FAIL-STOP SIGNATURE SCHEME FOR DIGITAL PAYMENT

Gopi Dinakaran

Department of Computer Science

The University of Auckland

2003

gdin007@ec.auckland.ac.nz

Lecturers: Prof Clark Thomborson and Prof Jim Goodman

Abstract. *Digital signature is one of the most important authentication techniques which could be used for any on-line transactions include Digital payment scheme, On-line shopping, E-government or whatever comes under electronic commerce. This paper focuses on using* ***FAIL-STOP Signature Scheme*** *which is considered as one of the most secure schemes among various digital signature schemes for* ***Digital payment scheme****. This paper discusses the advantages and disadvantages of using Fail-stop Signature Scheme for Digital payment scheme by the banks instead of using Ordinary security with Dual security scheme for Digital payment.*

1 Introduction

Digital signature is one of the best techniques used for on-line transactions to ensure the identification, authentication and non-repudiation [4] of the user. On-line transactions include Digital payment schemes between the banks and the people, On-line shopping between the vendors and the consumers, E-government services between the government and the people seeking the services [2] and whatever comes under electronic commerce. Digital signatures are not a digitalized version of handwritten signatures but they are specially developed classes of mathematical functions [3]. They guarantee the authenticity of a message to its recipient, and the recipient can prove the authenticity of

signer to third parties, such as courts when any disputes occur in future. This paper discusses about the **Fail-stop Signature scheme (FSS)** which is considered as one of the best schemes among the digital signature schemes. This paper also considers the advantages and disadvantages of using FSS scheme for Digital payment scheme instead of using Ordinary security with Dual security signature scheme. Organization of this paper: section 2 describes various terminologies which are used in this paper for effective understanding, section 3 describes the function of FSS and the property of FSS, section 4 describes the Digital payment scheme and discusses the advantages and disadvantages of using Ordinary security with dual security scheme for the digital payment scheme, section 5 discusses the advantages and disadvantages of using FSS instead of Ordinary security with Dual security scheme for the digital payment, section 6 concludes the whole paper and section 7 recommends some of the applications in my point of view.

2 Terminology

I would like to explain some of the terms used in this paper in this section.

2.1 Asymmetric cryptosystem

"A system which generates and employs a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify a digital signature" in [1] is known as asymmetric cryptosystem.

2.2 Authentication

"A process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that it has not been modified or replaced in transit" in [1] is known as authentication.

2.3 Key pair

"In an asymmetric cryptosystem, a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates" in [1] is called a key pair.

2.4 Private key and Public key

"The key of a key pair used to create a digital signature" in [1] is known as private key and "the key of a key pair used to verify digital signature" in [1] is known as a public key.

2.5 Nonrepudiation

"Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents" in [1] is known as nonrepudiation.

3 Introduction of Fail-stop Signature Scheme

In Ordinary digital signature scheme, if the cryptologic assumption is broken, the signature of the signer can be forged by an attacker and it is impossible to detect where the forging is happened [3]. This could be avoided by using Fail-stop Signature Scheme (FSS)

.

3.1 How does FSS work?

The structure of FSS contains all the components in Ordinary security signature scheme with two new components [3]:

(a) An algorithm to produce a proof of forgery from a forger signature and the secret key. This can be used by the signer to prove to the third party such as court that the cryptologic assumption has been broken, if any disputes arise after authentication transaction.

(b) Another algorithm which can be used by all of the remaining participants of the transactions to verify if something is really a proof of forgery.

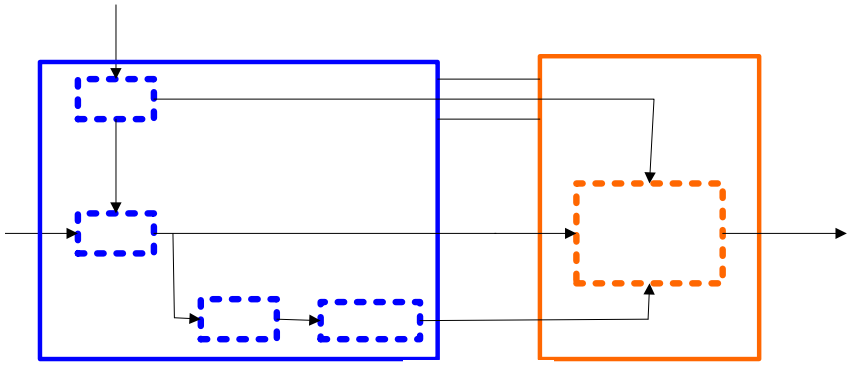


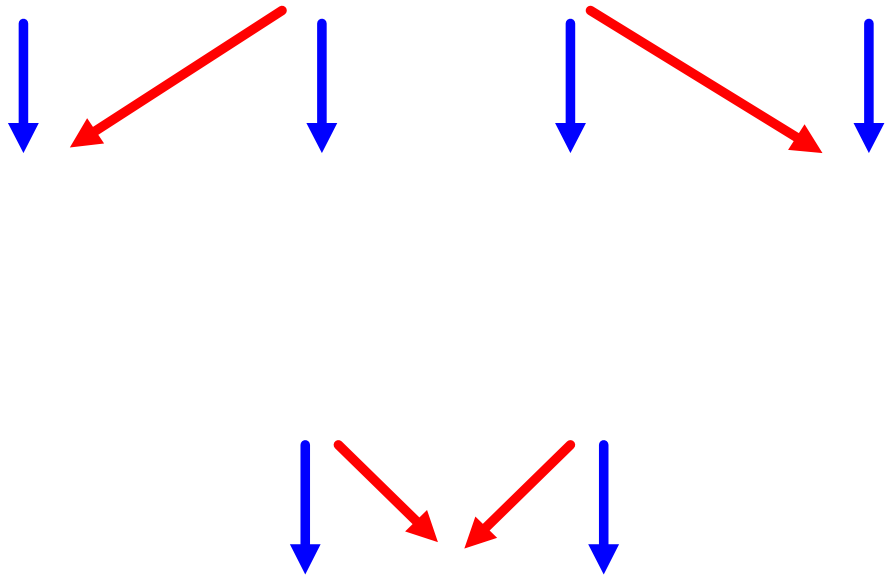
Figure 1. Components and working of FSS

From the figure 1, we can find four different algorithms in the signer's device namely **gen** [3] to generate the key pair, **sign** [3] to generate the signature, **proof** to generate the proof of forgery when forgery takes place, **alg_forg** to generate the algorithm to verify the proof of forgery and in the recipient's device, **test** [3] is used to test the authentication of the signer with the details sent by the signer. The Boolean acceptance value **acc** indicates the authentication of the signer.

3.2 Fail-stop property

I would like to discuss the Fail-stop property [3] by comparing Ordinary security and Dual security with Fail-stop security considering two cases such as normal case and extreme case.

Let us consider the third party as court which is responsible to solve the dispute arising by the recipient or the signer after the transaction. Figure 2 [3], Figure 3 [3] and Figure 4 [3] depict the result of the court for the Dual security, the Ordinary security and the Fail-stop Security respectively.



From the figure, the Boolean value **acc** [3] is the result of the court. Blue arrows denote the output of the normal situation and the red arrows denote the output of the extreme situation. In Dual signature scheme, acc may be FALSE in extreme conditions which shows that the signer's security is guaranteed on disputes but not the recipient's. In ordinary security, acc may be TRUE in extreme conditions which show that the recipient's security is guaranteed on disputes but not the signer's. These wrong conclusions can be avoided in fail-stop security by introducing new Boolean value 'broken' [3] which indicates when and where the cryptologic assumption has been broken since the value of acc sets as soon as the assumption has got broken. Considering these properties, I would like to discuss some of the advantages and the disadvantages of using Fail-stop signature scheme instead of using Ordinary security with Dual security scheme for Digital payment scheme in the rest of this paper.

Figu

4 Digital payment scheme using Ordinary security with Dual security Scheme

Digital payment is the process of exchanging funds or some other financial related transactions between banks and individuals or within individuals electronically.

Ordinary security with Dual security scheme is used for the existing digital payment scheme [3]. Figure 5 and figure 6 depict the function of digital payment scheme using ordinary security with Dual security scheme in normal situation and in extreme situation respectively. I would like to discuss both the disadvantages and advantages of using this scheme in the following sections.

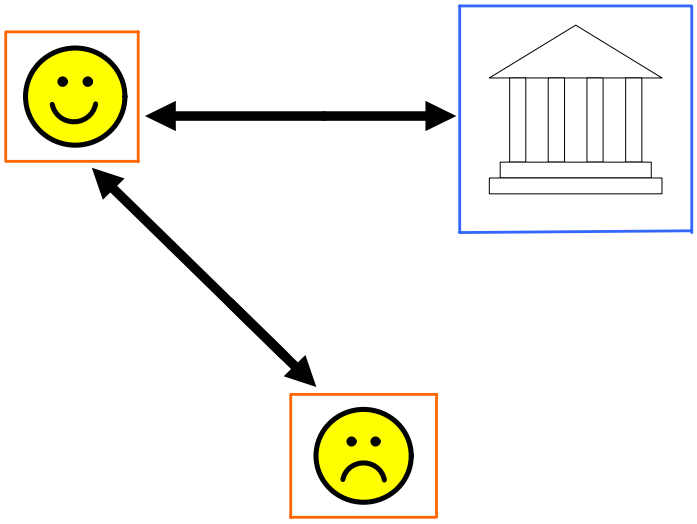


Figure 5. Function of Digital payment scheme using Ordinary security with Dual security in Normal situation.

In the figure 5, smiley face denotes the better security in the transaction between the bank and an individual and the frowning face denotes the poor security in the transaction between the individuals. In the figure 6, two frowning faces denote the poor security in both the transactions between an individual and the bank and within the individuals.

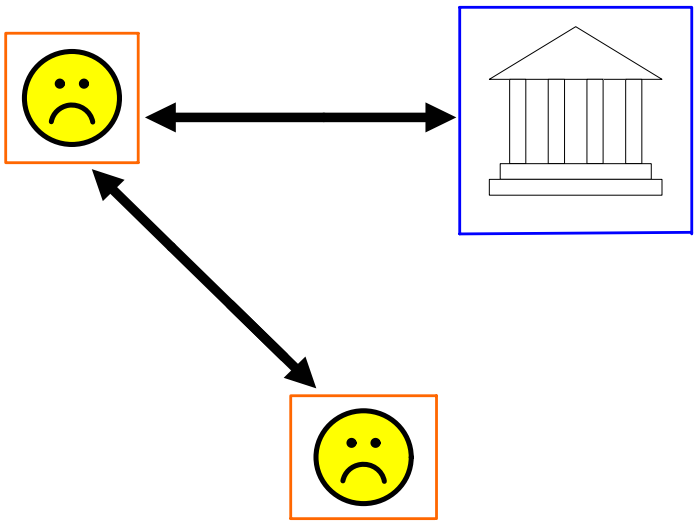


Figure 6. Function of Digital payment scheme using Ordinary security with Dual security in Extreme situation.

4.1 Disadvantages of using Ordinary security with Dual security scheme

(i) Since Dual security scheme is used by the bank and Ordinary security scheme is used by the individuals for digital message exchange, Asymmetric [3] approach is handled in this model. Though the asymmetric cryptography ensures a high level of security, it is not feasible to maintain two different schemes practically.

(ii) As two different schemes of two different properties are used, this digital payment scheme is giving more security to the transactions between the bank and the individuals than the transactions within the individuals. Dual signature scheme guarantees the signer requirement on disputes [3] and Ordinary signature scheme guarantees the recipient on disputes [3]. The individual whose security is by ordinary signature scheme is the sufferer on most of the disputes and hence the weak requirement of the individual on dispute is maintained in this scheme.

Ordinary s
scheme fo
message ex

(iii) Dual security scheme helps the bank to prove that the customers are cheated, when a forgery takes place. But this scheme can not find where and when the error was occurred. Moreover the occurrence of forgery can be revealed only after it was happened in the dual security scheme.

4.2 Advantage of using Ordinary security with Dual security scheme

In my opinion, as the high level security is maintained by the bank, the users might trust the bank and have any sort of risky transactions comfortably until a dispute arises.

5 Digital payment scheme using Fail-stop Signature Scheme (FSS)

Digital payment scheme using FSS uses Fail-stop signature scheme on both the individual side and the bank side.

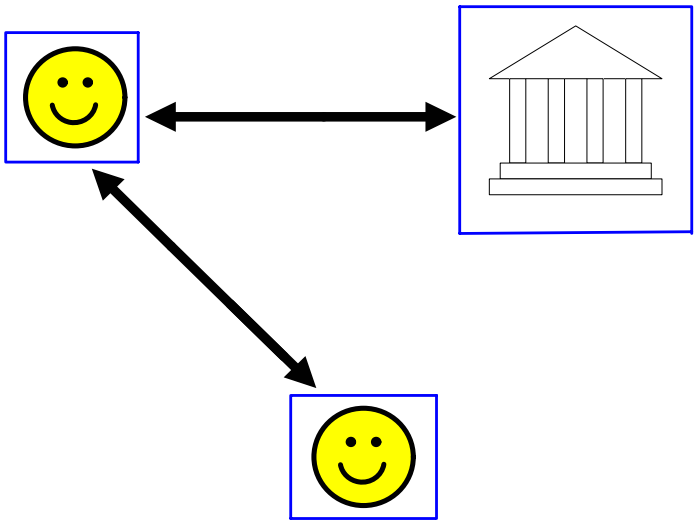


Figure 7. Function of Digital payment scheme using Fail-stop security in both the Normal and Extreme situations.

Figure 7 depicts the function of digital payment scheme using FSS. As the property of FSS is discussed in the section 3.2, the introduction of new Boolean value ‘broken’ helps to find the breakage of cryptologic assumptions during transactions. As soon as the forgery is detected, the transaction will be stopped. Thus both the individuals and the bank are secure enough to have some risky transactions too. I would like to discuss some of the advantages and disadvantages of using FSS for digital payment scheme in the sections 5.1 and 5.2 respectively.

5.1 Advantages of using FSS

(i) If the cryptologic assumption is broken, not only the sender and recipient know the occurrence of forgery but also everybody (such as court) who has taken part in the transactions will come to know about the forgery. And this let the users know who the cheaters of the particular forgery are and everybody could understand that it is the common disaster of the transaction.

(ii) This scheme is information-theoretically [3] secure. Thus the individuals can exchange the authenticated messages with each other securely.

(iii) Algorithm for generating the proof of forgery is the one which is used to construct the proof of forgery as soon as the forgery is occurred. This proof is useful for solving any disputes arise after the transaction. Nonrepudiation is maintained by the generation of proof of forgery.

(iv) The transaction will get stopped as soon as the cryptologic assumption is broken. It helps to stop the future transactions and avoids further damage on both the sender and the recipient sides.

(v) As any forgeries [3] can be recognized during transactions, the FSS would be legally acceptable for checking the authentication of any particular individual or any authenticated transactions between the bank and the individuals.

5.2 Disadvantages of using FSS

(i) Though FSS is considered as one of the highly secure signature schemes, some of the financial institutions such as insurance agencies seek handwritten signatures again to authenticate the concerned policy holder while dealing with higher insurance premiums. People may get annoyed using two different methods to authenticate themselves and they may lose their confidence on using FSS.

(ii) On the other hand, the continuous usage of FSS and its legal acceptance let people feel comfort with FSS psychologically. Then, people might be doing high risk transactions carelessly.

6 Conclusion

On my opinion, the Fail-stop Signature Scheme provides better security to the digital payment scheme than the ordinary security with dual security signature scheme. I have evaluated this by discussing the working of FSS, property of FSS compared with other schemes and some of the advantages and disadvantages of using both the Fail-stop signature and ordinary security with dual security schemes for the digital payment scheme.

7 Recommendation

In my point of view, I would appreciate using Fail-stop signature scheme for the digital payment scheme instead of using existing ordinary security with Dual security scheme despite the limited disadvantages of FSS. I would also like to suggest that the proposal of electronic government [2] which offers various services to the people seeking government services by New Zealand government can also be implemented using Fail-stop signature scheme. We can not expect all the services providing by the e-government be done by using FSS but the services with the considerable risk level can be implemented using FSS.

Acknowledgements

I would like to thank my lecturers Prof Clark Thomborson and Prof Jim Goodman for their valuable comments on the focus of this technical paper and Birgit Pfitzmann whose book in [3] helped me lot to know about the Fail-stop security.

"Learn as much by writing as by reading"
- Lord Acton

References

1. Information Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology, American Bar Association, "Digital signature guidelines : legal infrastructure for certification authorities and electronic commerce," : American Bar Association 1995, 1996. ISBN 1-57073-250-7
2. T Mallard, "E-Government: Authentication of Identity," State Services Commission, New Zealand Government, 16 April 2002. Available: http://www.e-government.govt.nz/authentication/cabinet-paper-2002-04-22.pdf, March 2003. (See also "Government plan 'resembles ID cards', NZ Herald, 7 March 2003. Available: http://www.nzherald.co.nz/storydisplay.cfm?storyID=3199555&thesection=technology&thesubsection=general, March 2003. The State Services Commission is currently consulting with professional groups in New Zealand regarding this online-authentication project; your instructors will be consulted on 1 April 2003.)
3. B. Pfitzmann, "Digital Signature Schemes-General Framework and Fail-Stop Signatures," in Lecture notes in Computer Science 1100, Springer-Verlag, 1996. ISBN 3-540-61517-2
4. C. Spyrelli, "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication," in *The Journal of Information, Law and Technology (JILT)* 2002(2) <http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html>