

PhD Subject in Computer Science: Computational Analysis of Homomorphic Encryption

Verimag*

October 23, 2007

Supervisor: P. Lafourcade¹
Contact: Pascal.Lafourcade@imag.fr
Also a master degree subject

1 Context

With internet and electronic devices recent explosion, cryptography is everywhere around us. The aim of this area is to secure different applications using mathematical problems that are proven hard according to complexity theory. Computational analysis tries to classify the security level of these encryption schemes, by testing the robustness of the scheme w.r.t. keeping information secret (OneWayness, Indistinguishability Non-Malleability) against different adversaries (CPA, CCA1, CCA2) modeled by Probabilistic Turing Machines (see [1] for a clear overview).

Among all existing encryption schemes we focus on encryption schemes called homomorphic [3, 6, 11, 10, 9, 4, 7, 2], for they have 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. This kind of encryption schemes are for instance used in voting protocols [8, 5].

2 Goals

The first task is to list all encryption schemes with the homomorphic property and to look at the level of security they achieve according to the literature.

According to various existing results, the student will try to propose attacks or security proofs for homomorphic encryption schemes to refine the analysis of their security level.

The second phase of this work consists in proposing generic computational analysis for a homomorphic scheme independently of the way it is designed. The

*<http://www-verimag.imag.fr>

¹<http://www-verimag.imag.fr/~plafourc>

goal is to find a kind of class of encryption scheme with the same security level based on the homomorphic property.

3 Bibliography

References

- [1] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO '98: Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, pages 26–45, London, UK, 1998. Springer-Verlag.
- [2] J. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret sharing. In *Proc. Advances in Cryptology (CRYPTO'86)*, volume 263 of *Lecture Notes in Computer Science*, pages 251–260, Santa Barbara, California, USA, 1987. Springer-Verlag.
- [3] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
- [4] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Proc. 14th Annual International Cryptology Conference (CRYPTO'94)*, volume 963 of *Lecture Notes in Computer Science*, pages 174–187, Santa Barbara, California, USA, 1994. Springer-Verlag.
- [5] R. Cramer, M. K. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret-ballot elections with linear work. In *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'96)*, volume 1070 of *Lecture Notes in Computer Science*, pages 72–83, Zaragoza, Spain, 1996. Springer-Verlag.
- [6] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proc. Advances in Cryptology (CRYPTO'84)*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18, Santa Barbara, California, USA, 1985. Springer-Verlag.
- [7] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.
- [8] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In *EUROCRYPT*, pages 539–556, 2000.
- [9] D. Naccache and J. Stern. A new public-key cryptosystem. *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'97)*, 1233:27–37, 1997.
- [10] T. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In *Proc. International Conference on the Theory and Application*

of Cryptographic Techniques (EUROCRYPT'98), volume 1403, pages 308–318, Helsinki, Finland, 1998. Springer-Verlag. Lecture Notes in Computer Science.

- [11] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'99)*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238, Prague, Czech Republic, 1999. Springer-Verlag.