The System design and application of the IC card

student identification no. : g753019, student name : Guo-zhan Huang

Abstract

The professor Hou has had a real vast experiment at IC card design and development for a long period time at the Peng-hu County and has speeches on the components, structure, classification and experiment of IC card. Now we will write some basics, transaction, categories, classifies, components of IC card and also talking about the questions.

key word: card reader, co-processor, contact IC card, contact-less IC card.

1. Introduction

IC cards are popularly used in any ranges of applications. So knowing the basic flows and structures are more and more important. Professor Hou had gave a speech in our school and sharing their team's experiments. Student Huang writing and collecting some basic mechanisms to present the outline of IC card. Major part of data were collecting by this speech which the professor even said. In the last, this writing will write the thought of this speech.

2. The IC card

This writing has divides four parts, flow of transaction, flow of data, categories, questions, to description of this speech on the IC card. The main purpose of this writing is to know the basic mechanism.

2.1 The Main flow of IC card transaction

Firstly, we have to know about the main flow of the IC card in perspectively for understanding the enormous mechanism. We simply divide three stages according to the similar functions for knowing the mechanism. At the beginning, we have to input the data, classify and filter data when we are used IC card for something right now, so the Card reading stage is produced. This stage is receiving, arranging the data for the next stage, communication stage. At the communication stage, the main purpose is to make sure personal information sending in security and reliability. This stage has a high connection oriented, that is, if the connection broken the mechanism would be error. When the information is successfully transfer into the destination, compose of the corporation, authorized third-party, insurance corporation etc, confirms the card owner wheather had published by our organization. The flow structure is draw below.

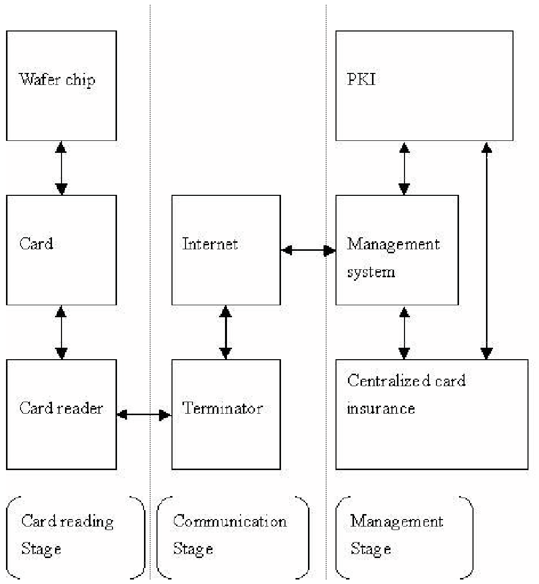

Figure1. Main flow of transaction

2.2 The characteristics and category of IC card

We have knows the general transaction mechanism in the IC card from the foregoing. In this subsection we have to know about the characteristics and category of IC card. The characteristics are description below in the table. We can find that some stranges that are the property of mobile and high speed need at main memory. The mobile mean that reader could computing card information when card is moving and the other starnge is that professor Hou had talked about the performance was due to the speed of EEPROM not micro-processor's. So for speeding up system, we have to use high speed EEPROM is effectively. The material to produce the IC card normally is divided into surface material, communication interface, micro-processor from external to internal.

Table 1. materials and characteristics

Materials to produced the IC card	Characteristics
PVC, ABC or other materials.(ISO standard materials)	Basic and not many operation is existence in the IC card.
Communication interface.	High security.
IC chip(micro-processor, MM, CU).	High speed need at main memory.
	Property of mobile.

In the category of IC card we divide three parts according to type of I/O, computing, CPU allocation. we can find that memory card has not need a lot of functions but just identification or other normal functions, even not use of CPU but memory. And the combi card means that really merges two micro-processors into one, but the hybrid means that two micro-processors are communicated by shared Main Memory, EEPROM.

Table 2. Category of IC card

Category By I/O	Contact card	Contact-less card
Category by if have computing	Memory card	Smart card
Category by CPU, Memory allocation	Combi card	Hybrid card

2.3 Components of the IC card

We will description of three pars, I/O, CPU and MM, in this subsection. The categorys of I/O component are divided easily by contact or contact-less. In Figure2. we can see that the important part is co-processor and MMU. The co-processor is encryption[1] or decryption of data for security hence speed up processing. The MMU is using paging to solve security issue, to make confusing the location of data. Now we draw a simple figure below that.

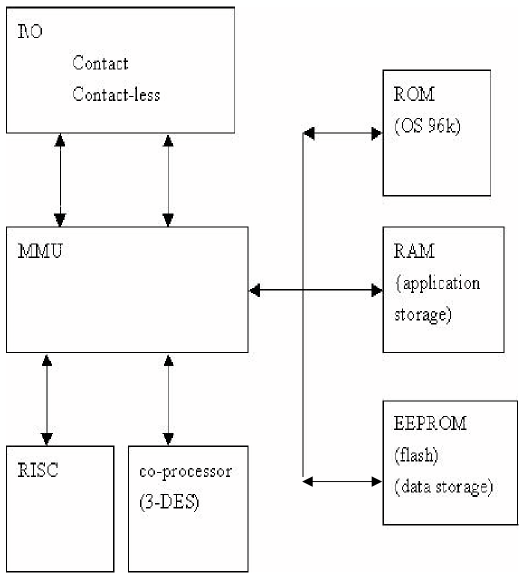

Figure 2. Components of the IC card

2.4 The existence question

In this subsection we list some questions and descriptions in table that professor had been talked about.

Table 3. Some quetions and their descriptions

Questions	Description
Collision avoidance	How to recognize multi-cards in one card reader.
Management of cards, Memory allocation	1. Every card has identification(unique) and series NO(candidate key). 2. Key management,Key diversification and key life time of card is complicate. 3. Key generator is also hard to find(prime).
One machine to recognizing multi-card or One card to recognized multi-machine., Memory allocation	Two strategies of construction.
Defensing attack	1 power analysis(SPA): Let people couldn't check out the distribution and volume of spesific electronic current. 2 time analysis(DPA): Let people couldn't check out the differential of electronic current. 3 fault induction: To prevent extreme temperature, infrared ray attack. 4 Destroyed by itself when there has a suspicious intruder.
Hardware is pass by authorization, but software does not or reverse the situation. Is it could be pass authorization test in such situation , Memory allocation	Authorization is most costly.

2.5 Conclusion

Through this writing we can know the basic mechanism of IC card and could image that several techniques like the recognition of figurer print maybe used to recognize the owner or support generate the key due to the relation beteen IC card and the owner is weak. Even different techniques we have, the most costly parts are still the fees of several authorizations. How to reduce the cost or union organizations are also important. In the last we also have to care about the synthesis of production cost and effect.

3. Reference

[1] Charlie Kaufman, radia perman and mike speciner, *"Network security private communication in a public world"*, 1995.