UNSL (Argentina) UFMG (Brasil)

Optimización de un Protocolo Dining Cryptographers Asíncrono

Tesis

Maestría en Ingeniería de Software (UNSL)
Mestrado em Ciência da Computação (UFMG)

Autor:

Ing. Pablo Marcelo García

Directores:

Jeroen van de Graaf, PhD. (UFMG)
Dr. Germán Montejano (UNSL)

- 2013 -

Optimización de un Protocolo Non-Interactive Dining Cryptographers

Autor:
Ing. Pablo Marcelo García.

Directores:
Jeroen van de Graaf, PhD.
Dr. Germán Montejano.

Texto impreso en San Luis
Noviembre, 2013

A Gilda, Agustina e Ignacio

Reconocimientos

- A mi esposa Gilda y a mis hijos Agustina e Ignacio, por apoyarme incondicionalmente, aún cuando esta tesis incluyó una estadía de un año en el ámbito de la Universidade Federal de Minas Gerais (UFMG) en Belo Horizonte, Brasil.

- A mi Director, Jeroen van de Graaf. por su enorme tarea como orientador, pero más por la contención recibida desde el punto de vista humano.

- A mi Co-director, Germán Montejano, por su apoyo permanente y sobre todo por la confianza depositada en mi persona.

- Al Dr. José Monteiro da Mata, aporte fundamental desde la logística durante toda mi estadía en Belo Horizonte.

- A los Dres. Roberto Uzal y Daniel Riesco, quienes junto con Germán Montejano son permanentes generadores de oportunidades para los estudiantes e investigadores.

- A la Lic. Silvia Bast (FCEyN − UNLPam), por sus pertinentes sugerencias, producto de una profunda revisión de todo el contenido del presente documento.

- Al Msg. Rubén Pizarro (FCEyN − UNLPam), por sus importantes aportes en lo referido a temas de análisis numérico.

- A la Doctora Marina Lattanzi y la Licenciada María Paula Dieser (FCEyN − UNLPam), por sus valiosos comentarios sobre los contenidos del capítulo 5.

- Al Dr. José Marcos Silva Nogueira, Director del Departamento de Ciencias de la Computación (DCC) del Instituto de Ciencias Exatas (ICEX) de la Universidad Federal de Minas Gerais (UFMG), y por su permanente apoyo durante mi estadía en Belo Horizonte.

- A Renata Viana Moraes Rocha, Secretária do Programa de Pós-Graduação em Ciência da Computação - ICEx - UFMG, por su disposición y amabilidad para atender todas mis consultas durante mi estadía en Belo Horizonte.

- Al Dr. Carlos Camarao, quien con enorme amabilidad guió mis primeros pasos en la UFMG.

- A los docentes a cargo del curso de Posgrado de UFMG *"Projeto e Analisse de Algoritmos*": Dr. Luiz Chaimowicz, Dr. Wagner Meira Jr., Dra. Giselle Lobo Papa y Dra. Jussara Almeida, por acompañar con enorme comprensión mi proceso de adaptación.

- A Norma Beatriz Pérez, querida amiga con quien compartimos muchos momentos en Belo Horizonte

- A Aclyse Mattos, mi entrañable compañero de apartamento durante toda mi estadía en la Moradía Universitaria de la UFMG.

- A todo el personal de la Moradía Universitaria de la UFMG, dependiente de la Fundación Mendes Pimentel.

Pablo Marcelo García

Resumen

Dining Cryptographers es un esquema criptográfico presentado por Chaum en [11] cuya característica más notable es la de proveer nivel incondicional de seguridad para la privacidad de los mensajes publicados por un grupo de usuarios de una red, elemento que otorga al modelo un altísimo nivel de interés para múltiples aplicaciones criptográficas. En ese grupo se puede incluir el voto electrónico.

El esquema original exige la concurrencia online de los participantes. Sin embargo, existen múltiples situaciones prácticas en las que esta condición no necesariamente se cumple. En consecuencia, y atendiendo a la riqueza del esquema original, en [48] se presenta una derivación denominada *Non Interactive Dining Cryptographers (NIDC)*. Esta variante busca explotar todo el potencial de la propuesta original de Chaum, pero intentando cubrir un rango más amplio de problemas a los que el esquema pueda aplicarse.

El presente trabajo tiene por objetivo central proponer técnicas concretas de optimización para dos puntos específicos del modelo NIDC:

- El primer punto se refiere a mejorar el manejo de las colisiones que se producen en el esquema original, basado en un arreglo de slots, capaces de almacenar información. La elección de los mismos por parte de los participantes es necesariamente aleatoria para garantizar el anonimato. Por lo tanto, las colisiones son posibles y su aparición implica la pérdida de todos los datos que coincidan en la elección. Se analiza el tema en profundidad y se propone un nuevo esquema de canales paralelos que permite una utilización mucho más eficiente del espacio destinado a este fin, en base a propiedades de los sucesos independientes.

- El segundo punto propone mejorar las técnicas utilizadas para combatir los intentos de fraude. El esquema original de Chaum advierte sobre la importancia de este punto y pone especial énfasis en determinados detalles que deben ser cuidadosamente observados; el trabajo de van de Graaf ([48]) propone un modelo que garantiza un nivel de seguridad incondicional pero a costa de una importante ineficiencia por utilizar un esquema basado en la utilización de bit commitments con XOR (BCX). Este modelo, que será analizado en profundidad en el capítulo 4, exige varias operaciones para cada bit de información, lo cuál genera un nivel de ineficiencia importante. Se propone, en consecuencia, un modelo basado en logaritmos discretos y compromisos de Pedersen, los cuales proporcionan un nivel similar de seguridad con una mayor eficiencia.

Se presenta, además, un análisis de la aplicación del modelo a aplicaciones de voto electrónico y se analiza la relación entre esta propuesta y los trabajos de Broadbent y Tapp ([7] y [8]) y Bos ([2]).