Receipt-freeness in Large-scale Elections without Untappable Channels

Emmanouil Magkos, Mike Burmester and Vassilis Chrissikopoulos
Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou, Piraeus, 18534, Greece; Department of Computer Science, Florida State University, 214 Love Building, Tallahassee, Florida 32306, USA; Department of Archiving and Library Studies, Ionian University, Old Palace Corfu, 49100, Greece.

Abstract: For an electronic election to be fully democratic there is a need for security mechanisms that will assure the privacy of the voters. With receipt-free electronic voting, a voter neither obtains nor is able to construct a receipt proving the content of her vote. In this paper we first consider the minimal requirements for receipt-free elections, without untappable communication channels between the voter and the voting authorities. We then propose a solution, which satisfies these requirements. This solution is based on an encryption blackbox, which uses its own randomness. Finally we present an implementation with smartcards, suitable for Internet voting.

1. INTRODUCTION

Electronic democracy refers to the use of Information & Communication Technologies (ICT) for communication between the politicians and citizens. In a representative democratic system, electronic elections (e-voting) constitute an important tool, which, if designed carefully, will strengthen the democratic substance of e-government. For an electronic election to be fully democratic, there is a need for security mechanisms that will assure the privacy of the vote.

In traditional elections, a voting booth does more than allow voters to keep their vote secret: it prevents vote-selling and coercion. Preventing such abuses in electronic voting schemes has been the subject of recent research. The notions of *receipt-freeness* and *uncoercibility* for electronic voting were introduced by Benaloh [1]. With the former the voters are convinced that their vote is counted without getting a receipt. With the latter the voters are not able to convince any other participant (e.g. a coercer) of the value of their vote. More specifically, in an

uncoercible voting scheme a voter neither obtains nor is able to construct a receipt that proves the content of her vote. While the concept of uncoercibility is stronger than receipt-freeness, the term “receipt-freeness” has been used in the literature as the prevalent expression to denote the security resulted by both the receipt-freeness and uncoercibility criterions.

Most electronic voting schemes sacrifice receipt-freeness at the cost of establishing correctness for the election results. In these schemes, voters get a receipt that will help them check the final tally. Note that this useful property, also known as *atomic* verifiability, is not met in current physical-based elections. An even more desirable property for electronic elections is *universal* verifiability (e.g. see [8]), which not only permits the voter to verify that the vote has been counted correctly, but also gives voters the means to verify that the election tally actually represents the "sum" of the votes cast. Current research is focused on receipt-free schemes that also establish universal verifiability.

All the receipt-free schemes [1-7] in the literature make some basic assumptions about the communication channel between the voter and the election authorities and about the voting process. These assumptions can be modelled by the following primitives:

- An *untappable channel*, from the voter to the voting authority [5, 6]. This channel models a one-way physical apparatus by which the voter can send a message to the authority. This message will be *perfectly* secret to all other parties (including the coercer).
- An *untappable channel*, from the voting authority to the voter [2, 3, 4]. This channel models a one-way physical apparatus, used by the voting authority to send a message to the voter. This message will be *perfectly* secret to all other parties (including the coercer).
- A *voting booth*, in which the voter casts the vote [1, 7]. This models a physical booth and guarantees the secrecy of the communication between the voting authority and the voter.

Several authors in the literature have pointed out the difficulty of implementing untappable channels. Hirst and Sako have recently stated that [4], “untappable channels from the authorities to the voters are the weakest physical assumption for receipt-freeness”. Such channels can also be quite cumbersome, particularly for large-scale voting with geographically distributed voters. For example, voters who abstain from elections because they find it inconvenient to go the polls, will find it equally inconvenient to cast their vote from a physically isolated voting booth in a dedicated computer network. Note that untappable channels will also force the voter to use specified voting locations.

Contribution/Organization. In this paper, we consider receipt-freeness in the presence of a coercer that can tap communication lines. In Section 2 we first define the minimal requirements for receipt-freeness and show that it can be achieved only

if the voter does not use any secret information, other than the vote itself. In Section 3 we propose a solution which uses an encryption blackbox to encrypt the votes in a verifiable way. Receipt-freeness is based on the difficulty of tampering with the blackbox. In Section 4 we present an implementation with a *tamper-resistant* smartcard, where receipt-freeness is achieved by distributing the voting procedure between the voter and the smartcard. This implementation is based on the voting scheme of Cramer-Gennaro-Schoenmakers [8], and is suitable for PCs and the Internet. Section 5 concludes the paper.

2. REQUIREMENTS FOR RECEIPT-FREENESS

Below we define the minimal requirements for an election scheme to be receipt-free without any assumptions on the untappability of the communication channels between the voter and the voting authorities.

2.1 Private and Authenticated Channels

It is clear that the vote should be encrypted, to achieve vote secrecy (private channel). Moreover, there should be an authenticated communication channel, which only the voter (and not the coercer) uses to submit the encrypted vote to the voting authorities. The control over this channel should at least involve a secret key that only the voter possesses. This could be for example a secret signature key or a biometric.

2.2 Knowledge of the Secret Decryption Key

If the secret decryption key is in the possession of the voter (as in [5, 6]), then receipt-freeness is lost: the key together with the encrypted vote (which the coercer can get by tapping the communication line) is a receipt. So the voter must not know the secret decryption key.

2.3 Knowledge of the Randomness

It is clear that some randomness must be used during the voting procedure, and in particular for the encryption of the vote. This is so because the adversary should not obtain any partial information about the vote given its encryption [9]. We examine three scenarios, based on which entity is aware of this randomness. The third scenario seems to be the only that offers a solution to our problem:

Randomness Chosen by the Voter. The voter chooses some randomness to encrypt her vote with a probabilistic encryption scheme [9]. This randomness may

be used later to lie against a coercer, as in the case of *deniable* encryption [10]. However, as shown in [4], the voter can use this randomness to construct a receipt, e.g., by using the hash of a pre-determined value. More dangerously, the coercer may have selected this randomness on behalf of the voter, and force the voter to use it (e.g. see [5]). Thus, a scheme in which the voter knows the randomness of the construction protocol is not receipt-free.

Randomness Chosen by the Voting Authority. Randomness may also be used by the voting authority, e.g., to shuffle the encrypted votes in a *mix-net* network [2, 4]. However, information about this shuffling must be secretly sent to the voter, and this cannot be done via an insecure channel: the coercer will eavesdrop on this channel. In this case, the untappable channel between the voter and the authority is inevitable.

Randomness Produced by an Encryption Blackbox. From the discussion above we see that while randomness is needed, neither the voter nor the authority must know this randomness. One way to achieve this is by using an Encryption Blackbox (EB) that uses its own randomness. The voter should not use the network facilities to communicate with the EB[1] (the coercer could tap the communication channels). Additionally, there should be a process, which produces some unpredictable randomness, i.e., a *beacon* [11]. This randomness will be used by the EB during the encryption. Finally the EB should be tamper-proof.

If a vote is encrypted in a way that the voter does not know the randomness used, then, before the vote is submitted to the voting authority, the voter must be given a proof of correctness of the encryption. This proof must be non-transferable; otherwise it may be used as a receipt for this vote. For this purpose we make use of *zero-knowledge* proofs.

2.4 Existence of a Virtual Booth

There should be a *virtual* voting booth, where the voter (and only the voter) interactively communicates with the blackbox. This booth is not necessarily physical: we only assume that, during the very moment of voting, the coercer does not observe the voter. Obviously, if voters use PCs to vote over the Internet, then there is no way to prevent the coercer from watching them while they vote. Our goal is not to prevent such attacks, but to prevent a voter from getting, or being able to construct, a receipt. The same assumption is made by all receipt-free schemes in the literature (except for [1, 7] where a physical voting booth is used), but it is made as an extra assumption to the untappability assumption.

3. A BASIC ELECTION SCHEME

Below we describe at high level, a basic receipt-free election scheme that satisfies all the minimal requirements described in Section 2. This scheme employs an Encryption Blackbox (EB) that uses its own randomness to encrypt the vote.

The election procedure has four distinctive phases: *Registration*, *Setup*, *Voting* and *Tallying*. During Registration, the Voter gets an EB, after being authenticated. The EB possesses the public encryption key of the Voting Authority.

During Setup, the Voter enters the virtual voting booth and interacts with the EB: the Voter first authenticates herself to the EB, and gives her input (her encrypted vote) to the EB, which encrypts this probabilistically, with the public key of the Voting Authority. The EB outputs this encryption and proves to the Voter in *zero-knowledge* (i.e., without giving away its randomness) that the encryption is correct.

During the Voting phase and given that the Voter is convinced of the correctness of the EB's encryption, the Voter signs the encrypted vote and uses an authenticated channel to submit this to the Voting Authority.

During the Tallying phase, the Voting Authority decrypts all encrypted votes and publishes the results.

Receipt-freeness. This is achieved because the coercer cannot tamper with the EB and access its randomness. The proof of correctness given to the Voter during the Voting phase has no off-line value to the coercer. Note that in this basic scheme, the Voting Authority is trusted not to conspire with the coercer. To prevent this we can use techniques from *threshold cryptography* [12] and distribute the Voting Authorities. In the next session, we will consider an implementation, which uses a smartcard instead of the Encryption Blackbox.

4. AN IMPLEMENTATION WITH SMARTCARDS

We present an implementation for which all the minimal requirements discussed in the previous section are satisfied, and receipt-freeness is established in a practical and affordable way. For this implementation, each voter uses a tamper-resistant smartcard that uses some pseudo-randomness to encrypt votes. Since tampering is not impossible (although extremely costly), we distribute the voting procedure between the voter and the smartcard to enhance security: the voter and the smartcard jointly contribute randomness for the encryption of the vote. Furthermore, the smartcard proves correctness of its actions to the voter in a non-transferable way. Communication between the Voters and the Voting Authorities takes place by means of a public broadcast channel with memory, namely a *bulletin board* (as in [8]).

Observe that a coercer cannot find the vote, without first getting the randomness of both, the voter and the smartcard. Even if the voter wishes to sell her vote, she cannot prove correctness without knowing the randomness of the smartcard (getting this randomness in this implementation is as hard as the Decision Diffie-Hellman problem-see Theorem 1).

This approach, if combined with a modified version of the Cramer-Gennaro-Schoenmakers election scheme [8], leads to an efficient receipt-free scheme for large-scale elections. For the proof of validity of the jointly encrypted votes we will use a 2-prover zero-knowledge proof (details are given in the Appendix).

The Election Scheme of Cramer-Gennaro-Schoenmakers. With this scheme [8] votes are encrypted by using an *homomorphic* version of the ElGamal cryptosystem [13]. The homomorhic aspect guarantees that the final tally is universally verifiable. Let p, q be large primes such that $q \mid p$-1, let G_q be the subgroup of Z_p^* of order q, and g, G be generators of G_q. Given a message $m \in Z_q$, the encryption of m is the ElGamal encryption of G^m with base g: that is $(x, y) = (g^a, h^a G^m)$, where $h = g^s$ is the public key, $s \in Z_q$ the secret key, and a a random element of Z_q. All operations are modulo p. For convenience we drop the operator mod p.

During the voting phase, the Voter encrypts her vote $v \in \{-1,1\}$ as the pair $(x, y) = (g^a, h^a G^v)$. The Voter constructs a proof that (x, y) encrypts $v \in \{-1,1\}$, and then publishes the encrypted vote and the proof on a Bulletin Board.

After the end of the voting period, the Voting Authorities "gather" all encrypted votes. They execute a (n,t) threshold decryption protocol [14] and jointly compute $G^T = Y / X^s$, where Y is the product of all y's, X is the product of all x's and T is the difference between the number of the yes-votes and the number of the no-votes. Here n is the number of Voting Authorities and t is an upper bound on the number of malicious Voting Authorities. Finally, the Voting Authorities determine T from G^T, by using $O(l)$ modular multiplications.

In the above scheme, vote secrecy is reduced to the *Discrete Logarithm* problem [15]. Furthermore, the decryption of the votes is correct and succesful even if up to t Voting Authorities are malicious or fail to execute the protocol.

4.1 Achieving Receipt-freeness

We modify the voting phase of the Cramer-Gennaro-Schoenmakers scheme, in order to achieve receipt-freeness, while maintaining security and efficiency. In this modification the encryption of the vote is distributed between the Voter and a Smartcard. The Voter, before getting a personal Smartcard, must register and be authenticated at a Registration Office. The Smartcard, which may be used for more than one elections, is provided with the certificate of the public signature key of the Voter. The Smartcard is also provided with the public encryption key of the

distributed Voting Authorities, and a secret signature key, with the corresponding certificate. The steps of the new protocol are presented in Figure 1.

Step (1): The Voter uses randomness $a_0, a_0' \in Z_q$ to ElGamal encrypt the two possible votes {yes, no}={+1, -1}, thus yielding $e(+1)$ and $e(-1)$. The Voter orders lexicographically these encryptions before submitting them to the Smartcard. This means that the Smartcard will not have any information on which encryption corresponds to which vote.

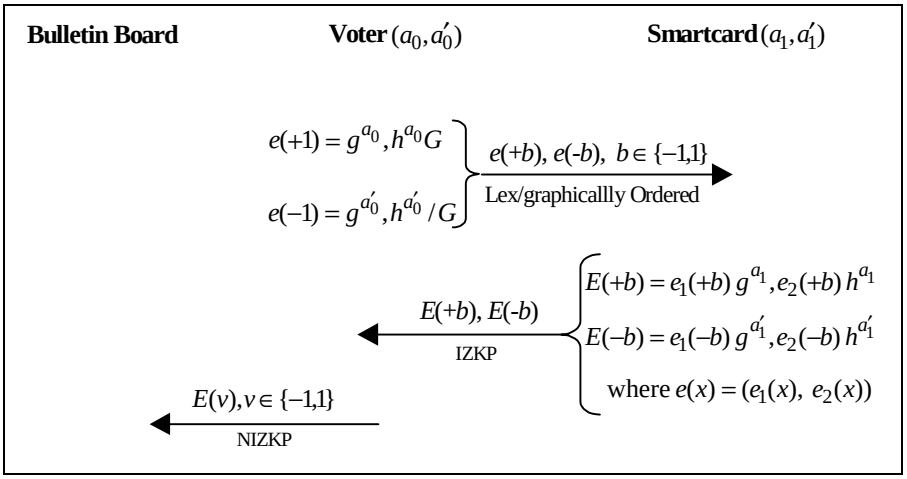

Figure 1. Voting with the use of a Smartcard

Step (2): The Smartcard chooses its own randomness $a_1, a_1' \in Z_q$ to create the final encryptions for the two possible votes, $E(+b)$ and $E(-b),\ b \in \{-1,1\}$. The encrypted votes are digitally signed by the Smartcard, for integrity. The Smartcard then outputs the encryptions to the Voter.

The Voter has to be convinced that the Smartcard has done things correctly, but without finding out the Smartcard's randomness. The proof has to be non-transferable. The Voter uses $E(+b), E(-b)$ and her knowledge of $e(+1), e(-1)$ to compute (g^{a_1}, h^{a_1}) and $(g^{a_1'}, h^{a_1'})$. If the Smartcard proves to the Voter that $\log(g^{a_1}) = \log(h^{a_1})$ and $\log(g^{a_1'}) = \log(h^{a_1'})$, then the Voter will be convinced that $E(+b)$ indeed encrypts $v = b$ and $E(-b)$ encrypts $v = -b$. The Smartcard can prove this in zero-knowledge, by using the *interactive* zero-knowledge proof (IZKP) of knowledge for equality of discrete logarithms, by Chaum-Petersen [16]. By its nature, the interactive zero-knowledge proof is not transferable. Even if the Voter records the exchanged messages, these messages do not have any "offline" value to a coercer. Thus, the Voter cannot use the transcripts of the proof to convince a coercer of her vote, even if the Voter wishes to sell her vote.

Step (3): The Voter decides which vote $v \in \{-1,1\}$ she will cast. For $E(v)$ to be valid, a proof of validity has to be constructed, i.e. that $E(v)$ encrypts $v \in \{-1,1\}$, without disclosing the vote *v*. This is necessary for *universal verifiability*. Such an interactive zero-knowledge proof, *jointly* executed by the Voter and the Smartcard, is presented in the Appendix. This can be converted to a non-interactive zero-knowledge proof (NIZKP) by using the Fiat-Shamir heuristic [17].

The Voter posts the encrypted vote $E(v)$ as well as the proof of validity, on the Bulletin Board. After the voting period ends, all encrypted votes will be decrypted by the Voting Authorities.

Theorem 1. *If the Decision Diffie-Hellman problem*[2] *is hard, the voting scheme above with a tamper-free smartcard is receipt-free.*

Proof. Suppose that the coercer and the Voter can prove that $E(v)$ is the encryption of the vote *v*. For example, that $E(v) = E(+1) = (g^{a_0 + a_1}, h^{a_0+a_1}G)$. Given that the Voter knows a_0, this reduces to proving that (g^{a_1}, h^{a_1}) is of the correct form, where a_1 is the Smartcard's randomness. Since $h^{a_1} = DH(g^{a_1}, h)$, this means that the Voter and the coercer jointly can solve the Decision Diffie-Hellman problem. The case for $v = -1$ is similar.

Remark 1. Our voting procedure could be generalized to multi-way voting, in which there are more than two votes (see also [8]).

5. CONCLUSION

With receipt-free electronic voting, a voter neither obtains nor is able to construct a receipt proving the content of her vote. In this paper we have considered the minimal requirements for receipt-free elections, without untappable communication channels between the voter and the voting authorities. We then proposed solutions that satisfied these requirements, and an implementation.

It is universally agreed that electronic voting will gain social acceptance in the years to come, especially Internet voting, despite several major security concerns. The use of tokens, such as smartcards, are also becoming more popular. Therefore we believe that our receipt-free voting scheme is consistent with the changes to come.

NOTES

1 An attentive reader will observe that the untappability assumption has not been completely removed. We assume that the “channel” between the Voter and the Encryption Blackbox is untappable.

2 The Diffie-Hellman operator DH is defined by $DH(g^a, g^b) = g^{ab}$, where g is a primitive element and the operations are modulo p. The problem of recognizing whether $z = DH(g^a, g^b)$, for a given $z \in \mathbb{Z}_p$, is called the *Decision Diffie-Hellman problem* [15].

ACKNOWLEDGEMENTS

This work is supported by the General Secretariat for Research and Technology (GSRT) of the Greek Ministry of Development.

REFERENCES

[1] Benaloh J, Tuinstra D. Receipt-free secret-ballot elections. Proceedings of the 26th ACM Symposium on the Theory of Computing; ACM, 1994; 544-553.
[2] Sako K, Killian J. Receipt-free mix-type voting schemes - a practical solution to the implementation of voting booth. Proceedings of EUROCRYPT '95, LNCS; Springer-Verlag, 1995; 921:393-403.
[3] Alpert D, Ellard D, Kavazovic O, Scheff M. Receipt-free secure elections 6.857 final project. 6.857 Network and Computer Security, 1998; http://www.eecs.harvard.edu/~ellard/6.857/final.ps.
[4] Hirt M, Sako K. Efficient receipt-free voting based on homomorphic encryption. Proceedings of EUROCRYPT 2000, LNCS; Springer-Verlag, 2000; 1807:539-556.
[5] Okamoto T. Receipt-free electronic voting schemes for large scale elections. Proceedings of Workshop of Security Protocols '97, LNCS; Springer-Verlag, 1996; 1163:125-132.
[6] Okamoto T. An electronic voting scheme. Proceedings of IFIP '96; Advanced IT Tools, Chapman & Hall, 1996; 21-30.
[7] Niemi V, Renvall A. How to prevent buying of votes in computer elections. Proceedings of ASIACRYPT '94, LNCS; Springer-Verlag, 1994; 917:141-148.
[8] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme. Proceedings of EUROCRYPT '97, LNCS; Springer-Verlag, 1997; 1233:103-118.
[9] Goldwasser S., Micali S. Probabilistic encryption. Journal of Computer and System Sciences 1984; 28:270-299.
[10] Canetti R, Dwork C, Naor M, Ostrovsky R. Deniable encryption. Proceedings of CRYPTO '97, LNCS; Springer-Verlag, 1997; 1294:90-104.
[11] Rabin M. Transaction protection by beacons. Journal of Computer Systems Science 1983; 27(2):256-267.
[12] Desmedt Y. Threshold cryptography. European Transactions on Telecommunications 1994; 22(6):449-457.
[13]ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 1985; IT-30(4):469-472.
[14]Pedersen T. A threshold cryptosystem without a trusted party. Proceedings of EUROCRYPT '91, LNCS; Springer-Verlag, 1991; 547:522-526.
[15]Diffie W., Helman M. New directions in cryptography. IEEE Transactions on Information Theory 1976; 22(6):644-654.

[16]Chaum D, Pedersen T. Wallet databases with observers. Proceedings of CRYPTO '92, LNCS; Springer-Verlag, 1993; 740:89-105.
[17]Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems. Proceedings of CRYPTO '86, LNCS; Springer-Verlag, 1987; 263:186-194.

APPENDIX

Our interactive zero-knowledge proof is a 2-prover modification of the proof in [8]. A flow diagram of the proof is sketched in Fig. 2. The common input is $E(v) = (x, y)$. The Smartcard's contribution to the proof of validity is given in Fig. 3. The Voter's contribution to the proof is given in Fig. 4. The proof of Completeness, Soundness and Zero-knowledge is similar to the one in [8].

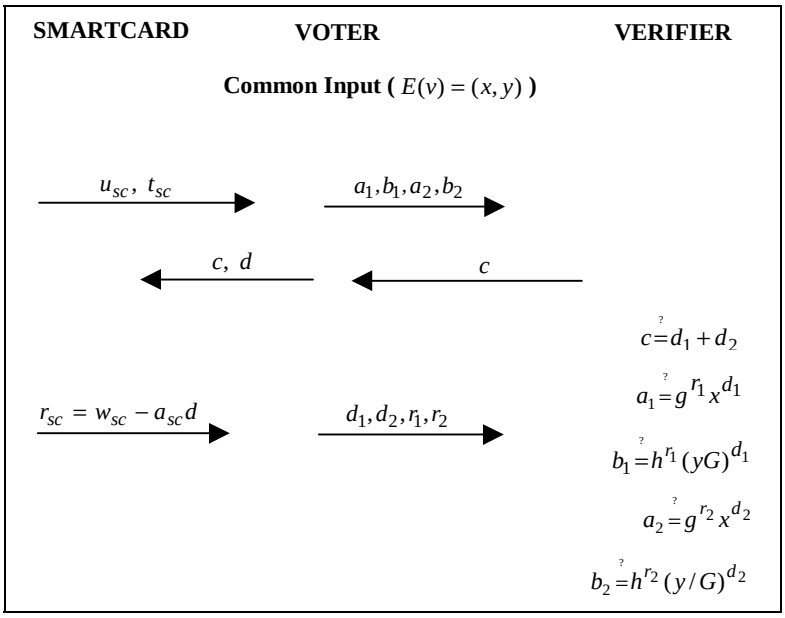

Figure 2. Proof of Validity for a Jointly Encrypted Vote

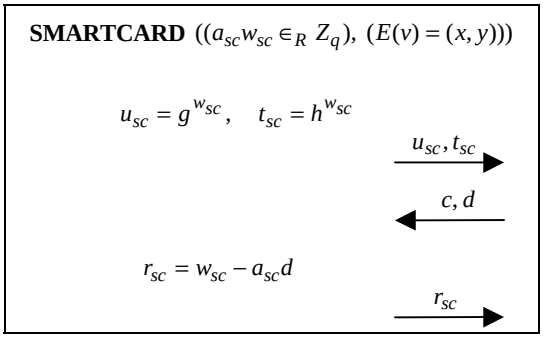

Figure 3. The Smartcard's Contribution to the Proof of Validity

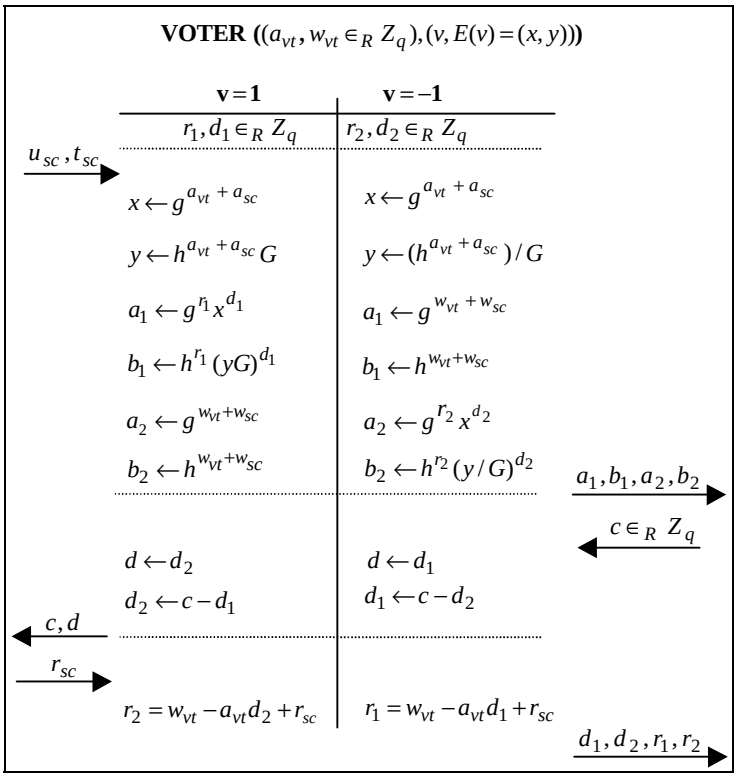

Figure 4. The Voter's Contribution to the Proof of Validity