Review Article

REVIEW OF FINANCIAL CRYPTOGRAPHY

Rani Srivastava

Address for Correspondence

Allen House Institute of Technology, Rooma, Kanpur

ABSTRACT

In this paper we propose a financial cryptography as a subset of financial transaction which plays a crucial role in business for privacy and trust management. Trapped between essential banking and cryptography or linking accountant and programmer, there is a serious threat that would result to create Financial Cryptography systems will make simpler or exclude significant disciplines. Financial cryptography is a composite expression for finance and cryptography which funds the use of cryptographic techniques to defend finance related data's. An anonymous communication is required for financial transaction. The primary use of cryptography for this is to assure privacy and allow anonymous electronic cash. For this, we believe that strong cryptography is legal and readily available. Still in that event, we state that strong cryptography will be used to maintain anonymity only in an extremely restricted subset of financial transactions. In this paper we propose some of the security flaws which are present in internet related business and in 7 layer financial cryptography model. We also explore the some of the properties of transaction system like anonymity, trust, reversibility of original entities, authentication and authorization related issues and how to maintain these properties in scenario of real time system transaction. Finally we will try to provide some practical solutions for a more secure financial cryptography model.

KEYWORDS: Secure electronic transactions, dual signature, cryptography, e-finance

1. INTRODUCTION

There has never been a more challenging time than now for corporate finance organizations in public and private sector companies.

- Faster and more accurate financial transaction processing
- Real time analysis of key performance indicators
- Proactive and strategic planning process that helps business managers
- Quick and accurate external reporting
- Ensuring compliance and control
- Effective risk management

Above are real demands placed on the corporate finance organization It seems that everything now has an "e" in front of it. Finance, like any other function, is subject to profound changes because of e-commerce, **Electronic commerce**, commonly known as (electronic marketing) **e-commerce** or **eCommerce**, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks[1]. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. The use of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at some point in the transaction's lifecycle E-finance is defined as "The provision of financial services and markets using electronic communication and computation. Cryptography is the practice and study of hiding information. In today's environment, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.

Cryptography is used in technologically advanced applications, including areas such as the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography.

Financial cryptography (FC) is the use of cryptography in applications in which financial loss could result [2].Anonymity is derived from the Greek word ανωνυμία, meaning "without a name" or "namelessness". In colloquial use, anonymous typically refers to a person, and often means that the personal identity, or personally identifiable information of that person is not known.[3] More strictly, and in reference to an arbitrary element (e.g. a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous". The term "anonymous message" typically refers to message (which is, for example, transmitted over some form of a network) that does not carry any information about its sender and its intended recipient. It is therefore unclear if multiple such messages have been sent by the same sender or if they have the same intended recipient.

Sometimes it is desired that a person can establish a long-term relationship (such as a reputation) with some other entity, without his/her personal identity being disclosed to that entity. In this case, it may be us pseudonym, with the other entity. Examples of pseudonyms are nicknames, credit card numbers, student numbers, bank account numbers, and IP addresses. A pseudonym enable useful for the person to establish a unique identifier, called other entity to link different messages from the same person and, thereby, the maintenance of a long-term relationship. lt from subversion of the message system.[4].

2. CRYPTOGRAPHY

Cryptography is the science of information security. The word is derived from the Greek *krypto* meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

2.1 Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2.2 Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

2.3 Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

2.4Authentication (the sender and receiver can confirm each others identity and the origin/destination of the information)

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering

3. SECURE ELECTRONIC TRANSACTION (SET)

Secure Electronic Transaction **(SET)** is an open encryption and security specification designed to protect credit card transactions on the Internet. The current version, SETv1, emerged from a call for security standards by MasterCard and Visa in February 1996. A wide range of companies were involved in developing the initial specification, including IBM, Microsoft, Netscape, RSA, Terisa, and Verisign. Since 1996 there have been numerous tests of the concept; by 1998, the first wave of SET-compliant products was available. SET is not itself a payment system. Rather, it's a set of security protocols and formats enabling users to employ the existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion. In essence, SET consists of three services:

- Providing a secure communications channel among all parties involved in a transaction.
- Providing trust by the use of X.509v3 digital certificates.
- Ensuring privacy because the information is only available to parties in a transaction when and where necessary.

Secure Electronic Transaction (SET) was a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. SET was not itself a payment system, but rather a set of security protocols and formats that enable users to employ the existing credit card payment infrastructure on an open network in a secure fashion. However, it fail SET allowed parties to cryptographically identify themselves to each other and exchange information securely. SET used a blinding algorithm that, in effect, would have let merchants substitute a certificate for a user's credit-card number. If SET were used, the merchant itself would never have had to know the credit-card numbers being sent from the buyer, which would have provided verified good payment but protected customers and credit companies from fraud.

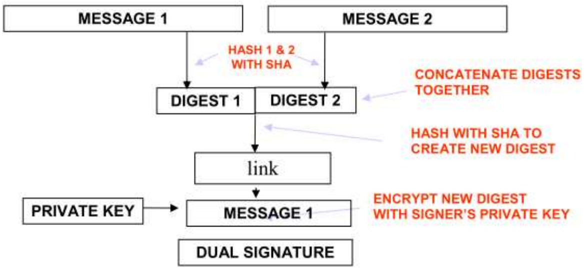

MESSAGE 1
MESSAGE 2
HASH 1 & 2 WITH SHA
CONCATENATE DIGESTS TOGETHER
DIGEST 1
DIGEST 2
HASH WITH SHA TO CREATE NEW DIGEST
link
PRIVATE KEY
MESSAGE 1
ENCRYPT NEW DIGEST WITH SIGNER'S PRIVATE KEY
DUAL SIGNATURE

Figure 1: Dual Signature in SET

An important innovation introduced in SET is the dual signature. The purpose of the dual signature is the same as the standard electronic signature: to guarantee the authentication and integrity of data. It links two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order. The link is needed so that the customer can prove that the payment is intended for this order.

The message digest (MD) of the OI and the PI are independently calculated by the customer. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual signature is sent to both the merchant and the bank. The protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not reveal the content of the OI or PI, and thus privacy is preserved.

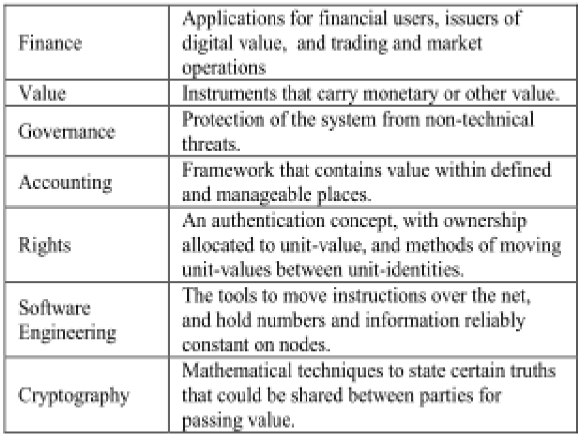
4. FINANCIAL CRYPTOGRAPHY

Financial cryptography (FC) is the use of **cryptography** in applications in which financial loss could result. Financial cryptography uses micropayment scheme like e-coupons [6] and micro word. ROADS [7][8][9] act as the trusted third party to achieve functional anonymity.Central Financial Cryptography is substantially complex [10]. For a field that is nominally only half a decade old, by some viewpoints, it is apparent from the implementation work that has been done that many more aspects were involved than envisaged by early pioneers. Financial Cryptography appears to be a science, or perhaps an art, that sits at the intersection of many previously unrelated disciplines[11]:

1. Accountancy and Auditing
2. Programming
3. Systems Architecture
4. Cryptography
5. Economics
6. Internet
7. Security
8. Finance and Banking
   - Risk
   - Marketing and Distribution
   - Central banking

At such a busy juncture of so many distinctive bases of knowledge, problems are bound to arise. Not only the inevitable confusion and wasted resources, but the difficulty in acquiring technical, management and marketing talent that can comfortably work in the field is an issue.

As a preliminary step to the better understanding of Financial Cryptography projects, it is often of some interest to structure these disciplines into models that aid dialogue, comparisons and decision making.



Finance	Applications for financial users, issuers of digital value, and trading and market operations
Value	Instruments that carry monetary or other value.
Governance	Protection of the system from non-technical threats.
Accounting	Framework that contains value within defined and manageable places.
Rights	An authentication concept, with ownership allocated to unit-value, and methods of moving unit-values between unit-identities.
Software Engineering	The tools to move instructions over the net, and hold numbers and information reliably constant on nodes.
Cryptography	Mathematical techniques to state certain truths that could be shared between parties for passing value.

Figure 2 Financial Cryptography in 7 layers

This paper presents one such model that attempts to describe the field in an introductory manner, as a preamble to greater learning. In this model, the terms Finance and Cryptography are stretched out in order to reveal the disciplines that might have been hidden within the name.

Of course, no one model can plausibly cover the depth and breadth of a complex subject. The intent of this present model is to allow the reader to conceptualize the entire field, identifying the relationships of the disciplines, without spending too much time on the detailed nature of each component. Depth is sacrificed for breadth

This introduces a 7 layer model, akin to the Open Systems Interconnect Reference Model of networking fame, as shown in Figure2.[12] [13]. In this model, Finance and Cryptography are stretched out, revealing five more areas of interest

5. ANONYMITY

Anonymity is the state of being not identifiable within a set of subjects with the technique of the anonymity; the users are able to hide their private information from the anonymity set. Two main aspect of anonymity are management of certificate and other is the two basic ideas on anonymity.

a. DC nets

b. Mix nets

The essential component of PKI is the CA (Certificate Authorities). CA always coordinates with RA (Register Authority), which is the supplement of CA in charge of verifying the reality of the entry by the social information such as the ID card. The certificate authority is in charge of the operation on the certificate such as generating, publicizing, revocation, etc. With in the public key certificate, there is information of the user’s identity and the corresponding public key. The digital signature of the authoritative third party guarantees the validation of such information .DC-Nets were first proposed by Chaum in [14] in 1988, and it featured that the receivers in the broadcast group can compute the content of the data while can not identify the sender of the data, which made this protocol one of the few that can provide the provable security. However, the DC-Nets protocol is of great limitation as well as its distinguishing advantage. Two main limitations of DC-Nets are channel collision and poor scalability. informatiMix-Nets were first introduced by Chaum in 1981.

The main idea of Mix is that the “mix” nodes reroute and shuffle the data so as to eliminate the relationship between the sender and the receiver.

It is an effective way to provide anonymity, and Chaum has proved the security of Mix against a completely passive adversary in [15]. However, the Mix mechanism is somewhat vulnerable to active adversary.

There are actually two types of anonymity: true and pseudo-anonymity

a. True anonymity

This kind of anonymity is untraceable. Indeed, only coincidence or purposeful self-exposure will bring the identity of the mystery sender to others; the identity of a person acting in a truly anonymous manner can not be definitively discovered through any amount of diligence.

b. Pseudo anonymity

Sometimes it is desired that a person can establish a long-term relationship (such as a reputation) with some other entity, without his/her personal identity being disclosed to that entity. In this case, it may be useful for the person to establish a unique identifier, called a pseudonym, with the other entity. Examples of pseudonyms are nicknames, credit card numbers, student numbers, bank account numbers, and IP addresses. A pseudonym enables the other entity to link different messages from the same person and, thereby, the maintenance of a long-term relationship. Although typically pseudonyms do not contain personally identifying information, communication that is based on pseudonyms is often not classified as "anonymous", but as "pseudonymous

6. CONCLUSION

In conclusion, I would like to reiterate a point I made earlier: that the migration of services to the internet world is infeasible without the provision of anonymizers to guarantee anonymity .Strength of the system to protect the system depends upon mixes so key escrow is major problem.

Any micro payment scheme like payword which is credit based, offline micro payment scheme that uses chain of paywords (one way hash value representing primitive monetary units) e-coupons, smart card, micromint uses cryptography in doing e-business.

If we use k-anonymity in financial cryptography with DC Nets and Mix Nets technique then we get more scalable, secure and collision free network.

REFERENCES

1. Gold served especially commonly as a form of early money, as described in " Origins of Money and of Banking" Davies, Glyn (2002). Ideas : A history of money from ancient times to the present day. University of Wales Press. ISBN 0-7083-1717-0.
2. http://en.wikipedia.org/wiki/Financial_cryptography
3. Donors Increasingly Make Their Big Gifts Anonymously, Chronicle Analysis Finds By Sam Kean (January 09, 2008) The Chronicle of Philanthropy
4. Anonymity on the Internet By Jacob Palme and Mikael Berglund - Jacob Palme- Home Page
5. "SSL protocol architecture"by Cisco Active Network Abstraction BQL User's Guide
6. "An Efficient, Secure and Delegable Micro-Payment System"by Vishwas Patil, and R.K. Shyamasundar, *Fellow, IEE* School of Technology andComputer Science Tata Institute of Fundamental Research.
7. Ronald Rivest, Carl Ellison et.al. (2001): "Certificate Chain Discovery in SPKI/SDSI"
8. D. Ferraiolo, Ravi Sandhu et.al. (2000): "A Proposed Standard for Role- Based Access Control", National Institute of Standards and Technology.
9. Matt Blaze, Feigenbaum, Ioannidis, Keromytis (1999): "The KeyNote Trust-Management System", Version 2
10. The term Financial Cryptography was invented by Robert Hettinga as a name for a conference held annually in Anguilla.
11. Ian Gregg, *Virtual Finance Report,* Digital Trading, November 1997 *RFC 2704. Computer Security*
12. Search on Google for ISO OSI Reference Model Seven Layer
13. It is mostly coincidence that there are 7 layers, and it may change if we find compelling reasons to add or subtract layers , 9(4):285-322.h
14. D. Chaum. "The Dining Cryptographers Problem: Unconditional Sender and Recipient untraceability", Journal of Cryptology, 1988, pp
15. D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, 1981, 24(2),pp. 84-88.. 65-75.