The design and implementation of 3DES algorithm in CA system

Hao Wang

Changchun University of Science and Technology, Changchun, Jilin, 130022, China

Abstract

Conditional access (CA) system is an integrated system, the system involves a variety of techniques, including decryption technology and solution plus descrambling technology, coding technology, multiplex technology, intelligent card technology, network technology, receiving technology, also related to the user management, program management, charge management, information management technology. The two key technologies of conditional access system for the security of the transmission stream and the security transmission of the scrambling control word. An encryption and decryption method for broadcast services or programs to ensure the safety of transmission, the transmission stream is added to the transmission stream, so that unauthorized recipients can not get the correct video and audio stream. Perturbation method is used to control the character of the video stream. The control word and the authorization information are transmitted to the connecting terminal through the encryption and the video stream multiplexing. Receiving end to decrypt. And the algorithm has high security, so far, in addition to using exhaustive search algorithm to attack was not found a more effective way. And a long key exhaustive space, this means that if the speed of a computer is per second to detect a million keys, he searched all the key needs in time. Thus, it is difficult to achieve. But now has been devised to search key special chip, make the cracking time is greatly reduced, in years, spent million cost to build an exhaustive cracking machine 3.5 hours to be able to find a key, if the cost of million dollar price are expected to search time to minutes. As computing power and storage capacity is increased greatly, take the exhaustive attack about expense will become smaller and smaller. And this undoubtedly to the encryption algorithm brought severe challenges. However, through the corresponding improvement of the original algorithm, still can achieve the security of data.Such as using triple algorithm. The algorithm is recommended by cryptographers Angela Merkel and Herman, its purpose is aiming at the shortcomings of the standard algorithm in bit length keys will not be very good against brute force method to crack the improvement. This paper studies and implements the encryption algorithm based on the advanced hardware description language, which is applied to the conditional access system, and the correct control words are used to correct the correct video and audio stream.

Keywords

Conditional access

1. Conditional access system for digital television

Digital TV is a television program from the aspect of recording, editing, transmission, reception and so on all use digital technology to achieve. Includes a digital photograph, manufacture, coding, modulation and receive etc. to achieve high quality transmission of television signals. Digital TV has a wealth of television programs, digital radio, sunshine government, information services, interactive games and other functions. Digital TV is relative to the analog TV TV, digital TV signals can be generated directly, such as the production of animation, subtitles and digital camera digital signal can also be is a digital

signal generated by the analog signal after the digital transformation. Now most families watch TV programs are used in traditional analog signals. Compared with analog TV, digital TV has the following characteristics and advantages of high definition, good audio effect, strong anti-interference ability. Digital TV signal transmission, unlike the analog signal is affected by noise accumulation in the transmission process, and is not limited by geographical factors, almost unlimited expansion of coverage in the TV image is received by a receiving terminal to see and listen to the sound quality is very close to the level of the studio. In addition, the audio effect of digital TV is good, can support five channels of Dolby digital surround sound home theater service. Channel number will increase exponentially. Using the existing analog TV channel, the high quality digital television program with high quality can be transmitted to the user. Encryption and decryption can be convenient to achieve the function of scrambling and scrambling, which is convenient for professional applications, including military and broadcast applications, especially to carry out various types of billing business. And the application of conditional access system, can achieve good management of users and business. System uses an open middleware technology, to achieve a wide range of interactive applications. Easy to implement signal storage, and storage time and the characteristics of the signal has nothing to do, easy to carry out a variety of value-added services. Because the existing analog television video format is reserved, the user can receive the digital TV program by adding a digital TV set top box only. In the new century, the world has entered into the digital and information age, digital technology is the inevitable trend of the development of science and technology, radio and television can not be free. Conditional access digital TV encryption control of core technology, to provide the necessary technical means for the operation of digital TV, the State Administration of radio, film and television will be as the main technologies of the cable TV industry transformation support, that is, through the system to solve the value-added service charges.

Conditional access is the effective means to the implementation of the various services of different protection and for the purchase of corresponding authorized user control, including encryption and decryption technology, descrambling technology, coding technology, multiplex technology, intelligent card technology, network technology, receiving technology, in addition to involving user management, program management, management fees and other information management technology, our country pay digital television is still in the initial stage.

2. Cryptography overview

Symmetric encryption, also known as traditional encryption or single key encryption, public key cryptography is the only one before the encryption technology. So far, it is still the most widely used one of the two types of encryption. It has five basic components, as shown in the table.

Table1. Composition description of symmetric encryption algorithm

component	Explain
proclaimed in writing	As the input of the algorithm, the original understandable message or data
encryption algorithm	To express various substitution or transform encryption algorithm
secret key	Input key and encryption algorithm, key independent on plain text, the algorithm will according to the specific key and different output, substitution and the transformation of the algorithm also depends on the encryption key
ciphertext	As the output of the algorithm, looks completely random and messy data, dependent on the plaintext and key, for a given message, different keys will produce different ciphertext ciphertext is random data stream, and its significance is incomprehensible
decipherment algorithm	In essence is the inverse of the encryption algorithm.

The cipher encoding science system has three independent features, which are transformed into the type of operation of the cipher text. All the encryption algorithms are based on the two principle of substitution and replacement. Substitution is to express each element potential, letters, byte or word

group mapping into another element replacement is expressly rearrange the elements. The basic requirements of the above operations are not allowed to have information is lost that all operations are reversible. Most cryptosystems use multilayer substitution and replacement. Number of keys used. If the sender and receiver use the same key, the code is called symmetric cipher, single key password or traditional password.

3. DES

In 1973, NIST publicly collects a national symmetric key encryption system. A program from the IBM, after the modification was identified as DES. The United States Federal Register in March 1975 will be published as a draft of the federal information processing standards. After the announcement, the draft was severely criticized. The main reasons are the two the critics only 156 length of secret key to very skeptical, that the scheme can not withstand brute force attack the other critics are very concerned about the internal structure of the hidden design. They suspect that can break some of the information structure in some parts of the words box to hide some secret door in the national security agency without a key.

Let's look at the encryption, and then look at the decryption. The encryption process is composed of two permutations. We call the initial permutation, the final permutation, and the wheel. Each round using a different bit of round key. The round key is generated from the password key according to the predetermined algorithm. The composition of the encrypted password is shown in the figure1.

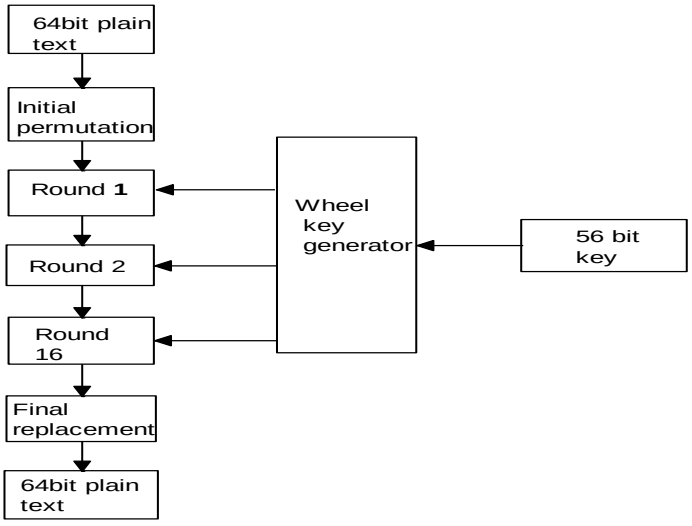

Fig.1 General structure of DES

If we can create a computer with one million chips in parallel, we can test the entire key field in an hour. When it comes, the cost of such a computer is more than a few million dollars, but the price is falling fast. Special computer made in the year, you can find the key within hours. With today's high-speed server design, and even in a few minutes to find the key. The above discussion can be seen, a bit key password is still not safe enough. Therefore, in the improved algorithm, we can use the three key bits with two key bits or three key bits with three key bits. Weak key in a weak key is called a weak key. A weak key is in operation after removal of parity, by all or all, or half an.

4. Implementation and application of Verilog in 3DES

In this design, the language is used to carry out the design and implementation. Language is a kind of advanced hardware description language. Compared with language, it can be more convenient to use the behavior and structure of the abstract circuit. It is easier to simplify the behavior and structure of the circuit, and easier to grasp. In front of our mastery of the algorithm based on, in the design, first of all to achieve and decryption algorithm of each module, such as a change in the type box, key generation module, in each round of key selection module, and the organization of each module, algorithm

modules, on the basis of these modules. According to the requirement of, from the top module will algorithm modules using three times, for encryption, using two encryption module, inserted in the middle a decryption module for decryption, using two decryption module, inserted in the middle a cryptographic module.

Definition of encryption and decryption module, where and are the system reset signal and a clock signal to operation on the bit data, operation data, for encryption and decryption key, and used to for realizing the extension bit box in the module, in the module, with the statement realized initial displacement and ultimate replacement, first of all data come in, first with a sentence initial replacement values into an industry and trade to do further processing, bits of data processing, by the last round of the output,. The final permutation is converted into the final result output by using the statement.

The CRP module is the most important module in the DES module. Its implementation of the module, such as

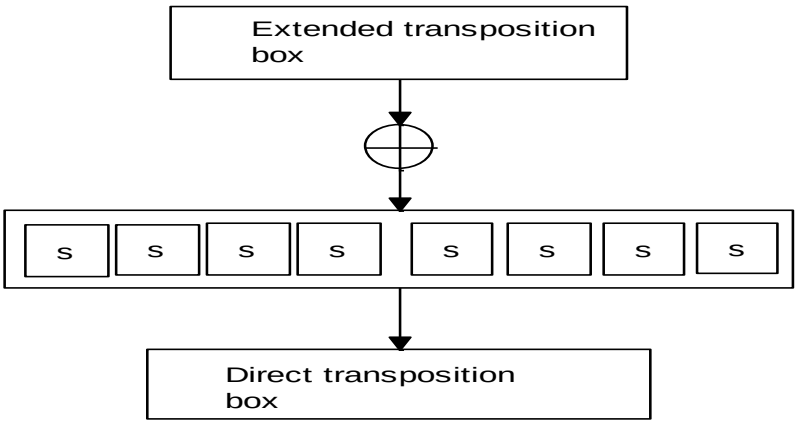

Fig.2 CRP module

In the top-level module design, the introduction of the global reset signal and the global clock signal, which is applicable in all sub modules. According to our previous statement of security, we use a bit key, using the representation is used to decrypt or encrypt, and give a signal to indicate the operation of the. The input is used for encryption or decryption of the encrypted text used to indicate that the output of the encryption or decryption of the encrypted text. We use a counter to indicate the number of rounds of encryption. With a clever representation of the first round of encryption, so when the coincidence is effective, you can output a data encryption or decryption. In the process of encryption, the password process needs to do two times, reverse the process needs to do a time, such as the front of our three. When the third time in the end of the first round of encryption, we can get the right.

5. development environment

In this design, VHDL language is used to design a hardware description language, which is used to model a variety of abstract design levels from algorithm level, gate level to switch level. The complexity of the modeling of the digital system Liu can be between a simple gate and a complete electronic digital system. The digital system can be described in a hierarchical manner, and the time sequence modeling can be explicitly performed in the same description. VHDL language has the following description ability design behavior characteristics, design of the data flow characteristics, design of the structure and contains response monitoring and design verification of delay and waveform generation mechanism. All of these use the same modeling language. In addition, language provides a programming language interface, through the interface can be simulated and verified during the design of external access from the design, including the simulation of the specific control and operation. Language not only defines the syntax, but also defines a clear simulation and simulation semantics for each syntax structure. Therefore, the model can be used to verify the model using this language. Language has inherited many operators and structures from programming languages. Provides an extension of the modeling capabilities, many of which are initially difficult to understand. However, the core subset of the language is very easy to

learn and use, which is sufficient for most modeling applications. Of course, the full hardware description language is sufficient to describe the entire electronic system from the most complex chips. The development of the language in the environment simulation. Is the industry's most excellent language simulator, it provides the most friendly debugging environment, is the only single kernel support and hybrid simulation of the simulator. Workmanship design level and gate level circuit simulation preferred. It uses direct optimization of compiler technology, technology, and single kernel simulation technology, compiled simulation speed, compiled code and platform independent, facilitate the protection of nuclear, customized graphical interface and user interface for users to speed up the wrong to provide powerful means. Full support and language of the work standards, support function calls and debugging with a fast simulation performance and the most advanced debugging capabilities, including a comprehensive support, and platform.

Reference

[1]Liu Xiuwen. Digital TV cable transmission technology Beijing Electronic Industry Publishing House.

[2]Gong Jianrong, Liu Da. Digital TV technology Beijing Electronic Industry Publishing House

[3]Zhao Xiaolin, network security technology course Beijing National Defense Industry Press

[4]XieXiren, Beijing Electronic Industry Publishing House, the first edition of computer network

[5]Lu Kaicheng, Beijing Tsinghua University press, computer cryptography

[6]Wu Shizhong, Zhu Shixiong, Zhang Wenzheng, et al. Application of cryptography in Beijing Machinery Industry Press

[7]Gao Chuanshan, Qian Songrong, Mao Dilin data communication and computer network Beijing Higher Education Publishing House

[8]Feng Dengguo, Pei, cryptography guide Beijing science and Technology Press