A Method and System for Tallying Encrypted Votes in an Electronic Voting System

This disclosure describes a method for reporting the results of an election after collecting encrypted votes from an electronic voting system.

Problem

Modern-day voting systems are moving away from the classical paper ballot method of voting and towards electronic voting machines. The use of electronic voting machines connected to a network allows for malicious parties to corrupt and/or change votes passing through the network. Therefore, there exists a need for a method of encrypting votes to avoid tampering, and a post-processing method to tally votes after being transmitted across a potentially insecure channel.

Detailed Description of the Invention

The proposed system would be comprised of two main components, a cluster of voting machines which communicate with a centralized tallying authority server through a network connection. Messages sent via this communication are strictly in a one-way manner from the voting machines to the tallying authority server. All messages are encrypted by means of an additively homomorphic encryption function to prevent tampering and allow privacy-preservation in vote tallying.

After registering voters, the tallying authority knows how many voters are participating in the election. This value is denoted by the value ***N***. The election itself has a total of ***M*** candidates. Each candidate choice is encoded in the voting machine to a numerical value corresponding to some integer base ***b*** raised to a designated exponent. An example of this configuration is as follows:

An election has ***N***= *5* voters and ***M*** = *3* candidates. Each candidate is encoded to the following values by the voting machine when they are chosen using the base ***b*** = *10*.

$$\text{Candidate 1} = 10^0$$
$$\text{Candidate 2} = 10^1$$
$$\text{Candidate 3} = 10^2$$

The voting machine then needs to encrypt the vote before sending it to the tallying authority. In order to correctly tally the votes, an ***additively homomorphic encryption algorithm*** must be chosen. A ***additively homomorphic encryption algorithm*** is one that has the following property:

$$\text{Decryption}(c_1 + c_2) = m_1 + m_2$$

or,

$$\text{Decryption}(c_1 \times c_2) = m_1 + m_2$$

In other words, the decryption of the sum of two encryptions of two different messages (known as ciphertexts) is equal to the sum of the original messages. There are many encryption algorithms in the literature that have this property - the most notable and practical being the Paillier Cryptosystem (http://link.springer.com/chapter/10.1007%2F3-540-48910-X_16). The voting machines encrypts the encoded values (as outlined above) for the votes using one of these algorithms and then sends them to the tallying authority which adds the encrypted votes together. The tallying authority then decrypts the sum of the encrypted vote values to obtain the sum of all the original encoded votes. The tallying agency can then factor this resultant sum to obtain the number of votes cast for each candidate as illustrated in the continuation of the example below:

Voter	**C1**	**C2**	**C3**	**Message**	**Ciphertext (using Paillier Cryptosystem)**
1	X			10^0	13039287935
2		X		10^1	9278648998
3			X	10^2	16008232463
4		X		10^1	4412140318
5			X	10^2	4941075705

The ciphertexts are then added or multiplied together (depending on the cryptosystem being used) and decrypted. In the example, all of the ciphertexts are sent to the tallying authority and are multiplied and the product is decrypted by the decryption algorithm of the cryptosystem. In this example, the product of the ciphertexts was evaluated (as dictated by the additive homomorphic property of the Paillier cryptosystem) and the product was decrypted to the value 221. The tallying authority is then able to factor this number as follows:

$$221 = 2 \times 10^0 + 2 \times 10^1 + 1 \times 10^0$$

From this factorization, the tallying authority can report that Candidate 1 received 1 vote, Candidate 2 received 2 votes, and candidate 3 received 2 votes.