



“UNIVERSAL” CREDIT CARD

Group 20
October 15, 2002

Faculty Advisor

Bruce McNair
bmcnair@stevens-tech.edu

Group Leader

Samir Shah
sshah7@stevens-tech.edu

Group Member

Nikhil Patel
npatel7@stevens-tech.edu

Group Member

Chintan Doshi
cdoshi@stevens-tech.edu

Group Member

Amzad Malique
amalique@stevens-tech.edu

Group Member

Ishrat Saifullah
isaifull@stevens-tech.edu

“We pledge our honor that we have abided by the Stevens’ Honor System.”

Table of Contents:

Abstract	Page	3
Introduction	Page	4-5
Design Approaches	Page	6-7
Design Requirements	Page	7-11
Financial Budget	Page	12
Project Schedule	Page	13-14
Conclusion	Page	15
References	Page	16

Abstract:

Our group decided to work on an idea that Professor McNair has trademarked called the Universal Credit Card. This credit card will combine all the credit cards that a person might have into one compact unit. This way people will not have to carry around multiple cards. One advantage of the card would be if you lose your wallet, you would usually have to go calling every company canceling each card separately, but with this idea, you only have one phone call to make.

The Universal Credit card would display a liquid crystal display with the bar code instead of the regular magnetic strip on the back. The bar code will be more secure than a magnetic strip because the last 4 digits of the account number will be dynamically changing with time. A pin number will also be stored in the memory of the card (ROM) to further enhance the security.

In our project we have to come up with a pseudorandom code that's going to make the end component of the account number vary with time. For example there has to be a way for the person to select which credit card it is that he wishes to use. Another feature that we are going to try to obtain is to make the card as compact as possible.

With a credit card like this, it's supposed to save space from having a whole bunch of cards, so we would have to make it small but yet have all the functions. It will also have to be secure enough so that you don't have to worry about someone else using your card.

Introduction:

In today's society, the credit card is used by millions of people for everyday transactions such as grocery shopping, gas, ATM's, online shopping. The credit card has a magnetic strip that contains machine-readable data. There is a serious security flaw with the credit card. If the credit card comes into the possession of an individual other than the user, it can be misused since there is no sort of feature within the credit card that will prevent it from being used by authorized individuals.

Bruce McNair is the inventor of the "Universal" Credit Card. Mr. McNair has the following patent explaining the invention using significant detailed technical documentation. The patent # [5,450,491](#) can be found in the *United States Patent and Trademark Office PATENT FULL-TEXT AND IMAGE DATABASE*.

The proposed "Universal" Credit Card that the group plans to design will solve the security flaws that are present in the current credit card. The "Universal" Credit card will not contain a magnetic stripe such as those found on typical credit cards. Instead of the magnetic stripe, the information relevant to the credit card will be coded within a Liquid Crystal Display medium. The card will contain circuitry that will enable the barcode to change according to a time varying algorithm. The time varying code will represent the account number of the credit card and optionally the PIN number and expiration date.

The goal of this project is to develop an authenticator card that includes a liquid crystal display that exhibits a dynamically changing barcode pattern.

The aims of this design project are as follows:

- Address the security flaws that are present in the current credit card system

- Eliminate unauthorized use of stolen or lost credit cards
- Eliminate the duplication of information contained in the magnetic strip found on common credit cards such as VISA, MASTERCARD, AMEX, DISCOVER, etc.
- Eliminate the need to carry around multiple credit cards. All of the different types of credits cards that an individual may carry can be stored via barcodes in the “Universal” Credit Card unit and therefore carry around one card rather than multiple plastic credit cards.
- Implement the new credit card system such that the “Universal” Credit Card can be mass produced at low cost and readily available bar code scanner can be used to authenticate the card and user.

Design Approaches:

As the group approached the Universal Credit Card project, the group realized eventually that there would be many different ways to go through with this project. This applied to both the hardware and software that were going to be involved. It is obvious that our overall goal is to create a “universal” credit card. Issues dealing with various different scenarios were raised during the planning process. Scenarios include: online shopping, when to lock/unlock the card, and how the selection of *which* card to use was to be made (*on* the card itself or on the Point of Sales system). These are the issues we have been dealing with thus far. As our knowledge base grows, I am sure we will be dealing with many more.

When considering a credit card in today’s market, online shopping most definitely has to be considered. If this card were to be changing its TOD (time of day) random number in time, how would one make an online purchase? This is where the issue of the time interval between each random number change came into place. We would have to go online, actually make mock purchases of products, and come up with an average time it takes for a customer to input the credit card information. To ensure the safety of the card for the customer, there would have to be a mechanism to lock/unlock the card. The problem we had to deal with here was *when* exactly the card would lock. Would it lock automatically? Or manually? How would the pin be entered to unlock the card? Would the buttons be *on* the card itself or would it be like a debit card mechanism where one can input the pin by the counter. We are still undecided on this part and will definitely be updated on this as we expand our knowledge base. Finally, the issue of *which* credit card to use when making a purchase has to be tackled. Since this universal credit card

combines all the credit cards into one, how would the customer and/or the clerk choose which credit card to use? The group came up with two options based on this: place the buttons on the card itself OR have the POS System have a popup window on the screen that enables the clerk to choose which card to use. The latter would most definitely be useful in the long run. If the customer decides to add a credit card to his/her universal card, no *hardware/physical* changes would need to be made. Also, this would make it easier for the customer—which is the eventual goal. Further technical detail will be explained once our knowledge base is enhanced.

Design Requirements:

The central focus of the “Universal” Credit Card project is the generation of a time varying code that will convert the digital signals into a dynamically changing bar code.

There are various other elements of the project that will also require knowledge of circuitry, software engineering,

FIG. 1

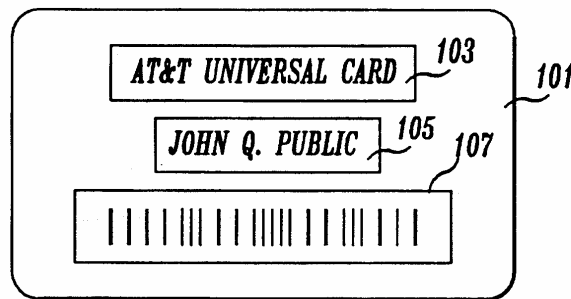


FIG. 1 illustrates the external arrangement of an authenticator card with a liquid crystal display.

This is the proposed layout of the authentication card that will be designed. The owner of the card whose name will appear on the card but neither the account number, expiration date, nor any other sort of information will appear on the card. The name will be printed on the casing of the card. The card will be about ¼ inch thick and approximately the same width and length of a standard credit card. The LCD will be controlled by electronic circuitry powered by solar/battery power. The liquid crystal display will contain the barcode. Information carried by the barcode will be easily decoded using a standard, readily available point of sale barcode scanner.

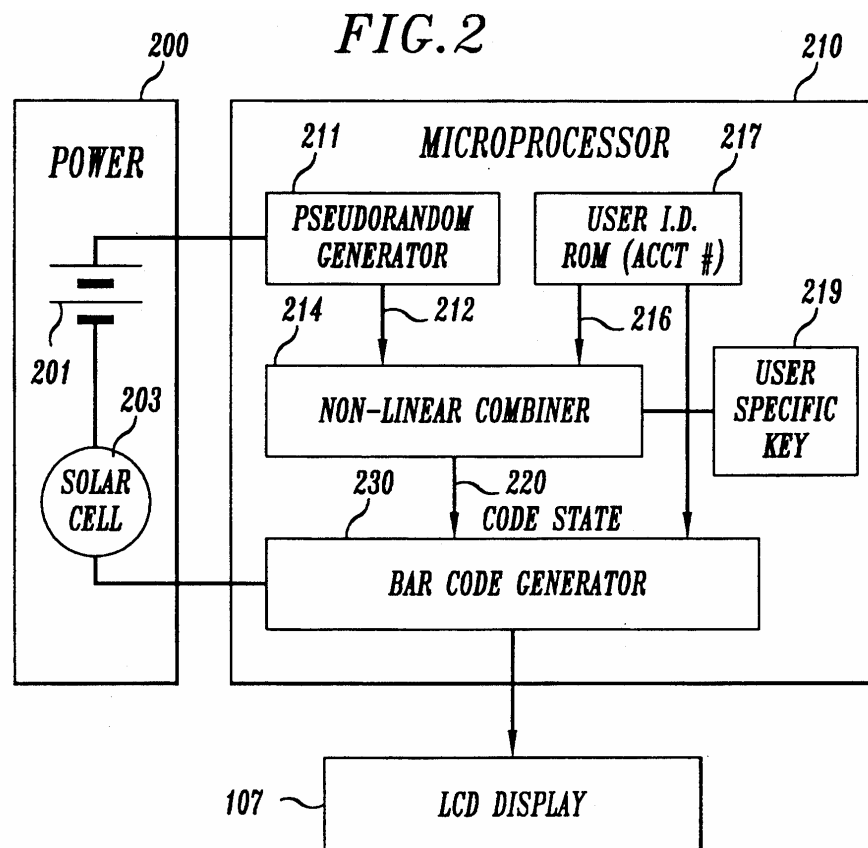


FIG. 2 is a block diagram of the circuitry that will be used to control the LCD

A microprocessor will be used in the circuitry since this will be the source of all functions that this credit card will serve and thus the microprocessor will act as the brain

of the credit card. We plan to code the microprocessor so that part of its function will be the generation of pseudorandom time-varying code that will modify the last 4 digits of a typical 16 digit credit card account number. However, at this time it is not known what microprocessor will be used.

A similar device is required to be available at the verification site in order to communicate the present value of the varying account number. Exactly how this will be implemented will be answered after further research is done and additional group/advisor discussions are held.

A read-only memory device will be used to store the first 12 digits of the account number(s) as well as the users PIN number(s). A non-linear combiner will be used to combine the information from the read only memory and the pseudorandom code generator. A cryptographic algorithm will be implemented in order to generate an authenticator code.

The multi-bit codeword output generated by the cryptographic algorithm will be sent to the barcode generator and this will in turn send the output to the LCD in the authenticator card. The barcode will become visible and is now able to be scanned by a conventional barcode reader.

Other considerations concerning additional features such as initial PIN login to activate card and reprogramming of card will be considered as the project becomes more developed and the knowledge base of the group substantiates.

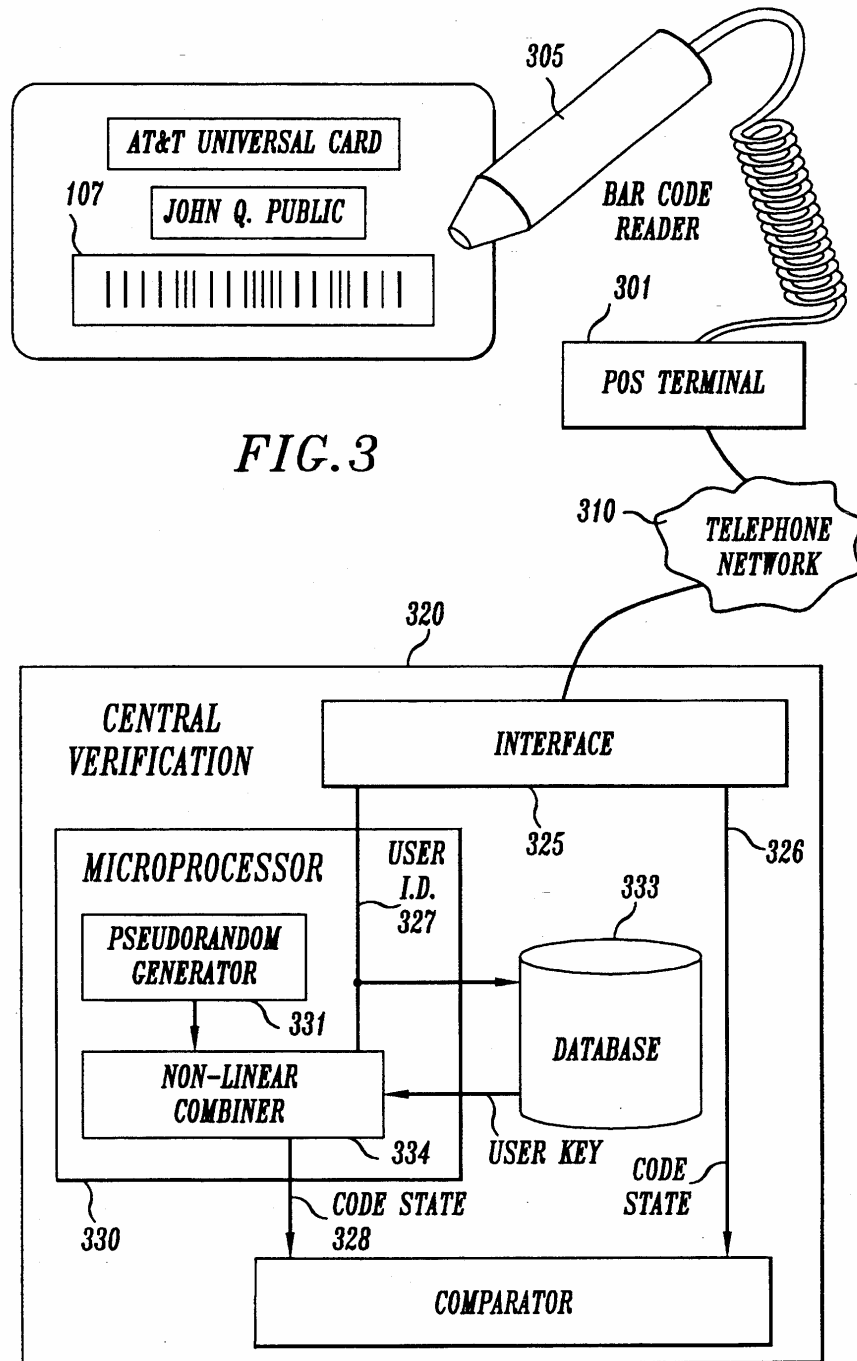


FIG. 3

FIG. 3 is a block diagram of a system using the authenticator card of the present invention in connection with a transaction at a point of sale terminal

The barcode is scanned at the point of sales terminal using a conventional barcode reader. The digital signal received by the scanner is then transferred to the Central

Verification site using a telephone line. The central verification site receives the signal that contains the account number (static and dynamic components) at the time the barcode was scanned, the PIN number and other information about the credit card. These various pieces of information are separated by an interface that is present on the central verification site.

The Central verification site includes a microprocessor, which, like the processor in the credit card, is implemented in an integrated circuit including a microprocessor operating in accordance with microcode in order to provide various functions similar to those performed in the credit card processor. More specifically, the processor at the central verification site includes a pseudorandom code generator that operates in a manner similar to the pseudorandom code generator in the credit card. The same goes for the non-linear combiner. The cryptographic algorithm used in the non linear combiner of the credit card and the non-linear combiner at the central verification site will be identical. The central verification site will query a database in order to determine the authenticity of the credit card.

Each input to the non-linear combiners in the credit card and at the central verification site have to be identical in order for the card to be authenticated. Therefore, it will be a major area of research to determine how to successfully synchronize these devices.

If the authenticator card is valid, the POS terminal is signaled, so that the transaction may proceed. Otherwise, the transaction may be halted, or the authentication retried in the case of transient errors.

Financial Budget:

Following is a draft of our budget, which outlines the most significant items of the project. This is by no means the final draft and more items and the costs will be added under all categories when we actually start the designing and implementation process.

Description of Item	Cost
Hardware	
Authenticator Card System	
Electronic circuit components	\$0.99-\$1.59
LCD	\$19.99
Bar code scanner	\$325
Plastic card body	\$20
Power module	\$1.59-\$9.99
Solar cell	\$50
Microprocessor	\$200
Software	
POS software	\$726
Software applications for Server	\$450
Other Items	
Reference books (for code writing)	\$200
Accessories:	
Key-button	\$0.99

Conclusion:

This proposal states how we are going to implement the authenticator card system into practice to function with direct implications for real-world transactions. Within the cost constraints and scope of present credit cards, such a system can be implemented by designing the interface between a bar code reader and a verification processor. The aim of this project is to create the “universal” credit card for the benefit of the general public and to further technology research in the credit card authentication process. The project also focuses on the need for understanding of third generation infrastructure and microcontroller architecture, which can be useful to people and also made use of as a test-bed in enhancing authenticator card applications. The eventual outcome that we expect out of this project will provide the convenience of one authenticator/identification card that will package many cards into one as well as have the added benefit of a higher security level. Also, added features like a card locking/unlocking system and an options key can be implemented.

From an engineering standpoint, once the infrastructure has been created, we intend to run several phases of test that will determine the practicality and usability of the “universal” credit card (e.g.: security tests.). This is a continuous process. It is anticipated that some problems may exhibit sensitivities to the infrastructure choices. Therefore current work is being conducted to explore the implications of various technologies that are available to us.

References:

**United States Patent
McNair**

**5,450,491
September 12, 1995**

"The 60 Second Password, Secure Computer Access; Security Dynamics"; 15 Dwight St, Boston, Mass., 1 page; 1984.

S. M. Matyas and C. H. Meyer "Cryptography: a New Dimension in Computer Data Security; a Guide for the Design and Implementation", Wiley, 1982, Table of Contents attached--also Chapter Three `The Data Encryption Standard` pp. 113-191.

J. Millman and H. Taub "Pulse and Digital Circuits", McGraw-Hill Book Company, Inc., 1956--Table of Contents attached--also Chapter 13-10 Registers, pp. 411-412.