French-Japanese cooperation on cybersecurity:
October 19, 2018

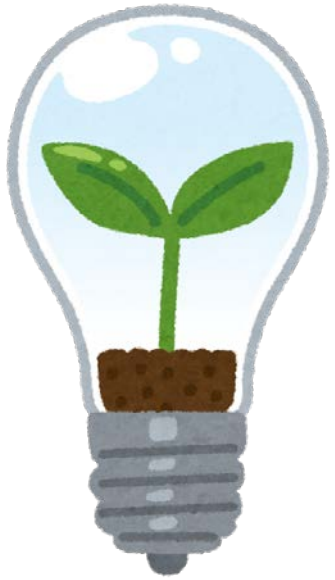
Towards Low-Energy Ciphers for IoT

Takanori Isobe
University of Hyogo

Summary

“Explore energy-efficient symmetric-key ciphers”

- First energy-efficient blockcipher: Midori
  - New Energy efficient components
  - Around 4 times lower energy than AES for short block



- Energy-efficient implementation for stream ciphers
  - Unrolling Implementation + Low energy architecture
  - Around 20 times lower energy than AES for long message

Agenda

1. Background
2. Low-Energy Block cipher [BBI+15, BBRI+18]
   - Energy efficient for short message
3. Low-Energy Stream cipher [BBAI+19]
   - Energy efficient for long message
4. Conclusion

[BBI+15] S. Banik, A. Bogdanov, T. Isobe, K.Shibutani, H. Hiwatari, T. Akishita, F. Regazzoni, “Midori: A Block Cipher for Low Energy”, ASIACRYPT 2015
[BBRI+18] S. Banik, A. Bogdanov, F. Regazzoni, T. Isobe, H. Hiwatari, T. Akishita, “Inverse Gating for Low Energy Block Ciphers”, IEEE HOST 2018
[BMAI+19] S. Banik, V. Mikhalev, F. Armknecht, T. Isobe, W. Meier, A. Bogdanov, Y. Watanabe, F. Regazzoni, "Toward Low Energy Stream Ciphers", FSE 2019

Background

- Lightweight crypto is important for IoT
  - Edge devices do not have a rich hardware resource.
- Over past 10 years, it has become a popular research area in crypto.
  - Many proposals: PRESENT(ISO), Piccolo(SONY), PRINCE(NXP), Simon/Speck(NSA), …
- CRYPTREC issued the guideline of lightweight cryptography in 2017
  - CRYPTREC: Cryptography Research and Evaluation Committees by Japanese government
- NIST started Lightweight project to develop lightweight encryption standard from 2018
  - Deadline of submission: February 25, 2019

NIST Issues First Call for 'Lightweight Cryptography' to Protect Small Electronics

April 18, 2018

Cryptography experts at the National Institute of Standards and Technology (NIST) are kicking off an effort to protect the data created by innumerable tiny networked devices such as those in the "internet of things" (IoT), which will need a new class of cryptographic

MEDIA CONTACT

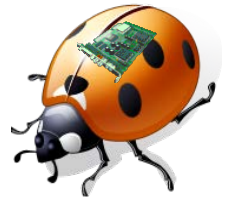
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

Lightweight Cryptography

- What is lightweight?
  - Small Area, Low Power, Low energy
- So far, small area (low power) design has been widely studied
  - AES: 2600 GE, Piccolo:800 GE

- Low energy → Not so much
  - Low energy is a more important parameter esp. in applications like medical implants/active RF-ID tags/Battery operated devices

Small Area = Low power



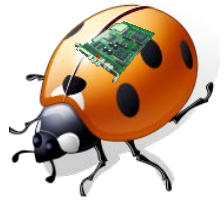
Less hardware area leads to low power consumption

Lightweight Cryptography

- What is lightweight?
  - Small Area, Low Power, Low energy
- So far, small area (low power) design has been widely studied
  - AES: 2600 GE, Piccolo:800 GE

- Low energy → Not so much
  - Low energy is a more important parameter esp. in applications like medical implants/active RF-ID tags/Battery operated devices

Small Area = Low power ≠ Low energy



Less hardware area leads to low power consumption

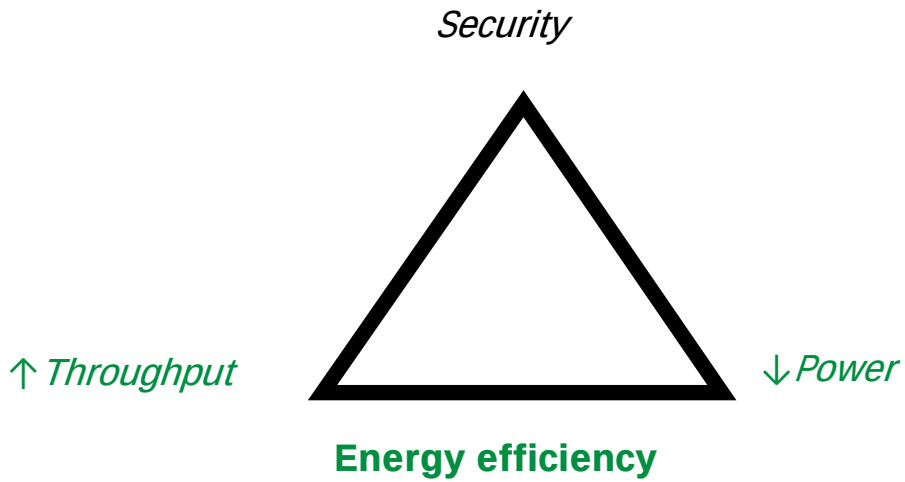
Energy-efficient AES requires 25,000 GE

Power vs Energy

- Relation between Power and Energy
  - Both are important lightweight design metrics
    - Power: rate of energy consumption
    - Energy: time integral of power

$$E = \int_t P dt$$

- Tradeoffs
  - Increase throughput
    - use more resources → high power
  - Reduce power/area:
    - Requires #cycle → high energy



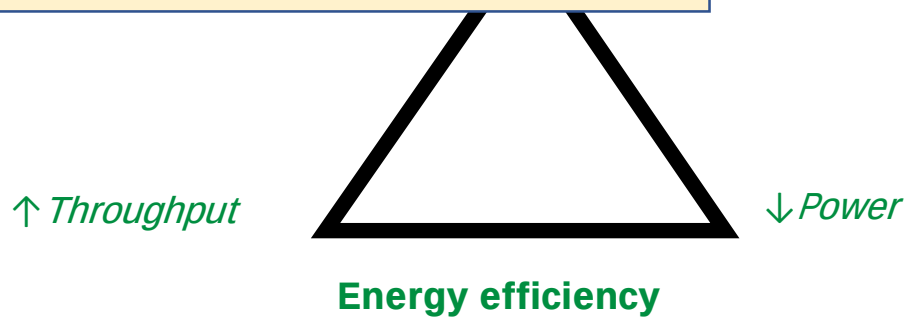
Power vs Energy

- Relation between Power and Energy
  - Both are important lightweight design metrics
    - Power: rate of energy consumption
    - Energy: time integral of power

$$E = \int_t P dt$$

- Tradeo
  - Incr
    - use more resources → high power
  - Reduce power/area:
    - Requires #cycle → high energy

For Low Energy
Small Area + High Throughput (Small # round)



Agenda

1. Background
2. Low-Energy Block cipher [BBI+15, BBRI+18]
   - Energy efficient for short message
3. Low-Energy Stream cipher [BBAI+19]
   - Energy efficient for long message
4. Conclusion

SONY

DTU Technical University of Denmark

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

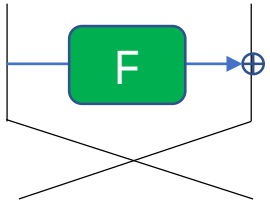
University of Lugano

[BBI+15] S. Banik, A. Bogdanov, T. Isobe, K.Shibutani, H. Hiwatari, T. Akishita, F. Regazzoni, “Midori: A Block Cipher for Low Energy”, ASIACRYPT 2015
[BBRI+18] S. Banik, A. Bogdanov, F. Regazzoni, T. Isobe, H. Hiwatari, T. Akishita, “Inverse Gating for Low Energy Block Ciphers”, IEEE HOST 2018
[BMAI+19] S. Banik, V. Mikhalev, F. Armknecht, T. Isobe, W. Meier, A. Bogdanov, Y. Watanabe, F. Regazzoni, "Toward Low Energy Stream Ciphers", FSE 2019

General Design For Low Energy

- SPN vs Feistel

SPN e.g. AES



Feistel e.g. DES

  - Feistel constructions apply round function to half the state
    - Twice the # rounds for security margin → bad for energy

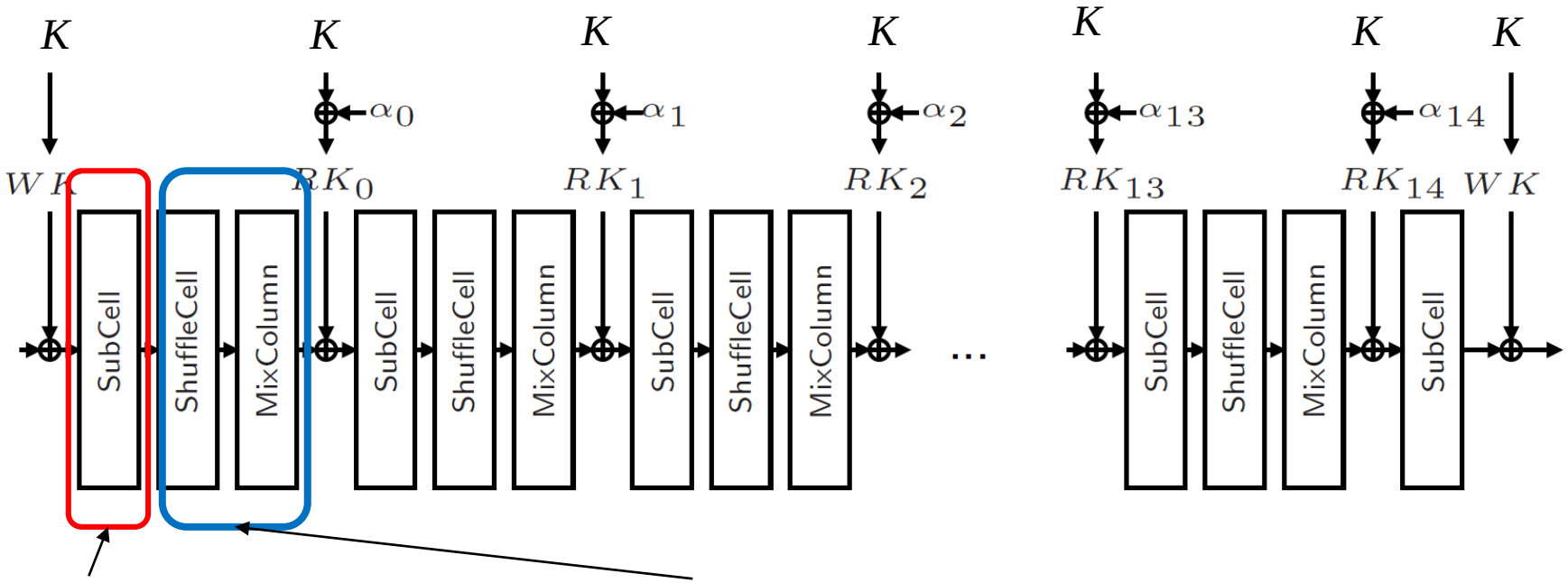
SPN Structure

- Key schedule: to or not to include
  - Consumes 25% of energy in AES and 32% in PRESENT
  - Undesirable for energy conservation

Lightweight Key Scheduling Function

Energy-Efficient Block cipher: Midori128

- General: SPN Construction like AES
- No key scheduling i.e. K is directly used as round keys



Energy-Efficient Nonlinear Layer: 4 bit-S-box vs 8-bit S-box

Table: A comparison of energy per cycle for round functions constructed with (A) 16 8-bit S-boxes, (B) 32 4-bit S-boxes.

	S-box	Delay in S (ns)	Energy per cycle (pJ)
A	DSE (8-bit)	2.25	14.00
	Rijndael(LUT)	2.10	38.88
	mCrypton	1.59	13.20
	Whirlpool	1.33	16.38
B	DSE (4-bit)	0.81	7.92
	PRINCE	0.36	4.87
	PRESENT	0.45	6.18

8 bit sbox

4 bit sbox

- 8-bit S-Box → higher signal delay → more energy

Energy-Efficient Nonlinear Layer: 4 bit-S-box vs 8-bit S-box

Table: A comparison of energy per cycle for round functions constructed with (A) 16 8-bit S-boxes, (B) 32 4-bit S-boxes.

	S-box	Delay in S (ns)	Energy per cycle (pJ)
A	DSE (8-bit)	2.25	14.00
	Rijndael(LUT)	2.10	38.88
	mCrypton	1.59	13.20
	Whirlpool	1.33	16.38
B	DSE (4-bit)	0.81	7.92
	PRINCE	0.36	4.87
	PRESENT	0.45	6.18

8 bit sbox

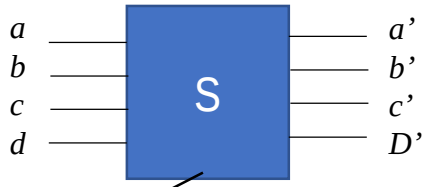
4 bit sbox

- 8-bit S-Box → higher signal delay → more energy

  Small delay 4-bit S-Box is preferable for low energy”

Energy-Efficient Nonlinear Layer: Lightweight and Low-Latency 4-bit Sbox

- Definition(Depth) :
  - The depth is defined as the sum of sequential path delays of basic operations AND, OR, NAND, NOR and NOT.
  - Assumption: Depth of XOR=2, AND/OR=1.5 NAND/NOR=1, NOT =0.5



DP/LP = 2^{-2}
Depth: 3.5

$$
\begin{aligned}
a' &= \left(\overline{c} \text{ NAND } (a \text{ NAND } b)\right) \text{ NAND } (a \text{ OR } d) \\
b' &= \left((a \text{ NOR } d) \text{ NOR } (b \text{ AND } c)\right) \text{ NAND } \left((a \text{ AND } c) \text{ NAND } d\right) \\
c' &= (b \text{ NAND } d) \text{ NAND } \left((b \text{ NOR } d) \text{ OR } a\right) \\
d' &= \left(a \text{ NOR } (b \text{ OR } c)\right) \text{ NOR } \left((a \text{ NAND } b) \text{ NAND } (c \text{ OR } d)\right)
\end{aligned}
$$

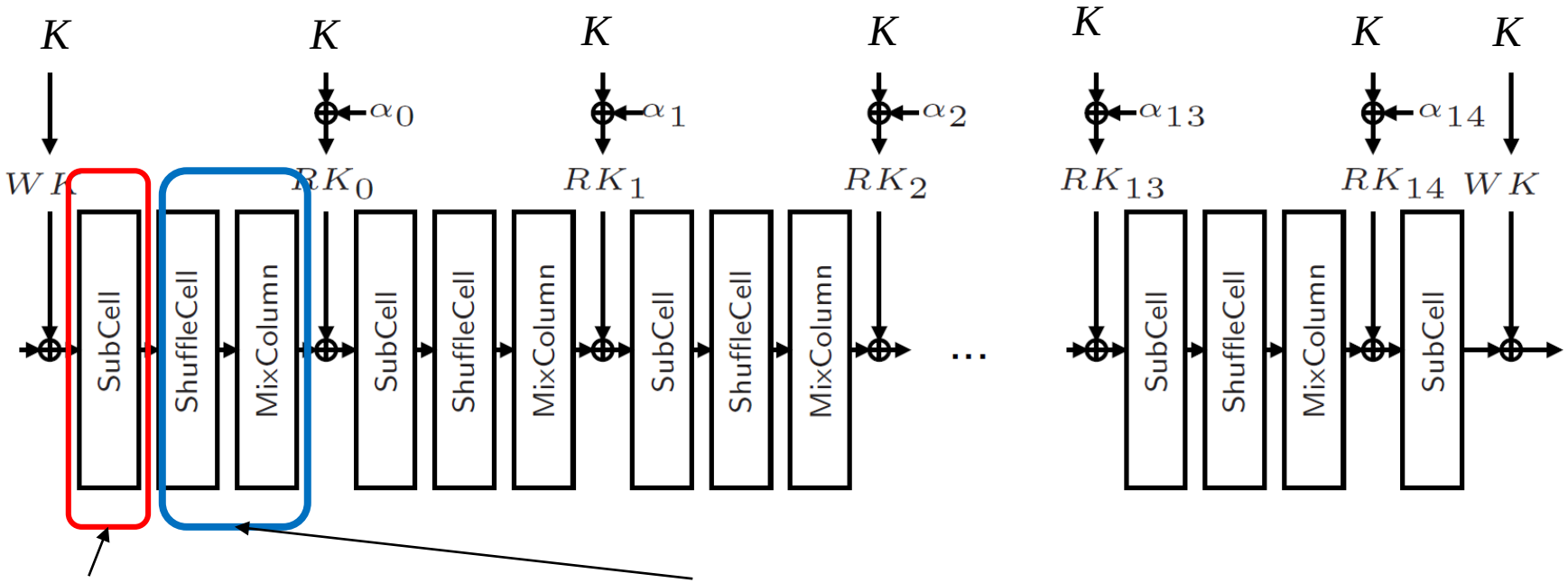
Table: Comparison of S-boxes

	PRESENT	PRINCE	Sb_0
Area [GE]	24.33	16	13.3
Path delay [ns]	0.47	0.36	0.24
Involution	No	No	Yes

Small delay and area while keeping security of S-box

Energy-Efficient Block cipher: Midori128

- General: SPN Construction like AES
- No key scheduling i.e. K is directly used as round keys



Energy-Efficient Nonlinear Layer

"New low-energy S-box"

Energy-Efficient Liner Layer

Matrix and Shuffle

Energy-Efficient Liner Layer: Lightweight and Low-Latency Matrix

- Investigate Three types of Lightweight Matrices

$$M_A = \begin{pmatrix} 1 & 2 & 6 & 4 \\ 2 & 1 & 4 & 6 \\ 6 & 4 & 1 & 2 \\ 4 & 6 & 2 & 1 \end{pmatrix}, M_B = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}, M_C = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Lightweight MDS + Involution

Lightweight MDS

Lightweight Almost MDS + Involution

Table: Comparison of three matrices

	M_A	M_B	M_C
Area [GE]	108	104	48
Delay [ns]	0.93	0.68	0.37
Diffusion	MDS	MDS	Almost MDS
Involution	yes	no	yes

Energy-Efficient Liner Layer: Lightweight and Low-Latency Matrix

- Investigate Three types of Lightweight Matrices

$$M_A = \begin{pmatrix} 1 & 2 & 6 & 4 \\ 2 & 1 & 4 & 6 \\ 6 & 4 & 1 & 2 \\ 4 & 6 & 2 & 1 \end{pmatrix}, M_B = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}, M_C = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Lightweight MDS + Involution

Lightweight MDS

Lightweight Almost MDS + Involution

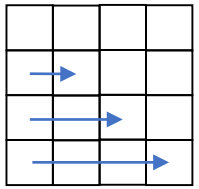
Table: Comparison of three matrices

	M_A	M_B	M_C
Area [GE]	108	104	48
Delay [ns]	0.93	0.68	0.37
Diffusion	MDS	MDS	Almost MDS
Involution	yes	no	yes

Small delay and area
but sub-optimal diffusion property

Energy-Efficient Liner Layer: Optimal Shuffle Cell Layer

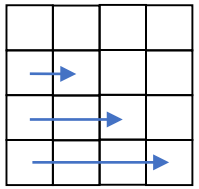
- Optimal Shuffle Cell Layer for improving diffusion property
  - Alternative of Shiftrow (AES)
    - Shiftrow



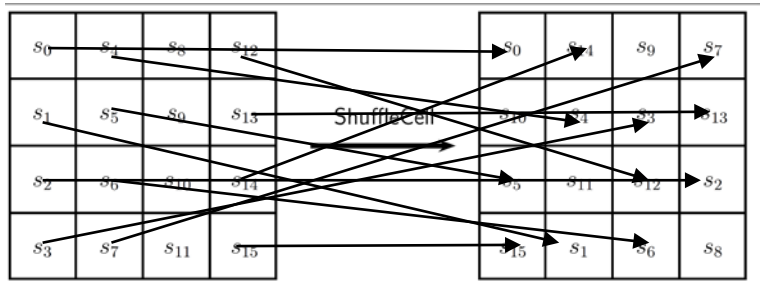
[BMAI+19] G. N. Alfarano, C.Beierle, T. Isobe, S. Kölbl, G. Leander, "ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny", FSE 2019

Energy-Efficient Liner Layer: Optimal Shuffle Cell Layer

- Optimal Shuffle Cell Layer for improving diffusion property
  - Alternative of Shiftrow (AES)
    - Shiftrow



    - Optimal Cell Shuffle Layer

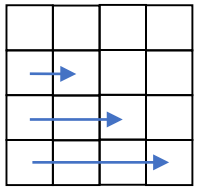


Complex shuffle but H/W free

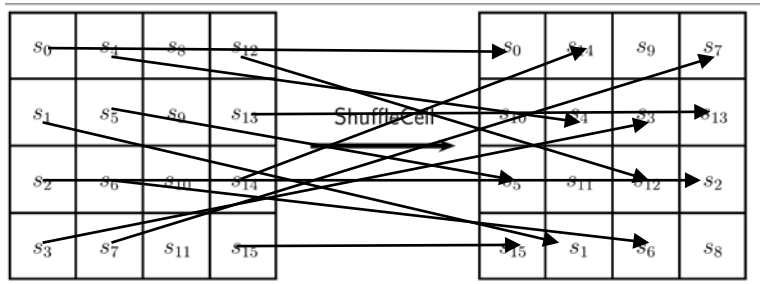
[BMAI+19] G. N. Alfarano, C.Beierle, T. Isobe, S. Kölbl, G. Leander, "ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny", FSE 2019

Energy-Efficient Liner Layer: Optimal Shuffle Cell Layer

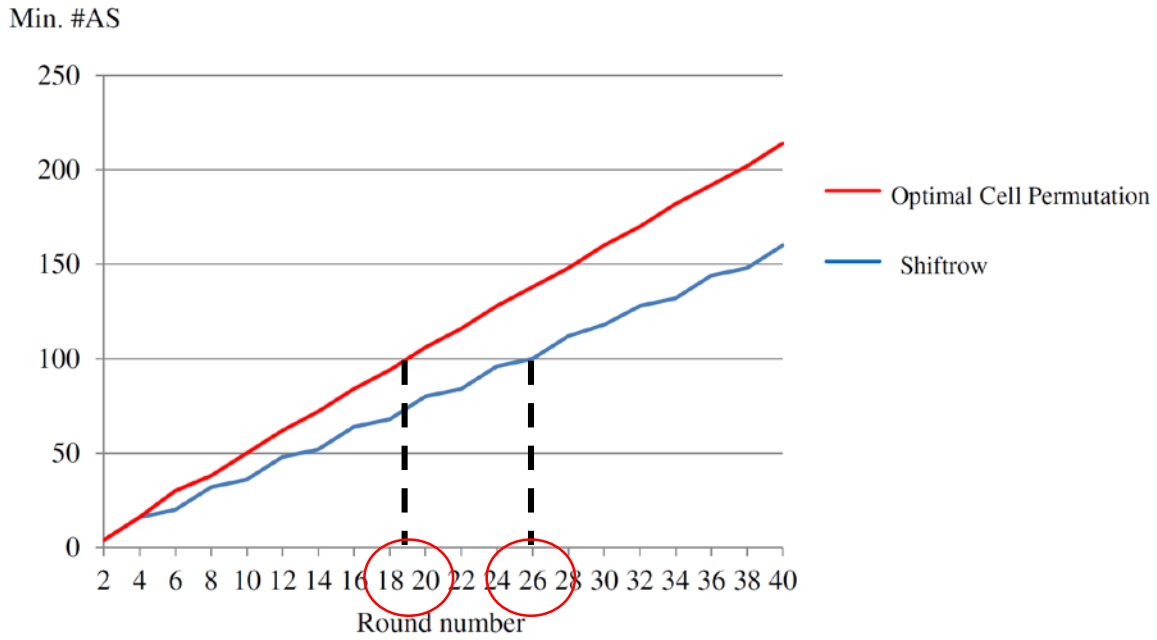
- Optimal Shuffle Cell Layer for improving diffusion property
  - Alternative of Shiftrow (AES)
    - Shiftrow



    - Optimal Cell Shuffle Layer



Complex shuffle but H/W free



Security is guaranteed in small #round
-Optimality is proved [ABIKL19]

[BMAI+19] G. N. Alfarano, C.Beierle, T. Isobe, S. Kölbl, G. Leander, "ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny", FSE 2019

Implementation Result

Standard Cell library based on STM 90nm logic process

#	Cipher	Block Size	Architecture	Area (in GE)	Energy pJ	Energy/bit pJ	Average Power (μW)	Critical Path (ns)
1	AES	128	ED	21274	769.0	6.01	699.1	4.08
			E	12459	350.7	2.74	318.8	3.32
2	NOEKEON	128	ED	3439	331.5	2.59	184.2	3.79
			E	2284	338.0	2.64	187.8	3.38
3	SIMON 128/128	128	ED	3480	855.6	6.68	124.0	2.67
			E	2420	664.1	5.19	96.2	2.66
4	Midori128	128	ED	3661	228.3	1.78	108.7	2.44
			E	2522	187.3	1.46	89.2	2.25

Midori128 is most energy efficient in existing blockciphers

Implementation Result

Standard Cell library based on STM 90nm logic process

#	Cipher	Block Size	Architecture	Area (in GE)	Energy pJ	Energy/bit pJ	Average Power (μW)	Critical Path (ns)
1	AES	128	ED	21274	769.0	6.01	699.1	4.08
			E	12459	350.7	2.74	318.8	3.32
2	NOEKEON	128	ED	3439	331.5	2.59	184.2	3.79
			E	2284	338.0	2.64		.38
3	SIMON 128/128	128	ED	3480	855.6	6.68		2.67
			E	2420	664.1	5.19	96.2	2.66
4	Midori128	128	ED	3661	228.3	1.78	108.7	2.44
			E	2522	187.3	1.46	89.2	2.25

Reduced by 70%

For circuit supporting both enc. and dec.,
energy consumption of Midori is about ¼ of AES

Implementation Result

Standard Cell library based on STM 90nm logic process

#	Cipher	Block Size	Architecture	Area (in GE)	Energy pJ	Energy/bit pJ	Average Power (μW)	Critical Path (ns)
1	AES	128	ED	21274	769.0	6.01	699.1	4.08
			E	12459	350.7	2.74	318.8	3.32
2	NOEKEON	128	ED	3439	331.5	2.59	184.2	3.79
			E	4284	338.0	2.64	124.6	2.38
3	SIMON 128/128	128	ED	3480	855.6	6.68	124.6	2.67
			E	2420	664.1	5.19	96.2	2.66
4	Midori128	128	ED	3661	228.3	1.78	108.7	2.44
			E	2522	187.3	1.46	89.2	2.25

Reduced by 85%

Reduced by 70%

For circuit supporting both enc. and dec.,
energy consumption of Midori is about ¼ of AES

Midori achieves low energy and small area (Low power)!!

Agenda

1. Background
2. Low-Energy Block Cipher [BBI+15, BBRI+18]
   - Energy efficient for short message
3. Low-Energy Stream Cipher [BBAI+19]
   - Energy efficient for long message
4. Conclusion

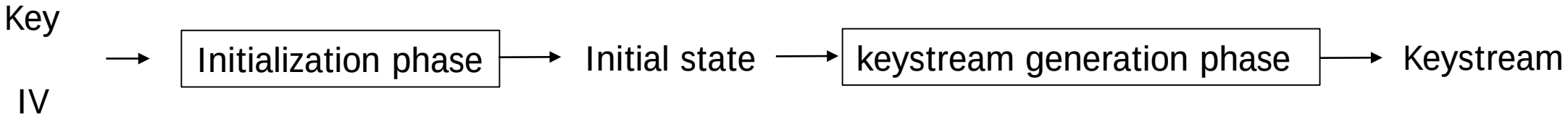
University of Lugano

FHNW Switzerland

[BBI+15] S. Banik, A. Bogdanov, T. Isobe, K.Shibutani, H. Hiwatari, T. Akishita, F. Regazzoni, “Midori: A Block Cipher for Low Energy”, ASIACRYPT 2015
[BBRI+18] S. Banik, A. Bogdanov, F. Regazzoni, T. Isobe, H. Hiwatari, T. Akishita, “Inverse Gating for Low Energy Block Ciphers”, IEEE HOST 2018
[BMAI+19] S. Banik, V. Mikhalev, F. Armknecht, T. Isobe, W. Meier, A. Bogdanov, Y. Watanabe, F. Regazzoni, "Toward Low Energy Stream Ciphers", FSE 2019

Stream Cipher vs Block Cipher

- Stream Cipher
  - Consist of “initialization phase” and “key generation phase”

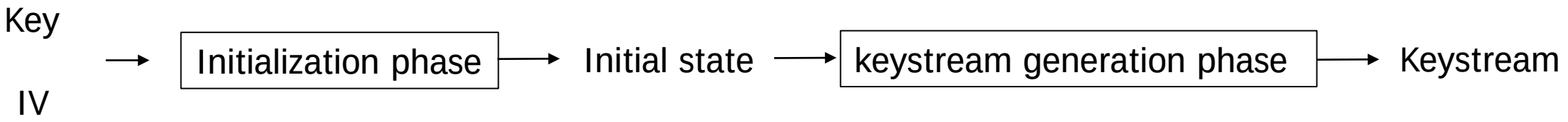


- Common Believe
  - Because of long initialization, it requires a lot of cycle to generate first keystream -> Not energy efficient

Our Question: Is this true?

Stream Cipher vs Block Cipher

- Stream Cipher
  - Consist of “initialization phase” and “key generation phase”

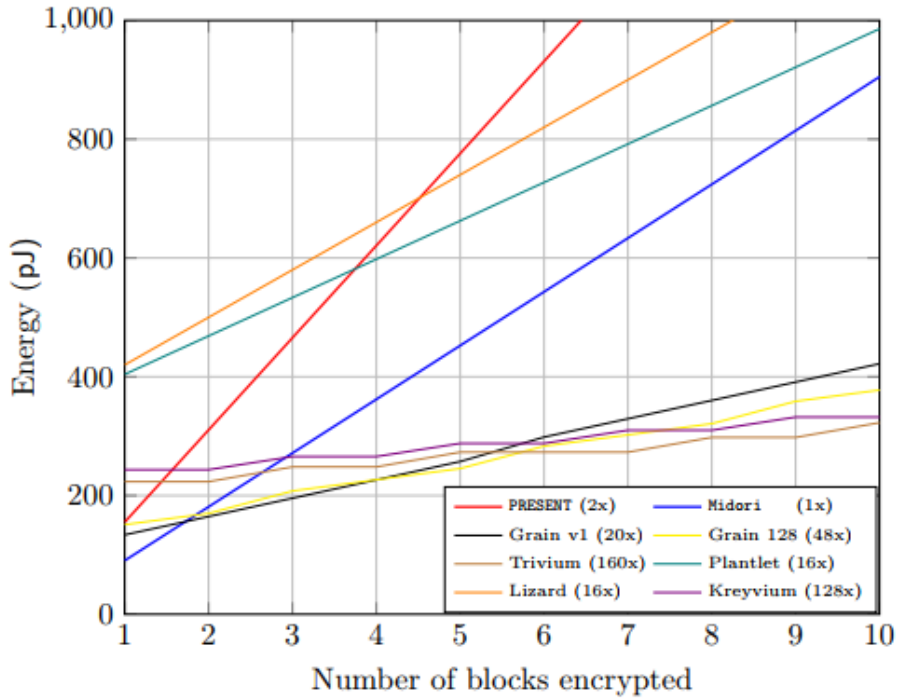


- Common Believe
  - Because of long initialization, it requires a lot of cycle to generate first keystream -> Not energy efficient

Our Question: Is this true?

Answer: No

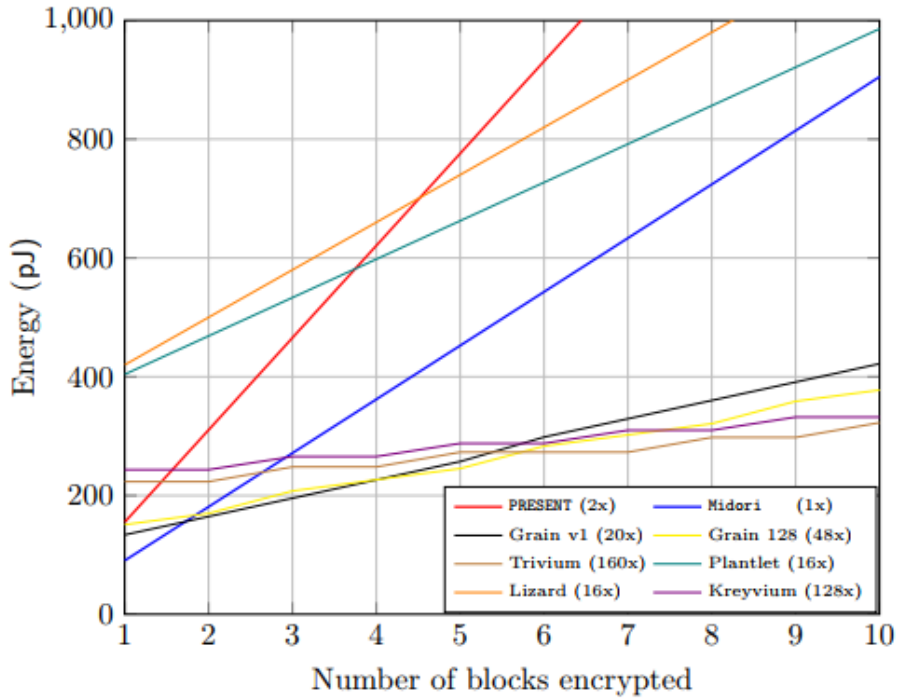
Stream Cipher vs Block Cipher



- Midori has the best energy efficiency if 1 block has to encrypted
- For 2 blocks of data (128 bits) Grain v1(20x) and Grain 128 (48x) have the lowest energy consumption
- After 6 blocks of data Trivium performs best

*1 block = 64 bits

Stream Cipher vs Block Cipher

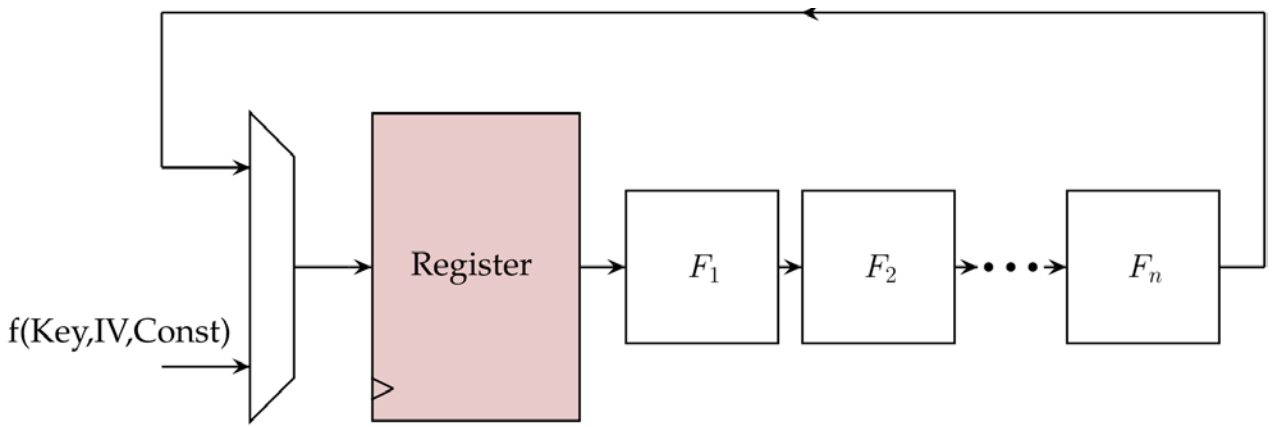


- Midori has the best energy efficiency if 1 block has to encrypted
- For 2 blocks of data (128 bits) Grain v1(20x) and Grain 128 (48x) have the lowest energy consumption
- After 6 blocks of data Trivium performs best

*1 block = 64 bits

Main Reason: Low energy implemenation of stream ciphers

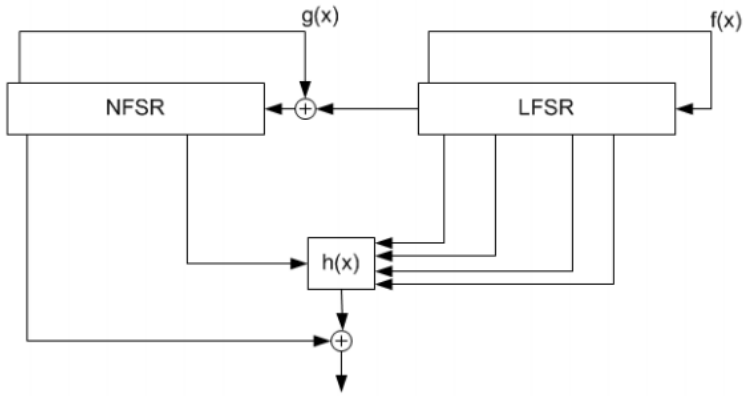
Unrolling rounds



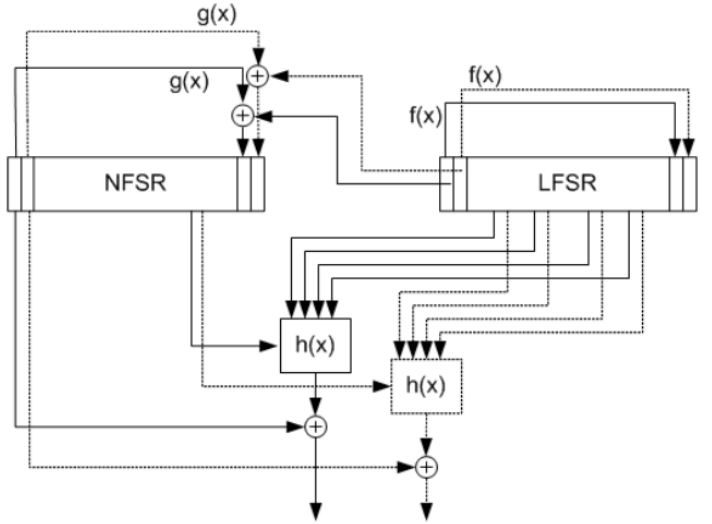
- Aim: increase throughput at the cost of area
  - Replace logic designed for one round by the one which implements several rounds

Unrolling rounds

- Grain v.1



1 bit/clock-cycle version



2 bit/clock-cycle version

Unrolling rounds

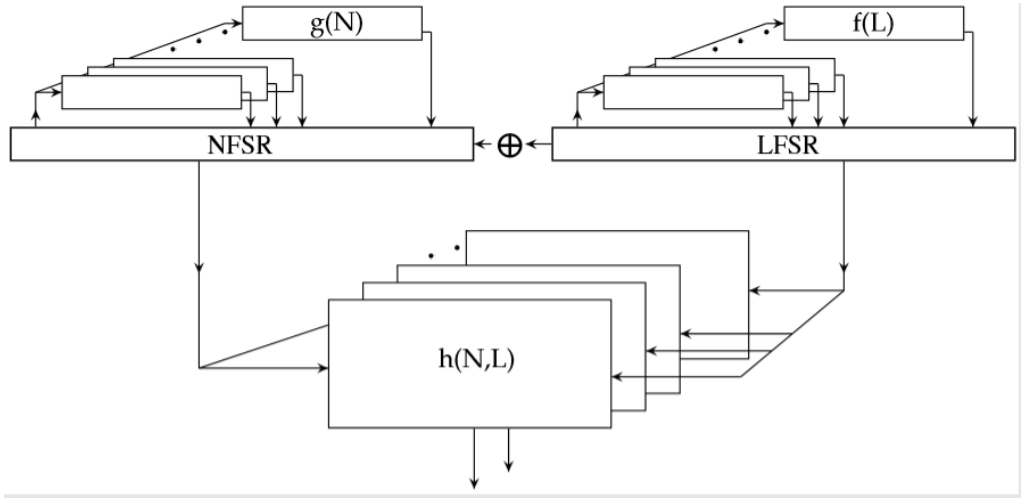
- Many modern stream ciphers were designed to allow easy unrolling
  - E.g. last 16 bits in both registers of Grain v1 are used neither in the update nor in the output function
  - Hence 16 rounds can be unrolled by implementing 16 copies of update and output functions

- No copies of registers are necessary

Increase throughput with small area overhead -> Low Energy

Unrolling rounds

- Grain v.1



16 bits/clock-cycle version

- Further unrolling requires more complicated algebraic structure of update functions

Parabolic behavior with unrolling

Cipher	r	Area (GE)	Power (uW) @ 10 MHz	Energy (pJ) 1 block	Energy (nJ) 1000 Blocks	Energy/bit (pJ)
Grain v1	1	1005	38.9	874.8	249.47	3.90
	16	2673	86.6	129.9	34.73	0.54
	20	2888	102.9	133.8	33.02	0.52
	24	3293	129.4	142.3	34.61	0.54
	28	3711	156.5	140.8	35.88	0.56
	32	3934	165.1	132.1	33.12	0.52
	48	5751	343.1	205.9	45.91	0.72
	64	7474	561.3	280.7	56.30	0.88
Trivium	1	1870	78.4	9527.6	510.48	7.97
	64	3051	128.7	257.4	13.11	0.20
	80	3457	148.1	251.7	12.08	0.19
	96	3839	169.4	237.1	11.51	0.18
	112	4241	189.3	227.1	11.04	0.17
	128	4593	207.1	227.8	10.56	0.17
	160	5409	248.2	223.4	10.15	0.16
	192	6179	306.2	244.9	10.44	0.16
	256	7755	419.5	251.7	10.73	0.17
	288	8584	490.0	294.0	11.17	0.17

r = degree of unrolling

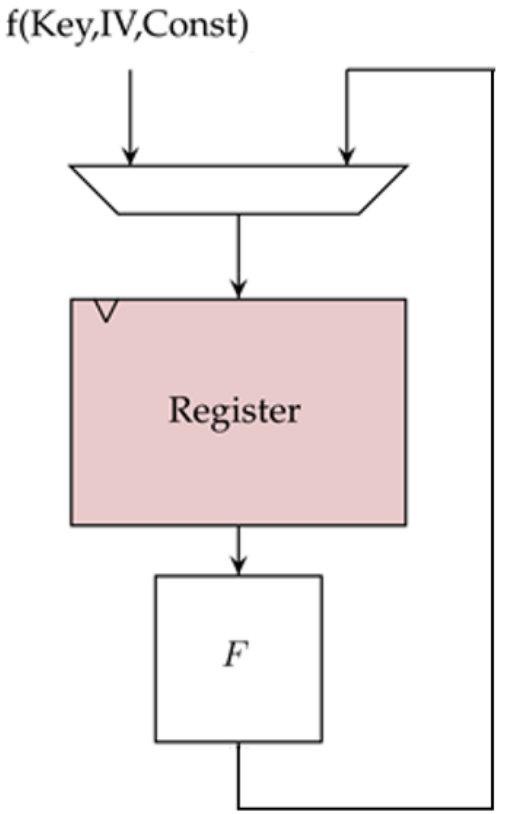
Reason: Trivium uses extremely simple round update functions

Lessons learned for Low energy implematation

- Rounds unrolling:
  - Simple update functions
  - State size less important
  - Initialization time effect becomes minimal with the increase in the length of data

Architecture: Scan flip-flops vs regular ones

- At first register is initialized by combination of the key and IV
- After that it is fed by the output of round function.
- For selection multiplexers are usually placed before flip-flops
- The combination of flip-flop and multiplexer can be replaced with a scan flip-flop



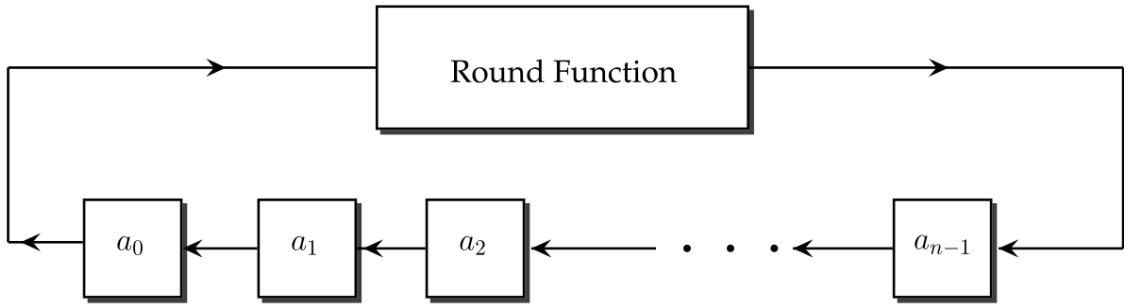
Architecture: Scan flip-flops vs regular ones

#	Cipher	FF	Area (GE)	Power (uW) @ 10 MHz	Energy (pJ) 1 block	Energy (nJ) 1000 Blocks
1	Grain v1	R	1164	40.6	912.8	260.28
		S	1005	38.9	874.8	249.47
2	Grain 128	R	1700	71.5	2287.1	459.23
		S	1455	57.8	1855.4	371.41
3	Trivium	R	1870	78.4	9527.6	510.48
		S	1584	75.6	9194.9	492.26
4	Plantlet	R	886	35.4	1364.7	227.99
		S	785	34.4	1363.1	227.73
5	Lizard[1]	R	1481	51.8	1663.2	332.93
		S	1360	50.4	1617.5	323.78
6	Kreyvium	R	3433	146.2	17792.5	952.53
		S	2892	140.8	17135.4	917.35

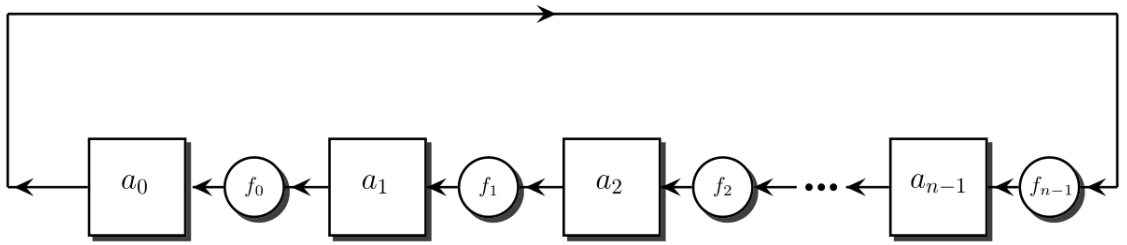
FF = flip flop type, R = regular flip flops. S = scan flip flops

- **Lesson learned:** Use scan flip-flops

Architecture: Fibonacci vs Galois FSRs



A. Fibonacci Configuration



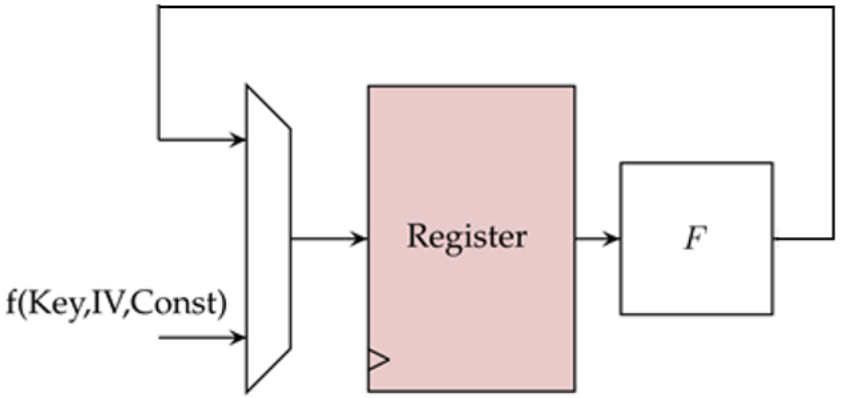
B. Galois Configuration

Architecture: Fibonacci vs Galois FSRs

#	Cipher	Conf	Area (GE)	Power (uW) @ 10 MHz	Energy (pJ) 1 block	Energy (nJ) 1000 Blocks
1	Grain v1	G	1016	39.8	894.4	255.05
		F	1005	38.9	874.8	249.47
2	Grain 128	G	1466	58.9	1890.9	378.52
		F	1455	57.8	1855.4	371.41
3	Trivium	G	1592	76.0	9253.6	495.40
		F	1584	75.6	9194.9	492.26
4	Lizard	G	1366	50.7	1626.0	325.49
		F	1360	50.4	1617.5	323.78
5	Kreyvium	G	2898	141.3	17196.2	920.61
		F	2892	140.8	17135.4	917.35

- No significant difference
- **Lesson learned:** Use Fibonacci FSRs to allow easier unrolling

Architecture: Implementation of round function



- Implementation of F:
  - A) Look-up table
  - B) Give functional description to synthesizer and let it optimize
  - C) Using Decoder-Switch-Encoder (DSE) configuration

Architecture: Implementation of round function

#	Cipher	Conf	Area (GE)	Power (uW) @ 10 MHz	Energy (pJ) 1 block	Energy (nJ) 1000 Blocks
1	Grain v1	LUT	1071	43.3	973.7	277.68
		FUN	1005	38.9	874.8	249.47
		DSE	1088	41.7	938.4	267.61
2	Grain 128	LUT	1449	57.9	1858.3	371.98
		FUN	1455	57.8	1855.4	371.41
		DSE	4165	76.3	2449.0	490.23
3	Trivium	LUT	1589	75.7	9211.1	493.12
		FUN	1584	75.6	9194.9	492.26
		DSE	1680	78.4	9542.8	510.88
4	Plantlet	LUT	785	34.5	1326.3	221.58
		FUN	785	34.4	1324.6	221.30
		DSE	1143	42.7	1644.1	274.68
5	Lizard	LUT	1327	49.9	1601.8	320.64
		FUN	1360	50.4	1617.5	323.78
		DSE	1946	58.5	1878.5	376.03
6	Kreyvium	LUT	2897	141.2	17184.0	919.96
		FUN	2892	140.8	17135.4	917.35
		DSE	2988	144.0	17524.8	938.20

- **Lesson learned:** Let synthesizer optimize F

Lessons learned for Low energy implematation

- Rounds unrolling:
  - Simple update functions
  - State size less important
  - Initialization time effect becomes minimal with the increase in the length of data

- Architecture:
  - Scan flip-flops
  - Fibonacci configuration
  - Let synthesizer to optimize update mapping

Implementation Result

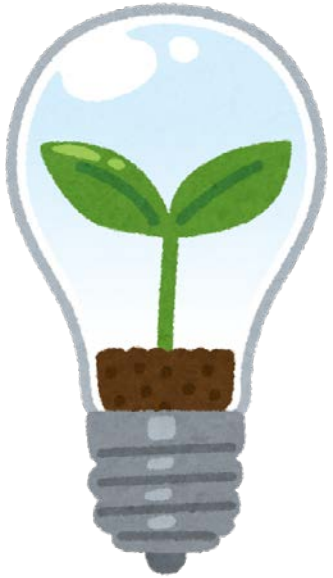
Cipher	Security level	Optimal configuration	Energy (nJ) 1000 blocks
PRESENT	80 bits	2x	155.2
Plantlet	80 bits	16x	64.98
Grain v1	80 bits	20x	33.02
Trivium	80 bits	160x	10.15
Lizard	80 bits	16x	80.34
Midori64	128 bits	2x	90.5

- Trivium (160x) is 9 times more energy efficient than the best Midori implementation when encrypting large amounts of data.

Conclusion

- Kickstart energy aware cryptographic designs!!

- Proposed first energy-efficient blockcipher Midori
  - New Energy efficient component
    - Low latency S-box
    - Optimal shuffle for binary matrix
  - Around 4 times lower energy than AES for 1 block



- Explored Energy-efficient Stream cipher
  - Unrolling Implementation + Low energy architecture
  - Around 20 times lower energy than AES for long message