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

Attualmente, la cifratura a chiave pubblica è ampiamente diffusa e utilizzata con successo in svariati ambiti. Ciononostante, alcuni svantaggi esistono. Infatti, dalla cifratura di un messaggio, il ricevente può estrarne l'interno messaggio o imparare nulla sul suo contenuto se non quello che intenzionalmente viene rilasciato dal testo cifrato. Negli ultimi anni, il paradigma del *cloud computing* sta emergendo come nuovo standard per l'utilizzo di risorse computazionali, come unità di calcolo e supporti di archiviazione, che sono offerte come servizi all'interno di una rete di calcolatori. In tale scenario, la nozione di cifratura a chiave pubblica mostra i suoi limiti. Infatti, sarebbe desiderabile poter specificare una politica di decifratura all'interno della cifratura di un messaggio in modo che solo le parti che soddisfano tale politica possano decifrare. In forma più generale, si vuole dare accesso solo ad una certa funzione del messaggio cifrato in base alle autorizzazioni che si posseggono.

Per questo motivo, nell'ultimo decennio i ricercatori hanno cominciato ad interessarsi ad un tipo più sofisticato di cifratura chiamato *functional encryption*. Una *funzionalità* F è una funziona $F : K \times M \rightarrow \Sigma$ dove K è lo *spazio delle chiavi* e M è lo *spazio dei messaggi*. Uno schema functional encryption per F è uno speciale schema di cifratura nel quale, per ogni *chiave* $k \in K$, il proprietario della *master secret key* msk associate alla *master public key* mpk può generate una speciale chiave segreta sk_k che consente il calcolo della funzione $F(k, m)$ a partite da una cifratura di $m \in M$ calcolata rispetto alla chiave pubblica mpk. In altri termini, in uno schema functional encryption, è possibile controllare minuziosamente il tipo e la quantità di informazioni che sono rilevato dalla cifratura di un messaggio. Uno dei più famosi esempi di functional encryption è *identity-based encryption* introdotto da Shamir come alternative alla classica nozione di cifratura a chiave pubblica.

In questo lavoro di tesi, discuteremo di diverse incarnazioni di schemi functional encryption, tutti riconoscibili come generalizzazione di identity-based encryption. In particolare mostreremo nuove costruzioni, di funzionalità già note in letteratura, che offrono vantaggi in termini di prestazioni e livelli di sicurezza garantiti.