FPGA-based DES encryption system for IoT encryption verification

Hanzhe Sun (hns18nty@bangor.ac.uk)
Supervisor: Dr Iestyn Pierce
School of Computer Science and Electronic Engineering

PRIFYSGOL BANGOR UNIVERSITY

Introduction & Background

What is IoT?

There is no strict definition of IoT. [1] But generally speaking, IoT can be simply understood as connecting all items to the Internet through information sensing equipment to exchange information, that is, to realize intelligent identification and management.

Why study this project?

The continuous development of IoT technology has brought a lot of benefits to people, and the number of users using IoT devices is also increasing. However, the ensuing security problems are getting more and more serious, and some security vulnerabilities can even cause heavy losses to users. As shown in Figure 1, this image shows IoT devices that have been exploited due to security vulnerabilities on a global scale.

Fig. 1: Global distribution of exploited IoT devices.(The red numbers on the left indicate the number of devices used.) [2]

Brief Description of DES Algorithm

The DES algorithm is a symmetric cryptosystem in the cryptosystem, also known as the American Data Encryption Standard. It is a symmetric cryptosystem encryption algorithm developed by IBM in the United States in 1972. The DES encryption algorithm is to encrypt 64-bit data as a group. Both encryption and decryption use the same algorithm. The key is usually expressed as 64 bits, and the last bit of each 8-bit is used as a parity bit and does not participate in the actual Operation. The flowchart of the entire algorithm is shown in Figure 2.

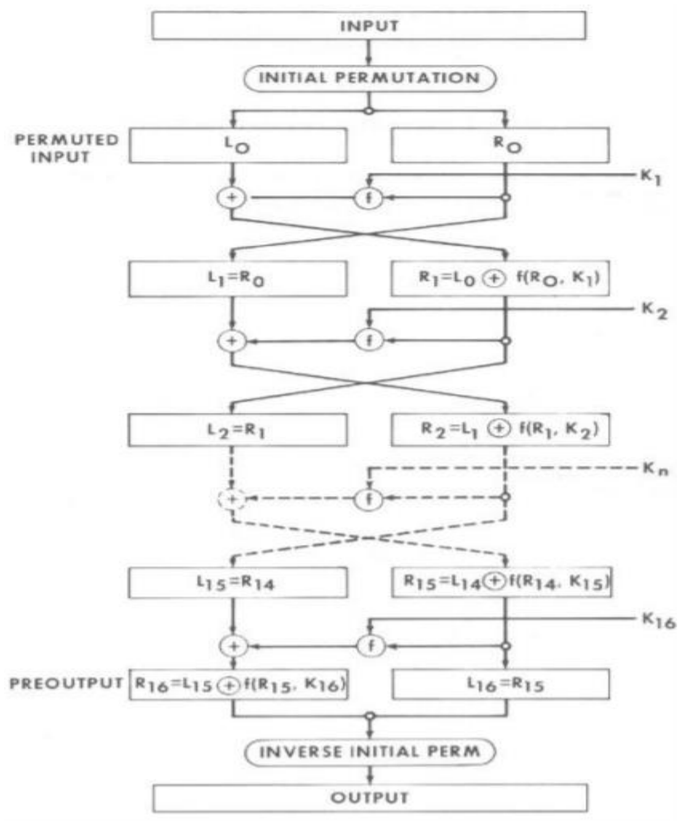

Fig. 2: Entire process of enciphering computation [3]

Aims & Objects

Overall objective

Establishing an FPGA-based DES encryption system for IoT encryption verification is the objectives of this project. According to the research theory of the above project, this project will be divided into four phased small objectives based on the final objective, as shown in the following Phase aims and Table. 1.

Phase aims

Project Phase	Objective
Phase 1	To understand and summarize various encryption methods.
Phase 2	Learn more about the DES algorithm to ensure proficiency. Begin to design an FPGA-based encryption engine and perform simulation verification.
Phase 3	Understand and summarize how to use encryption for identity verification in IoT systems.
Phase 4	Build an IoT system and test it by using two or more FPGA development boards linked by the designed encryption system.

Table. 1: Phase aims

Simulation Results

Overall situation

Due to the modularization of the project, the completion status of each module is visually shown in Table 2. In addition, due to the technical similarity of the modules "Initial permutation", "PC-1", "PC-2", "E function", "P permutation" and "Final permutation", this poster will only use one of the modules To show. In the same way, only one of the eight "S-boxes" will be displayed.

Modules	Degree of completion
Initial permutation	Completed
PC-1	Completed
Left shift	To be completed
PC-2	Completed
E function	Completed
S-box	Completed
P permutation	Completed
XOR calculation	To be completed
Final permutation	Completed
Bus controller	To be completed

Table. 2: The completion status of the module

Initial permutation section

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Fig. 3: Theoretical results of IP conversion [3]

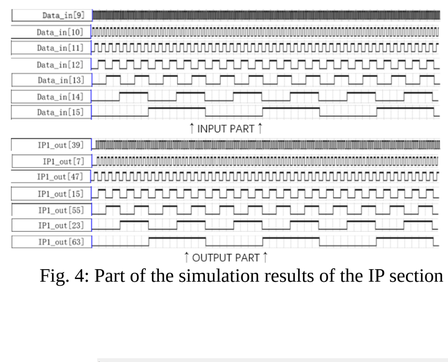

Fig. 4: Part of the simulation results of the IP section

S-box section

S_7	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
0yyyy1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1yyyy0	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
1yyyy1	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Fig. 5: Theoretical results and truth table of IP conversion [3]

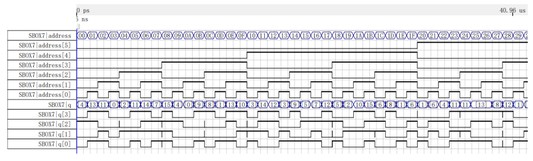

Fig. 6: Part of the simulation results of the S-box section

Future Work and Discussion

In the next 1 to 2 weeks, all modules except the "bus controller" will be completed, and the module will have entered the production state. Subsequently, all modules will be integrated and connected for piece together into a complete encryption engine. So far, all the completed modules are in good working condition and conform to the theoretical results.

[1] S. Oh and Y. Kim, "Development of IoT security component for interoperability," 2017 13th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 2017, pp. 41-44, doi: 10.1109/ICENCO.2017.8289760.
[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702-2733, thirdquarter 2019, doi: 10.1109/COMST.2019.2910750.
[3] *DATA ENCRYPTION STANDARD (DES)*, National Institute of Standards and Technology, FIPS PUB 46-3, Oct. 1999. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf