XII CONGRESSO DE INICIAÇÃO CIENTÍFICA DA UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

PROPEX
PRÓ-REITORIA DE PESQUISA
E EXTENSÃO

PIBIC/CNPq-UFCG 2015

IMPLEMENTAÇÃO DE FUNÇÕES HASH PARA USO EM ETIQUETAS RFID

Daniel Xavier Silva[1], Bruno Barbosa Albert[2]

RESUMO

Nesse projeto de iniciação científica pretende-se estudar e implementar funções hash universais em no contexto de aplicações de segurança envolvendo a tecnologia RFID. A quantidade de portas lógicas que uma etiqueta de um dispositivo RFID pode conter é limitada, principalmente, pelo baixo custo a que se propõe. Como consequência, a etiqueta possui uma limitada capacidade computacional e isso limita os esquemas de segurança que podem ser adotados. Como as funções hash fazem parte dos esquemas de segurança dos sistemas RFID, é necessário que sua implementação utilize algoritmos com o mínimo número de portas lógicas. Nossa abordagem consiste no estudo e aplicações de uma família de funções hash chamadas de NH e de suas variações de modo a se adequar as limitações da tecnologia.

Palavras-chave: RFID, Funções Hash Universais, Segurança.

HASH FUNCTIONS IMPLEMENTATIONS TO USE IN RFID TAGS

ABSTRACT

In this research project aims to study and implement universal hash functions in the context of security applications involving RFID technology. The amount of logic gates that a tag of RFID device is limited mainly by the low cost that it's proposed. As a result, the tag has a limited computational capacity and it bounds the security schemes that can be adopted. As long as hash functions are part of the RFID systems security schemes, it is necessary for its implementation use algorithms with the minimum number of logic gates. Our approach is the study and application of a family of hash functions NH calls and their changes in order to adapt the technology limitations.

Keywords: RFID, Universal Hash Functions, Security..

[1]Aluno doCurso de Engenharia Elétrica, Departamento de Engenharia Elétrica, UFCG, Campina Grande, PB, e-mail: daniel.silva@ee.ufcg.edu.br
[2]Engenharia Elétrica, Professor Doutor, Departamento de Engenharia Elétrica, UFCG, Campina Grande, PB, e-mail: albert@dee.ufcg.edu.br