**IC CHIP BANK ARCHITECTURE:**

Daniel Komac:

The Abstract for this report is: Bank chip architecture and how it manages bank accounts from the Integrated circuit chip in the credit card. The constraints that are needed for the chip to actually work and how to manage it from a console, the card reader has a chip reader as well which is a more secure way to transfer data. Not only that, but the security behind this architecture is much different than before with the magnetic strip. The field is vast and growing, this technology can be applied for more than just financial transactions such as transit or other means of social interactions or social purposes.

CPE 186, Computer Hardware Design, Spring 2016

March 20, 2016

**Table of Contents:**

1. Introduction
2. The building blocks
3. Power Management
4. Security Management
5. Other Smart Card Applications

**List of Figures:**

1. Invention picture
2. Real world smart card
3. RF IC circuit
4. RF Front end circuit
5. RF contactless circuit
6. Rectifier
7. Programmable shield
8. DES encryption/decryption

**Introduction:**

The IC Card, or integrated circuit card or chip, found on most common day credit cards is growing in most modern day transactions. As this technology proceeds to make advancements, so must every security measure and integration of this technology. The reason for these advancements is because there will always be a risk of security when finances or sensitive information are involved. These cards can also be called Flip chips because of the transaction method known as C4, controlled collapse chip connection. Using these basis for Integrated circuit cards, a foundation can be built upon for this invention, the innovations that people design using a smart card has changed drastically though the concept has been around for many years. Changes in security and production have taken very large leaps and still needs to be improved as the technology still has much room for improvement. This field of study has a potential for very high turnout and researchers are continuing to look deeper into the subject matter. Topics such as fault attack protection and power recovery are just a few concepts that researchers are dwelling into in order to optimize this new technology.

**The Building Block:**

The basic foundation of the Integrated circuit chip, also known as the smart card, are small plastic chips integrated onto plastic transaction cards for easy accessibility. Smart cards can provide the same utilities as traditional magnetic strips but uses a different method of transaction known as contact or contactless transactions. The first design was invented in 1975, see Figure 1, and first major implementation was for paying off telephones, the invention has changed over the years and has been used to supply many people with a way of making paperless transactions. All of these smart cards follow a public key infrastructure, which covers how to distribute keys amongst users and how the user is allowed to interact with the host of this key. Smart cards also follow protocols that are used as standards such as ISO/IEC 14443 and ISO/IEC 7816, these standards insure that these smart cards operate at 13.56 MHz, includes specifications for relations using frequencies, power, and certain protocols, also operating at a distance of four inches, and Parts 4 and above of ISO/IEC 7816 contain security operations and commands for interchange. Lots of standardization has happened with smart cards to ensure security, as the era moves forward the development of this technology must take advancing steps in ensuring great coverage over every potential scenario. These smart cards are microcontroller level memory cards that are embedded onto plastic cards, see Figure 2, which are able to transfer data through contactless radio frequency interfaces. These contactless interactions are achieved though magnetic or electromagnetic fields which supply power to the onboard chip on said device, in this case for the transfer of money from an Integrated circuit chip on a debit or credit card. This power allows the reader and card to supply important information to one another so the chip can perform functions such as: Energy transfer, clock signal transfer, data transfer two and from the smart card. This is achieved through the previously determined standard of power in smart cards or smart card readers, they must maintain a frequency of 13.56 MHz which in turn powers the card if the proximity is within the range of four inches, this information is obtained through an antenna embedded in the body of the card allowing access to information such a distance and for transfer of power through radio waves. Smart Card technologies have the ability to provide security measures such as: Authentication, Secure data storage, Encryption, Device security, secure communication, Biometrics, Personal device, and certifications. They continue to say, the card contains ways of authenticating requests for information to the card or device, this can be applied to banks who have been authorized access onto the chips data and or functions. Smart card alliance mentions means of authenticating such as, only allowing authorized personnel, banks or users that are granted access onto the chip, are able to access the device and a device reader such as a chip reader are needed to obtain this information. Smart card alliance proceeds to talk about encryption information saying that, the embedded smart card also contains built in encryption capabilities such as: key generation, secure key storage, hashing, and digital signing. All of these encryption methods allow for unique identities to be created providing validity to sender or receiver of content and further preventing fraud attacks or any other possible identity related issues. Apart from encryption, smart card technology is unique, hard to duplicate, and contains many tamper-resistant hardware and software features that combat and react to tampering attempts to prevent possible attacks. The communication methods used by Smart cards and smart cards readers are very similar to those found in computer networking, they use protocols to secure and establish a reliable connection ensuring that information is not intercepted or tapped into. Fingerprints or other biological features can also be stored on these smart cards allowing for an added layer of security, allowing for a completely unique way for a single individual to access their information. The Smart card is able to use this information and perform matching functions in order to distinguish and individual. Smart cards are also hand held, allowing for quick access to any personal information stored on the Integrated Circuit chip and can be used in many different ways to store a person’s individual information. Many Smart cards are rigorously tested to make sure that they comply with industry and government security standards. When operating with such sensitive information, security is a valuable asset to maintain in the development of Integrated Circuit chips. Although hardware attacks are very hard to achieve with the secure structure that is already implemented with the Integrated Circuit Chips on smart cards, it is possible that with the remaining functions tremendous amounts of damage can be done by manipulating sub routines or other actions in the Integrated circuit chip embedded on smart cards. This is the purpose of building up security for these chips because once they are implemented they must follow regulations and afterwards must perform adequately in the real world, where attackers try to infringe on peoples personal and classified information. This is the basis of these cards, small, secure, microcontroller/memory cards/ smart cards, following set protocol to ensure a uniform system is upheld in the real world.

**Power Management:**

These Integrated Circuit chips operate off of a 13.56 MHz frequency and are able to be operated through an electromagnetic field on one of the appropriate readers, such as the plug in credit card readers on the debit transaction machines. (Li, Wu, & Zhang, 2013) As today’s standards continue to change the need for embedded circuits in financial cards is actually a necessity and will need to be implemented on every bank card available within the next couple of years. (Li, Wu, and Zhang, 2013) With set regulations needing to be maintained a challenge arises, the challenge being that power efficient chips need to fit on these plastic cards, it has been achieved but over the years it wasn’t so simple. The independent cores that needed to be powered on a powerful computing Integrated Circuit Chip like the ones seen in modern society require a specific Radio Frequency front-end circuit lay out to supply lower end frequencies to the rest of the chips on board features, see Figure 3 for design of IC card with RF front-end circuits. This exists because of the radio antenna found on Integrated Circuit chips that supply power for the functions on the embedded chip. “A typical layout for a RF front-end circuit consists of: band-pass filter, which reduces strong out-of-band signals and image frequency response. An RF amplifier, often called the low-noise amplifier (LNA). Its primary responsibility is to increase the sensitivity of the receiver by amplifying weak signals without contaminating them with noise, so that they can stay above the noise level in succeeding stages. It must have a very low noise figure (NF). The RF amplifier may not be needed and is often omitted (or switched off) for frequencies below 30 MHz, where the signal-to-noise ratio is defined by atmospheric and man-made noise. A local oscillator (LO) which generates a radio frequency signal at an offset from the incoming signal, which is mixed with the incoming signal. The mixer which mixes the incoming signal from the local oscillator to convert the signal to intermediate frequency (IF).”(Wikipedia, RF front end) This is the standard layout of an implemented RF front end, see Figure 4 for RF front end with connections, which is being used by the Integrated circuit chips and this is connected to our embedded chip via a bus. This power is transmitted to the chip via electromagnetic waves from the reader, this power is dispersed from the previously stated RF front end circuit, see Figure 5 for RF front end circuitry that is connectionless, and powers the Integrated Circuit chip through contactless connection. But the conversion of this frequency to such a low level wouldn’t allow for the chips expensive cores to function properly, this can be achieved through High efficiency Rectifiers, allowing for a cheap way to supply power to the chip (Li, Wu, and Zhang, 2013), also see Figure 6 for a basic diagram of a rectifier. The full power of the chip is achieved through these electromagnetic interactions, the problem that has been solved is the high intensity of power needed to power such a powerful device.

**Security Management:**

When faced with the task of keeping all of the components of the microcontroller/smart card/memory cards safe there are many tasks that must be insured so that harm is not done to the personal information of the user or the database and no physical damage is retained from a malicious attacking of outside forces or corruption of hardware operations. The amount of security needed is also evaluated by the intensity of an attack or the importance of the functions being performed or the data being used. These attacks fall under 3 separate categories of attacks: Fault attacks, Side-Channel attacks, and Invasive attacks (hardware attacks) (Smart Card Alliance). Fault attacks aim to alter the IC’s workings by injecting an error or trying to induce an error, this a huge problem when it comes to financial interactions as we have to account for every bit and function that is operating. Smart card alliance proceeds to list faults that could occur, fault attacks attempt to try and reveal information from the chip, the security measure for this is that the Integrated Circuit chips have sensors to control redundant logical operations, and if it is being manipulated to act out of its normal parameters the Integrated Circuit chip will go into an alarm state and prevent further operations from being complete so that way the chip will remain secure and inaccessible to anyone trying to continue to tamper with it(Smart card alliance). Another method of attacks is the Side-channel attacks, these attacks involve accidental leaks of information through any other Medias being used such as: timing information, power consumption, electromagnetic leaks, sound, etc. can all give a pathway to important information. There are countermeasures that have been implemented to prevent such attacks, Smart card alliance states that, from being successful such as: Random wait state insertion, this can be used to determine whether the Integrated Circuit chip is obeying commands from the reader or from an outside source that has not been allowed access to manage such resources. Bus confusion and memory encryption, bus confusion is the state in which idle buses are given randomly generated noise to process, this counter measure protects against people who are analyzing information on the bus or outgoing communications. Continuous check of random characteristics, this is the process in which the chip runs functions to assure that the variables are in order and comply with currently running procedures and other variables to make sure that they are valid and have not been tampered with. Current scrambling/stabilizing, this feature in conjunction with the random wait states allows protection against power or timing analyses since the currents will be random and wait states will throw off timing for intruders trying to analyze the Integrated Circuit chip. Voltage regulation, the Integrated Circuit chip embedded on smart cards allow for monitoring of external sources that share frequencies and voltage with the chip, i.e. a clock. The final security feature to address Side-channel attacks is Dual bus rails, this allows for bus transmission to be transferred from one rail of the bus to another in order to confuse the embedded chips attacker. The more intrusive mean to obtain information from the Integrated Circuit chip is an Invasive attack, also known as hardware attacks. Some examples of Invasive attacks that the Integrated Circuit chip protects against are: probing with microprobe or focused ion beam, reverse engineering, and circuit modification. The secure microcontroller/chip/memory card contains methods to counteract these acts, these features include: Flexible and user-defined memory encryption of user memory, RAM, and ROM. Each Integrated Circuit chip developer has the right to use any language with their chip allowing for a very flexible and diverse form of protection from attackers. Usage of memory management unit that prohibits applications from accessing code of another application, restrictions that prevent users without access to be denied services from applications that are not granted to them, this further increases security ensuring that an unwanted client doesn’t tamper with restricted information. Active shielding that renders IC inactive when triggered, this shield is placed over the Integrated Circuit chip and monitors whether outside factors are trying to probe the chip to prevent tampering, it blocks signals as well apart from probing. A small Integrated Chip geometry allows for probe prevention. The native structure of the Integrated Circuit chip gives an extra layer of protection for invasive attacks, Bus confusion and encryption, continuous checking of random characteristics of the Integrated Circuit chip, timing and Integrated circuit layout are all means of protecting the chip from intrusive attacks. The components on the chip are what provide such valuable protection, the list of components are as follow: programmable active shield, sensors, internal timing circuitry, central processing unit, memory management unit, memory and processor bus encryption module, crypto coprocessors, data encryption standards, cyclical redundancy check, non-volatile memory, data bus encryption, random number generator, and a current masking device. Each one of these play a very large role in securely protecting the chip from any damage and this is why power is such a large asset to the chip. The shield as stated earlier protects the chip from attempted probes or forced internal modules or signal lines, see Figure 7 for a design of this shield. The sensors that are built in thwart fault or invasive attacks, these sensors include: “Low/High frequency sensors for the internal clock, Sensors and filters for the external clock, External high and low voltage sensors, internal voltage, Temperature, Peak voltages sensors, glitch sensors on internal voltage, and light sensors on the integrated surface.” (Smart Card Allaince) The internal timing circuitry is inaccessible and provides cryptographic and security operations. CPU, or central processing unit, has proprietary timing or a clock of its own to confuse an attacker and make it difficult for them to determine operations that the Integrated circuit chip is performing. The MMU, memory management unit, this unit manages access into certain compartments of the Integrated Circuit chip so that unauthorized personnel cannot retrieve data without grants from the Integrated Circuit chip. The memory and processor bus encryption module allows for a hashing system to take place by encrypting and decrypting stored data that hold keys which are stored in ROM, RAM, and NVM. The crypto coprocessors are processors used to execute symmetric or asymmetric algorithms allowing free space on the CPU and providing additional hardware security. DES, data encryption standard, is what all Integrated Circuit chips use to perform calculations of DES or 3DES algorithms. CRC, cyclical redundancy check, is a module that assures that the Integrated Circuit chip isn’t processing incorrect data and no errors occur during transmission. NVM, non-volatile memory, is programmed to prevent attackers from obtaining or viewing data in clear text if extracted from the Integrated Circuit Chip. Data bus encryption ensures that if an attacker peeks into the bus to obtain information that the Data is encrypted and is harder for the attacker to obtain or read. RNG, random number generator, allows for a true random variable to be used during Power analysis attacks, yielding false and random wait states for the attacker to see. Finally the masking device unit scrambles how much current the Integrated Circuit is using, essentially masking/hiding the true values that a power analysis would yield. To delve deeper into the Cryptographic engine of an Integrated Circuit chip we can looks at the DES structure used for encrypting, see Figure 8 for DES encryption and decryption method. In the 3DES model the countermeasures used to determine what to protect against is algorithmically programmed. The 3DES using a round encryption/ decryption method that checks it’s results constantly to assure that faults are not occurring and if faults do occur they are managed through bit adjustment or retransmission. The Integrated Circuit chip implements a large amount of resources in order to securely establish connections, process information, and maintain all data from being tampered with. The vast layers of protocols and security measures are very specific and precise because dealing with such sensitive and highly personal information must be monitored with extreme care, errors must be adjusted and all personal information must be kept secure, this is why Integrated Circuit chips on debit or credit cards must contain a large amount components to maintain this level of security.

**Other Applications:**

These Integrated Circuit chips allow smart cards to hold an abundance of energy on such a small scale allowing for a great library of knowledge to be held on this system, such overwhelming power on such a small chip. With the capabilities it has these cards can be used for several identification means and for much more financial transactions other than bank and customer relations. These smart cards are applied to many platforms like SIM cards for phones, Identification cards for personnel, Transits, Computer security, and even personal wellbeing such as healthcare (Wikipedia, Smart card). Relating to phones, the SIM card is a small smart card, with less features than some of the more sophisticated ones, but still contains the same format and some of the same feature. These SIM cards are called subscriber identity modules and provide key information for who the owner of the device using the SIM card is. This application of a smart card allows for users to connect worldwide and have an identity on their device, such as a telephone number which is accessible to any other member connected to the telephone network, and these SIM cards retain valuable contact information storing other peoples information as well as allowing the user/owner the ability to program a passcode to prevent others from using their device. Apart from a worldwide identity these smart cards can hold much more personal information about our bodies, allowing for readily available information of who is holding this card. These smart cards tend to employ a public key infrastructure which utilizes personal information from these public key distributors to grant access into databases or other forms of data. These Identification cards can hold incriminating evidence such as criminal records or other information like that as well as other biometrics that identify the user as being the unique owner of the device. These smart cards can be used for driver’s licenses and can identify a person with a Smart card reader, carrying driver records, date of birth, and other information that our standard driver’s license would show to anyone that wanted to look at. Apart from that many of these smart cards could be used for public transportation to bring together the way society pays for transit, a perfect example of modern society implementation of smart card technology for public transits is the use of a “swiper” card for Municipal Transportation in San Francisco. These cards are a plane piece of plastic which are then checked once entering the vehicle, train or bus, this holds the information/logs into the Municipal Transports database how long you were on for and where you departed from and where you arrived, this information does not affect the amount being paid but the public must pay for this utility as a tax every month. This example shows how a smart card can be used as verification for a ride by swiping it past a smart card reader. Having society be able to pay for a public good allows for finances to be narrowed down to a tax if these services are being used meaning money management is much simpler. Another application for these smart cards is for Computer or network security, granting access to a user that is able to provide it from a smart card that has a key distributed onto it. An perfect example of these security measure smart cards would be ones that could provide access to a private network that only a select few members of society have access to, another example would be FOB key cards which supply access to the given area once swiped past a reader, these could grant access to high level security areas or computer labs. Apart from granting high level access to areas they can provide a bountiful amount of information about the user, this being the users medical records and pharmaceutical data. All of this being applied to an individual can lead to paperless records of clients all being managed through smart chips that retain information from the hospitals database (Hermamto, Mengko, Indrayanto, & Rahman, 2013). A system like this would allow hospitals to disperse smart cards with Integrated Circuit chips that contain medical keys for the patient so that once they come in they can be properly diagnosed without need of managing all of the files and paperwork needed for the client. Each client would be represented as their record descries and in a study conducted for small villages or rural areas, these small scale hospitals and health providers are able to keep check of their patients through paperless means instead of writing down all the information (Hermamto, Mengko, Indrayanto, & Rahman, 2013). Providing a smart card to every member of the community would allow the information to stay secure as long as no one else is able to obtain a way of tampering with the information, private personnel would be the only members able to edit data from these smart cards using basic functions such as adding, removing, or editing existing data. This personal identification leads to the ease of information as these powerful embedded chips can provide an incredible amount of knowledge to anyone authorized to manage the data. All these smart cards would have to follow same rules and regulations to maintain their stature of being secure modes of data transfer but they can also be altered to fit custom needs of a business or of society. These cards functionality is greatly increasing as time proceeds to go by, the rate of technological growth is exponential and before we know it smart cards could be implemented into every aspect of modern day society. Smart cards allow for a vast amount of applicability to any circumstance and give another depth into portable data. Personal devices that can hold any information that is programed onto it and interact with it securely and efficiently is what modern society is moving towards. The movement towards more secure means of communication is always adapting and smart cards are keeping up with the societal change that is happening. Society understands the need for easily accessible valuable information and has been pushing forward with the technology, there is little risk in using an efficient technology like a smart card because of the effort that went into applying these Integrated Circuit chips into today’s society. The use of smart cards will apply to multiple systems over time and society may begin to see a system in which all of the population’s information and government access is supplied by a smart card giving a simple system that allows for uniform accessibility across the nation and even the world. The flexibility of these cards allows for society to be able to make a huge advancement into any field that is needed, smart cards will be applicable to much more than just financial areas even with the encryption data and protocols that must be followed so uniformity can be achieved. Application of the smart card and Integrated Circuit chip may extend farther than just a smart card in the future as we do use chips to track our pets or animals in the wild tags may be a feasible future for humans as well, providing information when needed depending on information supplied and flexibility. The technology for smart cards and Integrated Circuit chips is vast and may continue to advance further down the road of versatility as new applications may arise and give rise to new problems that need to be solved or old problems that are then solvable through the technology that has been worked upon for years.

**Conclusion:**

In conclusion, this report covers the aspects that a Smart card can cover, from financial to personal possibilities. The architecture of these Integrated Circuit chips and how expansive they are and have become over the years, the amount of security protocols and layers that are used to retain safe a secure information. The concepts that were first developed in order to develop a smart card. How power management has become efficient and how it is designed to support such a powerful structure in a small chip.

**References:**

"RF Front End." *Wikipedia*. Wikimedia Foundation. Web. 23 Mar. 2016. <https://en.wikipedia.org/wiki/RF\_front\_end>.

Smart Card Alliance. *What Makes a Smart Card Secure*. New Jersey: 191 Clarksville Rd. Princeton Junction, NJ 08550, Oct. 2008. Pdf.

"Design of 13.56MHz Power Recovery Circuit with Signal Transmission for Contactless Bank IC Card." *IEEE Xplore*. Web. 14 Feb. 2016.

"Efficient Countermeasures against Fault Attacks for 3DES Crypto Engine in Bank IC Card." *IEEE Xplore*. Web. 14 Feb. 2016.

"Smart Card." *Wikipedia*. Wikimedia Foundation. Web. 23 Mar. 2016.

Hermanto, Beni Rio, Tati R. Mengko, Adi Indrayanto, and Taufiqur Rahman. *Application Protocol Data Unit Implementation In E-Health Smart Card For Health and Medical Data Record*. Bandung, Indonesia: Sch. of Electr. Eng. & Informatic, Inst. Teknol. Bandung, Bandung, Indonesia, 7-8 Nov. 2013. Pdf.

**Bibliography:**

"Flip Chip Method in Smart Card/smart Label Packaging." *IEEE Xplore*. Web. 14 Feb. 2016.

"Public Key Infrastructure." *Wikipedia*. Wikimedia Foundation. Web. 23 Mar. 2016.

Cunningham, Ronald F. *Smart Card Applications in Integrated Transit Fare, Parking Fee and Automated Toll Payment Systems the Maps Concept*. Teaneck, NJ, USA: Lockheed Inf. Manage. Services Co., 16-17 June 1993. Pdf.