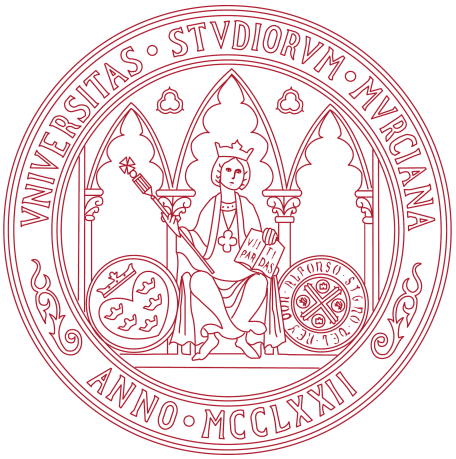
PRUEBAS DE CONOCIMIENTO CERO Y SUS APLICACIONES

JOSÉ LUIS CÁNOVAS SÁNCHEZ

Tutores
LEANDRO MARÍN MUÑOZ
ANTONIO JOSÉ PALLARÉS RUIZ



Facultad de Matemáticas
Universidad de Murcia

José Luis Cánovas Sánchez: *Pruebas de Conocimiento Cero y sus Aplicaciones,* Junio 2017

RESUMEN

TODO

Short summary of the contents in -English- Spanish... a great guide by Kent Beck how to write good abstracts can be found here:

https://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html

ABSTRACT

1500 words of Introduction in English...

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTINGS

ACRONYMS

1

INTRODUCCIÓN

2 PRELIMINARES

2.1 PRELIMINARES DE ÁLGEBRA

Teoría necesaria de grupos y anillos

2.2 PRELIMINARES DE ALGORITMIA ?

Teoría de complejidad algorítmica, problema de P NP, problema RSA de factorizar N, problemas de decisión, estadística usada en el estudio de los ZKP (*ensembles*), *probabilistic computations*, ...

La mayor parte está en los primeros capítulos de Fundamentals of Computer Security, y de sus referencias se podrá sacar más detallado.

3

RESIDUOS CUADRÁTICOS

Teoría de símbolos de Lebesgue, ..., residuos cuadráticos, cálculo de raíz discreta?

4 PRUEBAS DE CONOCIMIENTO CERO

4.1 DEFINICIÓN

4.2 ESTUDIO DE ZKPS

Una subsección por cada ZKP analizado.

5 APLICACIONES DE ZKP

?

Aplicación de ZKP en los certificados de Idemix. Analizar cómo realizan pruebas de Y, O, etc.

6 IMPLEMENTACIONES

?

Implementaciones de símbolos, raíz discreta, ZKPs, ...

APPENDIX

A

CÓDIGO FUENTE

Listing 1: A floating example (`listings` manual)

```
for i:=maxint downto 0 do
begin
{ do nothing }
end;
```

BIBLIOGRAFÍA

[1] Jon Bentley. *Programming Pearls*. 2nd. Boston, MA, USA: Addison–Wesley, 1999.

[2] Robert Bringhurst. *The Elements of Typographic Style*. Version 4.0: 20th Anniversary Edition. Point Roberts, WA, USA: Hartley & Marks Publishers, 2013.

[3] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest y Clifford Stein. *Introduction to Algorithms*. 3rd. Cambridge, MA, USA: The MIT Press, 2009.

[4] Gunter Dueck. *Dueck's Trilogie: Omnisophie – Supramanie – Topothesie*. http://www.omnisophie.com. Springer, Berlin, Germany, 2005.

[5] Donald E. Knuth. "Computer Programming as an Art". En: *Communications of the ACM* 17.12 (1974), págs. 667-673.

[6] Donald E. Knuth. "Big Omicron and Big Omega and Big Theta". En: *SIGACT News* 8.2 (1976), págs. 18-24.

[7] Ian Sommerville. *Software Engineering*. 10th. Boston, MA, USA: Addison-Wesley, 2015.

[8] Nassim Nicholas Taleb. *Antifragile: Things That Gain from Disorder (Incerto Book 3)*. New York, NY, USA: Random House, 2012.

DECLARACIÓN DE ORIGINALIDAD

Yo, José Luis Cánovas Sánchez, autor del TFG PRUEBAS DE CONOCIMIENTO CERO Y SUS APLICACIONES, bajo la tutela de los profesores Leandro Marín Muñoz y Antonio José Pallarés Ruiz, declaro que el trabajo que presento es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas.

Murcia, Junio 2017

José Luis Cánovas Sánchez