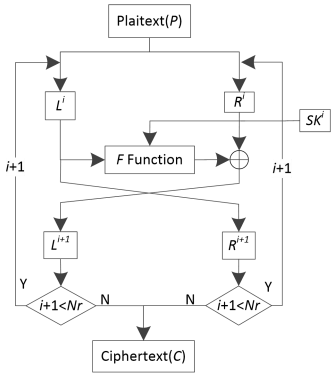
SCENERY: A lightweight block cipher based on Feistel structure

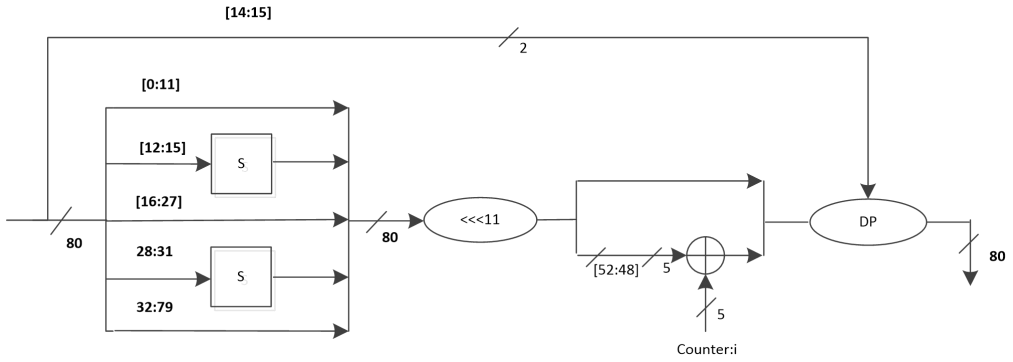
Jingya Feng , Lang Li

Frontiers of Computer Science, 10.1007/s11704-020-0115-9

Problems & Ideas

- Information security issues on IoT software and hardware.
  - IoT urgently needs lightweight technology to protect sensitive data.
  - The master key of some lightweight block ciphers can be obtained by simply pushed backward.
- Ideas: A new lightweight block cipher named SCENERY
  - SCENERY designed by bit-slice techniques suitable for hardware and software platforms.
  - A new key scheduing that can increase the complexity of reverse.





Main Contributions

- **The result of hardware implementation**

ciphers	structure	latency	block size	key size	area(GE)	speed (kbps@100KHz)	logic process
SFN	SPN	32	64	96	1877	200*	0.18um
PRESENT	SPN	32	64	80	1570	200*	0.18μm
QTL	GFN	16	64	64	1026	200	0.18μm
RECTANGLE	SPN	25	64	80	1600	246	0.13μm
KLEIN	SPN	16	64	80	2202	400*	0.18μm
LBock	Feistel	32	64	80	1320	200*	0.18μm
Twine	GFN	36	64	80	1503	178.78*	0.09μm
LED	SPN	32	64	80	1,040	3.4	0.18μm
Piccolo	GFN	25	64	80	1496	237.04	0.13μm
SIMON	Feistel	44	64	128	1751	145.45*	0.13μm
SPECK	Feistel	27	64	128	2014	237.04*	0.13μm
Midori	SPN	16	64	128	1542	400*	0.09um
SKINNY	SPN	36	64	128	1696	177.78*	0.18μm
SCENERY	**Feistel**	**28**	**64**	**80**	**1438**	**228.57***	**0.18μm**

- **The result of software implementation**

The result on 64-bit processors.

ciphers	block size	key size	one block enc.
LED	64	64	65
Piccolo	64	80	67.1
PRESENT	64	80	62
RECTANGLE	64	80	30.5
TWINE	64	80	52.8
SIMON	64	128	28.7
SPECK	64	128	10.1
SCENERY	**64**	**80**	**45.5**

"one block enc." means the encryption of a single block.

The result on 8-bit AVR.

ciphers	block/key size	Enc(cycles)
SIMON	64/128	1969
SPECK	64/128	1141
SKINNY	64/128	2551
RECTANGLE	64/80	1823
SCENERY	**64/80**	**1516**

"Enc" means the encryption process.