An Efficient Identification Protocol for Electronic Payment Systems

Ottó Poszet, Stefan Vári-Kakas

Department of Computer Science, University of Oradea
5 Universităţii Street, 410087 Oradea, Romania
e-mail: {poszet, vari}@uoradea.ro

Abstract: In this paper we propose a new mutual identification scheme to be used in Electronic Payment Systems, which implements an enhanced McEliece signature. Based on the framework of a three-step identification protocol, we'd like to obtain increasing security and fault tolerance, maintaining a low amount of execution time.

Keywords: Electronic Payment System, identification protocol, three-step protocol, McEliece signature, Reed-Solomon code

1 Introduction

The Electronic Payment Systems are growing in importance with the rapid spread of e-commerce. The comfortable use of these systems raise a lot of technical problems, like the need of a secure and reliable communication between participant entities. These problems appear more seriously in the case of wireless networks because of the unstable and interceptable connection.

The first aspect in assurance of the security is a secure mutual identification before any kind of transaction. The identification protocols are based on the idea challenge – response: if an entity A would like to ensure about the real identity of the entity B, then A will generate a random number named *challenge*. A will ask B to make a well known computation based on this challenge and based on a secret information that only the real B knows (for example the secret key of B). If the computed answer (*response*) is identical with the expected response computed by A, then B has successfully convinced A about his real identity.

The basic identification protocol is the *three-step identification protocol* (Figure 1), which offers a theoretical frame for further enhancements [1, 2]. The three-step

This research was supported by grant nr.7, code CNCSIS 260, of the Romanian Ministry of Education and Research.

identification protocol is a verification of knowledge based identification protocol. The interactions between *prover* and *verifier* are executed in three steps and the protocol uses the secret key of the prover, which can identify in a unique way the prover. For the implementation of the protocol, two Abelian groups are used: $(G, +, 0)$ and $(J, \cdot, 1)$ and a homomorphism f: $G \rightarrow J$:

$$\forall x, y \in G, f(x+y) = f(x) \cdot f(y) \quad (1)$$

The prover must convince the verifier that he knows the secret key $x \in G$, so that $h = f(x)$, where $h \in J$ is the corresponding public key, well known even by the prover and the verifier too.

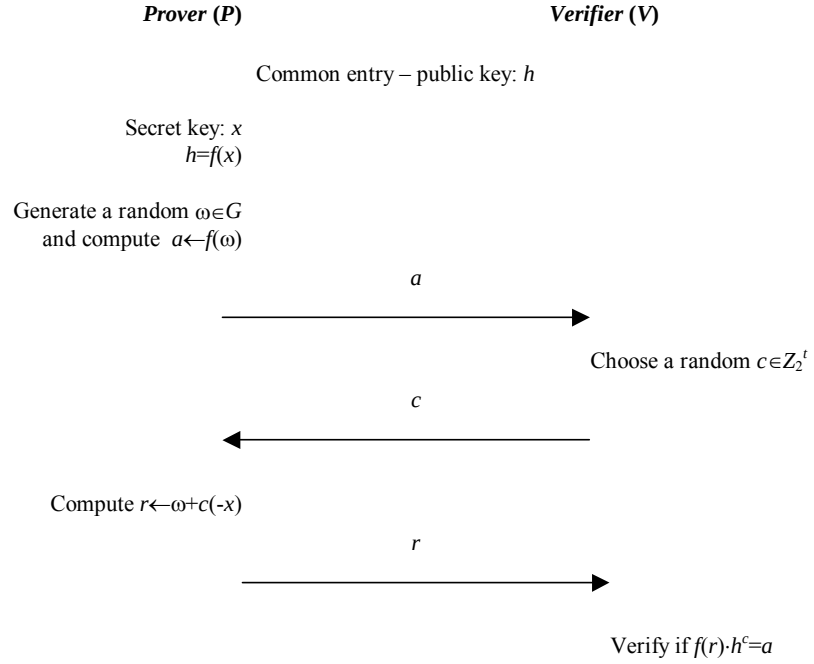

Figure 1
The three-step identification protocol

This basic protocol accepts different implementations. The best-known implementation is the *Schnorr protocol*, which uses the RSA encryption method and reduces the number of messages from 3 to 1 [3]. To obtain the Schnorr identification protocol from the three-step identification protocol, the Abelian group $(G, +, 0)$ will be replaced with the group $(Z_q, + \pmod q, 0)$ and the group $(J, \cdot, 1)$ with the Abelian group $(G_q, \cdot \pmod q, 1)$. The homomorphism will be the one way function $f_{p,q,g}$: $Z_q \rightarrow G_q$, $f_{p,q,g}(x) = g^x \bmod p$. The parameters p, q, g, must satisfy the special discrete logarithm problem specifications. With these modifications the

three-step identification protocol is transformed in the Schnorr identification scheme. This protocol has powerful security properties, but it doesn't provide any fault tolerant capabilities.

In this paper we propose a new secure and fault tolerant protocol, with reduced execution speed. We investigate the execution time of this protocol compared to the above-mentioned protocols.

2 The Proposed Protocol

The basic idea for the development of a new, fault tolerant identification protocol is the common use of the same error correcting code for security and fault tolerance. Such a method was proposed by McEliece, who has elaborated a public key cryptosystem based on Goppa codes [4]. The high security of this system is given by the deliberate injection of random errors during the encoding of a message, which are corrected by the decoding algorithm. We make use of this theory by implementing a similar scheme for our purposes in the identification problem.

We propose a modification of the original three-step protocol using an enhancement of McEliece signature for the purpose of a systematic design. (We have proposed also a modified version of the Schnorr protocol in [5].) The enhancement consists of the use of Reed-Solomon error correcting codes instead of Goppa codes, the design methodology being described in [6]. The modified three-step identification protocol is presented in figure 2. P_{MEV} and P_{MEP} are the verifier and prover McEliece public keys; S_{MEV} and S_{MEP} are the verifier and the prover McEliece secret keys. The encoding of a message *m* follows the equation

$$P_{ME}(m) = E\, m + z, \tag{2}$$

where

$$E = S\, G\, P \tag{3}$$

is the encryption matrix. *G* is the generator matrix of the Reed-Solomon code, *P* is a randomly generated permutation matrix, and *S* is a randomly generated non-singular matrix. The random error pattern, denoted by z, must satisfy

$$\omega(z) < \frac{d-1}{2}, \tag{4}$$

where $\omega(z)$ is the Hamming weight of *z*, and *d* is the Hamming distance of the used Reed-Solomon code.

This protocol is complete, witness hiding and zero knowledge in the sense of [7].

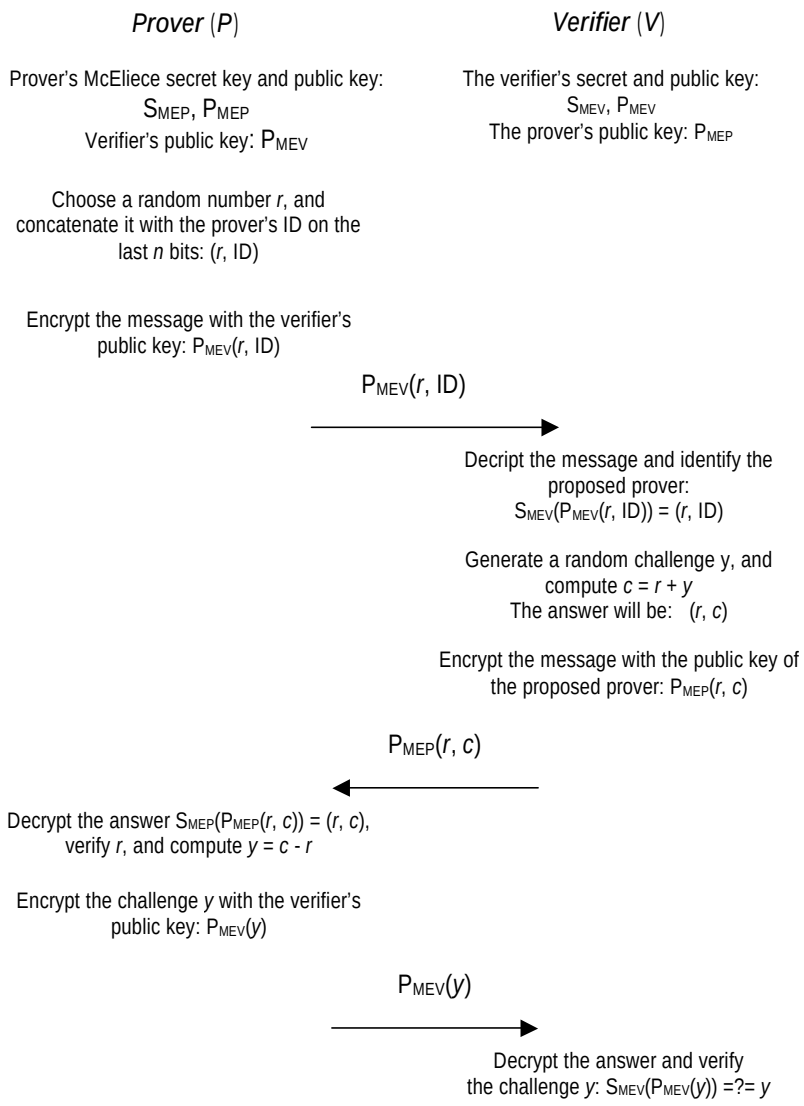

Figure 2

The proposed mutual identification protocol based on enhanced McEliece signature

The security of our protocol is based on the security of the three-step identification protocol, but is further enhanced by use of McEliece cryptosystem in the encoding of all the messages. The fault tolerant capability of the proposed scheme depends

on the difference between the Hamming distance d of the code and the weight of the used error pattern z.

3 Experimental Results

In order to compare the execution times, we have implemented the following three protocols:

- the three-step identification protocol with RSA encryption,
- the Schnorr protocol,
- the proposed, enhanced McEliece based protocol.

The tests were executed on six different platforms, because many types of equipment in Electronic Payment Systems make use of cheap, low performance processors (e.g. smart cards). The execution times are shown in table 1. The Schnorr identification protocol is faster than the three-step protocol, because there are fewer messages. The proposed, enhanced McEliece based protocol is the most efficient in execution time, because it uses matrix computation for encoding and decoding, instead of time consuming exponential computation used in RSA. Beyond this advantage, our protocol provides fault tolerant capability for the occurring errors in the transmission channel.

Protocol type and key length		**PI, 166 MHz**	**PII, 300 MHz**	**PIII, 550 MHz**	**AMD D, 900 MHz**	**AMD D, 1300 MHz**	**P4, 1800 MHz**
Three-step	*64*	*5,173*	*4,717*	*4,041*	*3,197*	*2,951*	*2,677*
	128	*11,528*	*9,872*	*9,184*	*8,573*	*7,612*	*6,291*
Schnorr	*64*	*3,074*	*2,073*	*1,292*	*0,983*	*0,816*	*0,581*
	128	*9,381*	*7,586*	*6,087*	*4,475*	*3,166*	*1,537*
McEliece	*64*	*0,879*	*0,625*	*0,417*	*0,305*	*0,275*	*0,128*
	128	*1,752*	*1,427*	*1,039*	*0,877*	*0,629*	*0,453*

Table 1

The protocol execution times in function of key length for different processors [seconds]

Conclusions

For increasing security, fault tolerance and execution speed, we presented a new mutual identification protocol based on the three-step identification protocol and enhanced McEliece signature. Because of the use of error correcting Reed-Solomon codes both for encryption and fault tolerance, the protocol has a low

execution time and is suitable to be used in the presence of perturbations and noises.

References

[1] S. Brands: Electronic cash, Handbook on algorithms and theory of computation, CRC Press, 1998

[2] O. Poszet, I. Ignat, About information security in Electronic Payment Systems, Proceedings of the 1st ROEDUNET Conference, Cluj-Napoca, 2002, pp. 146-151

[3] C. P. Schnorr, Efficient identification and signatures for smart cards, in G. Brassard (ed.): Advances in Cryptology, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, Berlin, 1990, pp. 239-252

[4] A. Fiat., A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, Advances in Cryptology, Proceedings Crypto'86, Odlyzko A.M., Springer-Verlag, 1987, pp. 186-194

[5] O. Poszet, S. Vári-Kakas, O. Novac, H. Drăgan, I. Ignat, Efficiency of identification protocols in electronic payment systems, Annals of the University of Oradea, Volume Electrotechnics, Session Computer Science and Control Systems, 2005, pp. 118-121

[6] O. Poszet, I. Ignat, H. Drăgan, Analysis and design of error correcting cyclic codes using a new rank encoding algorithm, Annals of the University of Oradea, Volume Electrotechnics, Section C, 2003, pp. 179-184

[7] U. Feige, A. Shamir, Witness indistinguishable and witness hiding protocols, Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, 1990, pp. 416-426