Privacy and mutual authentication under temporary state disclosure in RFID Systems

Ferucio Laurențiu Țiplea[1], Cristian Hristea[2], Bulai Rodica [3]
[1] "Alexandru Ioan Cuza" University of Iasi, Romania, ferucio.tiplea@uaic.ro
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy, Romania, cristi.hristea@gmail.com
[3] Technical University of Moldova, rodica.bulai@ati.utm.md

Privacy and mutual authentication are two significant requirements for real-life applications of RFID schemes. These two requirements have been studied for a long time only for adversaries that cannot corrupt the temporary internal state of the tags. Recently, however, it has been shown that corrupting the temporary internal state of the tag is practically possible. This raises the question: do the current RFID protocols that ensure mutual authentication and privacy keep these properties in the temporary state disclosure model? The answer is negative and thus it justifies the effort to propose new RFID protocols that are secure under temporary state disclosure.

In this paper, we amply discuss how temporary state disclosure affects mutual authentication and privacy of RFID protocols, and illustrate this on two well-known protocols. We argue then in favor of using the PUF technology in order to achieve mutual authentication and a reasonable enough level of privacy under temporary state disclosure. We close by presenting two RFID schemes that achieve destructive privacy, one of the most important levels of privacy in the context of the physical corruption of tags.