

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 H  llstr  min 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 of the serving network serves as the public key. And the SN obtains corresponding private key from the HN using a secure channel
2. Every serving network is given a public and private key pair by the HN
3. The HN owns the public and private key pair.

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

2.1 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 ID. The SN obtains (possibly already have obtained) its private key from the mentioned HN. Using this private key, the SN can decrypt IMSI.

2.2 Based on HN generated public private key pair for every SN

3 Conclusion

4 Acknowledgement

References