ATLANTIS PRESS

Advances in Engineering Research, volume 159

8th International Conference on Applied Science, Engineering and Technology (ICASET 2018)

The IP-core Design of Controller and F/F' Transformer in High-speed and Low-cost SM4 Chip

Lv Qian[a] , Li Li[b], Cao Yan-yan[c]

Binzhou Polytechnic, Binzhou, China

[a]214741819@qq.com, [b]lili_thesky@163.com, [c]yaya_sd@163.com

Abstract. The single cycle structure with a small area is difficult to encrypting high-speed SM4 streams in real time, while fully pipelined design is not available for the system's application in low-cost areas. Aiming at this, the pipeline method and the single cycle scheme are combined to build a high-speed and low-cost SM4 chip. At first, the common of the key expansion and encryption algorithm are compared, and then a multifunctional F/F' transformation module are present in detail. The designed IP core can be applied to each of the key expansion, encryption and decryption modules. At second, the startup module and data-path module are separated, and the feedback for iterative signal and serials of numbering mechanisms are set. Therefore a high-speed control module is designed, which can timely start every operation module to streamline the work efficiently. Finally, based on the FPGA simulation, it is seen that the designed controller can promptly manage the encryption system and the soft core of F/F' conversion can be easily transplanted to all types of SM4 system. So it's quite promising in broad market.

Keywords: Controller, F/F' conversion module, SM4 chip

Introduction

With Chinese National Security Agency formally promulgating SM4 as a commercial encryption standard in WLAN industry [1], SM4 system will be widely used in national defense, smart financial cards and mobile communications, and etc. As a block cipher algorithm, SM4 can effectively resist the square attacks and differential attacks [2], which has reached the safety standards in Europe and America [3]. Following this, the computing process is so long that it cost at least 64 round nonlinear iteration. Thus, to improve the speed of encryption and decryption under the control of area and cost, according to characteristics of SM4 algorithm, a high-speed and low-cost SM4 chip architecture is designed, in which the commonly used IP core - Controller and F/F' transformer are also researched and presented in detail.

The system architecture of the high-speed & low-cost SM4 chip

To control the size and cost, the whole pipeline system will be not feasible. To improve processing speed, a simple loop structure is not suitable too. In the traditional single-cycle structure, repeated key expansion is to be done even if the key unchanged, and also the encryption can't restart until all the 32 rounds of key expansion has completed, which have both caused a huge waste of time. While in multitasking, the operation speed of the single cycle system appears more undesirable. Thus, the authors design SM4 hardware architecture, which can be widely used in the high-speed and low-cost occasions, such as smart card, video encryption and network transmission. It is shown in Figure 1.

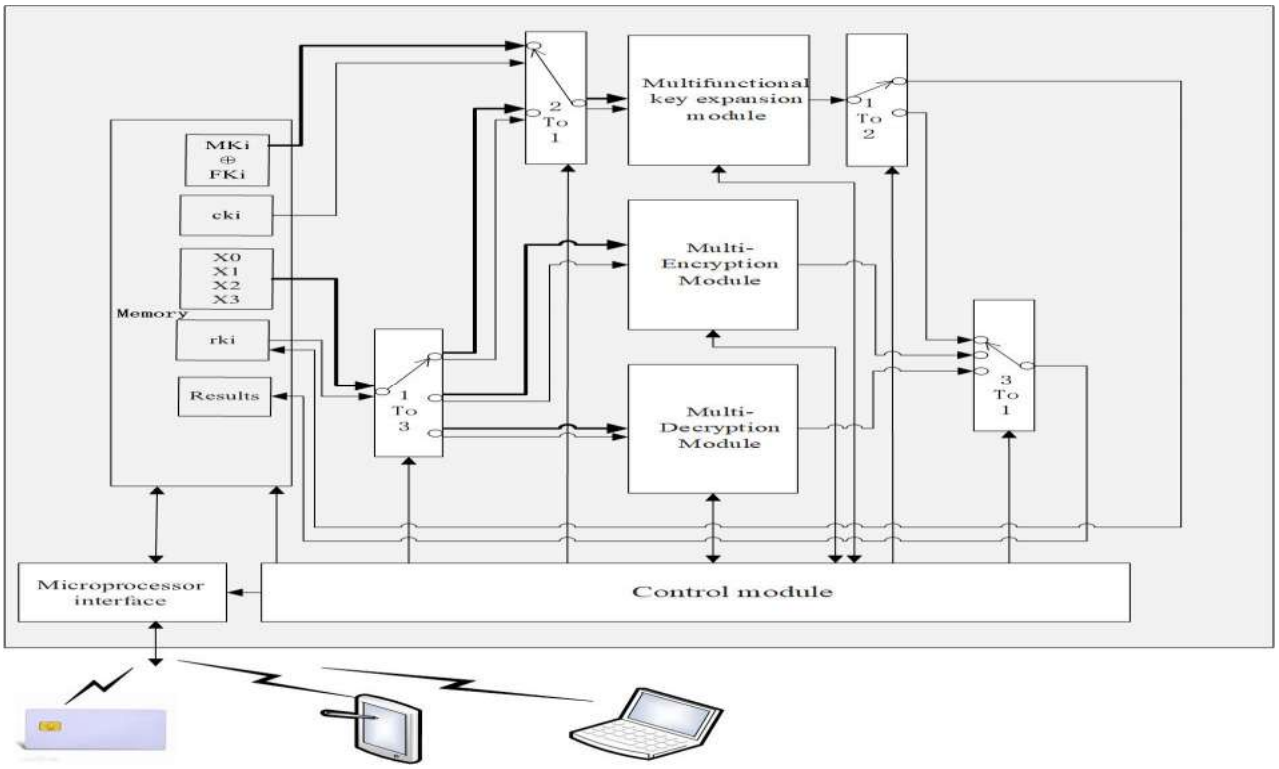

Fig.1 Hardware architecture for the high-speed and low-cost SM4 Chip

Based on the common of key expansion and encryption algorithms in SM4, this architecture uses IP-reuse ideas to design multifunctional single cycle module including key expansion, encryption module and decryption module. The multifunctional key-expansion module can complete encrypting or decrypting operations when no key expansion, the multi-encryption module is capable of decrypting without encryption task, and the decryption module as well. Thus, the system's redundancy has been effectively reduced, which could decrease the area and the cost. At the same time, because of pipelining scheme, the system can start encryption immediately once the key-expansion module completes the first round. Each module's work can be coordinated so well that at most three tasks of encryption and decryption can be achieved simultaneous, which greatly improves the chip's speed. The design of multi-purpose operation modules and the pipeline control of all the modules are the key point of the program, which will be respectively explained as below.

The research and design of the multifunctional key expansion module

(i) Research of SM4 algorithm

To design multifunctional key expansion module in the low-cost SM4 chip, the writers' emphases are to reduce the algorithm's redundancy and the chip's area.

SM4 is a block cipher algorithm, whose data and key are both 128 bits length. And its encryption algorithm, decryption algorithm, and key expansion algorithm are all used in 32 rounds of non-linear iterative structure [4].

In the key expansion, once iteration is a round of F' transformation. MK is the 128 bits of entered key, whose quarters are MK_0, MK_1, MK_2, and MK_3. Also, FK_0, FK_1, FK_2, and FK_3 are the system parameters. Then the formula 1 is shown as below.

$$(K_0,K_1,K_2,K_3)=(MK_0\oplus FK_0,\ MK_1\oplus FK_1,\ MK_2\oplus FK_2,\ MK_3\oplus FK_3) \quad (1)$$

Let Cki is the i-th intrinsic parameter, rki indicates the i-Wheel generated key, and the symbol "⊕" represents the XOR of 32-bit data. Then a key expansion process is as formula 2.

$$rk_i=K_{i+4}=F'(K_i,\ K_{i+1},\ K_{i+2},\ K_{i+3},\ CK_i)=K_i\oplus L'(\tau(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i)) \quad (2)$$

In formula 2, the function of τ includes four parallel S-boxes of lookup table structure. If referring i-bits ring shift left for 32-bit data to "<<< i", then the L' function in formula 2 is expressed as formula 3.

$$L'(B)=B\oplus(B<<<13))\oplus(B<<<23) \quad (3)$$

After these 32 F' transformations, each desired round key is obtained.

While in encryption, once iteration is a round of F conversion. Let X0, X1, X2 and X3 is for the quarter data of the input plaintexts. So we get the encryption process as formula 4.

$$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)=X_i\oplus L(\tau(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)) \quad (4)$$

The L function above is expressed by formula 5 as below.

$$L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24) \quad (5)$$

After these 32 times F conversions, the data of X32, X33, X34 and X35 generated from the last four rounds will be output in reverse. So far the desired cipher text has been obtained.

The decryption algorithm is almost the same as encryption, while exactly the only opposite is the order of the round key.

Comparing Formula 2 with 4, Formula 3 with 5, it is found that in the key expansion algorithm, the encryption and decryption algorithms, except for different input data, the only slightly different is in L' and L function.

(ii)The design of F/F' transformer

According to the characteristics of SM4 algorithm, the key expansion and the decryption algorithm on the structure have great consistency. Aiming at the L' module, two XOR operations are added and the numbers of shifts are changed, so as to run L transform as well. Therefore, the transform IP core carrying out F and F' transform simultaneously is designed as Fig.2.

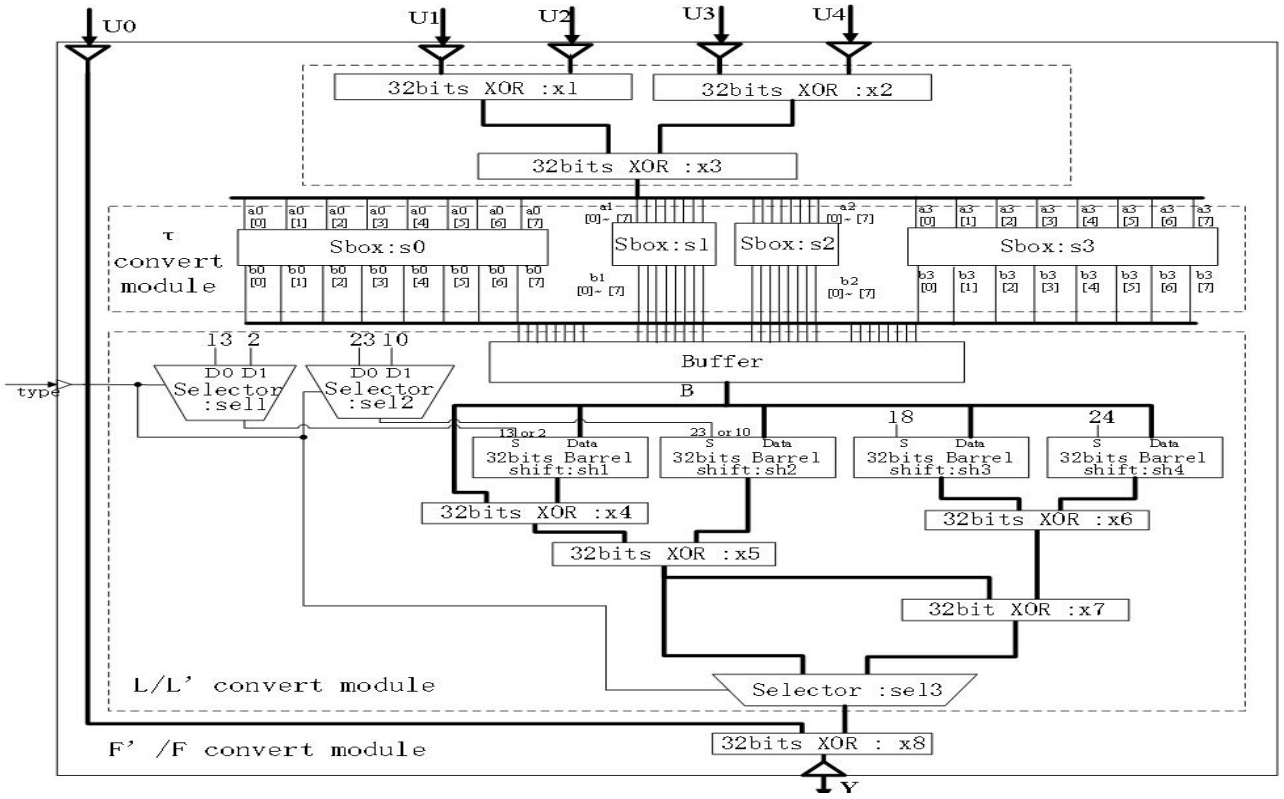

Fig.2 F/F' Transformer

Seen from the figure, the F/F' transformer has a input of signal type, five 32-bit inputs called U0-U4, and a set of 32-bit outputs named Y. Through 32-bit XOR units called x1, x2 and x3, the

input data can be turned into the 32-bit result, and that is U1 ⊕ U2 ⊕ U3 ⊕ U4. Then the τ conversion module will compute this result. Firstly, it quarters the input to 8-bit data named a0, a1, a2 and a3. Secondly the four respectively go through the S-boxes of s0, s1, s2 and s3. At last the outputs b0, b1, b2 and b3 are synthesized to a 32-bit data known as B. In other words, the B equals τ (U1 ⊕ U2 ⊕ U3 ⊕ U4). Then the L/L' conversion module will compute the data B. At first, it is cached in a buffer. At second, the 32-bit barrel shifters named sh1, sh2, sh3 and sh4 respectively shift B with 13 or 2 bits, 23 or 10 bits, 18 bits, 24 bits. At third, the 32-bit XOR operators x4, x5, x6 and x7 work to obtain L'(B) equaling B ⊕ (B <<< 13) ⊕ (B <<< 23) and L (B) equaling B ⊕ (B <<< 2) ⊕ (B <<< 10) ⊕ (B <<< 18) ⊕ (B <<< 24). And then either L'(B) or L (B) is output by the selector sel3. Finally, through the 32-bit XOR operator x8, we can get U0 ⊕ L (B) or U0 ⊕ L'(B), completing the transformation of F or F'.

In this design, the shift register is replaced by the barrel shifter with combinational logic circuit, effectively avoiding an increase in timing. The associative law is used in design to reduce the time of XOR operation. The pure combinational logic scheme of the CASE statement is used instead of the lookup table structure to implement the S box, which further avoids the delay caused by the sequential circuit.

The mode of the F/F' transformer is determined by the input called “type". One way of the type signal is output to the data selectors called “sel1” and “sel2”, so that 13 or 2, 23 or 10 outputs are selected to control the shifting number of the barrel shifters of “sh1” and “sh2”, which completing L' or L conversions respectively. The other way of the type signal is output to the data selector “sel3”, thereby selecting whether to output the L' transform or the L transform. Thus, one iteration of key expansion or encryption/decryption operations is completed. In this way, the multifunctional key-expansion module composed of the F/F' transforming IP core can also perform encryption and decryption tasks without key expansion. Thereby this chip improves the utilization and processing speed.

Design of multifunctional encrypting operation module and multifunctional decrypting operation module

Between the SM4 encryption algorithm and the decryption algorithm, the only difference is that the encryption is a sequential input round key, and the other reverse. The difference lies only in the input data and there is no difference in the algorithm structure. Therefore, it is possible to design an encrypting operation module and a decrypting operation module that have the same internal structure. Its core devices are all F-transform modules. It is only necessary to remove the type input port and data selectors sel1, sel2, and sel3 in the F/F' transformer. At the same time, it is possible to switch the encryption or decryption task depending on the order of the input round keys. Therefore, the multifunctional encrypting operation module can decrypt without encryption, and the multifunctional decrypting operation module can encrypt without decryption. This avoids the long-term idleness of the decryption module when the continuous encryption task is performed, and effectively improving the operating efficiency of the system.

Design of Controller

F-transform or F'-transform in the multifunctional key-expansion module should be selected. Also the input data to the multifunctional encryption module, the multifunctional decryption module, and the multifunctional key-expansion module should be choosed. All of this call for uniformly control by the controller module. At the same time, the control module needs to control

the start of encryption immediately after the first round of key expansion, to control the synchronous running of each computing module, so as to further speed up the chip operation. Therefore, it is the key to this SM4 encryption and decryption system, that designing a control module operating at high speed and efficiency

The traditional hardware and software systems must wait for the internal path when receiving new external tasks, which greatly reduces the processing speed of the system. In this design, the control module is designed as a startup module and a data path module. In this way, the data path module is independent in the control module, and the system can query the path request at any time. Thus it can determine the module that satisfies the new round of computing conditions at the fastest speed, and giving the path in time, effectively reducing the task response time. Meanwhile, the startup module can also start each multifunctional computing module at a faster speed according to the current task allocation. The start signal output to the key expansion module includes F-transform or F'-transformed information by time series.

In the traditional single-round loop structure, it starts the encryption operation after all the iterations are completed. Analyzing the SM4 encryption algorithm and according to formula (4), the i-th round encryption can be started immediately when the i-th round key expansion is completed. Therefore, it replaces the "task completion" signal in the conventional design by the "iterative number" signal in this controller. By monitoring the operation progress of each module, reasonably analyzing and starting a new round of operations timely, the pipeline running of the entire system is realized.

Since the same user's key is almost constant, key expansion again in a traditional design is bound to waste resources and time. Therefore, the system sets a new and old key comparison mechanism. Then the control module determines whether or not to expand key according to the the comparison result. At the same time, in order to continually use the old round key when expanding the key, the control module respectively numbers the process of key expansion, the data being processed by each module, and the round keys required for encryption and decryption. Also, correspondingly there is comparison and data selection mechanisms in the design. Thus, when the key is changed, the newly expanded round key can be taken out to the respective required module synchronously with the old round key. So that data of different keys can be encrypted or decrypted at the same time, further accelerating the operation speed of the system.

The control module is shown in Fig.3, in which the multifunctional operation modules 0, 1, and 2 respectively refer to the multifunctional key-expansion module, the multifunctional encryption module, and the multifunctional decryption module. The signals "Dan", "Pat", "Nkn", "Iter", "St", and "Open" all consist of three components [0], [1], and [2], which respectively express corresponding functions of the modules 0, 1, and 2.

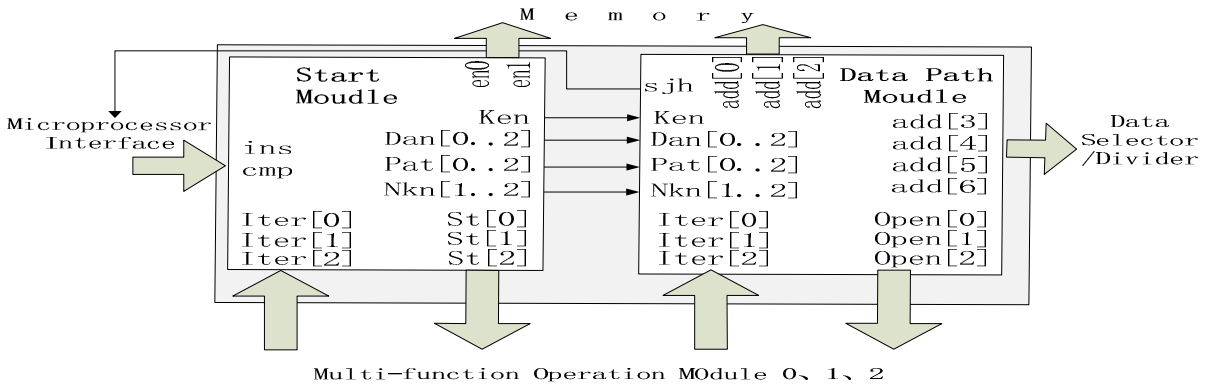

Fig.3 Control module

The startup module is in charge of receiving the system instruction "ins" and the key converted signal "cmp" output by the microprocessor interface, and the iteration number signal "Iter" output by the multifunctional operation module. Simultaneously the startup module comprehensively analyzes and determines the current working module and its working mode. Then the system key extension number "ken", each module's data number "Dan", working mode "Pat", and the required key number "Nkn" are sent to the data path module. And the start instruction "St" is output to the selected module, to run the corresponding module. The output enable signals "en0" and "en1" respectively control the assignment of new key to old key and the assignment of new round key to old round key in the memory.

The data path module is in charge of receiving "Ken", "Dan", Pat", "Nkn", and "Iter". Then it comprehensively analyzes and timely determines which module satisfies the new round of calculation conditions. So that the data path to be set is determined. Then it respectively provides address signals "add[0]"-"add[2]" for the intrinsic parameter storage, the new/old round key storage, new/old round key selector. It outputs address signal "add[3]"-"add[6]" for each data selector in Fig. 1, so as to control the data to the required module quickly. Finally the signal "Open" expressing the path ready is output to the arithmetic module requesting access.

Function Test

The controller and F/F' transform IP core in the SM4 chip are designed by the VHDL language in Quartus II, and the high-speed SM4 encryption/decryption system is constructed. Download the design to Altera's FPGA development board and build a test platform. Write the incentive to verify the system's functionality as follows.

1.According to the reference data given in [4], a set of plaintext 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10 is encrypted once with the same key to verify the encryption function of the system. By observing the simulation waveforms, the generated ciphertexts 68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46 and the key expansion results are consistent with the results provided by the literature. All of these indicate that the system can successfully complete the expected encryption operations.

2.Using the above key and plaintext for 1 million times encryption operations, the ciphertext 59 52 98 c7 c6 fd 27 1f 04 02 f8 04 c3 3d 3f 66 is obtained. The test results show that not only the calculation results are consistent with the results provided by the literature, but also the whole process is only used in the Quartus II for approximately 0.1 s, which is equivalent to 100 ns/encryption.

3.Using the designed F/F' transform IP core, a traditional single-cycle structure of SM4 system is constructed. Under the test platform, the same encryption operations were performed for 1 million times. It was found that the designed traditional system can also successfully complete the task, but the time was increased and about 0.3s.

Conclusion

Seen from above all, the designed F/F' transformer IP-core, can successfully set up kinds of SM4 encoder and decoder. This can effectively speed up the chip’s developing process. Simultaneously, the controller and super-speed pipeline can make the designed three operating module cooperate with each other，which complete the en/decode task triplely. In short, this design greatly promotes the promotion and application of SM4 algorithm in the field of high-speed network transmission.

Acknowledgements

This thesis is supported by the 2015 Shandong University Science and Technology Project, numbered J15LN67 and named Research and Application for Super-speed Encryption & Decryption System of National Cipher SM4 Algorithm .

References

[1]China National Cryptography Administration. http://www.oscca.gov.cn/News/201204/News_1227. htm.
[2]Zhong Mingfu.Security Analysis for Blocking Password SMS4 .Xi'an:Xi'an Electronic Science and Technology University, 2008.
[3]Liu Jia, Wei Baodian,Dai Xianhua. The Cryptographic Properties of the S-box in SMS4 Algorithm . Computer Engineering, 2008; 34(5):158-160.
[4]National Cryptography Administration. SMS4 Cryptographic Algorithm for Wireless LAN Products. http://www.oscca.gov.cn /UpFile /200621016423197990.pdf，2006.