PhD Subject in Computer Science:
Formal Verification of E-voting Protocols

Verimag

October 23, 2007

Supervisor: P. Lafourcade
Contact: Pascal.Lafourcade@imag.fr
Also a master degree subject

1 Context

In the last few years, formal analysis of cryptographic protocols has become classical. Many formal methods exist or are still being designed for automatic verification of security properties such as secrecy or authentication [11][3][1] [2][4][2], aiming in the end at proving concrete protocols actually are secure. Here, we focus our analysis more specifically on voting protocols [2][3]. In such protocols, a kind of secrecy and authentication is required to guarantee the secret of one vote and authentication of the voter. But some more complex properties have to be achieved by voting protocols like for instance the property that nobody, except the voter himself, can link one vote to his voter. One usual method developed in voting protocols is to use a homomorphic encryption (see [5] for a survey). A homomorphic encryption scheme has the following property:

$$\prod \{v_i\}_k = \{\sum v_i\}_k$$

The product of encrypted messages with the same key is equal to the encryption of the sum of the messages.

2 Goals

The first goal of this work is to list existing e-voting protocols using homomorphic encryption from the state of the art. From this list, the student should understand which properties are consequences of this homomorphic property.

The second phase of this study is to perform an automatic formal analysis for homomorphic encryptions. We strongly expect that existing methods based on constraints and resolution of equations systems can be extended to analyze this specific property [3].

*http://www-verimag.imag.fr*
*http://www-verimag.imag.fr/~plafourc*
The last phase of this work consists in proposing a first draft of formal definition of these properties for voting protocols. Some recent results have been obtained in this direction [10, 1], but many properties have not been formally analyzed yet.

3 Bibliography

References


