OPTIMALLY EFFICIENT MULTI AUTHORITY SECRET BALLOT E-ELECTION SCHEME

[1]G. Anjan Babu, [2]Dr. M. Padmavathamma
[1]Lecturer in Computer Science, S.V. Arts College for Men, Tirupati, India
[2]Head, Department of Computer Application. S.V.University, Tirupati, India
Email: comp_mpv@svuniversity.in

ABSTRACT

An electronic voting scheme is a set of protocols that allow a collection of voters to cost their votes, while enabling a collection of authorities to collect votes, compute the final tally, and communicate the final tally that is checked by talliers. This scheme is based on the RSA and factoring assumptions. We apply the protocols of [CDS – 88] to Guillon – Quisqnater's identification protocol [GQ –88] to constant proofs of validity for ballots.

1. INTRODUCTION:

An electronic scheme is a set of protocols that allow a collection of voters to cost their votes, while enabling a collection of authorities to collect votes, compute the final tally, and communicate the final tally that is checked by talliers. In cryptographic literature on voting schemes, three important requirements are identified.

Privacy:

A system maintains privacy if:

1. Neither election authorities nor any one can link any ballot to the voter who cost it.
2. No voters can prove that he or she voted in a particular way.

Verifiability:

A system is verifiable if all voters can independently verify that their voters have been counted correctly without sacrificing privacy. In addition each voter must be able to verify the final results of the tally.

Robustness:

A system is robust if it ensures that all the system can recover from the faulty behavior of any (reasonably sized) location of parties.

The main contribution of this paper is presenting an efficient voting scheme that satisfies universal verifiability privacy and robustness.

2. OVERVIEW OF THE APPROACH

The parties in a voting scheme are modeled as probabilistic polynomial time process. Two means of communication are typically assumed to be available for these parties.

A bulletin board:

The communication model required for our election scheme is viewed as a public broadcast channel with memory, which is called a bulletin board. All the communications through the bulletin board is public and can be read by any party (including passive observers). No party can erase any information from the bulletin board.

Private channels:

To support private communication between voters and authorities. Fro this task any secure public key encryption scheme is suitable.

The parties of the voting scheme perform the following steps to execute an election. To cast a vote, each voter constructs a ballot as an encryption of the desired vote and post the ballot to the bulletin board. At his point, a proof of validity is also required that convinces all parties that the posted encryption contains a valid vote, without revealing it.

The auhorities, how ever, are able to decrypt the ballots (because of the extra information received from the voter through the private channel). In the end, the final tally is published together with some auxiliary information to enable universal verifiability.

More technically, universal verifiability is achieved by requiring the encryption function to be suitably homomorphic.

Central to our results is the way we achieve an efficient proof of validity for ballots. The proof of validity shows t any interested party that a ballot actually represent a vote e.g., that it either represents a yes or a no, and nothing else.

To maintain privacy for the voters, the general idea is to use some sort of zero – knowledge proof. The problem is however that ZK proofs usually require a large number of repetitions before the desired level of confidence is achieved. The efficiency of the whole scheme is influences by these proofs.

Our contribution now is two fold. We use a particular efficient homomorphic encryption scheme, based on q-th residuary assumption.

" a number is a q-th residue modulo n if there exists an α such that $\alpha^q = x \pmod n$", moreover , by applying the results from [CDS – 94] , the proof of validity is simple three – move – protocol which is witness indistinguisible (in fact , witness hiding as well). Instead of ZK proofs.

3. CRYPTOGRAPHIC PRIMITIVES

We implement our election based on q-th residuosity assumption.

"A number x is a q-th residue modulo n if there exists an α such that

$\alpha^q = x \pmod N$".

Homomorphic Encryption with Efficient Proof of Validity:

Initialization:

Initialized the parameters of the scheme are a modulus N, Which is a product of two large primes, a prime q with gcd (q, Φ (N))=1. Also an element $h \in Z^*_N$ - are available to all parties.

The fixed number h is not a q-th residue modulo N.

Encryption:

A participant encrypts V by choosing $\alpha \in_R Z_N$ and computes

$B \leftarrow \alpha^q h^v$.

Opening: A participant can later open B by revealing v and α. A verifying party then checks whether $B = \alpha^q h^v$ and accepts v as the encrypted value.

Homomorphic property:

Encryption is homorphic in the sense that; if B_1 and B_2 are encryptions of v_1 and v_2 respectively, then $B_1 . B_2$ is an encryption of $(v_1+v_2) \bmod q$.

Proof of knowledge for q-th residuosity: Using thenotations above, we present proof of knowledge for q-th residuosity, where by a proper shows possession of an $\alpha \in Z_q$ satisfying $x = \alpha^q$.

PROTOCOL –1

$[x= \alpha^{q}]$

Prover		**Verifier**
$W \in_R Z^*_N$		
$A \leftarrow w^q$		
	$\rightarrow a$	
		$C \in_R Z_q$
	$\leftarrow c$	
$r \leftarrow w \alpha^c$		
	$\rightarrow r$	
		$r^{q?} \equiv a\, x^c$

Figure- 1

Theorem: 1:

The above protocol is a three – more public coin proof of knowledge for q-th residuosity. The proof satisfies special sound ness and special honest verifier zero knowledge.

Proof: Special soundness now holds because for any two accepting conversations (a,r,r) and (a, c^1, r^1), $c > c^1$, it follows that $\left[\frac{r}{r^1}\right]^q = x^{c-c^1}$.

Since $0 < c - c^1 < q$, we have that there exist integers terms k, 1 such that

$(c - c^1)\, k = lq$.

Hence

$$\left[\frac{r}{r^1}\right]^{kq} = x^{k\,(c-c^1)}$$

$$= x^{lq}$$

$$\Rightarrow \left[\frac{r}{r^1}\right]^{kq} . x^{-lq} = x$$

$$\Rightarrow \left[\left(\frac{r}{r^{1}} \right)^{k} \right]^{q} = x$$

which is contradiction to the q-th residuosity assumption. Further more, by the result of [CDS – 94], the protocol of fig(2), in a proof of knowledge that a voter knows q-th residue of (Bh) or $\left[\frac{B}{h}\right]$. Thus the verifier learns that the voter knows α and v ∈ {1, -1} such that B = $\alpha^{q} h^{v}$ without obtaining any information about actual value of v.

Proof of validity: in our voting scheme to follow, it will be the case that a voter posts an encryption of a value v Є {1, -1}. To demonstrate that the encrypted value is indeed is {1, -1} without revealing it, the voter and the verifier execute the following efficient proof of validity.

PROTOCOL-2

VOTER		VERIFIER
V=1		V=-1
$\alpha , r_1, d_1, w_2 \in Z_q$		$\alpha , r_2, d_2, w_1 \in_R Z_n$
$B \leftarrow \alpha^{q} . h$		$B \leftarrow \alpha^{q} / h$
$a_1 \leftarrow r_1^{q} (Bh)^{-d_1}$		$a_1 \leftarrow w_1^{q}$
$a_2 \leftarrow w_2^{q}$		$a_2 \leftarrow r_2^{q} \left[\frac{B}{h}\right]^{-d_2}$
	$B, a_1, a_2 \rightarrow$	
		$C \in_R Z_n$
	$\leftarrow C$	
$d_2 = c - d_1$		$d_1 = c - d_2$
$r_2 = w_2 . \alpha^{d_2}$		$r_1 = w_1 . \alpha^{d_1}$
	$d_1, d_2, r_1, r_2 \rightarrow$	
		$d_1 + d_2 = c$
		$r_1^{q} \equiv a_1 (Bh)^{d_1}$
		$r_2^{q} \equiv \left[\frac{B}{h}\right]^{d_2}$

(Figure 2)

Verifiable secret sharing: To achieve robustness efficiently, non – interactive verifiable secret sharing, efficient solution for n out of n case is possible can apply.

Under the q-th residusity assumption, our election scheme satisfies universal verifiability, robustness and privacy.

4. SECRET BALLOT ELECTION SCHEME

We now present our main result, a secret ballot election scheme. The participant in the election scheme are n authorities. A_1, A_2,…., A_n and m voters V_1, V_2, ….V_m. The scheme works as follows: Each voter V_i prepares a vote by randomly selecting $b_i \in \{1,-1\}$. The voter first encrypts b_i by computing $B_i = \alpha_i{}^q . h^{b_i}$, *where* $\alpha_i \in Z_q$ is chosen randomly, and post B_i to the bulletin board. Subsequently b_i is considered as a secret which is to be shared among the authorities. The voter also posts proof (B_i). In the end the aggregate value $T = \sum_{i=l}^{n} b_i$ reduced module q represent the result of the election.

Ballot Construction and Vote costing : Each voter V_i posts $b_i \in \{1,-1\}$. In the following.

1. The voter randomly chooses $b_i \in \{1,-1\}$ and computes $B_i = \alpha_i{}^q . h^{b_i}$, the voter also computes proof of (B_i) also the voter computes.

   $B_{in} = (\alpha_{in})^q h^{b_{in}}$, $1 \le l \le n$
2. The voter posts B_i, proof (B_i), B_{i1}, B_{i2},…., B_{in} to the bulletin board.
3. All participants verify which the ballot B_i is correctly formed by checking proof of (B_i).
4. The voter chooses the shares (a_{ij}, b_{ij})

   Where $\prod_{j=l}^{n} a_{ij} = \alpha_i$

   $$\sum_{i=l}^{n} b_{ij} = b_i$$

   Sends (a_{ij}, b_{ij}) to the authority a_j using a private channel.
5. Each authority checks the received shares (a_{ij}, b_{ij}) by using that $(a_{ij})^q h^{b}{}_{ij} = B_{ij}$.

Tallying : Each authority A_j posts S_j, T_j and sends to the bulletein

$S_j = \prod_{i=l}^{m} a_{ij}$, $T_j = \sum_{i=l}^{n} b_{ij}$

Each tallier checks the share (S_j, T_j) posted by A_j by verifying that

$$S^q{}_j . h^{T_j} = \sum_{i=l}^{m} (B_{ij})$$

The final stage is the tally itself. Let us denote as A = {j | T_j is correct}. The tally is the interpolation of the polynomial and may be calculated as

$$T = \sum_{j \in A} T_j \prod_{l \in A\{j\}} \frac{l}{l-j}$$

We assume that in the successful election, the shares of every voter have been accepted by all authorities. i.e., all verification by

the authorities in the last step of the ballot construction is successful. In case an authority receives a false share, the authority may post the share so that any body can verify that share is not correct and that it corresponds to the posted encryption of step (4) in the ballot construction.

Theorem: 2 Under the q-th residuosity assumption , our election scheme saties universial verifiability, robustness and privacy.

Proof:

To prove universal verifiability, first note that only ballots are contact on account of theorem (1). Further the final tally is correct, if the step (2) of the tallying holds for all authorities. This deals with universal verifiability and robustness. The privacy property can easily prove from the fact that the secret sharing scheme used and the proof of validity (protocol) are information – theoretical scheme.

5. CONCLUSION

We have shown a very efficient scheme for secure election based on q-th residuosity assumption. The scheme satisfies well-known requirements privacy, universal verifiability and robustness.

REFERENCES

[1]. [BEN 87a] J. Benaloh. Cryptographic capsules**:** A disjunctive primitive for interactive protocols. In advances in cryptology – CRYPTO ’86, Volume 263 Of Lecture Notes In Computer Science, pages 213 – 222, BERLIN, 1987. Springer – Verlag.

[2]. [CDS-94] R.CRAMER, I. DAMGARD, AND B. SCHOENMAKERS.

[3]. Proofs of partial knowledge and simplified design of witness hiding protocols. In Advances In Cryptology – CRYPTO ‘94. Volume 839 of Lecture Notes In Computer Science, pages 174 – 187, BERLIN, 1994.Springer – Verlag.

[4]. [CFSY 96] R.CRAMER, M. FRANKLIN, B. SCHOENMAKERS AND M.YUNG.

[5]. Multi authority secret ballot elections with linear work. In Advances In Cryptology – EUROCRYPT ‘96, Volume 1070 of Lecture Notes In Computer Science, pages 72 –83, BERLIN, 1996. Springer – Verlag.