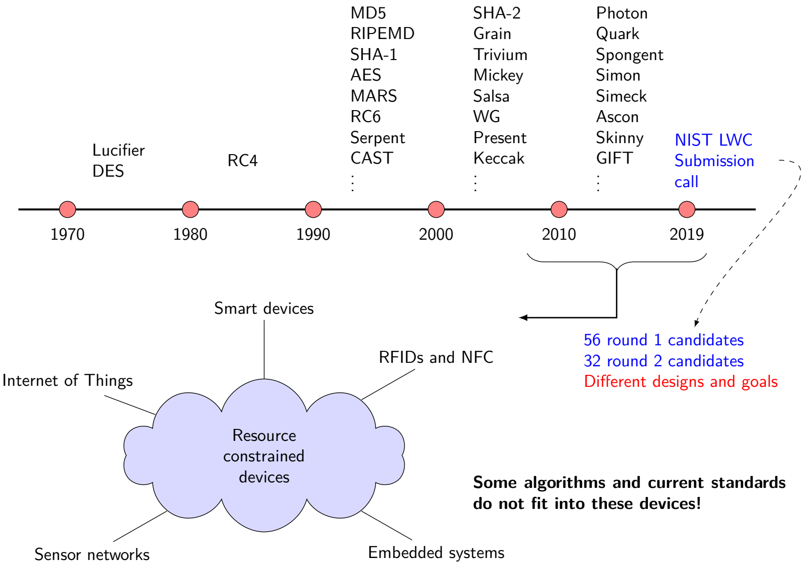



56 round 1 candidates
32 round 2 candidates
Different designs and goals



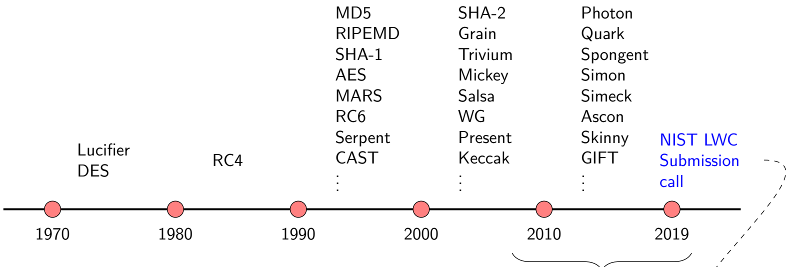

**Some algorithms and current standards do not fit into these devices!**

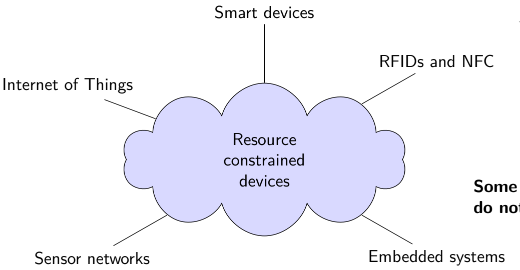
# Developments in symmetric key cryptography




**Some algorithms and current standards do not fit into these devices!**

# Developments in symmetric key cryptography




56 round 1 candidates
32 round 2 candidates
Different designs and goals

WAGE

**Some algorithms and current standards do not fit into these devices!**

# Our Contributions

- Permutation design: We design a hardware-friendly permutation of size 259 bits based on a 37-stage Galois NLFSR over $\mathbb{F}_{2^7}$.

# Our Contributions

- Permutation design: We design a hardware-friendly permutation of size 259 bits based on a 37-stage Galois NLFSR over $\mathbb{F}_{2^7}$.

- Security analysis: We analyze the diffusion, algebraic, differential, and linear properties of the WAGE permutation and the WAGE authenticated encryption.

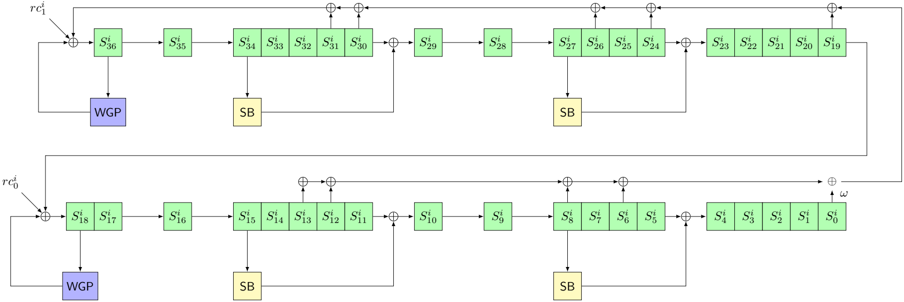
# Our Contributions

- Permutation design: We design a hardware-friendly permutation of size 259 bits based on a 37-stage Galois NLFSR over $\mathbb{F}_{2^7}$.

- Security analysis: We analyze the diffusion, algebraic, differential, and linear properties of the WAGE permutation and the WAGE authenticated encryption.

- WG-PRBG: We present the construction of WG based pseudo random bit generator with guaranteed randomness properties from WAGE.

# Design of WAGE




- $S_i^j$ is a 7-bit word, WGP and SB are 7-bit S-boxes, $\omega$ is a linear operation over 7-bit word, and $rc_j^i$ are 7-bit round constants.

# Rationale of the overall design

- Reuse and adopt the initialization phase of the well-studied WG stream cipher for authenticated encryption

# Rationale of the overall design

- Reuse and adopt the initialization phase of the well-studied WG stream cipher for authenticated encryption

- Cheap hardware cost for WGP over $\mathbb{F}_{2^7}$ than $\mathbb{F}_{2^8}$

- 1 WGP S-box to 5 additional S-boxes (1 WGP + 4 SB) for faster confusion

- Extra XORs for strong diffusion in addition to feedback

# Rationale of the overall design

- Reuse and adopt the initialization phase of the well-studied WG stream cipher for authenticated encryption
- Cheap hardware cost for WGP over $\mathbb{F}_{2^7}$ than $\mathbb{F}_{2^8}$
- 1 WGP S-box to 5 additional S-boxes (1 WGP + 4 SB) for faster confusion
- Extra XORs for strong diffusion in addition to feedback
- Minimal overhead for tweaking the WAGE permutation to an independent WG-PRBG

- WGP S-Box: Defined over $\mathbb{F}_{2^7}$:

$$\mathsf{WGP}(x) = \mathsf{WGP7}(x^{13})$$

$$\mathsf{WGP7}(x) = x + (x+1)^{33} + (x+1)^{39} + (x+1)^{41} + (x+1)^{104}$$

  $d = 13$ chosen to achieve low differential uniformity and high nonlinearity

# S-boxes

- WGP S-Box: Defined over $\mathbb{F}_{2^7}$:

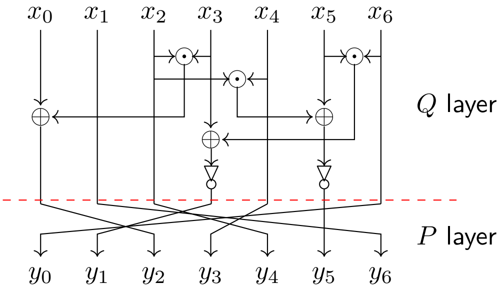
$$\mathsf{WGP}(x) = \mathsf{WGP7}(x^{13})$$

$$\mathsf{WGP7}(x) = x + (x+1)^{33} + (x+1)^{39} + (x+1)^{41} + (x+1)^{104}$$

$d = 13$ chosen to achieve low differential uniformity and high nonlinearity

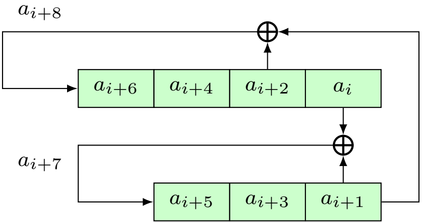
- SB S-Box: Defined in a bit-wise and iterative fashion:

$$(x_0, x_1, x_2, x_3, x_4, x_5, x_6) \leftarrow R^5(x_0, x_1, x_2, x_3, x_4, x_5, x_6)$$
$$(x_0, x_1, x_2, x_3, x_4, x_5, x_6) \leftarrow Q(x_0, x_1, x_2, x_3, x_4, x_5, x_6)$$
$$x_0 \leftarrow x_0 \oplus 1$$
$$x_2 \leftarrow x_2 \oplus 1$$




A block diagram of $R$

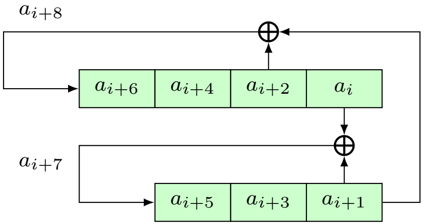
- Lightweight 7-bit LFSR for generating the constants




$$\overbrace{a_{i+7},\rlap{$\underbrace{\phantom{a_{i+6}, a_{i+5}, a_{i+4}, a_{i+3}, a_{i+2}, a_{i+1}, a_i}}_{rc_0^i}$} a_{i+6}, a_{i+5}, a_{i+4}, a_{i+3}, a_{i+2}, a_{i+1}}^{rc_1^i}, a_i$$

# Round constants

- Lightweight 7-bit LFSR for generating the constants




$$\overbrace{a_{i+7},\, \mathrlap{\underbrace{\phantom{a_{i+6},\, a_{i+5},\, a_{i+4},\, a_{i+3},\, a_{i+2},\, a_{i+1},\, a_i}}_{rc_0^i}}a_{i+6},\, a_{i+5},\, a_{i+4},\, a_{i+3},\, a_{i+2},\, a_{i+1}}^{rc_1^i},\, a_i$$

- **Property:** $(rc_0^i, rc_1^i) \neq (rc_0^j, rc_1^j)$ for $0 \leq i, j \leq 110$ and $i \neq j$. Ensures that all the rounds of WAGE are distinct and provides resistance against slide and invariant subspace attacks.

# Number of rounds

- Number of rounds: 111
- Selection based on the security analysis: diffusion, algebraic degree, differential and linear bounds
- Overall criterion: WAGE permutation is indistinguishable from a random permutation

# Diffusion and algebraic degree behavior

- Diffusion: Full bit diffusion in 28+28 rounds in both forward and backward directions. 56/111 rounds are sufficient against meet-in the-middle attacks.

- Algebraic degree: WGP and SB sboxes each are of degree 6. Faster growth in algebraic degree and 111 rounds provides huge security margin against algebraic attacks.

# Differential and linear bounds

- WGP S-box: DP $= 2^{-4.4}$ and LSC $= 2^{-5.08}$
- SB S-box: DP $= 2^{-4}$ and LSC $= 2^{-5.35}$

# Differential and linear bounds

- WGP S-box: DP $= 2^{-4.4}$ and LSC $= 2^{-5.08}$
- SB S-box: DP $= 2^{-4}$ and LSC $= 2^{-5.35}$
- **Case I:** No constraints on the positions of input and output differences
- **Case II:** Input and output differences are restricted to only rate positions

Table: Upper bounds of MEDCP and MELCSC values of WAGE in $\log_2(\cdot)$ scale

| | Rounds | Minimum # active sboxes | MEDCP $\log_2(\cdot)$ | MELSC $\log_2(\cdot)$ |
|---|---|---|---|---|
| Case I | 74 | 59 | $-59 \times 4 = -236$ | $-59 \times 5.08 \approx -299.7$ |
| Case II | 74 | 72 | $-72 \times 4 = -288$ | $-72 \times 5.08 \approx -365.7$ |

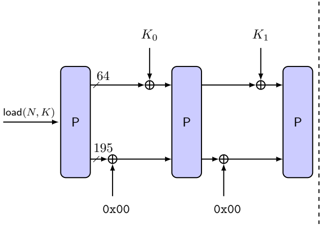
WAGE Authenticated Encryption and WG-PRBG

# WAGE Authenticated Encryption

- Supports 128-bit key, 128-bit nonce and 128-bit tag
- Operates in sponge-duplex mode with stronger keyed initialization and finalization phases

# WAGE Authenticated Encryption

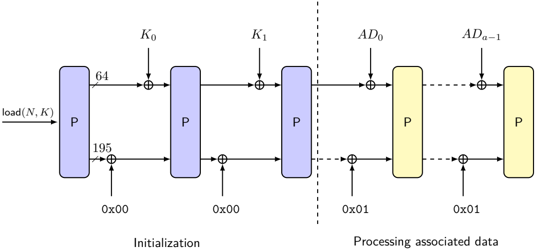
- Supports 128-bit key, 128-bit nonce and 128-bit tag
- Operates in sponge-duplex mode with stronger keyed initialization and finalization phases




Initialization

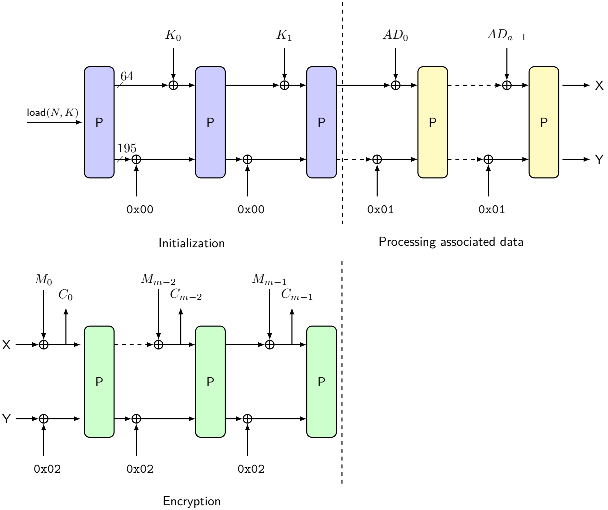
# WAGE Authenticated Encryption

- Supports 128-bit key, 128-bit nonce and 128-bit tag
- Operates in sponge-duplex mode with stronger keyed initialization and finalization phases



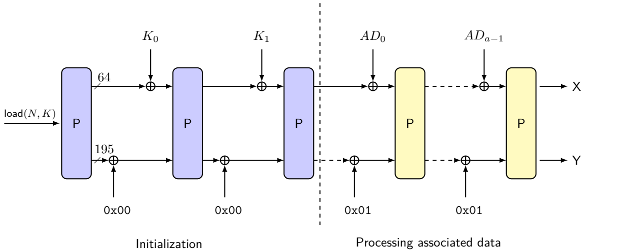
# WAGE Authenticated Encryption

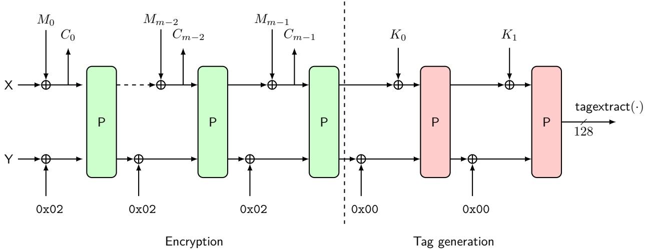
- Supports 128-bit key, 128-bit nonce and 128-bit tag
- Operates in sponge-duplex mode with stronger keyed initialization and finalization phases



# WAGE Authenticated Encryption

- Supports 128-bit key, 128-bit nonce and 128-bit tag
- Operates in sponge-duplex mode with stronger keyed initialization and finalization phases



# Security claims

- Confidentiality, Integrity and Authenticity in nonce-respecting setting: 128 bits
- Data limit per key: $2^{64}$ bits
- Strong security guarantees in related-key setting because of absorbing key blocks via rate

# Sponge-PRBG and WG-PRBG

- Sponge-PRBG: Start with an intial seed and output $64$ bits after each call of WAGE permutation. Number of rounds to generate 64 bits is 111.

- WG-PRBG: Null some components of WAGE round function (construction in next slide) and use WG stream cipher over $\mathbb{F}_{2^7}$ to generate random bits. Number of rounds in initialization phase is 74. Then, each output bit is generated in 1 clock cycle.

# Sponge-PRBG and WG-PRBG

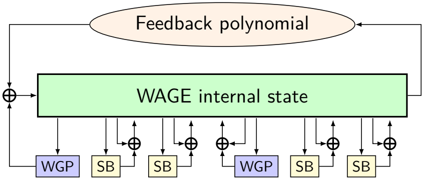
- Sponge-PRBG: Start with an intial seed and output $64$ bits after each call of WAGE permutation. Number of rounds to generate 64 bits is 111.

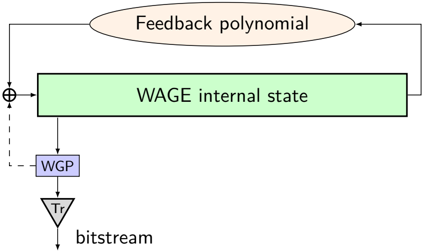
- WG-PRBG: Null some components of WAGE round function (construction in next slide) and use WG stream cipher over $\mathbb{F}_{2^7}$ to generate random bits. Number of rounds in initialization phase is 74. Then, each output bit is generated in 1 clock cycle.

  Advantages:

  - Low power and energy consumption
  - Low latency
  - Efficient source for generating random nonces for authenticated encryption

# WG-PRBG FROM WAGE ROUND FUNCTION



# Hardware Performance

- Comparison of the different ASIC implementation results of WAGE with other NIST LWC round 2 candidates. Tput, A, F, and E denote throughput, area, maximum frequency, and energy, respectively.

| **Algorithm**‡‡ | ST Micro 65 nm | | | | ST Micro 90 nm | | | | IBM 130 nm | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A [GE] | F [MHz] | Tput [Mbit/s] | E [nJ] | A [GE] | F [MHz] | Tput [Mbit/s] | E [nJ] | A [GE] | F [MHz] | Tput [Mbit/s] | E [nJ] |
| WAGE◇ | 2900 | 907 | 517 | 20.0 | 2540 | 940 | 535 | 39.2 | 2960 | 153 | 87.21 | 30.4 |
| SKINNY-AEAD | - | - | - | - | 7179 | 422 | 53 | - | 7456 | 267 | 34 | - |
| ASCON | - | - | - | - | 2570 | 672 | 14 | 5,706 $\mu$J/B | - | - | - | - |
| GIFT-COFB | - | - | - | - | 3927 | 10 | 22.3 † | 2.69 † | - | - | - | - |
| Grain-128AEAD | 3638.5 | 1120 | 560 | - | - | - | - | - | - | - | - | - |
| Isap-A-128a | - | - | - | - | $\leq$12780 | $\geq$169 | 2.9 bpc | - | - | - | - | - |
| SPIX‡ | 2611 | 100 kHz | 81.8 Kbps | - | - | - | - | - | 2742 | 100 kHz | 81.8 Kbps | - |
| SpoC-64‡ | 2329 | 100 kHz | 58.3 Kbps | - | - | - | - | - | 2389 | 100 kHz | 58.3 Kbps | - |
| SUNDAE-GIFT | - | - | - | - | 3494 | 10 | 15.9 †† | 4.2 † | - | - | - | - |
| TinyJAMBU-128 | - | - | - | - | 1352⋆ | - | 24.6 | - | - | - | - | - |

‡‡ Implementations numbers from round 2 submissions.
◇ Entire cipher including encryption, decryption and control logic
† For 16 B and 32 B of associated data and plaintext, respectively
‡ Encryption circuit only. †† #cycles = 242, ⋆ only 112 bit security

- Fair comparison is hard at this stage.

# Conclusions

- We have proposed WAGE, a sponge-based authenticated encryption algorithm, tailored for resource-constrained environments.
- Simple underlying permutation based on Galois NLFSR, two sboxes: WGP and SB, a primitive feedback polynomial, and partial word-wise XORs.
- Offers good security guarantees and hardware efficiency.
- Easily tweakable to WG-PRBG.

# Thank you!

Full paper available at:
https://tosc.iacr.org/index.php/ToSC/article/view/8620
https://eprint.iacr.org/2020/435

For any questions, comments or suggestions, please email us.

Special thanks to TikZ for Cryptographers for the diagrams.