UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA "RENATO M. CAPOCELLI"

CORSO DI DOTTORATO IN
"TEORIE, METODOLOGIE E APPLICAZIONI AVANZATE PER LA COMUNICAZIONE,
L'INFORMATICA E LA FISICA"
XI CICLO – NUOVA SERIE

ANNO ACCADEMICO 2011-2012

TESI DI DOTTORATO IN INFORMATICA

On the Generalizations of Identity-Based Encryption

Hidden Vector Encryption and Inner-Product

Tutor
prof. **Carlo Blundo**

Candidato
Angelo De Caro

Coordinatore
prof. **Giuseppe Persiano**

Abstract

Today public-key cryptographic is widely deployed and successfully used but still a major drawback exists. In fact, from encrypted data a party can either decrypt or cannot learn anything at all about the message other than intentionally leaked information such as its length. In the recent years, the cloud computing paradigm has emerged as the new standard to use computing resources, such as storage devices, that are delivered as a service over a network. In such a scenario, the notion of public key cryptography is not enough. It would be desirable to specify a decryption policy in the encrypted data in such a way that only the parties who satisfy the policy can decrypt. In a more general form, we may want to only give access to a function of the message, depending on the decryptor's authorization.

Thus, in the last decade researchers have started looking at a more sophisticated type of encryption called *functional encryption*. A *functionality* F is a function $F : K \times M \to \Sigma$ where K is the *key space* and M is the *message space*. In the public-key setting, a functional encryption scheme for F is a special encryption scheme in which, for every *key* $k \in K$, the owner of the master secret key msk associated with the master public key mpk can generate a special secret-key sk_k that allows the computation of $F(k, m)$ from a ciphertext of $m \in M$ computed under public key mpk. In other words, whereas in traditional encryption schemes decryption is an all-or-nothing affair, in functional encryption it is possible to finely control the amount of information that is revealed by a ciphertext. One of the most notable example of functional encryption is *identity-based encryption* first introduced by Shamir as an alternative to the standard notion of public-key encryption.

In this thesis, we discuss several instantiations of function encryption that can all be seen as generalisations of identity-based encryption. We improve on previous constructions in terms of performance and security guarantees.