Lang LI, Jingya FENG, Botao LIU, Ying GUO, Qiuping LI, 2021. Implementation of PRINCE with resource-efficient structures based on FPGAs. *Frontiers of Information Technology & Electronic Engineering*, 22(11):1505-1516. https://doi.org/10.1631/FITEE.2000688

Front Inform Technol Electron Eng

Implementation of PRINCE with resource-efficient structures based on FPGAs

Key words: Lightweight block cipher; Field-programmable gate array (FPGA); Low-cost; PRINCE; Embedded security

Corresponding authors: Lang LI; Jingya FENG
E-mail: Lang LI, lilang911@126.com; Jingya FENG, fengjyk@126.com
ORCID: Lang LI, https://orcid.org/0000-0002-4832-4499; Jingya FENG, https://orcid.org/0000-0002-8109-1201

Motivation

1. In the era of pervasive computing, lightweight block ciphers have become more popular in resource-constrained environments, and the hardware implementation based on the field-programmable gate array (FPGA) has attracted much attention from researchers.

2. Due to the limitations of low-resource devices in terms of memory and computing power, the low-resource hardware implementation has attracted much attention.

3. The proposed hardware structures of PRINCE can be further optimized in terms of resource and throughput.

Front Inform Technol Electron Eng

Main idea

1. The hardware implementation structure and components of PRINCE are analyzed.

2. The optimized components of PRINCE are designed with the minimum number of logic circuits.

3. The hardware implementation structures of PRINCE are designed based on the optimized components.

4. The proposed hardware implementation structures are evaluated and compared with existing works through FPGA experiments.

Front Inform Technol Electron Eng

Method

1. A new structure for multiplying by $\boldsymbol{M}'$ using a smaller number of logic gates by sharing and simplifying the logic circuit is proposed.

2. The implementation of RC_i-add and K_1-add is simplified. It needs to store only five round constants ($RC_{1\text{-to-}5}$) and obtain the value of $K_1 \oplus \alpha$ to achieve the same result.

3. The low-cost, unrolled, and two-cycle structures of PRINCE are proposed.

Front Inform Technol Electron Eng

Method (Cont'd)

The unrolled structure of PRINCE

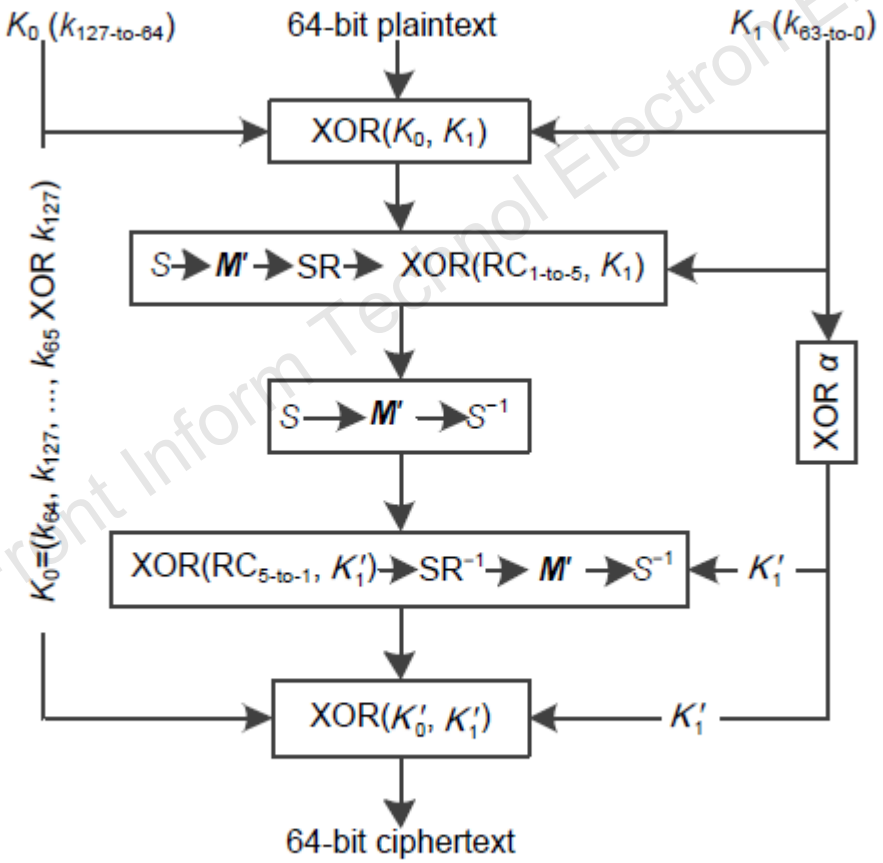

Fig. 2 Data flow of the new unrolled structure of PRINCE

Front Inform Technol Electron Eng

Method (Cont'd)

The low-cost structure of PRINCE

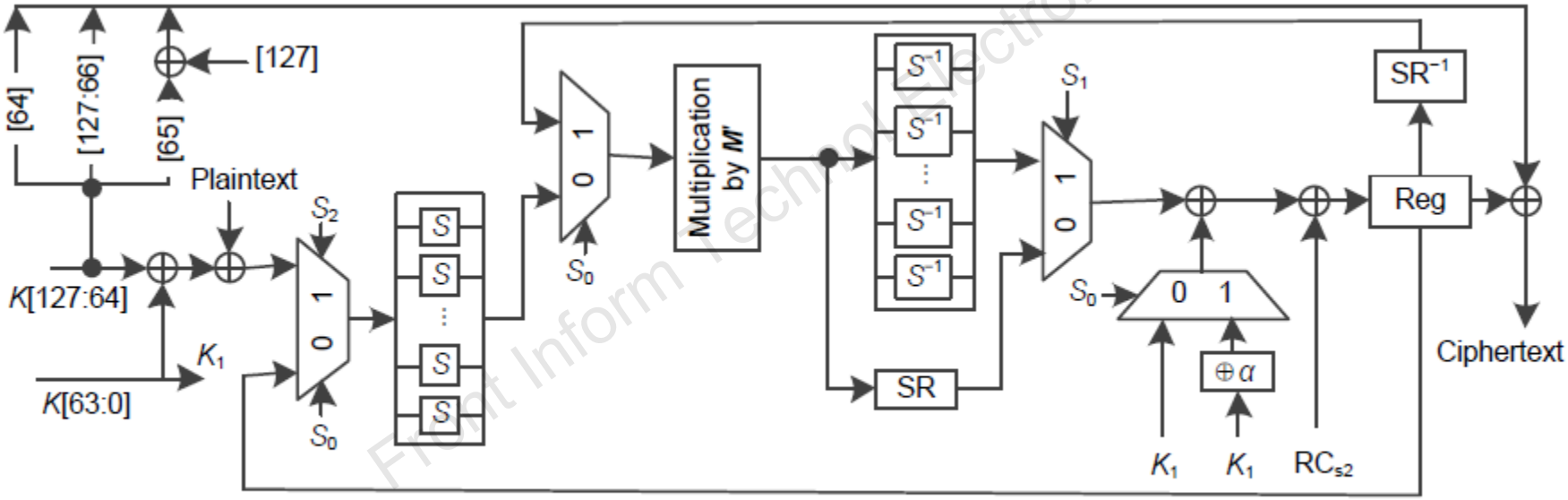

Fig. 6 New low-cost structure of PRINCE

Method (Cont'd)

The two-cycle structure of PRINCE

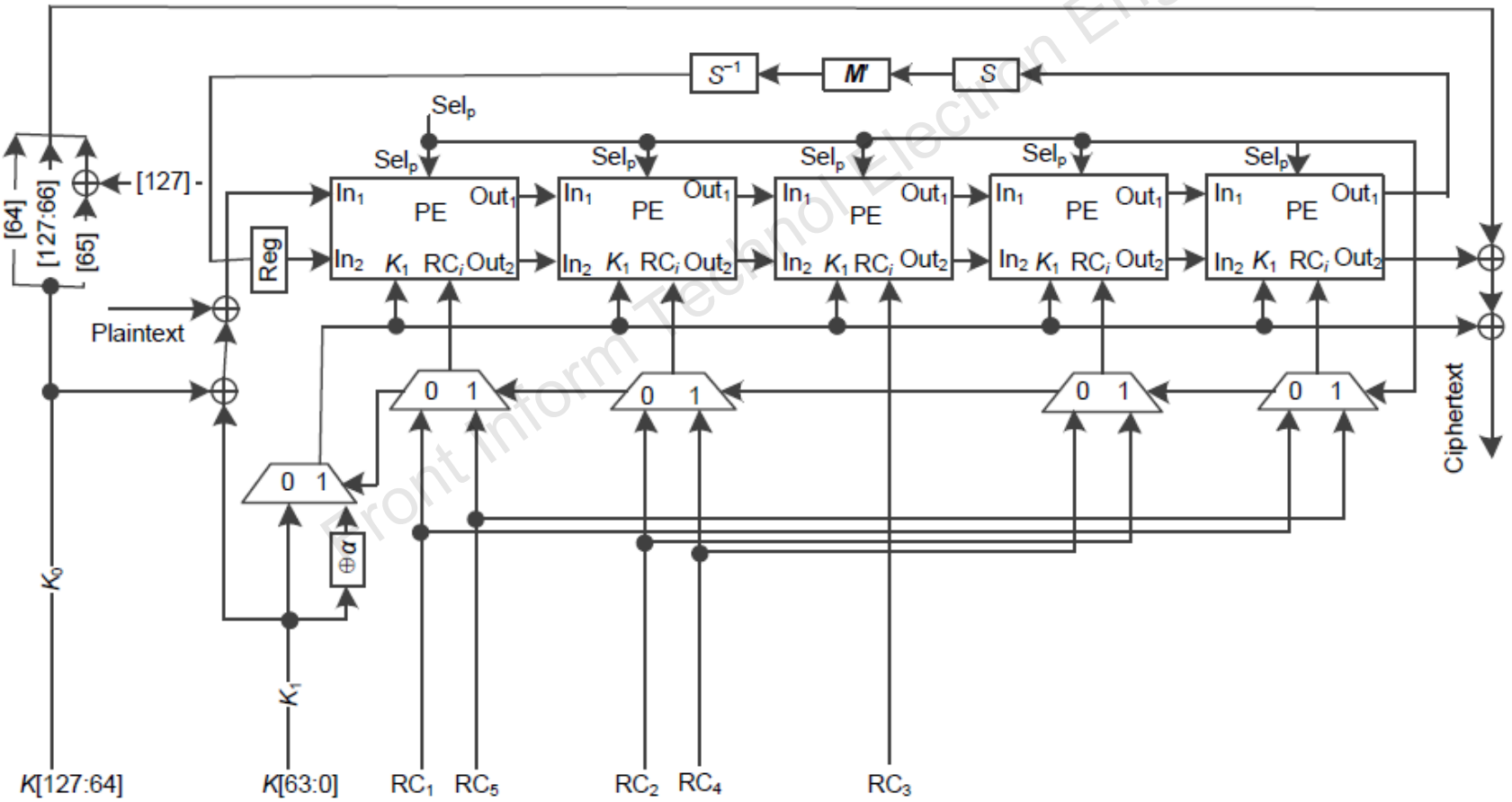

Fig. 10 New two-cycle structure of PRINCE

Front Inform Technol Electron Eng

Major results

1. Test results of our structures and existing structures

Table 4 Comparison of the new structures with existing structures

Structure	Device	Area			Maximum frequency (MHz)	Throughput**** (Mb/s)	Efficiency***** (Mb/s)
		Flip flop*	LUT**	Slice***			
Unrolled (Abbas et al., 2014)	Virtex-4			956	31.76	2032.64	2.13
Unrolled (this work)			1840	941	31.69	2028.16	2.16
Low-cost (Rashidi, 2020b)				387	357.78	2081.63	5.38
Low-cost (this work)		75	644	334	147.53	858.36	2.60
Two-cycle (Rashidi, 2020b)				1305	136.04	4353.15	3.34
Two-cycle (this work)		65	1920	1018	60.70	1942.40	1.91
Unrolled (this work)	Virtex-5		1489	576	32.44	2076.16	3.60
Low-cost (this work)		72	431	187	178.88	1040.76	5.57
Two-cycle (this work)		65	1634	623	115.54	3697.28	5.93
Unrolled (Abbas et al., 2014)	Virtex-6			482	65.38	4184.32	8.68
Unrolled (Maene and Verbauwhede, 2015)			1244		61.04	3902.72	3.14
Unrolled (this work)			1153	409	83.45	5340.80	13.06
Low-cost (Rashidi, 2020b)				256	465.12	2706.13	10.57
Low-cost (this work)		73	330	137	304.18	1769.77	12.92
Two-cycle (Rashidi, 2020b)				831	172.27	5512.49	6.63
Two-cycle (this work)		69	1279	451	138.63	4436.16	9.84
Unrolled (this work)	Spartan-6		1153	485	38.10	2438.40	5.03
Low-cost (this work)		77	333	127	145.10	844.22	6.65
Two-cycle (this work)		74	1236	433	68.86	2203.52	5.09
Unrolled (this work)	Kintex-7		1153	646	102.54	6562.56	10.16
Low-cost (this work)		73	330	162	374.49	2178.85	13.45
Two-cycle (this work)		65	1275	432	172.71	5526.72	12.79

* Number of flip flops; ** number of LUTs; ***: number of slices; **** throughput=(block size×maximum frequency)/number of clock cycles; ***** efficiency=throughput/number of slices

Front Inform Technol Electron Eng

Major results (Cont'd)

2. Test results of the unrolled structure and other ciphers

Front Inform Technol Electron Eng

Table 5 Comparison of the unrolled structure and other ciphers

Structure	Device	Area		Maximum frequency (MHz)	Throughput*** (Mb/s)	Efficiency**** (Mb/s)
		LUT*	Slice**			
SIMON (Maene and Verbauwhede, 2015)	Virtex-4	2688		36.63	2344.32	
SPECK (Maene and Verbauwhede, 2015)		3594		19.88	1272.32	
PRESENT (Maene and Verbauwhede, 2015)		2089		30.67	1962.88	
RECTANGLE (Maene and Verbauwhede, 2015)		1668		38.31	2451.84	
AES (Maene and Verbauwhede, 2015)		8984		40.49	5182.72	
Unrolled (this work)		1153	409	83.45	5340.80	13.6

* Number of flip flops; ** number of slices; *** throughput=(block size×maximum frequency)/number of clock cycles; **** efficiency= throughput/number of slices

Major results (Cont'd)

3. Test results of the low-cost structure with other ciphers

Front Inform Technol Electron Eng

Table 6 Comparison of the low-cost structure with other ciphers

Structure	Device	Area			Maximum frequency (MHz)	Throughput**** (Mb/s)	Efficiency***** (Mb/s)
		Flip flop*	LUT**	Slice***			
ANU (Dahiphale et al, 2020)	Virtex-5	199	270	103	559.57	1432.48	13.91
RECTANGLE (Dahiphale et al., 2019)		199	395	149	529.47	1303.30	8.75
PRESENT (Rashidi, 2020a)		149	230	68	397.60	848.21	12.47
Low-cost (this work)		70	437	185	226.38	1317.12	7.12
LED (Rashidi, 2020a)	Kintex-7	70	273	122	485.79	971.58	7.96
Low-cost (this work)		73	330	162	374.49	2178.85	13.45
RECTANGLE (Dahiphale et al., 2019)	Spartan-6	199	220	73	277.03	681.92	9.34
Midori (Lara-Nino et al., 2018)		200	356	118	166.17	259.38	2.20
GIFT (Lara-Nino et al., 2018)		205	189	58	218.10	268.43	4.63
Lilliput (Singh et al., 2019)		149	198	58	237.07	505.74	8.71
Low-cost (this work)		77	333	127	145.10	844.22	6.65

* Number of flip flops; **: number of LUTs; *** number of slices; **** throughput=(block size×maximum frequency)/number of clock cycles; ***** efficiency=throughput/number of slices

Conclusions

1. New structures for the multiplication of $\boldsymbol{M}'$ and the K_1-add and RC_i-add implementations require less resource than existing methods.

2. For the hardware implementation of PRINCE, the new low-cost architecture sets new area records, and the new unrolled architecture sets new throughput records.

3. Compared with existing structures, the newly proposed structures are more resource-efficient and suitable for lightweight, latency-critical applications.

Front Inform Technol Electron Eng

Lang LI received his BS degree in Circuits and Systems from Hunan Normal University, Changsha, in 1996, and his MS and PhD degrees in Computer Science from Hunan University, China, in 2006 and 2010, respectively. Since 2011, he has been a professor with the College of Computer Science and Technology, Hengyang Normal University, Hengyang, China. His research interests include embedded computing and information security.

Jingya FENG received her BS degree from Hebei University of Science and Technology, Hebei, China, in 2015. She is currently an MS candidate in the College of Information Science and Engineering, Hunan Normal University, China. Her research interests include embedded computing and information security.

Front Inform Technol Electron Eng