Abstract

The purpose of this study is to prevent fraud in elections by developing digital stamps. Traditional stamps are used to print vote in a ballot in elections all over the world. Those stamps usually print YES (да in Russian, Evet in Turkish) with ink in a ballot. In developing and underdeveloped countries frauds happen in elections. Digital and encrypted stamp setup can solve fraud problem. This type of digital stamp will print 'yes', 'current time', 'unique stampID' for each vote. In addition, different combination of 'a list of numbers and letters' like a bitcoin address will be printed next to them. This vote code will be different for each printing. This vote code will be generated by embedded cpu and encryption algorithm in embedded setup with in the digital stamp. So a hashed identifier is printed for each voting. Already, there are products that print timestamps on a paper. But they do not solve the problem since a copy of a product can easily be produced. This study will provide a digital stamp which produce unique, validatable vote code, and this vote code can be checked from a webpage. Hashing and validation processes of encryption technologies will be used. Thus a combination of traditional voting and digital voting will be applied against fraud in election.

Definition of Problem

Governments usually create a special stamp for every election. However those stamps are not unique and stamping time cannot be found. Thus three major problems occur.

First, a stamp cannot be differentiated from other stamps. That is, you cannot find out which stamp is used by looking a stamped ballot. Even cheaters can produce the stamps and use them.

The second is, malevolent officers can make rigging by using stamps. That might be done by stamping bulks of empty ballots and putting them to ballot box (google search: Russian election rigging, Russian election fraud, Turkish election fraud). Moreover, an officer can change a valid vote to invalid vote by stamping other candidates in the same ballot. For example, suppose an officer opens a ballot box and separated votes of candidate A. Then the officer used the stamp to print Yes on Candidate B and Candidate C in the separated ballots. Than all the votes become invalid.

Lastly, pre-stamped ballots can be put in ballot boxes. For example, in a newspaper it was written that a factory owner distributed pre-stamped votes to his workers and ordered that bring me empty ballot from voting panel and put the given ballot to ballot box.

Product specification

Instead of traditional ink powered stamps, digital and encryption supported stamps will be used with below specifications:

1) This digital stamp will print current date and product number in a paper with one press. Products with those capabilities exist in the market. What this study will add those capabilities will be explained in later.
   http://hathawaystamps.com/st-rapid.html
   https://www.amazon.com/dp/B00006IBFR?aaxitk=nnDAMIF1gBwTiG.biKkfUQ
   https://www.youtube.com/watch?v=0gpn1Y4OQkQ
   https://www.youtube.com/watch?v=wOJytxlvoEA

2) Each digital stamp's time is defined in production and it cannot be changed. A separate and dedicated battery will be used for timer. So even the battery of the stamp runs out, the timer still runs perfectly.
3) The stamp design will have its own embedded microprocessor and memory. Each microprocessor will be unique for each stamp. The processor or memory cannot be changed. If the case of stamp is opened the circuit will make itself unusable again. In other words, if some one tries to open the case neither timer nor printing will work.
4) This is the functionality that makes this product unique, and what is applied for patent. Encryption will be applied to generate a barcode for each press. This code can be used to check if the stamping is valid. Any one can write the code to a website date and time will be displayed for each barcode. Note that I am not an encryption expert. I found two major way to provide this functionality. Since the encryption has infinitely many ways just like all other information technologies, other encryption methods can be applied. My new idea is just applying barcode (just like bitcoin address) for each stamping to validate vote. Here I will provide two methods.
   a. The first way is using encryption and decryption method. Known as Advanced Encryption Standard (AES). In this method each digital stamp has its own embedded, and unchangeable encryption algorithm function. Lets say we are using ssh1 algorithm for product with productID 1000
      Ssh1 (timestamp, productID) will produce a unique hash.
      This website used encryption and decryption:
      http://md5decrypt.net/en/Sha1/
      For the date: 12.01.2018 18:30:45 it will produce.

Sha1(12.01.2018 18:30:45, 1000) = **d7b26caf165d10019384e8df9d15df18a8020733**

Of course this is just explaining fundamental basics. This is a predictable algorithm. I will add secret variables and secret formulas. Those secret 'salt' variables and formulas will be different for each product. Lets say for product 1000 we have Xa1 in beginning and English name of (month+1) at the end. So we have December+1=January at the end. And lest put a formula to make hash unpredictable Formula might be month^2 +(day*3)-first base of second. This formula will produce 12^2+(1*3)-4=144+3-4=143

Put all together:

Sha1(Xa1, 12.01.2018 18:30:45, 1000, January, 143) = **f4f13526d1b70988b330ab0b89535f600fbc9481**

Our website database will store each function for each of the product in encrypted way. Any one can reach the website and writes the hash result, writes productID and validate if the hash is generated from the product.

The web site will show Stamp date=12.01.2018 18:30:45, ProductID=1000 for the hash=

f4f13526d1b70988b330ab0b89535f600fbc9481

Another validation approach can be writing time and productID and generating hash from the webpage. The web page can be used for dates smaller than current day. So in the second approach the user writes 12.01.2018 18:30:45 and 1000. Then hash address will be generated at the webpage. The user will compare hash result of the web page and hash result on the pager.

In order to prevent brute force cracking different algorithms and randomly changing functions can be used. A cryptology expert and an embedded system developer can guide or even I research those topics deeply and provide an unbreakable solution.

b. This method will use public key – private key or asymmetric cryptography approach just like bitcoin or litecoin. In this method each product will have a unique randomly generated private key. Those private keys cannot be found by anyone. The private key will be stored in the processor of the product and on the website. On the website data base private key will be stored in encrypted way so no one can read even they hack data base of website. From the private key, date, and productID a public key will be generated by using a complex asymmetric function. This public key, date and productID can be used in the website to validate the public key. In the website success or fail message will be displayed. Just like sending bitcoin to a bitcoin public address. Note that this way might require a bit more processing power.

https://en.wikipedia.org/wiki/Public-key_cryptography

Conclusion

Digital stamps can solve fraud problems in elections in developing countries. A stamp, which prints current date and time, yes, productID and a hash verifies that the date and time the stamp is used. Thus the stamp cannot be used before or after voting time, cannot be copied and can be validated from a webpage. Moreover, if a stamp is used to print bulk vote, say just 20 seconds between two votes of the same stamp, it will be obvious, because timestamp will be on the vote.

In fact, this method is neither completely digital nor traditional. Note that there are startups, which use computers as voting pane and blockchain as storing the votes. But this approach combines the both traditional and digital voting. Thus it is easy to adopt since nothing is changed for the voters. In other words, voters do not need training.