**UNIVERSITÀ DEGLI STUDI DI SALERNO**

# DIPARTIMENTO DI INFORMATICA "RENATO M. CAPOCELLI"

DOTTORATO DI RICERCA IN INFORMATICA

XIII CICLO


# ABSTRACT

## *ID-Based Key Agreement for WANETs*

**Coordinatore:**
Prof. Giuseppe Persiano

**Candidato:**
Francesco Rossi

**Tutor:**
Prof. Alfredo De Santis

**Co-tutor:**
Prof. Giovanni Schmid

**ANNO ACCADEMICO 2013/2014**

# Abstract

L'interesse crescente per le wireless ad hoc networks (WANETs) è dovuto alle loro caratteristiche fondamentali non possedute dalle reti tradizionali, come la mobilità dei nodi, la capacità delle rete di auto organizzarsi e configurarsi senza l'ausilio di un'infrastruttura fissa. Le WANETs possono essere utilizzate in molteplici scenari, tra cui applicazioni sanitarie, monitoraggio ambientale, applicazioni militari e molte altre applicazioni commerciali.

Sfortunatamente, l'accessibilità del canale di comunicazione espone le WANETs ad un gran numero di minacce, tra cui (e.g. jamming, eavesdropping, node replication, unfairness, wormhole, packet injection). La loro sicurezza dipende dall'autenticazione dei nodi, che da un punto di vista crittografico, può essere ottenuta tramite meccanismi di distribuzione delle chiavi su base identità. Inoltre, le comunicazioni tra i nodi delle WANETs richiedono spesso l'instaurarsi di chiavi simmetriche di sessione, che possono essere utilizzate per la cifratura, l'autenticazione di messaggio ed altri algoritmi crittografici.

In questa tesi presentiamo un nuova libreria crittografica, denominata JIKA (Java framework for ID-based key agreement) che simula un key generation center (KGC) e offre un servizio di distribuzione delle chiavi su base identità usate per schemi di firma e protocolli di key agreement. Inoltre, JIKA usa la crittografia su curve ellittiche (ECC) che consente calcoli veloci, chiavi di piccole dimensioni e firme corte dei messaggi.

JIKA include due nuovi schemi di firma su base identità (IBS-1 and IBS-2) che ottengono firme corte, un protocollo di key agreement per due parti su base identità (eFG) e due nuovi protocolli di key agreement gruppali (GKA v1 and GKA v2). I due nuovi protocolli di key agreement gruppali sono full-contributory e offrono autenticazione di chiave implicita attraverso gli schemi di firma su base identità citati sopra, al costo di due comunicazioni di gruppo. Tali protocolli inoltre offrono resilienza contro attacchi passivi e attivi eseguiti da avversari esterni. Per simulare l'esecuzione degli algoritmi proposti sui nodi di una WANET, abbiamo eseguito dei test su un dispositivo Raspberry PI. Tale dispositivo supporta adattatori wireless standard che possono essere usati per la configurazione di un nodo attraverso settaggi opportuni. Gli stessi test sono stati eseguiti su un Personal Computer in maniera tale da comparare i risultati sperimentali ottenuti su piattaforme con diverse risorse computazionali. I risultati sperimentali mostrano che i nostri algoritmi offrono prestazioni migliori di altri algoritmi equivalenti noti in letteratura. In particolare i protocolli di group key agreement richiedono un basso costo computazionale considerando anche un gran numero di parti coinvolte, anche su dispositivi con risorse limitate come i Raspberry PI.