December 3, 2007

Dear NIST,

We would like to introduce a new Voting Technology called “Retro-control”. This is the first method which combines full transparency with complete anonymity guaranteed and prevents from selling and buying one’s votes.

Below is an overview of the method, while details could be found in a patent description, patent application # PCT /RU2007 /000500. (see http://www.retro-control.narod.ru/eng/html/solution.html).

Provided, there is an electronic voting system we propose to equip it with a printing device and adjust the software so that the screen before one casts a vote shows his/her unique identity code which is on the screen until the voter finishes his/her voting session.

After that the screen shows the list of nominees for the voter to choose from and vote for.

The printing device then prints out a document for the voter that we call “voter certificate” or simply “certificate”. The differences between a ballot paper and a certificate are outlines below:

a) A voter keeps a certificate with himself/herself instead of casting it into a ballot box.

b) To the right from nominee names printing devise inserts the identity codes of various voters into each line of the certificate but not into the only one. The line which is corresponding to the voter choice is inserted with a code visible on the screen. The rest of lines are inserted with different codes of the real voters who took their votes earlier.

For example, if a voter is coded 2201 with his/her vote for the Republican Party, his/her certificate would look as follows (in case a voter is unique within a ballot district):

Democratic Party	0112
Republican Party	2201
Socialistic Party	0943
Green Party	1118

Numbers 0112, 0943 and 1118 are codes of unknown voters who voted for democratic, socialistic and green party accordingly. Once the voter is given the certificate, he/she ascertains that his/her code 2201, which has been shown on screen, is the same as that in the second line of the certificate standing for

Republican Party. After that the code disappears from the screen and a voter leaves the ballot station with certificate.

It is then proposed to publish the returns in codes like in above example so that a voter using his/her certificate could control both his/her vote and those of other unknown voters whose codes are shown in the certificates. Each discrepancy should be document supported, corrected and, perhaps, repaid for to the voter that found a discrepancy. Showing the certificate with discrepancies to any authority, a voter does not disclose his/her vote, because one can not prove that the identity code in the line with discrepancy belongs to him/her.

In this way, a voter has a document to be able to question the returns, if the data in his/her certificate are not completely the same as in officially published code returns. Moreover, one can not sell and buy votes using this kind of certificate. It is impossible to define with this document the choice of the voter, because only original recipient knows his/her identity code, therefore, the seller cannot prove that he/she voted as required by the buyer, thus, making no sense in the deal.

Our method is an opportunity to control one's own vote for those who did not take a vote. For this purpose we propose to publish the list of voters who has taken their votes with so arrangement by address that it guarantees anonymity for voters who has taken and has not taken theirs votes. If the quantity of the voters in one apartment is nil, or it is equal to the quantity of the voters so the information on this address can not be published separately. It can demonstrate the choice of voters who took the vote or who didn't take. This address should be combined in the list with neighbor apartment. If the combined sum after two apartments is equal neither to nil nor the total quantity of the voters it can't be defined who personally took the vote and who didn't. There can be many combinations of addresses. It can be the quantity of the voters within the story or within the entire house or few houses. It is easier for the neighbors to exchange the information and check the authenticity of the address list of the voter quantity.

Because the total quantity of the voters must be equal to the quantity of the voters in the list of code returns then it's enough to make sure after returns publication. Nobody can accuse in falsification of the factious votes neither election committee nor electronic system designers.

If there is no centralized electronic system of the voting we propose to create simplex electronic system of the local scale when using "Retro-Control".
It consists of usual computers with printing devise. It is desirable to combine the computers in the Local Network but it is enough to use the diskette for the computer exchange. To follow the principle of secret ballot the monitor of the computer should be covered with pyramid-shaped housing. There is an eyehole on the top of the pyramid and it is the voter who may see the screen picture. The voter can make a choice with the help of the electronic pointing

devise for example the mouse. The rest procedure doesn't differ from the one described above.

For the voting at home and at the remote locations it is advisable to use portable computers instead of ballot box. The screen of such computer also should be hidden from the extraneous eyes with curtains for example. If there is a portable printing devise so the certificate is printed automatically. If there is no devise the certificate should be filled in by the present member of the election committee manually. In this case the voter should memorize his/her code and press the button. After it the code should be erased and one can see the image of his/her certificate with the lines filled in. Then the screen can be seen and all codes are written down in the certificate manually.

If there is no possibility to use the computers at polling place (it is a very rare situation nowadays) we propose to use so called voting counter. It is the isolate cabin with the cashier one of the members of the committee inside. The voting counter is equipped with the observation eyehole. It is only the voter who can see from outside the process of voting inside. Instead of the computer mouse the choice is made with the pointing devise for example the fescue available outside the voting counter. The cashier acts as a computer algorism. He defines the code of the voter at random; cumulates code returns; fills in the certificates manually and gives this paper thru the extending window.

The results of the voting can be published at the Internet and be sent thru mobile telecommunication system, by means of sms short message service. But
it is easy for the voter to get the lists of code returns and addresses of the voters from the election district by regular mail as a newspaper. Besides, local press contains the election returns tables of each district; the regional press the election returns tables of all districts; central press the election return tables of all region (province). So it is easy to check if the returns in tables were counted wrong. Thus, each voter can buy three newspapers (local, central and regional) after the election to make sure if:

1) the district returns were included correctly into central ones;
2) the central returns were included correctly into regional ones;
3) the regional returns were included correctly into general returns.
So each voter can control every stage of elections.

As a conclusion let's get back to the advantages of our method.

1. As we proved before the system of poll is getting more transparent but the anonymity provides the freedom of choice and the secret ballot principle. It is advantage of the method. If the voters control the election returns the possibility of sporadic errors in counting and malicious falsification of the results are expelled. Whatever small the break between winners and loser of the elections within the new system people may not worry because the loser party has to find honest the victory in even one vote or to prove the opposite.

2. Besides the practical aspects there are moral and personal ones. The right and possibility to control your own vote is the development of the civil rights and freedoms. It brings the moral value to each citizen which must be developed.

3. Public affair and social significant advantages of the “Retro-control” system come from the situation when it is impossible to accuse without adducing any proof or just to suspect somebody in falsification of the election returns. It follows that the legitimacy and authority of the person or party elected are getting higher and the social concord is becoming stronger.

4. The party or a person elected thru the “Retro-control” method will be granted the prestige on the international arena and the whole country will be accepted as an advanced country with the democratic elections system.

5. Nowadays many designers of the electronic elections system have to make their inventions more transparent for control. Sometimes they have to provide the primary codes of the software. Because when one relies on the honesty of the designers the scholars believe that the possibility of coup d’etat exists. However the more transparent the system is the more possible this system can be exposed to the unauthorized break-in. The “Retro-control” method solves this problem drastically. When the voters can control their votes there is no need to control the electronic system organization. The protection from the outer break-in is the prerogative of the system designers and they will get the right and responsibility to protect the system anywise and to blackout its organization.

6. The proposed system of the view thru the eyehole gives the possibility to the watchers to control even the fingers movements of the voter. So the sharp voter can’t make a picture of his/her choice on the cell phone camera to sell his vote then.

With best regards,
the designer of the “Retro-control” method
Zulin A.M.
Ul. Soyuza Respublik 17-15
Barnaul, Russia, 656038