Voting With a Tripartite Designated Verifier Scheme Based On Threshold RSA Signatures

Jérôme Dossogne Olivier Markowitch
Université Libre de Bruxelles
Boulevard du Triomphe CP212, 1050 Brussels, Belgium
jerome.dossogne@ulb.ac.be olivier.markowitch@ulb.ac.be

Abstract

In this paper we propose a new voting scheme that provides a receipt to each voters. The receipt is build in a way that prevents that the vote can be revealed to third entities other than a judge. The scheme is based on the concept of strong designated verifier signature scheme and threshold RSA signatures. The signing key size remains bounded by the size of a RSA modulus. The computational cost for each participant is very low, in addition to the computation of a classical RSA signature, the signature generation of our scheme needs only one modular multiplication; the verification process in our scheme remains the same than a classical RSA signature verification.

1 Introduction

Electronic voting is a reality in companies, national ballot, etc. The existing mechanisms take different forms from automated voting system to vote through networks. Problems arise when trying to combine voting privacy with the ability for the voter to check the correctness of his own voting by the mean of a receipt. On the basis of voting receipts a dishonest third party may possibly force a voter to reveal his vote. To avoid this weakness, some works [1, 4, 6, 7] propose receipt-free voting protocols but in that case, the main problem becomes the difficulty for the voter to be sure his vote is taken into account. Some schemes have been proposed to manage this problem, but at the price of important amount of data transmissions and computations [8, 6, 4] or by assuming that the voters have to trust the polling office to behave honestly [6].

This paper proposes a new voting scheme where the voter receives a receipt of his vote that cannot be used to reveal the vote to someone else. This feature allows the voters to verify their own vote, but also to complain if necessary, while it forbids an attacker buy the votes. The scheme, based on a designated verifier signature scheme such as [5, 9, 10, 3], allows the polling office to sign a vote in such a way that only a designated verifier will be able to check its validity. Moreover the designated verifier will not be able to convince other entities that the signature is valid. The designated verifier scheme is used to create the voting receipts and the voters are the designated verifiers. We propose a voting scheme based on the designated verifier signature scheme introduced in [3] where a trusted judge can intervene in case of conflicts between voters and the polling office.

To summarize, Alice, the voter, wants to cast a ballot by sending it to Bob, the polling office. Alice wishes that her vote remains confidential as well as the ability to check the correctness of her own vote by the mean of a receipt signed by Bob. But most of the time, being in possession of such a receipt implies that a dishonest third party might coerce the voter. To avoid this situation, thanks to the designated verifier property of the signature scheme, Bob will sign the receipt in such a way that Alice cannot use it to reveal her vote to someone else. In order to achieve this property, our scheme relies on the help of Cecile who is trusted to sign any message coming from Alice or Bob. Thus, to make such a signature, Alice, Bob and Cecile obtain a

distinct share of a signing key, and only Alice receives the corresponding verification key. Therefore, in order to submit the receipt, Bob blinds his receipt and sends it to Cecile who signs the message with her key-share and sends the result to Bob. Bob unblinds the signed receipt, signs the original receipt with his key-share and combines the result with the unblinded receipt signed by Cecile. By doing so, Bob obtains a valid signature on his receipt, signature computed on the basis of the whole secret signature key. Bob can now send the signed receipt to Alice who will assert the validity of the signature with the verification key. The designated verifier scheme is designed in such a way that Alice could have followed the same protocol with Cecile and obtain the same signature. Therefore, on the basis of the signed receipt, if the communications of Alice are not monitored or are scrambled, Alice cannot convince anyone that the received receipt was signed by Bob.

2 The voting scheme

In this section, we describe our voting protocol during which the voter V, after being identified by an identification authority I, submits a vote (yes/no, names, etc.) to a polling office P under the authority of a unique judge J. In this protocol, we trust the judge to cooperate with a signer by signing the messages he receives, to keep secret his private signing key and to be honest during the procedure dedicated to resolving conflicts *.

We use the following notations:

- $A \rightarrow B : m$: the transmission of a message m from A to B
- blindSign(): a blind signature
- blind(): a blinding function related to blindSign()
- unblind(): the corresponding unblinding function
- $A \overset{Auth.}{\longleftrightarrow} B$: the mutual authentication of the entities A and B
- $r_{V,b}$: a receipt r created from the ballot b casted by V
- $\sigma_{P,r_{V,b}}$: the partial signature of P on the receipt r
- $\sigma_{r_{V,b}}$: the signature on the receipt r
- $a|b$: the concatenation of a and b

2.1 Initialization

On the basis of the designated verifier signature scheme [3] used in the protocol, the following values and keys are computed and distributed to the entities:

- $n = pq$ where p and q are two large primes
- e and d such that $ed = 1 \bmod \phi(n)$
- d_1, d_{2a}, d_{2b} and d_3 such that $d_1 + d_{2a} = d_{2b} + d_3 = d \bmod n$
- e_{u_1} and d_{u_1} such that $e_{u_1} d_{u_1} = 1 \bmod \phi(n)$

*This can be assured by appropriate laws and concrete measures.

- e_{u_3} and d_{u_3} such that $e_{u_3} d_{u_3} = 1 \bmod \phi(n)$
- $I_{A1} = \frac{d_1 + d_{2a} - d}{n}$
- $I_{A3} = \frac{d_{2b} + d_3 - d}{n}$

The keys and values $(e, n), d_1, e_{u_1}, d_{u_1}, d_{2a}, d_{2b}, d_3, e_{u_3}, d_{u_3}, I_{A1}$ and I_{A3} are distributed from the entity generating them to each participant:

- $(d_1, e_{u_1}, d_{u_1}, n, I_{A1})$ is transmitted to the signer P,
- $(d_{2a}, d_{2b}, I_{A3}, n)$ to the contributor J,
- $(e, n, d_3, e_{u_3}, d_{u_3}, I_{A3})$ to the designated verifier V.

We suppose that the transmissions are done via secure channels.

2.2 Voters identification

We have to make sure that the vote remains anonymous, even for the voting authorities. Therefore, each voter has to obtain a voting ticket, i.e. a random number signed from an identification authority that will allow the voter to send anonymously his vote to the polling office. The identification authority must be distinct from the polling office[†].

The authority keeps a list of all the already registered voters (i.e. voters that have already obtained a voting ticket). When a voter asks for a voting ticket, he starts a mutual authentication protocol with the identification authority that also checks in its list if this voter already appears. If not, the voter is allowed to submit to the authority a blinded random value r (using a blinding operator of a blind signature scheme such as described in [2]) to be signed by the authority. The voter will unblind the received signature in order to recover the signature of the identification authority on the original random value.

1. $V \overset{Auth.}{\longleftrightarrow} I$
2. The voter chooses a random number a and computes $\text{blind}(a)$
   $V \rightarrow I$: $\text{blind}(a)$
3. $I \rightarrow V : \sigma_{\text{blind}_I} = \text{blindSign}(\text{blind}(a))$
4. The voter computes $\sigma_{I_a} = \text{unblind}(\sigma_{\text{blind}_I})$

Once unblinded, the signature on r is used as a random and untraceable identification number for the voter.

2.3 Vote

The voter sends his ballot and his voting ticket (the random value signed by the identification authority) to the polling office that keeps a list of the voting ticket already submitted. The polling office verifies the validity of the signature of the voting ticket and checks in its list to be sure that the voter has not already voted. If the checks succeed, the polling office replies with a designated verifier signature on a receipt for the received vote.

[†]As for the judge, the role of the identification authority could be divided into several parts and handled by different identification authorities.

1. The voter fills in his ballot b
   $V \rightarrow P : b, a, \sigma_{I_a}$

2. The polling office checks whether a was not previously submitted and verifies the validity of σ_{I_a}, the signature of the identification authority on a.

3. If the previous checks succeed, the polling office records the vote b and the value a.

4. The polling office creates a receipt $r_{V,b} = (a|\sigma_{I_a}|b)$ and computes, with the help of the judge, $\sigma_{r_{V,b}}$, the designated verifier signature [3] on the receipt:

   (a) $P \rightarrow J : m' = {r_{V,b}}^{e_{u_1}} \bmod n$

   (b) $J \rightarrow P : s' = m'^{d_{2a}} = \sigma_{J,r_{V,b}}^{e_{u_1}} \bmod n$

   (c) $P \rightarrow V : \sigma_{r_{V,b}} = {r_{V,b}}^{d_1} s'^{d_{u_1}} m^{-I_{A1}n} \bmod n$

Using his secret key e the voter checks if the receipt and his signature matches his vote by verifying if: $r_{V,b} = (a|\sigma_{I_a}|b)$ and $\sigma_{r_{V,b}}^{e} = r_{V,b}$

Notice that this verification can be made even without using e since the voter can collaborate with the judge in order to generate a same signature $\sigma_{r_{V,b}}$[‡]:

1. $V \rightarrow J : m' = {r_{V,b}}^{e_{u_3}} \bmod n$

2. $J \rightarrow V : s' = m'^{d_{2b}} = \sigma_{J,r_{V,b}}^{e_{u_3}} \bmod n$

3. The voter computes $\sigma_{r_{V,b}} = {r_{V,b}}^{d_3} s'^{d_{u_3}} m^{-I_{A3}n} \bmod n$

If the receipt is incorrect, the voter cancels his vote by asking the judge to vote on his name. The loss of anonymity is not a problem as the judge is supposed to behave honestly when resolving conflicts, therefore, the blinding part is not necessary anymore. This procedure is achieved by the following steps:

1. The voter fills in his ballot b
   $V \rightarrow J : b, a, \sigma_{I_a}$

2. $J \rightarrow P : b, a, \sigma_{I_a}$

3. The polling office checks whether a was not previously submitted and verifies the validity of σ_{I_a}, the signature of the identification authority on a.

4. If the previous checks succeed, the polling office records the vote b and the value a.

5. The polling office creates a receipt $r_{V,b} = (a|\sigma_{I_a}|b)$ and computes $\sigma_{r_{V,b}}$, the designated verifier signature on the receipt, with the help of the judge:

   (a) $P \rightarrow J : \sigma_{P,r_{V,b}} = {r_{V,b}}^{d_1} \bmod n$

   (b) $J \rightarrow V : \sigma_{r_{V,b}} = \sigma_{P,r_{V,b}} {r_{V,b}}^{d_{2a}} m^{-I_{A1}n} \bmod n$

[‡]In practice, since the voter is able to realize the verification offline (by using e), there is no need to involve the judge.

Using his secret key e the voter checks if the receipt and his signature matches his vote by verifying if: $r_{V,b} = (a|\sigma_{I_a}|b)$ and $\sigma^e_{r_{V,b}} = r_{V,b}$

If the receipt or the signature provided by the polling office is incorrect, the voter contacts the judge and collaborates with him to verify together the validity of the forwarded signature by checking: $r_{V,b} = (a|\sigma_{I_a}|b)$, $\sigma^e_{r_{V,b}} = r_{V,b}$ after having computed $\sigma_{V,r_{V,b}} = m^{d_3} \bmod n$, $\sigma_{J,r_{V,b}} = m^{d_{2b}} \bmod n$ and $\sigma_{r_{V,b}} = \sigma_{V,r_{V,b}}\sigma_{J,r_{V,b}}r_{V,b}^{-I_{A3}n} \bmod n$.

Since the judge recorded $\sigma_{r_{V,b}}$ before sending it to the voter, he knows the signature comes from the polling office and by revealing e to the judge, the voter cannot cheat him by using a fake d_3 to wrongly accuse the polling office. If it appears that the voter is honest, the judge contacts this polling office to resolve the problem, possibly using appropriate legal procedures.

2.4 Results publication and possible complaints

Before closing the vote, a delay is left to the voters in order to complain if the transmitted receipt was incorrect. This delay is supposed long enough to prevent course problems. The polling office then publishes a list of all the votes, each associated with the corresponding random number. The voter checks if his vote is correct and contacts the judge in case of problem.

If a vote is corrupted or lost, the corresponding voter authenticates with the judge and provides him with $r_{V,b}$, $\sigma_{r_{V,b}}$, $\sigma_{V,r_{V,b}}$ and e. The judge verifies the receipt, using his secret key d_{2b}, by verifying if $r_{V,b} = (a|\sigma_{I_a}|b)$, $\sigma^e_{r_{V,b}} = r_{V,b}$ after having computed $\sigma_{J,r_{V,b}} = m^{d_{2b}} \bmod n$ and $\sigma_{r_{V,b}} = \sigma_{V,r_{V,b}}\sigma_{J,r_{V,b}}r_{V,b}^{-I_{A3}n} \bmod n$.

3 Conclusion

We have introduced an efficient voting system based on a designated verifier scheme, which allows the voter, and only him, to check his voting, and possibly complain about it. In case of problem during the voting protocol, a trusted judge can help to acknowledge a vote, or point out that a vote has been miscounted. The aim of our voting protocol is to ensure anonymity while being resistant against impersonalization, dishonest voters and dishonnest polling office.

References

[1] J. C. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In 26th ACM Symposium on the Theory of Computing, pages 544-553. ACM Press, 1994.

[2] D. Chaum. Blind signatures for untraceable payments. In Advances in Cryptology Proceedings of Crypto 82, pages 199-203. D. Chaum, R.L. Rivest, and A.T. Sherman (Eds.), Plenum, 1983.

[3] J. Dossogne and O. Markowitch, A family of Multi-Party Strong Designated Verifier Schemes, Technical Report, March 2009, Université Libre de Bruxelles

[4] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In Proceedings of Eurocrypt 2000, volume 1807 of Lecture Notes in Computer Science, pages 539-556. Springer-Verlag, 2000.

[5] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In Proceedings of Eurocrypt 1996, volume 1070 of Lecture Notes in Computer Science, pages 143-154. Springer-Verlag, 1996

[6] B. Lee and K. Kim. Receipt-free electronic voting through collaboration of voter and honest verifier. In Korea-Japan Joint Workshop on Information Security and Cryptology, pages 101-108, 2000.

[7] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In First IFIP Conference on E-Commerce, E-Business and E-Government, pages 683-694. Kluwer Academic Publishers, 2001.

[8] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In 5th International Security Protocols Workshop, volume 1361, pages 25-35. Springer-Verlag, 1997.

[9] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In Proceedings of Asiacrypt 2001, volume 2248 of Lecture Notes in Computer Science, pages 552-564. Springer-Verlag, 2001.

[10] S. Saeednia, S. Kremer, O. Markowitch, An efficient strong designated verifier signature scheme, ICISC'03, Lecture Notes in Computer Science, vol. 2971, Springer Berlin, 2004, pp. 40-54.