Security Technologies for Voting Processes

Mirosław Kutyłowski

Wrocław University of Technology

Warsaw 2013

Motto

Impact of electronic processing on voting processes

- direct and indirect costs
- correctness
- efficiency

The impact might be both positive and negative

- e.g. spending any amount of money on software verification does not guarantee that it is secure
- on the other hand one can design a system so that any fraud by the computer will be detected

Homomorphic encryption

main properties

- anybody can encrypt - no secret key necessary
- decryption requires secret key or keys
- **one can add encrypted numbers by multiplying the ciphertexts**

$$Enc_{key}(k_1) \cdot Enc_{key}(k_2) = E_{key}(k_1 + k_2)$$

Application of homomorphic encryption

1. local election authorities A, B, C compute the number of votes k_A, k_B, k_C in their constituency
2. ... and encrypt them getting, respectively $E(k_A)$, $E(k_B)$, $E(k_C)$
3. ... and then publish the ciphertexts
4. the ciphertexts get multiplied, the result e equals

$$E(k_A) \cdot E(k_B) \cdot E(k_C) = E(k_A + k_B + k_C)$$

5. central voting authority decrypts e and publishes the voting result $k_1 + k_2 + k_3$

Application of homomorphic encryption

1. k_A, k_B, k_C
2. $E(k_A)$, $E(k_B)$, $E(k_C)$
3. multiplication
4. decryption
5. result $k_A + k_B + k_C$

Advantages and consequences

1. it is not necessary to publish k_A, k_B, k_C
2. useful if the number of voters small and revealing k_A,k_B, k_C might endanger voter's privacy
3. anybody can check correctness of multiplication result
4. decryption process may be performed so that its correctness can be checked without the private key

Anonymous voter's identification

Goals of identification

- only a voter admitted to cast a vote
- no voter can cast a valid vote twice

problem: lack of participation is sometimes also a way of casting a vote

identification and recording voters on a list breaks voters' privacy
...but can we do anything about it?

Restricted identification

M.Kutyłowski

new techniques for electronic identity documents

1. a smartcard holds a single secret key
2. card authentication proves that this is a valid id card of a citizen
   – an undeniable cryptographic proof presented
3. the card may generate only one anonymous password for a concrete election
   – one cannot vote twice
4. vote selling would require borrowing personal id card
5. one cannot link the passwords from different elections

Defense against computers

M.Kutyłowski

a computer can be hacked and reveal some information

- can we fully protect computers? no!
- is it a hopeless situation? no!

idea of a protocol

how to encrypt a number x so that a computer does not know what is encrypted?

- choose y at random
- compute $z = x + y$ manually
- encrypt z on the computer and send the ciphertext per internet
- make a call and tell y (no voIP!)

Conclusions

- for many problems we cannot provide a satisfactory solutions
- . . . but in some cases we may achieve a lot at a surprisingly low price

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl
2. http://kutylowski.im.pwr.wroc.pl
3. +48 71 3202109, +48 71 3202105
   fax: +48 71 3202105