Proceedings of the International Conference on
Information Technologies (InfoTech-2009)
17th – 20th September 2009
Bulgaria

E-EVALUATION IN OPEN AND DISTANCE LEARNING ENVIRONMENTS

V. I. Galanis[1,3,*], E. C. Laskari[1,3,$], G. C. Meletiou[2,#], M. N. Vrahatis[1,3,§]

[1] Computational Intelligence Laboratory (CI Lab), Department of Mathematics, University of Patras, GR-26110 Patras
[2]ATEI of Epirus, Arta, Greece
[3]Univerisity of Patras Artificial Intelligence Research Center (UPAIRC), University of Patras, GR-26110 Patras
{ [*] basgal, [$]elena }@master.math.upatras.gr
[#]gmelet@teiep.gr
[§]vrahatis@math.upatras.gr
Greece

Abstract: In this contribution, we explore the use of e-voting based cryptographic protocols to implement synchronous as well as asynchronous online electronic evaluation procedures in order to alleviate the problems arising from the lack of interpersonal transaction in open and distance learning environments. Our approach is based on the similarity of privacy requirements exhibited on such environments to the security and privacy requirements that are being met by electronic voting protocols.
Key words: e-evaluation, distance learning, cryptographic protocols, e-voting

1. INTRODUCTION

The process of evaluation in education refers to measurement of performance of the educational process. This process encompasses every aspect of the administrative and educational procedure such as teacher performance, adaptability and communicability, the efficiency of the educational unit, the educational activities, the educational material, whether books or software and many others and its goal is the improvement of the educational procedure by the providing of feedback regarding each of its features by the participants.

In an open and distance education framework, accurate evaluation is a difficult process due, mainly, to a lack of physical contact between the participants of the educational procedure. The online-based nature of modern open education enables the use of cryptographic tools to facilitate such a procedure, since the protection of privacy in the internet is feasible only through the use of cryptographic techniques.

In this contribution we will compare the requirements that are common between electronic voting (e-voting) procedures and electronic evaluation in open and distance educational environments, and we will provide a brief overview of the e-voting protocols that are suitable for educational evaluation purposes.

2. E-EVALUATION BASED ON E-VOTING

2.1. Requirements

In a traditional, classroom education, the most common practice regarding the evaluation of the educational procedure is the utilization of questionnaires where the students can anonymously answer to specific questions regarding every aspect of the educational procedure. This process of evaluation has several structural flaws, such as the presence of error and the amount of time, cost and effort required for the processing of the questionnaires.

As with traditional education, in open and distance education specific requirements must be met so as to enable the adaptation of the evaluation process we described above (Laskari *et al.*, 2005):

1. the submission of opinion or the choice of opinion must be secret,
2. only legitimate evaluators can participate in the evaluation procedure,
3. each evaluator can cast evaluation for a specific issue once,
4. in any case the results of the evaluation procedure should remain secret, until the process of evaluation is terminated.

The requirements for e-voting procedures (Menezes *et al.*, 1997) are quite similar to the aforementioned and are as follows:

1. the vote of each voter is secret,
2. only those registered in the election lists can vote,
3. no one can vote more than once in an election,
4. the result of the election is unknown before the end of the voting,
5. each voter is able to verify that his vote has been counted in the final tabulation without providing any information of his vote,
6. it is not feasible for a voter to transfer his right of participating to the elections to a third person.

Thus, the protocols used in e-voting procedures of the votes can also apply to an educational e-evaluation environment. The techniques used to ensure the vote secrecy

are based on public-key cryptography methods that are encapsulated within the e-voting protocols and form the core of their security.

2.2. The Basic Model

The following entities are met within any e-evaluation model:

1. **Evaluators**: the evaluators can be any group of participants taking part in the educational procedure, with the most obvious group being the students as they constitute the subject of the educational procedure and, thus, its most reliable judge. As evaluators can also be considered members of the business community or professors working in graduate programs that are able to evaluate the effectiveness of the undergraduate program. The actions of evaluators should be explicit, evident and short. The evaluators will be able to interrupt or even retract their choice until the termination of evaluation.
2. **Authorities**: the authorities that manage the evaluations are information systems capable of secure storage of large data sets.
3. **The choices of evaluation**: the structure of choices depends from the type of elections and depends on the type of questions that are offered to the evaluators and the possible answers.

The types of questions offered to the questionnaires in an e-evaluation process can vary and accommodate several needs of the evaluation procedure:

1. (yes/no) questions.
2. Choice of 1 between L cases.
3. Choice of K between L cases.
4. Categorized, structured and weighted choices of K between L cases.

In open environments there can be several types of communication channels that can ensure privacy of communication. To this end the employment of a "bulletin board" which is a secure common use channel with memory. Information traffic within these channels is encrypted using public-key cryptographic algorithms, due to the fact that communication channels in such schemes are common to all participants. There are three cases of such a channel:

1. **Untappable channel**: a secure communication channel between two entities where a third party cannot see or change the data exchanged within the channel.
2. **Anonymous channel**: a communication channel that preserves anonymity of the entities.
3. **Untappable anonymous channel**: a communication channel that combines the properties of both channels mentioned above.

These types of communication channels and basic setup are similar to the ones being used in e-voting protocols. In the following section we will provide a brief overview of the types of e-voting that can be utilized for e-evaluation purposes.

3. E-VOTING PROTOCOLS FOR E-EVALUATION

An e-evaluation scheme must be designed in such a way as to be unaffected by fraudulent actions and to be able to facilitate the evaluating process. Each scheme comprises of three stages:

1. **Initialization**.
2. **Evaluation**.
3. **Counting and result presentation.**

Depending on the educational enviroment and case-dependent factors in the evaluation process, an e-evaluation scheme should meet some additional requirements in order to be able to satisfy the evaluation requirements:

1. **Eligibility**: One evaluation form per evaluator.
2. **Privacy**: An evaluator cannot be connected to the contents of his evaluation.
3. **Individual and universal verifiability**: Any participant and observer should be able to verify the fairness of the evaluation process and each individual evaluator should be able to verify that his evaluation was included.
4. **Fairness**: No participant should be able to know even a fraction of the results of the evaluation procedure before the counting stage.
5. **Robustness**: The e-evaluation scheme should be fault-tolerant and fraud-resistant.
6. **Receipt-Freeness**: An evaluator cannot prove the contents of his evaluation to another participant or observer.

There are various e-voting protocols that meet the aforementioned requirements (Benaloh and Tuinstra, 1994), (Hirt and Sako, 2000), (Chaum, 1981), (Okamoto 1997), (Schoenmakers, 1997), (Iverson, 1991), (Park *et al.*, 1993) for an e-evaluation scheme. In this contribution we will showcase the four most widely used e-voting protocols that are suitable for use in e-evaluation schemes.

3.1. The Anonymous Channel for Casting Votes protocols

This type of e-voting protocols (Park *et al.,* 1993) utilizes an anonymous channel to provide anonymity for the participants in the e-evaluation process. This protocol has certain disadvantages like the *absence of the universal verifiability feature* (as digital signatures are omitted in the last stages of protocols of this family), the *rigidness of the evaluation procedure* (the evaluator must follow predetermined steps) and the *absence of a cancelation feature within the evaluation process* (in the case of regret or error, an evaluator must restart the procedure).

3.2. Blind signatures and anonymous channel protocol

This type of protocols (Okamoto, 1997) is based on untraceable “tokens” that each participant receives during the e-evaluation process along with the e-evaluation

questionnaire and sends back to the authority that conducts the e-evaluation process. The authority then publishes both the evaluations along with the tokens. Depending on the scheme, the authority for token publishing and collecting may be the same or may be two distinct entities. The disadvantages of this approach include the possibility of some participants knowing partial results of the evaluation before the conclusion of the counting process, non collision-freeness, (two evaluators may receive the same token) and the inability of an evaluator to protest the evaluation process before the conclusion of the counting process without revealing his choices. Moreover, a corrupt authority may poise as an evaluator or secretly distribute more than one tokens to some evaluators. The adding of a double token feature to the protocol eliminates many of these flaws.

3.3. Homomorphic cryptography protocols

Protocols of this type (Hirt and Sako, 2000) (Sako and Killian, 1994) are more secure as every evaluator submits digitally signed and encrypted questionnaires and the final results are produced by a public algorithm. Apart from increased communication complexity a minor flaw of these protocols are vulnerable to an attack by combining all of the evaluation authorities to decrypt the evaluation of a participant and violate privacy. Another disadvantage is that these protocols only support multiple choice type questionnaires ([yes/no], 1- between-*L*, *K*-between-*L*).

3.4. Advantages of e-evaluation

Despite these disadvantages, that are mostly the result of adapting e-voting protocols for this purpose, e-evaluation has certain advantages for the educational procedure:

1. It is an automated, cost-effective and flexible way of performing evaluation for a huge variety of aspects of the educational procedure.
2. Its online-based nature provides features such as result data storage and reusability as well as the ability to conduct evaluation processes in either asynchronous or synchronous manner.
3. It offers great potential for the statistical processing of the results.
4. It can be used as a platform for fully representative and objective evaluation as it allows the participation as evaluators of all the participants in the educational process.

4. CONCLUSIONS

Evaluation is a vital part of the educational process and an important factor for its continual improvement. Traditional methods of evaluation cannot be efficiently

applied in open and distance educational environments. With the use of e-evaluation we attempt to, not only address these problems, but also to enrich this process with new features. Through the use of e-voting protocols we are able to provide evaluation platforms for a variety of environments that can be applied in a case-specific manner and offer valuable information to aid strategic decision making in educational policy. In conclusion, e-evaluation, through the use of modern e-voting technology, is both feasible and essential in open and distance educational environments.

REFERENCES

Benaloh, J.C., Tuinstra, D. (1994), Receipt-free secret-ballot elections, In: *Proc. of the twenty-sixth annual ACM STOC'94*, pp. 544-553.

Chaum, D.L. (1981), Untraceable electronic mail, return address, and digital pseudo-nyms, *Communication of ACM* **24**, pp. 84-90.

Hirt, M., Sako, K. (2000), Efficient receipt-free voting based on homomorphic encry-ption, In: *Advances in Cryptology-EUROCRYPT'00, LNCS* **1807** pp. 539-556.

Iverson, K.R. (1991), A cryptographic scheme for computerized general elections, In: *Proc. of Crypto '91, LNCS* **576**, pp. 405-419.

Laskari, E.C., Meletiou, G.C., Stergiou, E., Vrahatis, M.N. (2005), Electronic eva-luation in open and distance education (in Greek), In: *Proc. of the Third International Conference on Open and Distance Learning (ICODL'05)*, Hellenic Open University, A. Lionarakis (Ed.), Vol. **1**, pp. 497-507, Propobos, Greece.

Menezes, A.J., Oorschot, P.C., Vanstone, S.A. (1997), *Handbook of Applied Crypto-graphy*, CRC Press.

Park, C., Itoh, K., Kurosawa, K. (1993), Efficient receipt-free voting based on homo-morphic encryption, Advances in Cryptology: In *Proc. of EuroCrypt '93, LNCS* **765**, pp. 248-259.

Sako, K., Kilian, J. (1994), Secure voting using partially compatible homomor-phisms, In: *Advances in Cryptology - CRYPTO '94, LNCS* **839**, pp. 411-424.

Schoenmakers, B. (1999), A simple publicly verifiable secret sharing scheme and its application to electronic voting, In: *Advances in Cryptology-CRYPTO'99, LNCS* **1666**, pp. 148-164.

Okamoto, T. (1997), Receipt-free electronic voting scheme for large scale election, In: *Proc. of Workshop on Security Protocols '97, LNCS* **1361**, pp. 25-35.