A Note on a Secure Voting System on a Public Network

M. G. Karagiannopoulos, M. N. Vrahatis
Department of Mathematics, University of Patras Artificial Intelligence Research Center (UPAIRC), University of Patras, GR-26110 Patras, Greece

G. C. Meletiou
Technological Educational Institute (TEI) of Epirus, GR-47100 Arta, Greece; University of Patras Artificial Intelligence Research Center (UPAIRC), University of Patras, GR-26110 Patras, Greece

This article shows that the procedure proposed in Chang and Wu (1997) and extended in Dini (2001) does not always produce accurate results. A modification that makes the procedure correct is suggested. © 2004 Wiley Periodicals, Inc.

Keywords: secure voting; electronic voting; voting protocols

1. NONINVERTIBILITY OF THE ENCRYPTION PROCESS

We point out that the encryption process of [1, 2] is not invertible. This becomes evident through the following, illustrative, example.

In accordance with Chang and Wu's [1] protocol, let us assume that there are n eligible voters $U_1, \ldots, U_n$, participating in the election. Further assume that the Voting Center chooses a prime number P, for example $P = 31$, and a primitive element $e = 7$ over $GF(31)$, and publicizes them.

Based on the above assumptions we describe the voting phase. The purpose of this phase is to support the casting of votes and the secure encryption and decryption of ballots. Assume that the Voting Center's {*private, public*} key pair is $(x_0, y_0) = (5, 5)$. Let the Voter's voting strategy be $V_i = 6$. In accordance with the Chang and Wu protocol, the following steps have to be performed:

STEP 1. U_i chooses a random number r_i, for example, $r_i = 3$.

STEP 2. U_i calculates the cipher quantities $C_{i,1}$, $C_{i,2}$ as follows:

$$C_{i,1} = e^{r_i} \bmod P$$

$$= 7^3 \bmod 31 = 2.$$

$$C_{i,2} = y_0^{r_i} \oplus V_i \bmod P$$

$$= 5^3 \oplus 6 \bmod 31 = 30.$$

Next, U_i encrypts the message $\{a_i, C_{i,2}\}$, where a_i is the identification tag that has been sent to the voter U_i by the Voting Center, using a public key cryptosystem. Then, U_i sends the ciphertext to the Voting Center.

STEP 3. The Voting Center decrypts the above ciphertext and acknowledges that the information has been received, by publishing the value $C_{i,2}$.

STEP 4. U_i encrypts and sends the other message $\{a_i, C_{i,1}\}$, following the same procedure.

STEP 5. The Voting Center decrypts the above message and publishes $\{C_{i,2}, C_{i,1}\}$.

STEP 6. U_i recasts his/her ballot, using a different r_i' by repeating Steps 1–5 prior to the expiration of the deadline for casting ballots.

STEP 7. Voting Strategy Recovery:

$$V_i = C_{i,1}^{x_0} \oplus C_{i,2} \bmod P$$

$$= 2^5 \oplus 30 \bmod 31$$

$$= 32 \oplus 30 \bmod 31$$

$$= 62 \bmod 31 = 0 \neq 6.$$

Due to the fact that the transformation considered is not

Received July 2002; accepted December 2003
Correspondence to: M. N. Vrahatis; e-mail: vrahatis@math.upatros.gr

invertible, it is not possible to recover the voting strategies. Because XOR is a symbolic operation, it is incompatible with arithmetic modulo P.

Having tested the protocol on a number of examples considering a wide range of parameters, we witnessed incorrect results. Occasionally, a correct result was obtained, but it tended to be the exception to the rule. Next, we suggest modifications to overcome this shortcoming.

2. PROPOSED MODIFICATION

To render the encryption process invertible, it suffices to change the ciphertexts in Steps 2 and 7 to the following ones:

$$C_{i,2} = (y_o^{r_i} \bmod P) \oplus V_i \text{ and}$$

$$V_i = (C_{i,1}^{x_0} \bmod P) \oplus C_{i,2}.$$

The reason why we decided to change the encryption and decryption processes is the operation over $GF(P)$. We need to abandon the $GF(P)$ group and continue our operations using Boolean algebra, or binary strings, due to the fact that the XOR operation is not compatible with arithmetic modulo P, as previously mentioned.

Acknowledgments

We would like to thank the editor and the referees for their useful remarks and suggestions.

REFERENCES

[1] C.C. Chang and W.B. Wu, A secure voting system on a public network, Networks 29 (1997), 81–87.

[2] G. Dini, Electronic voting in a large-scale distributed system, Networks 38 (2001), 22–32.