Multimed Tools Appl
https://doi.org/10.1007/s11042-017-5293-6

Counting-based secret sharing technique for multimedia applications

Adnan Gutub[1] · **Nouf Al-Juaid**[2] · **Esam Khan**[3]

Received: 9 July 2017 / Revised: 1 October 2017 / Accepted: 5 October 2017

Abstract Secret Sharing is required in situations where access to important resources has to be protected by more than one person. We propose new secret-sharing scheme that works based on parallel counting of the ones within the shares to generate the secret output. Our work presented two different modeling variations that are mainly different in the secret-sharing keys generation where both are studied elaborating their pros and cons. Our counting-based secret shares key reconstruction is implemented and simulated considering the security level required by the usage functions. Comparisons showed interesting results that are attractive to be considered. This secret sharing method is of great benefit to all multimedia secret sharing applications such as securing bank sensitive accounts and error tracking, voting systems trust, medical agreements, wills and inheritance authentication management.

Keywords Secret sharing · Key management · Shares generation · Information security · Key distribution technique

1 Introduction

Due to the increase demand on information technology and multimedia communication, information security is being very important aspect. Many techniques have been

✉ Adnan Gutub
aagutub@uqu.edu.sa

Nouf Al-Juaid
naljuaid@su.edu.sa

Esam Khan
eakhan@uqu.edu.sa

[1] Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia

[2] Shaqra University, Riyadh, Saudi Arabia

[3] The Custodian of Two Holy Mosques Institute for Hajj and Umrah Research, Umm Al-Qura University, Makkah, Saudi Arabia

Published online: 02 November 2017

Adnan Gutub is currently working as Professor in Computer Engineering Department specialized in Information and Computer Security within Umm Al Qura University (UQU), Makkah -Saudi Arabia.

His experience was gained from his previous long-time work in Computer Engineering Department at King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran, Saudi Arabia. He received his Ph.D. degree (2002) in Electrical & Computer Engineering from Oregon State University, USA. He had his BS in Electrical Engineering and MS in Computer Engineering both from KFUPM, Saudi Arabia.

Adnan's research interests involved optimizing, modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has some work in modeling architectures for RSA and elliptic curve crypto operations. His current interest in computer security also involved steganography such as image based steganography and Arabic text steganography.

In summer 2013, Adnan has been awarded 3-month visiting scholar grant in collaboration with Purdue University, West Lafayette, Indiana, USA. He had been involved in research of current studies related to Arabic Text Steganography in Data Security as well as Elliptic Curve Crypto Processor Designs. He then completed parts of this research work in summer 2015 visiting University of California Santa Barbra. He had been involving his work in discussion ideas and outcomes relating to them and their exploration within the information security field as overall ultimate research as well as opening-up new ideas with Crypto-Code (a focus research group at University of California Santa Barbra) making his specific scientific investigation internationally recognized.

Previously, Adnan have been twice awarded the UK visiting internship for 2 months of summer 2005 and summer 2008, both sponsored by the British Council in Saudi Arabia. The 2005 summer research visit was at Brunel University to collaborate with the Bio-Inspired Intelligent System (BIIS) research group in a project to speed-up a scalable modular inversion hardware architecture. The 2008 visit was at University of Southampton with the Pervasive Systems Centre (PSC) for research related to text steganography and data security.

Administratively, Prof. Adnan Gutub filled many executive and managerial academic positions at KFUPM as well as UQU. At KFUPM - Dhahran, he had the experience of chairing the Computer Engineering department (COE) for five years until moving to UQU - Makkah in 2010. Then, at UQU - Makkah, Adnan Chaired the Information Systems Department at the College of Computer & Information Systems followed by his leadership of the Center of Research Excellence in Hajj and Omrah (HajjCoRE) serving as HajjCoRE director for around 3-years until the end of 2013. Then, he was assigned his previous position as the Vice Dean of the Custodian of the Two Holy Mosques Institute of the Hajj & Omrah Research, within Umm Al Qura University (UQU), Makkah - Saudi Arabia.

Nouf Al-Juaid is a Teacher Assistant at Shaqra University, Shaqra, Saudi Arabia. She obtained Master of Sciences (MS) degree in Computer Sciences & Engineering, at Umm Al Qura University (UQU) fully sponsored by Shaqra University under the umbrella of Ministry of Higher Education. Her MS program at UQU is specialized in the information security track offered by the College of Computer and Information Systems offered at UQU-Makkah Campus, Saudi Arabia. In 2010, Nouf completed her Bachelor of Sciences (BS) degree with honors from Taif University Saudi Arabia. Nouf followed her BS studies by pursuing a higher diploma degree in education also from Taif University completed by the end of 2011. She, then, worked as official trainers at the Saudi Institute of Taif for around a year, i.e. until 2012, were she has been employed by Shaqra University as Graduate Teaching Assistant in the field of computing. At Shaqra, Nouf was assigned to teach introduction to computer science course classes as well as MATLAB classes based on her strong background and experience with programming languages such as MATLAB, Java, C++, PHP, and her outstanding ability to work with some databases like Oracle and SQL Nouf research capability started by her BS graduation project about multimedia medical records in radiology department using techniques of expert systems. Then, in her MS studies at UQU, she worked on building a program that is reconstructing permutations from differences sequence, which was a project related to the graduate course of analysis of algorithms. After, completing her tenure of her scholarship at UQU, she had been assigned the vice role of Computer Department Chairman at Shaqra University. Nouf Al-Juaid research interest focused on Computer and Information Security include Cryptography, Steganography, Cyber Security, Network Security, Networks, Artificial Intelligence, Image Processing, and Expert Systems.

Esam Khan is currently the vice dean of academic affairs at the Custodian of the Two Holy Mosques Institute for Hajj and Umrah Research, Umm Al-Qura University, Makkah, Saudi Arabia. He is an assistant professor in computer engineering. He received his B.Sc. in Computer Engineering (first class honor) in June 1999, and his M.Sc. in Computer Engineering in June 2001, both from the Department of Computer Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. He received his PhD in Electrical and Computer Engineering in November 2005 from the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada. His M.Sc. thesis was about compression techniques of testing data. His Ph.D. dissertation was about hardware implementation of hash functions. His research interests include security and cryptography, and applications of information technology in Hajj and Umrah. He published several journal and conference papers in the areas of his research.