With the informatization of society, the Earth has become the global village and the contact between people is closer. Now the conception of the IoT(Internet of Things) rises and the Earth is ready to accept another revolution. Experimental products like smart furniture and car networking appear in the market. The media describes the future life which is full of IoT as beautiful as a painting. Though the IoT may make our life more convenient, it is irresponsible that the media only introduces the advantages of the Iot without mentioning the disadvantages at the meantime. We have seen how destructive it is when the secure incidents occur in the Internet though no doubt that the Internet has brought good change to our life. What we should learn is that everything has its good side and bad side. When we talk about the convenience the IoT may brought, we should not forget that the IoT may also be dangerous. For example, factories may stop producing, cars may become out of control, smart furniture may cause fire. So the security of the IoT should be paid attention to.

Another problem is that there isn’t an exact definition of the IoT even now. In 1999, MITAutoIDCenter gave the early definition of the IoT: using RFID/wireless communication technology to build an Internet of Things based on the Internet. In 2005, ITU formally gave the conception of the IoT and expanded its meaning. It pointed out that the IoT was the expansion of the Internet and four core technology to realize the IoT was RFID, sensor technology, nanotechnology and intelligent embedding technology. In 2009, EU published CERPIoTSRA which defined the IoT as indivisible part of the Internet and a dynamic global networking frame which had self- organized ability based on certain standard and communication protocols. Though there isn’t an exact definition of the IoT and there is no standard now, secure standard will no doubt be a must.

Nowadays, there are various research about the IoT because it is regarded as strategic developing aim. But most paper focuses on the developing direction or the frame of the IoT, and some just adapt the IoT to systems in other area while few research the possible security problems in the IoT. So it is meaningful to research the secure problems in the IoT.

Since various things with different chips within them will be connected to the IoT, encryption algorithm like RSA/AES may not be suitable because of the difference in computing ability of those chips. So a lightweight cryptographic algorithm is needed which could be used even in chips whose cimputing ability isn’t pretty strong. And Trivium is exactly a lightweight cryptographic algorithm, so it is possible that Trivium may be the cryptographic algorithm in the IoT in the future.

Trivium is a hardware-based stream cipher algorithm, which is one of eSTREAM Project's final victorious algorithms. It is proposed by Christophe De Canniere and Bart Preneel. It gained great attention once it was published because of its simple and elegant design. It was designed to see if an algorithm could be simple without sacrificing its security, efficiency and flexibility. Trivium also declares that it is very secure. And until April 2015, several attacks are close to break Trivium. First an attack due to Michael Vielhaber broke a variant of Trivium where the number of initialization rounds was reduced to 576 in only 212.3 steps. Then other authors speculated that attacks which built on Michael Vielhaber’s cound lead to a break for 1100 initialization rounds or even the original Trivium. Then the cube attack which need 268 steps to break a variant of Trivium where reducing the number of initialization rounds to 799. Another attack use around 289.5 steps (where each step is roughly the cost of a single trial in exhaustive search) to recover the internal state (and thus the key) of the full cipher. By using an equation-solving technique reduced variants of Trivium using the same design principles have been broken. Though these attacks are close to succeed in breaking Trivium, these attacks all have their own supposition. For example, some reduce the number of the initialization rounds in the origin Trivium, some suppose that they can control the plaintext, and some even suppose that they can control the internal states. It was these supposition that make their attacks break the variant Trivium and it was these supposition that make their attacks close to succeed in breaking the origin Trivium instead of succeeding in breaking the origin Trivium. For example, some suppose that they can control the plaintext, and it is possible in most situation, but in the IoT chips may only send the set message and thus make it more difficunt control the plaintext. And we should notice that the best attack method until April 2015 was still brute force attack, so Trivium is still a secure algorithm, and we can use it in the IoT.

Trivium Is still a new algorithm and there isn’t much research on Trivum, and most as mentioned above study the security of Trivium by trying to break it. But there is rarely research on Trivium itself like the structure of Trivium, what should be paid attention to when design the algorithm which is similar to the origin Trivium, not mentioning the application of Trivium. But we may learn more about Trivium when trying to adapt it to a real application environment. When we try to adapt Trivium to a real-world scenario, we will have several mark like the efficiency and security needed in the IoT. And when we try to improve Trivium to reach these marks, we may learn more about Trivium. So it is meaningful to study how to adapt Trivium to a real-world scenario.

In this paper, we study Trivium in two ways. In one way, we study the Trivium algorithm itself like what the structure Trivium has or the period of Trivium. While in the other way, we suppose that we use Trivium in a real-world scenario and see if Trivium is suitable for the scenario. If Trivium doesn’t work well in this scenario, we try to improve it.

In the first chapter, we simply introduce the Trivium algorithm and the development of the IoT.

In the second chapter, we will introduce the Trivium algorithm in detail. First, we introduce the traditional Trivium. We will introduce how to use Trivium to generate key stream, how to initialize the internal states of Trivium and how to realize Trivium by hardware. Then we will analyze the structure of Trivium. We will analyze the state-transition matrix of Trivium. And we will parameterize Trivium, which we call the Trivium type algorithm. Finally, we will study the period of the linear part of Trivium, and then the nonlinear part. We will try to construct some internal states which will lead to the appearance of minor cycle. We try to construct these internal states so that when we try to use Trivium, we can avoid using these internal states to keep Trivium safe.

In the third chapter, we will try to suppose a real-world scenario where we will use Trivium. First, we will analyze why we should use Trivium in the IoT like what are the advantages if we use Trivium in the IoT. We will judge it by analyzing the efficiency and secure of Trivium. Then we will try to adapt Trivium in tracking valuables. We will introduce the background of tracking valuables first, and then the design. How to locate the valuables will be the first part of the design. Then several RFID protocols will be analyzed to see their efficiency and secure and then choose one to change to the Trivium type. The design of Trivium type RFID protocol will be the third part of the total design. And the design of hardware will be the final part where we will show the frame diagram of the whole design. Then we will analyze whether the design is reasonable which means we will discuss whether the privacy of communication is assured and whether the valuables can be kept safely. Finally, we will raise some other scenario where Trivium may also be used and make the conclusion of this chapter.

In the last chapter, we will make the conclusion.