MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____ 2024

IMPLEMENTAREA UNOR FUNCȚII DE DISPERSIE ASUPRA CARDURILOR DE IDENTIFICARE CU RADIOFRECVENȚĂ

Proiect de master

Student: _____ **Tanasoglo Mihail, TI-221M**

Coordonator: _____ **Bulai Rodica, asist. univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2024

АННОТАЦИЯ

Исследовательская работа посвящена проблеме обеспечения безопасности данных в системах RFID (Radio-Frequency Identification). Введение отмечает актуальность вопроса в современном информационном мире, где RFID-технологии широко применяются в различных сферах, но сопряжены с увеличивающимися угрозами безопасности.

Основной фокус работы – исследование и реализация облегченных хэш-функций для повышения безопасности и эффективности RFID-карт доступа. Хэш-функции рассматриваются как инструмент криптографической защиты, способный усилить безопасность данных и снизить риск несанкционированного доступа к системам. Особое внимание уделяется практической реализации этих функций с учетом ограниченных ресурсов, типичных для RFID-карт.

Цель исследования заключается в анализе существующих подходов и разработке новых методов обеспечения безопасности RFID-систем через применение облегченных хэш-функций. Результаты работы будут содержать практические рекомендации для специалистов по информационной безопасности и системам авторизации, способствуя развитию современных систем идентификации и контроля доступа.

ADNOTARE

Lucrarea de cercetare este dedicată problemei asigurării securității datelor în sistemele RFID (Radio-Frequency Identification). Introducerea notează relevanța problemei în lumea informațională modernă, unde tehnologiile RFID sunt utilizate pe scară largă în diverse domenii, dar sunt asociate cu amenințări tot mai mari de securitate.

Obiectivul principal al lucrării este cercetarea și implementarea funcțiilor hash ușoare pentru a îmbunătăți securitatea și eficiența cardurilor de acces RFID. Funcțiile hash sunt văzute ca un instrument de securitate criptografică care poate îmbunătăți securitatea datelor și poate reduce riscul accesului neautorizat la sisteme. O atenție deosebită este acordată implementării practice a acestor funcții, ținând cont de resursele limitate tipice pentru cardurile RFID.

Scopul studiului este de a analiza abordările existente și de a dezvolta noi metode pentru asigurarea securității sistemelor RFID prin utilizarea funcțiilor hash ușoare. Rezultatele lucrării vor conține recomandări practice pentru specialiștii în securitatea informațiilor și sisteme de autorizare, contribuind la dezvoltarea sistemelor moderne de identificare și control al accesului.

ABSTRACT

The research work is devoted to the problem of ensuring data security in RFID (Radio-Frequency Identification) systems. The introduction notes the relevance of the issue in the modern information world, where RFID technologies are widely used in various fields, but are associated with increasing security threats.

The main focus of the work is the research and implementation of lightweight hash functions to improve the security and efficiency of RFID access cards. Hash functions are seen as a cryptographic security tool that can enhance data security and reduce the risk of unauthorized access to systems. Particular attention is paid to the practical implementation of these functions, taking into account the limited resources typical for RFID cards.

The purpose of the study is to analyze existing approaches and develop new methods for ensuring the security of RFID systems through the use of lightweight hash functions. The results of the work will contain practical recommendations for specialists in information security and authorization systems, contributing to the development of modern identification and access control systems.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире, где информационные технологии проникают во все сферы жизни, вопрос обеспечения безопасности данных становится все более актуальным. Одним из ключевых аспектов в этой области является обеспечение безопасности систем и механизмов, использующих RFID-технологии (Radio-Frequency Identification). RFID-карты доступа, широко применяемые в различных сферах, таких как корпоративные офисы, медицинские учреждения, и даже государственные учреждения, представляют собой одну из наиболее распространенных форм идентификации и авторизации. Вместе с тем, с увеличением числа таких систем растет и уровень угроз и рисков, связанных с их использованием.

Данная работа посвящена исследованию и реализации использования облегченных хэш-функций для карт доступа RFID с целью повышения их безопасности и эффективности. Хэш-функции, как важное средство криптографической защиты, могут существенно усилить уровень защиты данных и снизить риск несанкционированного доступа к системам. Работа охватывает теоретические аспекты использования хэш-функций в контексте RFID-технологий, а также их практическую реализацию с учетом ограниченных ресурсов, характерных для RFID-карт доступа.

Целью данного исследования является анализ существующих подходов и разработка новых методов обеспечения безопасности RFID-систем через интеграцию облегченных хэш-функций. Результаты данной работы предоставят практические рекомендации для специалистов в области информационной безопасности и систем авторизации, а также способствуют дальнейшему развитию и совершенствованию современных систем идентификации и контроля доступа.

БИБЛИОГРАФИЯ

[1] A. Juels, «RFID security and privacy: a research survey», *IEEE J. Sel. Areas Commun.*, т. 24, вып. 2, сс. 381–394, фев. 2006, doi: 10.1109/JSAC.2005.861395.

[2] J.-P. Aumasson, L. Henzen, W. Meier, и M. Naya-Plasencia, «Quark: A Lightweight Hash», *J. Cryptol.*, т. 26, вып. 2, сс. 313–339, апр. 2013, doi: 10.1007/s00145-012-9125-6.

[3] M. Shand и J. Vuillemin, «Fast implementations of RSA cryptography», в *Proceedings of IEEE 11th Symposium on Computer Arithmetic*, июн. 1993, сс. 252–259. doi: 10.1109/ARITH.1993.378085.

[4] M. Feldhofer, S. Dominikus, и J. Wolkerstorfer, «Strong Authentication for RFID Systems Using the AES Algorithm», в *Cryptographic Hardware and Embedded Systems - CHES 2004*, M. Joye и J.-J. Quisquater, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2004, сс. 357–370. doi: 10.1007/978-3-540-28632-5_26.

[5] S. Hendry Leo Kanickam и L. Jayasimman, «Comparative Analysis of Hash Authentication Algorithms and ECC Based Security Algorithms in Cloud Data», *Asian J. Comput. Sci. Technol.*, т. 8, вып. 1, сс. 53–61, фев. 2019, doi: 10.51983/ajcst-2019.8.1.2118.

[6] M. R. S. Abyaneh, «Security Analysis Of Lightweight Schemes for RFID Systems», Doctoral thesis, The University of Bergen, 2012. Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://bora.uib.no/bora-xmlui/handle/1956/6106

[7] H. Tiwari, «Merkle-Damgård Construction Method and Alternatives: A Review», *J. Inf. Organ. Sci.*, т. 41, вып. 2, сс. 283–304, 2017.

[8] «Neeva: A Lightweight Hash Function». Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://eprint.iacr.org/2016/042

[9] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, и I. Verbauwhede, «SPONGENT: The Design Space of Lightweight Cryptographic Hashing». 2011 г. Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://eprint.iacr.org/2011/697

[10] «Hash-One: a lightweight cryptographic hash function - Megha Mukundan - 2016 - IET Information Security - Wiley Online Library». Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-ifs.2015.0385

[11] J.-P. Aumasson, L. Henzen, W. Meier, и M. Naya-Plasencia, «Quark: A Lightweight Hash», *J. Cryptol.*, т. 26, вып. 2, сс. 313–339, апр. 2013, doi: 10.1007/s00145-012-9125-6.

[12] C. Cannière, O. Dunkelman, и M. Knežević, *Katan and Ktantan —A Family of Small and Efficient Hardware-Oriented Block Ciphers*. 2009, с. 288.

[13] S. O'Melia и A. J. Elbirt, «Instruction Set Extensions for Enhancing the Performance of Symmetric-Key Cryptography», в *2008 Annual Computer Security Applications Conference (ACSAC)*, дек. 2008, сс. 465–474. doi: 10.1109/ACSAC.2008.10.

[14] B. Cogliati и Y. Seurin, «Analysis of the single-permutation encrypted Davies–Meyer construction», *Des. Codes Cryptogr.*, т. 86, вып. 12, сс. 2703–2723, дек. 2018, doi: 10.1007/s10623-018-0470-9.

[15] A. Bogdanov *и др.*, «PRESENT: An Ultra-Lightweight Block Cipher», в *Cryptographic Hardware and Embedded Systems - CHES 2007*, т. 4727, P. Paillier и I. Verbauwhede, Ред., в Lecture Notes in Computer Science, vol. 4727. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, сс. 450–466. doi: 10.1007/978-3-540-74735-2_31.

[16] J. Guo, T. Peyrin, и A. Poschmann, «The PHOTON Family of Lightweight Hash Functions». 2011 г. Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://eprint.iacr.org/2011/609

[17] T. P. Berger, J. D'Hayer, K. Marquet, M. Minier, и G. Thomas, «The GLUON Family: A Lightweight Hash Function Family Based on FCSRs», в *Progress in Cryptology - AFRICACRYPT 2012*, A. Mitrokotsa и S. Vaudenay, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2012, сс. 306–323. doi: 10.1007/978-3-642-31410-0_19.

[18] E. B. Kavun и T. Yalcin, «A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications», в *Radio Frequency Identification: Security and Privacy*

Issues, т. 6370, S. B. Ors Yalcin, Ред., в Lecture Notes in Computer Science, vol. 6370. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, сс. 258–269. doi: 10.1007/978-3-642-16822-2_20.
[19] S. Badel *и др.*, «ARMADILLO: A Multi-purpose Cryptographic Primitive Dedicated to Hardware», в *Cryptographic Hardware and Embedded Systems, CHES 2010*, S. Mangard и F.-X. Standaert, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2010, сс. 398–412. doi: 10.1007/978-3-642-15031-9_27.
[20] A. Luykx, B. Preneel, E. Tischhauser, и K. Yasuda, «A MAC Mode for Lightweight Block Ciphers», в *Fast Software Encryption*, T. Peyrin, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2016, сс. 43–59. doi: 10.1007/978-3-662-52993-5_3.
[21] F. Arnault, T. Berger, C. Lauradoux, M. Minier, и B. Pousse, «A New Approach for FCSRs», в *Selected Areas in Cryptography*, M. J. Jacobson, V. Rijmen, и R. Safavi-Naini, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009, сс. 433–448. doi: 10.1007/978-3-642-05445-7_27.
[22] B. H. Susanti, J. Jimmy, и M. W. Ardyani, «ENT Randomness Test on DM-PRESENT-80 and DM-PRESENT-128-based Pseudorandom Number Generator», в *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, дек. 2021, сс. 324–328. doi: 10.1109/ISRITI54043.2021.9702862.
[23] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, и H. Yoshida, «A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW», в *Information Security and Cryptology - ICISC 2010*, K.-H. Rhee и D. Nyang, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2011, сс. 151–168. doi: 10.1007/978-3-642-24209-0_10.
[24] «A lightweight implementation of the Tav-128 hash function». Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://www.jstage.jst.go.jp/article/elex/14/11/14_14.20161255/_article/-char/ja/
[25] B. Adida, S. Hohenberger, и R. L. Rivest, «Lightweight Encryption for Email».
[26] G. Hanaoka, Y. Zheng, и H. Imai, «LITESET: A light-weight secure electronic transaction protocol», в *Information Security and Privacy*, C. Boyd и E. Dawson, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1998, сс. 215–226. doi: 10.1007/BFb0053735.
[27] A. Bogdanov, F. Mendel, F. Regazzoni, V. Rijmen, и E. Tischhauser, «ALE: AES-Based Lightweight Authenticated Encryption», в *Fast Software Encryption*, S. Moriai, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2014, сс. 447–466. doi: 10.1007/978-3-662-43933-3_23.
[28] J. Alizadeh, M. R. Aref, N. Bagheri, и A. Rahimi, «JHAE: A Novel Permutation-Based Authenticated Encryption Mode Based on the Hash Mode JH», *J. Comput. Secur.*, т. 2, вып. 1, сс. 3–20, янв. 2015.
[29] D. Engels, X. Fan, G. Gong, H. Hu, и E. M. Smith, «Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices», в *Financial Cryptography and Data Security*, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, и F. Sebé, Ред., в Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2010, сс. 3–18. doi: 10.1007/978-3-642-14992-4_2.
[30] «jh.pdf». Просмотрено: 10 январь 2024 г. [Онлайн]. Доступно на: https://perso.uclouvain.be/fstandae/source_codes/hash_atmel/specs/jh.pdf
[31] M. Alizadeh, M. Salleh, M. Zamani, J. Shayan, и S. Karamizadeh, «Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID».
[32] J.-P. Aumasson, W. Meier, R. C.-W. Phan, и L. Henzen, «BLAKE2», в *The Hash Function BLAKE*, J.-P. Aumasson, W. Meier, R. C.-W. Phan, и L. Henzen, Ред., в Information Security and Cryptography. , Berlin, Heidelberg: Springer, 2014, сс. 165–183. doi: 10.1007/978-3-662-44757-4_9.
[33] M. Chen, Q. Xiao, K. Matsumoto, M. Yoshida, X. Luo, и K. Kita, «A Fast Retrieval Algorithm Based on Fibonacci Hashing for Audio Fingerprinting Systems», представлено на 2013 International Conference on Advanced Information Engineering and Education Science (ICAIEES 2013), Atlantis Press, дек. 2013, сс. 219–222. doi: 10.2991/icaiees-13.2013.59.