Attack against RFID transponders * †

Tibor Radványi[a], Csaba Bíró[b], Sándor Király[c], Péter Szigetváry[d], Péter Takács[e]

Eszterházy Károly College
[a] radvanyi.tibor@ektf.hu
[b] birocs@aries.ektf.hu
[c] ksanyi@aries.ektf.hu
[d] szigipet@aries.ektf.hu
[e] takip@aries.ektf.hu

Abstract

In this article we are dealing with the connections between nowadays most dynamically improving automatic identification-related RFID technology and cryptographic algorithms. You are going to be introduced to the possibilities of RFID system attacks and the ways to defeat them. We also dwell on the suitable and non-suitable cryptographic algorithms among the well known and frequently used ones. The type of the RFID tag highly influences the group of the suitable algorithms. The size of the tag's integrated memory matters a lot, as well as the fact that it uses its own intelligence or we are working with a cheap passive tag.

Keywords: RFID, cryptography, data security

MSC: 68M01, 90B18, 94A860, 68P25

*Csaba Biro, Sándor Király, Péter Szigetváry, Péter Takács research was supported by: FutureRFID – Development possibilities in the RFID / NFC technology TÁMOP-4.2.2.C-11/1/KONV-2012-0014

†Tibor Radványi's research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP-4.2.4.A/ 2-11/1-2012-0001 'National Excellence Program'.