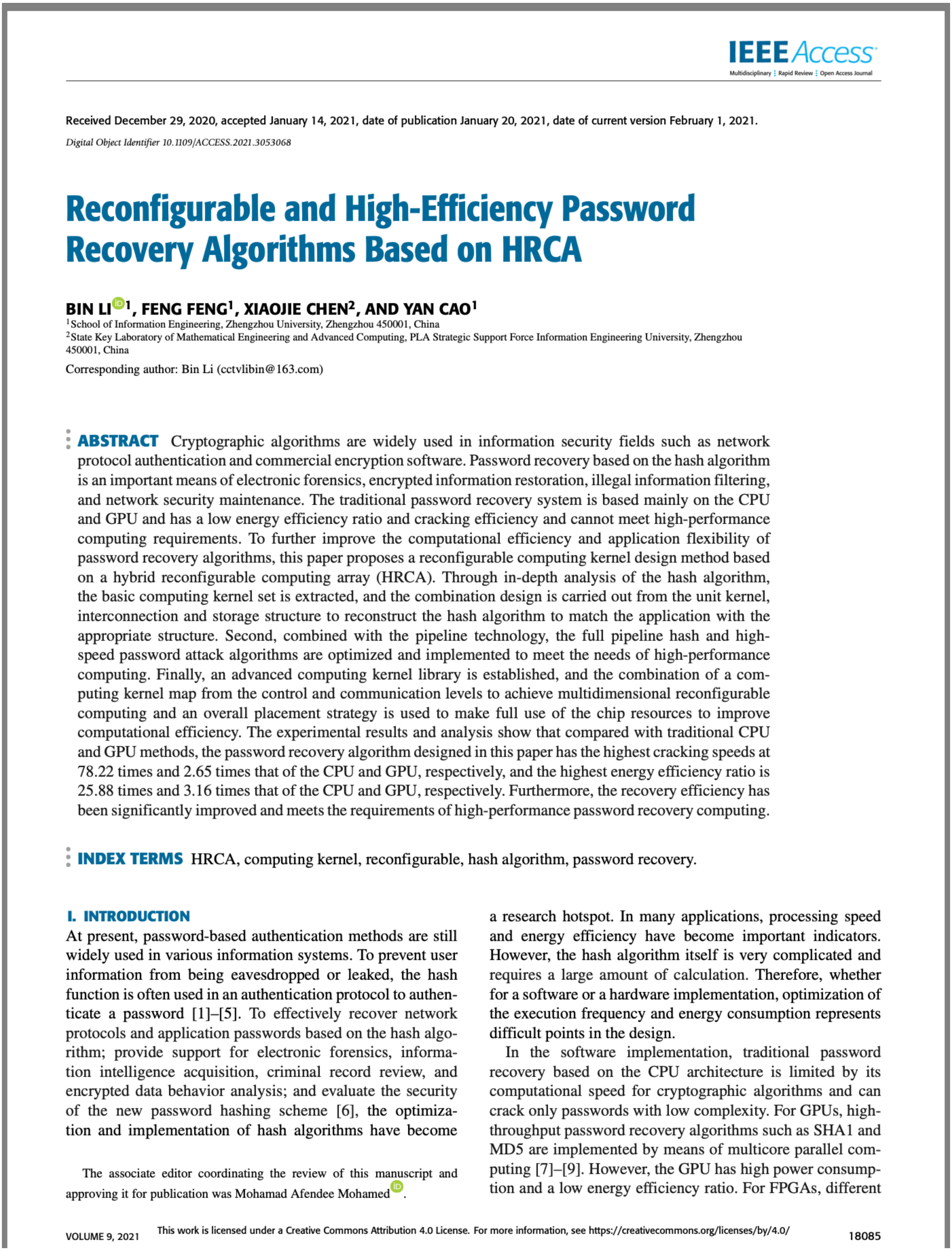

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 29, 2020, accepted January 14, 2021, date of publication January 20, 2021, date of current version February 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3053068

Reconfigurable and High-Efficiency Password Recovery Algorithms Based on HRCA

BIN LI[1], FENG FENG[1], XIAOJIE CHEN[2], AND YAN CAO[1]

[1] School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China
[2] State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China

Corresponding author: Bin Li (cctvlibin@163.com)

ABSTRACT Cryptographic algorithms are widely used in information security fields such as network protocol authentication and commercial encryption software. Password recovery based on the hash algorithm is an important means of electronic forensics, encrypted information restoration, illegal information filtering, and network security maintenance. The traditional password recovery system is based mainly on the CPU and GPU and has a low energy efficiency ratio and cracking efficiency and cannot meet high-performance computing requirements. To further improve the computational efficiency and application flexibility of password recovery algorithms, this paper proposes a reconfigurable computing kernel design method based on a hybrid reconfigurable computing array (HRCA). Through in-depth analysis of the hash algorithm, the basic computing kernel set is extracted, and the combination design is carried out from the unit kernel, interconnection and storage structure to reconstruct the hash algorithm to match the application with the appropriate structure. Second, combined with the pipeline technology, the full pipeline hash and high-speed password attack algorithms are optimized and implemented to meet the needs of high-performance computing. Finally, an advanced computing kernel library is established, and the combination of a computing kernel map from the control and communication levels to achieve multidimensional reconfigurable computing and an overall placement strategy is used to make full use of the chip resources to improve computational efficiency. The experimental results and analysis show that compared with traditional CPU and GPU methods, the password recovery algorithm designed in this paper has the highest cracking speeds at 78.22 times and 2.65 times that of the CPU and GPU, respectively, and the highest energy efficiency ratio is 25.88 times and 3.16 times that of the CPU and GPU, respectively. Furthermore, the recovery efficiency has been significantly improved and meets the requirements of high-performance password recovery computing.

INDEX TERMS HRCA, computing kernel, reconfigurable, hash algorithm, password recovery.

I. INTRODUCTION

At present, password-based authentication methods are still widely used in various information systems. To prevent user information from being eavesdropped or leaked, the hash function is often used in an authentication protocol to authenticate a password [1]–[5]. To effectively recover network protocols and application passwords based on the hash algorithm; provide support for electronic forensics, information intelligence acquisition, criminal record review, and encrypted data behavior analysis; and evaluate the security of the new password hashing scheme [6], the optimization and implementation of hash algorithms have become a research hotspot. In many applications, processing speed and energy efficiency have become important indicators. However, the hash algorithm itself is very complicated and requires a large amount of calculation. Therefore, whether for a software or a hardware implementation, optimization of the execution frequency and energy consumption represents difficult points in the design.

In the software implementation, traditional password recovery based on the CPU architecture is limited by its computational speed for cryptographic algorithms and can crack only passwords with low complexity. For GPUs, high-throughput password recovery algorithms such as SHA1 and MD5 are implemented by means of multicore parallel computing [7]–[9]. However, the GPU has high power consumption and a low energy efficiency ratio. For FPGAs, different

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.