

Document details

[Back to results](#) | 1 of 1[Export](#) | [Download](#) | [Add to List](#) | [More...](#)[Journal of Theoretical and Applied Information Technology](#)

Volume 95, Issue 6, 31 March 2017, Pages 1489-1498

[Open Access](#)**A symmetric cryptosystem based on nondeterministic finite automata** (Article)Khaleel, G.^a , Turaev, S.^a , Alshakhli, I.^a , Zhukabayeva, T.^b , Tamrin, M.I.M.^a^a Faculty of Information and Communication Technology, International Islamic University Malaysia, Gombak, Selangor, Malaysia^b Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan[View references \(14\)](#)

Abstract

This paper proposes a new **symmetric cryptosystem based on nondeterministic finite automata**. It is shown that nondeterminism allows to reduce the dependency of key **automata** on a large descriptonal complexity and irreversibility of **automata**. Moreover, it is proven that the introduced **cryptosystem** has higher security and more efficient performance than its deterministic counterparts – Dömösi's **cryptosystem** and its modified version. © 2005 – ongoing JATIT & LLS.

Author keywords

Cryptography; Dömösi's **cryptosystem**; **Nondeterministic finite automata**; Stream cipher

ISSN: 19928645 Source Type: Journal Original language: English

Document Type: Article

Publisher: Asian Research Publishing Network

Funding details

Funding number	Funding sponsor	Acronym
RIGS16-368-0532	International Islamic University Malaysia	IIUM

Funding text

This work has been supported through International Islamic University Malaysia Research Initiative Grant Scheme RIGS16-368-0532.

References (14)

[View in search results format](#) All [Export](#) | [Print](#) | [E-mail](#) | [Save to PDF](#) | [Create bibliography](#) Tao, R., Chen, S.

1 **A finite automaton public key cryptosystem and digital signature**
Chinese Journal of Computers, 8 (6). [Cited 28 times](#).

 Tao, R., Chen, S.

2 **Two varieties of finite automaton public key cryptosystem and digital signatures**
Journal of Computer Science and Technology, 1 (1), pp. 9-18. [Cited 23 times](#).
doi: 10.1007/BF02943296
[View at Publisher](#)

 Bao, F., Igarashi, Y.

3 **Break finite automata public key cryptosystem**
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 944, pp. 147-158. [Cited 4 times](#).

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert](#) | [Set citation feed](#)

Related documents

The generalization of public key cryptosystem FAPKC4Tao, R. , Chen, S.
(1999) *Chinese Science Bulletin***DAFA - A lightweight DES augmented finite automaton cryptosystem**Abubaker, S. , Wu, K.
(2013) *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering***Cryptanalysis on a finite automaton public key cryptosystem**Dai, D. , Wu, K. , Zhang, H.
(1996) *Science in China, Series E: Technological Sciences*[View all related documents based on references](#)

Find more related documents in Scopus based on:

[Authors](#) | [Keywords](#)

<http://springerlink.com/content/0302-9743/copyright/2005/>

ISBN: 3540600841; 978-354060084-8

doi: 10.1007/3-540-60084-1_70

[View at Publisher](#)

Tao, R., Chen, S., Chen, X.

4 **FAPKC3: A new finite automaton public key cryptosystem**

Journal of Computer Science and Technology, 12 (4), pp. 289-305. Cited 11 times.

doi: 10.1007/BF02943149

[View at Publisher](#)

Tao, R., Chen, S.

5 **The generalization of public key cryptosystem FAPKC4**

Chinese Science Bulletin, 44 (9), pp. 784-790. Cited 8 times.

[View at Publisher](#)

Gysin, M.

6 **A one-key cryptosystem based on a finite nonlinear automaton**

Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1029, pp. 165-173. Cited 2 times.

<http://springerlink.com/content/0302-9743/copyright/2005/>

ISBN: 978-354060759-5

doi: 10.1007/BFb0032342

[View at Publisher](#)

Dömösi, P.

7 A novel cryptosystem based on finite automata without outputs

Automata, Formal Languages and Algebraic Systems, World Scientific, pp. 23-32.

M. Ito, Y. Kobayashi, and K. Shoji (eds.)

Dömösi, P.

8 A novel stream cipher based on finite automata

Intellisec – the 1st International Workshop on Intelligent Security Systems, pp. 11-14.

Bucharest, Romania (November)

Dömösi, P.

9 P.: US. Pub. No. US 2009/0092251 A1

Khaleel, S., Turaev, M.I.

10 Mohd Tamrin and I.F. Al-Shaikhli, "A Performance Improvement of Dömösi's Cryptosystem

AIP Conference Proceedings, 1705, p. 020007.

A Pseudorandom Number Sequence Test Program. Cited 4 times.

11 <http://www.fourmilab.ch/random>

Angluin, D.

12 **Inference of Reversible Languages**

Journal of the ACM (JACM), 29 (3), pp. 741-765. Cited 19 times.

doi: 10.1145/322326.322334

[View at Publisher](#)

Eric, J.

13 On the languages accepted by finite reversible automata

Series Lecture Notes in Computer Science, 267, pp. 237-249.

Springer

Falucskai, J.

14 **On the k-reversibility of finite automata**

Annales Mathematicae et Informaticae, 36 (1), pp. 71-75.

<http://www.ektf.hu/tanszek/matematika/ami/2009/ami2009-falucskai.pdf>

© Copyright 2017 Elsevier B.V., All rights reserved.

[Back to results](#) | 1 of 1

[Top of page](#)

About Scopus

- [What is Scopus](#)
- [Content coverage](#)
- [Scopus blog](#)
- [Scopus API](#)
- [Privacy matters](#)

Language

- [日本語に切り替える](#)
- [切换到简体中文](#)
- [切换到繁體中文](#)

Customer Service

- [Help](#)
- [Contact us](#)

ELSEVIER

[Terms and conditions](#) [Privacy policy](#)

Copyright © 2017 Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.
Cookies are set by this site. To decline them or learn more, visit our [Cookies page](#).

 RELX Group™