Protection Against the IMSI Catchers Using Identity Based Crypto in 5G

Mohsin Khan and Valtteri Niemi

University of Helsinki, Department of Computer Science,
P.O. Box 68 (Gustaf Hällströmin katu 2b)
FI-00014 University of Helsinki
Finland
{mohsin.khan,valtteri.niemi}@helsinki.fi

Abstract.

1 Introduction

2 Public key cryptography against IMSI catchers

Here we use public key cryptography which may or may not be based on identity based crypto to secure the privacy of the long term identity of a mobile phone user called IMSI (International mobile subscriber identity). We discuss different techniques of using the public key cryptography:

1. Identity based crypto based on the identity of SN where the HN is the key generator
2. HN assigned public private key pair for each SN
3. HN owned public private key pair

In the consequent sections we describe the aforementioned techniques in further detail.

3 Based on Identity of Serving Network

In this technique the HN has a public and private key pair. Every phone knows the public key of the HN. Whenever a SN asks the phone to provide its IMSI, the phone computes the public key of the SN using the public key of the HN. Then the phone encrypts the IMSI with the computed public key of the SN and sends it to the SN along with the HN identity. The SN obtains (possibly already have obtained) its private key from the mentioned HN. Using this private key, the SN can decrypt IMSI. Figure **??** represents the high level protocol.

3.1 Concerns and Solutions

1. How to provision, revoke and re-provision the public key of HN in the phone?
2. How to black list a SN?