Secure Remote Voter Registration

Victor Morales-Rocha[1], Jordi Puiggalí[1], Miguel Soriano[2]

[1]Scytl Secure Electronic Voting
Tuset 20 1-7 Barcelona, Spain
{victor.morales| jordi.puiggali}@scytl.com

[2]Technical University of Catalonia
Department of Telematics Engineering
Jordi Girona 1-3 Barcelona, Spain
soriano@entel.upc.edu

Abstract: Voter registration is an important issue in election processes. In order to protect the election accuracy, it is necessary to have an accurate electoral roll of eligible voters. The electoral roll is usually constructed by means of a voter registration system that compiles voter data either in person or remotely. Current solutions for remote voter registration lack effective methods to prevent impersonation, multiple registrations and alterations on voter information. In this paper we propose a remote voter registration scheme that increases the accuracy of the current systems. In this scheme the voter identification is carried out by means of some biometric systems. Biometrics is also used to prevent impersonation, detect multiple registrations from the same person and protect from alterations of the registration information.

1 Introduction

Lately, there has been an increasing interest to improve the efficiency in the election processes, which has resulted in a wide range of proposals for new election systems. Most of the proposals have been focused in voting and tallying stages, giving least interest to voter registration stage.

Voter registration is the process of collecting the voters' data in order to constitute an electoral roll. Because of the fact that the electoral roll determines if a voter has the right to cast a vote during the voting stage, it has to be formed in an efficient way. Even when voting and tallying stages have the greatest security level, a deficient voter registration system can facilitate fraud practices that can even affect the accuracy of the election.

Voter registration is conventionally carried out face to face with the registration authority. However, since many voters are residing abroad during an election process, it has been necessary to have new methods to collect, remotely and in a secure manner, the information of such voters. As in most of the remote transactions, current remote voter registration systems face some security problems. These problems are mainly related to the inability to accurately verify the identity of the voter, which can facilitate impersonation or multiple registrations by the same voter with different data [El07].

In this paper we propose a remote voter registration scheme, in which some biometric systems play an important roll to protect the accuracy of the electoral roll. Biometric systems have already considered in electronic voting in the voting phase, e.g. [Ho07]. However, they have not been extensively used in the voting or in the registration phase.

It is important to note that sometimes voter registration is related to the voter credential generation process. Some authors have made proposals about this subject [Ac04, Kr07, Sc06]. However, in the context of this paper, voter registration is related to the creation of the electoral roll.

Section 2 presents a panorama of the current voter registration systems, as well as an analysis of biometrics and how these can be applied to improve the voter registration process. In section 3, our proposal is described. Section 4 concludes by emphasizing the advantages that our proposal gives to the remote voter registration process.

2 Voter Registration

2.1 Current Voter Registration Systems

Nowadays, in some countries like The United States [Fv08] or United Kingdom [El08] it is common to carry out remote voter registration. These methods allow the voter to fill out his or her own paper registration form remotely (e.g., at home) and return this form to the registration officers by using a delivery channel or optionally attending in person to a registration site. Registration forms are usually available to voters through postal delivery or downloading them from the network. In both cases voters fill out handwrite sign and return the forms to the registration officers using a postal delivery or any other alternative channels such as fax or e-mail (attaching a scanned copy of the filled form) [Fv08]. Furthermore, there are countries [De06] introducing the use of web interfaces to allow voters to fill out the registration form online, speeding up the remote acquisition of voter registration information.

After sending the registration form, if a voter wishes to verify that the registration has been received by the registration officers, he or she can contact them through e-mail or a phone call.

In the cases previously described, the identification of the voter is done by one or the combination of the following techniques: the verification of personal information of the voter and the verification of some physical characteristics of the voter. The first technique consists of registration officers checking to see if the voter included in the form some personal information that it is also stored in the voter register. Some examples could be the date of birth, the social security number or any other familiar information (e.g., mothers' maiden name, etc.). The problem with using such information for identifying the voter is that this information could be available in other databases (e.g., the member database of a social club) or could be known by people close to the voter. Therefore, it could be easy to impersonate a voter in the registration process just using this information.

The second technique consists of requiring verifying the identity of the voter based on checking some voter personal characteristics, such as a handwriting signature stamped on the form or the face or fingerprint of the voter against an image or template contained in some identity card or database. Face recognition requires the physical presence of the voter and therefore, it is not suitable for a real remote voter registration. However, handwriting recognition is the usual way implemented by remote registration and therefore the main one considered in this paper. In any case, the accuracy of this second technique of voter identification is based on the ability of the registration officers to validate the voter authentication data. Considering that most of these officers are not handwriting or physiognomy experts, we cannot expect high levels of accuracy.

Furthermore, current remote voter registration methods do not check if the same person has filled out more than a registration form by using the names of different valid voters. That is, using handwriting signatures as a reference, the verification process is based on looking for similarities between the signature on the form and a pre-existing signature. Therefore, detecting a person filling out more than one registration form signed with different signatures could be unfeasible for a registration officer. In this case, registration officers must have the ability to extract the identity of a person from the handwriting signature instead of looking for similarities. It is important to mention that registration officers usually do not have a pre-existing signature of the voter. Therefore, the signature contained in the registration form is only used to create a temporary database of signatures that will be used to identify the voters during the vote casting process. For example, in the case of postal voting, the voter signature stored during the registration process is compared against the signature contained in the postal envelope to detect if the vote has been cast by the legitimate voter.

Finally, in addition to identification accuracy, there are additional problems in current remote registration scheme. The contents of the registration form can be altered after the voter has sent this form. Furthermore, the handwriting signature on the form can be re-used by an attacker to fill out a different registration form. This problem lies in the fact that handwriting signatures (as well as face recognition) are not bound to the contents of the register. Therefore, any change in the contents of the registration form or the re-use of a valid handwriting signature in a different form cannot be detected by simply verifying the signature.

Summarizing, current voter registration systems face the following problems:

- Accuracy to validate the voter identity;
- Prevention of multiple registers by voters; and
- Integrity of voter registration information.

To increase the accuracy of remote registration process, we propose the combination of biometric systems and cryptographic functions. Below we analyze which are the improvements of adding both techniques in remote registration process.

2.2 Accuracy on Biometric Systems

In some way, the voter registration systems previously described are based on the use of biometrics. Registration officers usually verify some physical characteristics that uniquely identify the voter, such as a picture (facial identification) or the signature of the voter. However, one of the main issues of this identification is the accuracy on the process, since not all the registration officers are, for example, handwriting or physiological experts. In this sense, we propose the use of biometric systems to help registration officers to improve the accuracy of voter identification. However, are all the biometrics systems suitable for a remote voter registration?

Biometric systems are electronic systems specialized on identifying a user by means of processing unique physiological or behavioural characteristic of the user. Biometrics systems are classified based on the unique characteristic of the user that is used for the identification, for instance: DNA, face, fingerprint, iris, palmprint, retina, writing/signature and voice. However, the accuracy on the different biometric system is not the same, since each of the biometric characteristics processed has advantages and disadvantages.

A good biometric characteristic must fulfil some requirements [JR04]:

- Universality- Each individual should have the characteristic.
- Uniqueness- How well the characteristic makes different two individuals.
- Permanence- How well the characteristic endures over time.
- Collectability- Ease of acquiring the characteristic.
- Performance- Refers to the speed and accuracy of recognition as well as the resources required to do it (cost).
- Acceptability. It indicates the level of acceptance of people to use the characteristic.
- Robustness. It reflects the level of resistance against fraudulent methods attempting to mislead the system.

In our analysis, we considered an additional requirement for remote voter registration: the biometric system must be remotely available for most of the voters. Therefore, the acquisition of the biometric information must be supported using standard means or devices. This reduces the number of potential candidates to handwriting signatures and voice biometrics, since these allow biometric information to be acquired by means of scanning the signature written in the paper registration form or a voice recording made from a standard telephone. About handwriting biometrics, there are two distinct techniques, namely on-line and off-line handwriting. Besides the shape of the signature, on-line signatures take into account other aspects such as pen timing, pressure or writing trajectory. However, we do not consider on-line signatures a good candidate, since it requires voters to have available a digital-pad for acquiring a writing of a text (e.g., the signature of the voter). Therefore we will focus on off-line signatures.

Using pre-existing biometric systems comparative analysis [JR04, Ti06] and taking fingerprint biometrics as reference, the proposed biometrics systems fulfil the requirements previously introduced as follows (L=Low, M=Medium and H=High).

Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Robustness**
Fingerprint	H	H	H	M	H	M	M
Off-line Signature	M	M	L	H	L	H	L
Voice	M	M	M	H	M	H	L

Table 1. Comparison of three example biometric systems

From this comparison we can conclude that off-line signatures and voice biometrics are not as robust as fingerprint biometrics systems. However, the introduction of voice biometrics could improve the current systems based on handwriting signatures.

Another important aspect of performance on biometrics is the accuracy of the identification process. There are three parameters that can help to determine in a quantitative manner such accuracy:

- *False rejection rate* (FRR). It is the percentage of eligible user requesting access declared by the system as non-eligible;
- *False acceptance rate* (FAR). It is the percentage of non-eligible access attempts identified as valid users.
- *Equal error rate* (ERR). The point at which FRR and FAR are the same.

Additional comparative analysis of the same biometrics systems used in Table 1, provide the following measures from the accuracy point of view.

Biometrics	FRR	FAR	EER	References
Fingerprint	2.2%	2.2%	2.2%	[Ca06], [Bi06]
Signature off-line	10-30 %	10-30%	10-30%	[KSX04], [YJX07]
Voice	5-10%	2-5%	6%	[Re05], [PM04]

Table 2. Accuracy performance of biometric systems

Based on the values shown in table 2, fingerprints are again, the best positioned biometric characteristic. However, as we will explain in the definition of our proposal, fingerprints do not give any advantage over the current solutions on remote registration environment. Furthermore, voice biometrics behave better than handwriting signatures. The values for voice have been obtained by using a telephone communication [Re05].

2.3 Preventing Multiple Registration on Biometric Systems

Another issue detected during the study of the current remote registration systems is the capacity to detect multiple registers from the same voter. To analyze how biometric systems can manage this issue, we considered the two main operation contexts implemented by biometric systems for user authentication: verification and identification.

Verification. In this context, the system verifies a user identity by comparing the given biometric data with a template stored in the system database. To start the comparison, the user gives a personal ID or username known by the system. The system then retrieves the template related to such user and carries out a one-to-one comparison. That way it is possible to determine if a user is who she claims to be.

Identification. In this context, the user does not need a personal ID or username. Based on the biometric characteristic given by the user, the system has to identify if such characteristic corresponds to one stored in its database. In this case, a one-to-n comparison is carried out.

Based on the operation of both contexts, we can identify that current remote voter registration methods only use the verification context; registration officers use voter personal information to retrieve the signature stored in their database for the comparison. However, using a biometric system in the identification context, the signature of the register could be checked against the complete database of signatures stored. Then, in case the same voter attempts to register more than once using different personal information, she will be detected. Therefore, the use of an identification context prevents multiple registrations by voter.

2.4 Binding Biometrics and Contents

Finally, in order to overcome the feasibility of an attacker changing the contents of a registration form, or separating such contents from the voter identification element, it is necessary to get a link between the contents of the registration form and the voter identification element.

Nowadays, a usual method to protect information is the digital signature. A digital signature protects the information from alterations and binds such information to its author. However, digital signatures have important logistic problems, for example it is necessary for a PKI to generate and provide users with digital certificates.

On the other hand, despite the advantages that biometrics can give to the identification or verification aspects, not all the biometric techniques provide a bind between the biometric characteristic and the contents of a message. For example, in the comparisons presented, fingerprint is considered the most efficient biometric in the values scale given. However, neither fingerprints nor signatures, are usable for binding the contents. In both cases the contents of a message can be manipulated and this cannot be detected by means of the fingerprint or signature.

We have evaluated how to take advantage from the most usable biometrics to carry out the voter registration process in a more effective way. The main idea, as we already have mentioned, is to bind the contents of the registration form to the identification element (i.e. the biometric characteristic). Table 3 shows a new element (hand-writing) and a new requirement (content binding). The handwriting element is added as an extension of signature. Handwriting refers to the unique characteristics that an individual posseses in his or her writing. The new requirement added in table 3 refers to the ability to bind the contents, in our case registration information, to the biometric characteristic. Note that both signature and writing have the same values in the initial compared requirements. However, writing biometrics as well as voice possesses that peculiar characteristic, which is the binding that can give between the biometric characteristic and the contents of the message. In the proposal, we take advantage of such binding to improve the current registration systems.

Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Robustness**	**Content binding**
Fingerprint	H	H	H	M	H	M	M	No
Signature off-line	M	M	L	H	L	H	L	No
Handwriting	M	M	L	H	L	H	L	Yes
Voice	H	M	M	H	M	H	L	Yes

Table 3. An extended comparison of biometric characteristics

3. Proposal

This proposal carries out a remote voter registration in a secure way. It protects from alterations the contents of the voter registration information by binding such information to the voter identity. This is reached by means of combining biometrics and cryptographic techniques that do not require a public key infrastructure. It consists of creating a kind of biometric digital signature. That means a biometric characteristic that can give at the same time both authentication and integrity to the contents.

The scenario for the application of the scheme is a voter registration over Internet. However, other application scenarios are currently possible.

In this scheme, four participants are necessary during the voter registration process: a citizen requesting to be a voter, a registration module, a validation module and the registration officer.

Voter- The voter provides her personal data in order to generate the registration information. The voter also will collaborate to generate a registration proof based on both, her biometric characteristic and the registration information.

Registration module- This module is used to enter the voter registration information and generate an integrity proof of such registration information.

Validation module- The registration proof is generated by means of this module. Such proof is generated with the biometric information provided by the voter.

Registration officers- The registration officers receive the voter register information and carry out some validation processes.

The scheme is divided in two main stages:

- Introduction of the voter registration information and protection of the integrity
- Generation and validation of a registration proof

Based on this division the scheme behaves as follows.

3.1 Introduction of the Voter Registration Information and Protection of the Integrity

The voter connects to the Web site of the Registration Module by means of a secure and encrypted channel, e.g. SSL. The Web site provides a registration form. The voter fills out the registration form with his or her required personal data. Once the registration form is completed, an integrity proof is generated by the Registration Module. Such integrity proof is a cryptographic hash function of the registration information provided by the voter.

The integrity proof is then represented in a format that can be legible by the voter, for instance, a base-32 notation [RFC06]. We selected base-32 notation instead of others available notations (e.g., base-64) for usability reasons: it uses a reduced set of characters focused on minimizing interpretation mistakes. For example, the number 0 is not included in the representation set to prevent being confused by the letter "O."

This representation is shown to the voter by means of the same communication channel. Figure 1 shows the interaction between the voter and the Registration Module to carry out the remote registration and get the integrity proof.

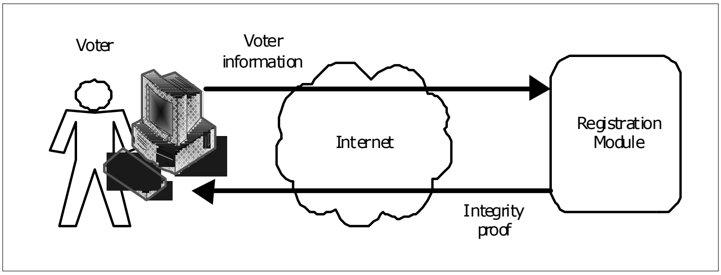

Figure 1: Interaction between Voter and Registration Module

In order to get the integrity proof it is used as a combination of MD5 and SHA1 hash functions. The latest is used in its MAC implementation. This combination is conceived with the aim of preventing collisions between the digest messages, such as was found in the last years for MD5 [Ha04, Kl05, Wa05, WY05] and for SHA1 [Wa05, WY05]. The integrity proof generation is then as follows:

1. Get a digest *k* from the registration information M_i:

$$K = \text{MD5}\ [M_i]$$

2. Use *k* as a key to get a HMAC-SHA1 from the same registration information M_i:

$$H = \text{HMAC-SHA1}\ [M_i, K]$$

The resultant *H* is the integrity proof.

Using a combination of MD5 and HMAC-SHA1, the probability to have a collision decreases significantly. An attacker needs to find a coincidence of collision for the same text on both systems. In addition, we are reducing the probability of these collisions without increasing the size of the digest that remains the same as a SHA1 (160 bits).

Since *H* is based on an HMAC-SHA1, it is 160 bits long, i.e. 2^{160} different digests. Therefore, a base-32 notation (which is 2^5) allows a representation of SHA1 in 32 characters. These 32 characters can be shown to the voter in six groups of five characters plus the two remaining ones. However, the integrity proof *H* can be truncated in order to give a higher usability. For example, taking only the first 20 characters, they can be shown in five groups of four characters or four groups of five characters, which is usable enough.

To prevent reply attacks, each form has a unique number. Therefore, two forms with the same contents will always have different integrity proofs.

Finally, the form with the voter register information and integrity proof is sent to the registration officers. This can be done by posting the on-line registration form or by printing and sending it by a postal service. The preferred option is using an on-line channel, since it allows the implementation of cryptographic techniques that cannot be applied on a postal delivery (e.g., encryption of the information). The received information is stored by the registration officers pending for further validation.

3.2 Generation and Validation of a Registration Proof

The second stage is the generation of a registration proof and the validation of the registration information. Based on the previous analysis, we will use a voice biometric system in this stage.

The voter carries out a communication with the Validation Module. This communication is done by means of a phone call. Then the voter is asked to give the integrity proof. He or she speeches the proof previously shown by the Registration Module, i.e. the groups of characters that represent the integrity proof. By doing this process, the voice of the voter is bound to the contents of the registration information. This is called the registration proof. The registration proof is then stored by the Validation Module. Figure 2 shows the interaction between the voter and the Validation Module in order to generate the registration proof.

The registration proof protects the integrity of the registration information. Any change in the registration information causes the registration proof to not correspond to the contents of the registration information. The registration proof also binds the contents of the registration information to the author, that is, the voter who provides his or her personal information.

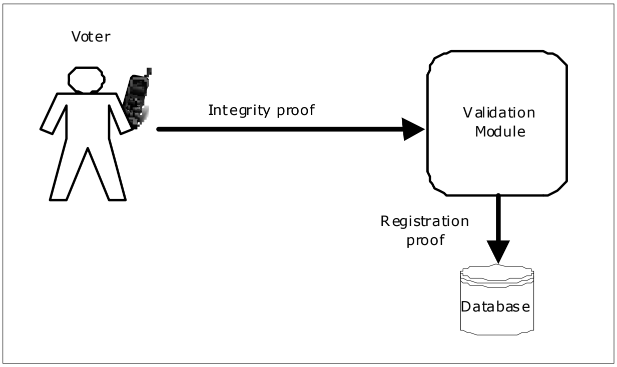

Figure 2: Interaction between Voter and Validation Module

The interaction between the voter and the Validation Module includes, besides the speech of the integrity proof, other dynamic data in order to prevent reply attacks in which an attacker could use a pre-recorded voice of a voter. Such dynamic data could consist of a challenge to the voter who has to repeat a word or a set of words said by the Validation Module. That way, the Validation Module can be sure that the integrity proof is being spoken by a person who is on the other side of the communication line and not by a pre-recorded or automatic process.

Once the registration officers have recorded the validation proof, they can start the validation process.

The validation process facilitates the detection of people who attempt to create more than one record. It is possible to compare the voice of a voter who is validating a new registration with the set of voices previously recorded. That way, a person attempting to create a bogus or an additional record will be rejected, and the registration information associated with the proof provided by such a person will be identified as invalid. Therefore, the probability of impersonation is low. This verification is not necessarily carried out on-line but it can be made after the registration process.

Since any attempt at creating bogus records can be detected through the validation process, the scheme does not require a previous database with the recorded voice of voters. However, for future registrations, the previous records can be used in order to validate the voice of the voter who is making the new record.

An additional validation consists on checking the voter registration information against the associated registration proof. This check will consist on verifying if the integrity proofs match. That means, if the hash of the voter registration form has the same value as the one recorded as part of the registration proof.

If registration proofs and voter registration records pass all the validations, election officers can accept the voter registration information of the voter. If any of the validations fail, the voter registration form and corresponding registration proof can be classified as non-validated records. Therefore, registration officers can implement additional manual checks or contact the voter for checking the process if required.

In a subsequent voting stage, it could be possible to use the registration proof to verify that the person who is voting is the same who created the registration information by checking his or her voice.

Our scheme can be also used as a means to activate the voter credentials once they have been received by the voter. This is usable if the voter credentials are sent to voters by remote means. In such cases, there is the risk that voter credentials are received or intercepted by a third person. The activation technique prevents somebody using the voter credentials instead of the legitimate voter. The activation is carried out by means of an activation code, which is enclosed to the voter credentials. The voter has to call and say the activation code to the registration authority and then a process of comparison between the activation voice and the voice recorded during the registration process is carried out. If the activation voice is the corresponding one, then the voter credentials are validated and authorized to participate in the election. That way, an illegitimate use of the voter credentials is prevented.

Another possible scenario in which our voter registration process can be applied is by using handwriting biometrics instead of voice. The first part of the process (generation of the registration information and integrity proof) could be the same as the previously described, that is, through Internet. The second part of the process (generation of the integrity proof) is carried by the voter by writing by hand the representation of the integrity proof. That way, the registration proof binds the contents of the registration information with the handwriting biometrics of the voter. The handwriting of the integrity proof is carried out in a form provided by the election authority. Once filled out by the voter with the hand-written integrity proof, this form is sent to the election authority by means of postal mail. The sending can be also by electronic means such as fax or e-mail. In the case of electronic sending, the form has to be previously converted to a digital format by scanning it. Even when the verification of a writing text is as difficult as the signature verification, the advantage of the writing text respect to the signature is that it can do the linking to the contents as we have explained before.

4 Conclusions

Current remote voter registration systems have important issues that can facilitate voter impersonation. These issues are mainly voter identification accuracy, multiple registrations from the same person and voter registration information integrity. In this paper we proposed the use of biometrics systems to increase the voter identification accuracy of voters that make a remote registration. In addition, operating on an identification context, biometrics systems can automate the detection of multi registrations made by the same person. Finally, we identified and proposed some biometrics methods, such as handwriting and voice biometrics that can also bind the registration information to the voter identity. Combining this later feature with the use of cryptographic algorithms, such as hash functions, we also provided a way to protect the integrity of voter registration information that can be suitable to implement in current environments.

References

[Ac04] Acquisti, A: Receipt-free homomorphic elections and write-in ballots, Cryptology ePrint Archive, Report 2004/105, http://eprint.iacr.org/, 2004.

[Bi06] Biometric System Laboratory - University of Bologna: “FVC2006: The Fourth International Fingerprint Verification Competition,” 2006. Available at http://bias.csr.unibo.it/fvc2006/default.asp.

[Ca06] Cappelli, R. et. al.: Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, January 2006.

[De06] Department of Defense U.S., Report on IVAS 2006, As Required by Section 596 of the National Defense Authorization Act for Fiscal Year 2007, December 2006.

[El07] Election Law Blog. The Extremely Weak Evidence of Voter Fraud in Crawford, the Indiana Voter ID Case. May, 2007. Available at http://electionlawblog.org/archives/008378.html

[El08] Electoral Commission’ website to register to vote. Available online at http://www.aboutmyvote.co.uk/register/CitzSelect.cfm?officeID=214&CFID=12799012&CFTOKEN=71181288

[Fv08] FVAP Voting Assistance Guide. Available online at http://www.fvap.gov/pubs/vag.html#ch3

[Ha04] Hawkes, P. et. al.: MD5 collision, October 2004. Available at http://eprint.iacr.org/2004/264.

[Ho07] Hof, S.: E-Voting and Biometric Systems? Electronic Voting in Europe. pp. 63-72. 2004.

[JR04] Jain, A.; Ross, A.; Prabhakar, S: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, pp. 4-20, January 2004.

[Kl05] Klima, V.: Finding MD5 collisions on a notebook PC using multi-message modifications. In International Scientific Conference Security and Protection of Information, May 2005.

[Kr07] Krivoruchko, T: Robust Coercion-Resistant Registration for Remote E-Voting, Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007), 2007.

[KSX04] Kalera, M.; Srihari, S.; Xu, A.: Offline signature verification and identification using distance statistics. International Journal of Pattern Recognition and Artificial Intelligence, Vol. 18, No. 7 pp. 1339-1360. 2004.

[PM04] Przybocki, M.; Martin, A.: NIST, Speaker Recognition Evaluation Chronicles. In Odyssey: The Speaker and Language Recognition Workshop, pp. 12–22. Toledo, Spain, May 2004.

[Re05] Reynolds, D. et. al.: The 2004 MIT Lincoln laboratory speaker recognition system, in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Philadelphia, PA, March 2005.

[RFC06] RFC 4648. October 2006. Available at http://tools.ietf.org/html/rfc4648#section-6

[Sc06] Schweisgut, J: Coercion-resistant electronic elections with observer, 2nd International Workshop on Electronic Voting, Bregenz, August 2006.

[Ti06] Tiltont, C.: The Role of Biometrics in enterprise Security. Dell Power Solutions. 2006. Available online at http://www.dell.com/downloads/global/power/ps1q06-20050132-Tilton-OE.pdf.

[Wa05] Wang, X. et. al.: Cryptanalysis of the hash functions MD4 and RIPEMD. In Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings (2005), vol. 3494 of Lecture Notes in Computer Science, Springer, pp. 1-18.

[WY05] Wang, X.; Yu, H.: How to break MD5 and other hash functions. In Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings (2005), vol. 3494 of Lecture Notes in Computer Science, Springer, pp. 19-35.

[YJX07] Yu, Q.; Jianzhuang, L.; Xiaoou T.: Offline Signature Verification Using Online Handwriting Registration. Computer Vision and Pattern Recognition, CVPR '07. IEEE Conference on. pp. 1-8. June 2007.