



مهندسی برق - الکترونیک و مخابرات / مخابرات

زهرا

احمدیان

شماره تماس: ۲۹۹۰۴۱۹۳

رایانامه: z_ahmadian@sbu.ac.ir

وب سایت:

پروفايل علم سنجی:

http://scimet.sbu.ac.ir/Zahra_Ahmadian

تحصیلات

- کارشناسی: دانشگاه صنعتی امیرکبیر - تهران، مهندسی برق - الکترونیک، ۱۳۸۱-۱۳۸۵
- کارشناسی: دانشگاه صنعتی امیرکبیر - تهران، مهندسی برق - مخابرات، ۱۳۸۱-۱۳۸۵
- دکتری: دانشگاه صنعتی شریف - تهران، مهندسی برق - مخابرات، ۱۳۸۹-۱۳۹۳
- کارشناسی ارشد: دانشگاه صنعتی شریف - تهران، مهندسی برق - مخابرات امن و رمز نگاری، ۱۳۸۵-۱۳۸۷

علايق پژوهشی

■ رمزنگاری

■ امنیت شبکه های مخابرات بی سیم

فعالیت‌های اجرایی

- استاد مشاور انجمن علمی برق (ولنجک)، ۱۴۰۲-۱۴۰۳
- عضو تخصصی کمیته علمی انجمن رمز ایران، ۱۴۰۱-۱۴۰۳

کتاب

■ رمزشناسی در ایران و جهان : چالش های پژوهشی، آموزش و ساختارهای اجرایی

زهرا احمدیان

دانشگاه صنعتی شریف - تهران، ایران، ۱۳۹۵، شابک: ۹۷۸۹۶۴۲۰۸۱۷۹۰

ارتباط با صنعت

■ تحلیل پروتکل های امنیتی مخابرات گروهی مبتنی بر تسهیم راز

۱۳۹۶

■ IoT-friendly, pre-computed and outsourced attribute based encryption

Mahdi Mahdavi Oliaee, Mohammad Hesam Tadayon, Mohammad Sayad Haghighi, Zahra Ahmadian
Future Generation Computer Systems-The International Journal of eScience, Vol.150, pp. 115-126, 2024

■ New Variations of Discrete Logarithm Problem

Mahdi Mahdavi Oliaee, Sahar Khaleghi fard, Zahra Ahmadian
ISeCure-ISC International Journal of Information Security, Vol.15, pp. 1-11, 2023

■ Provably minimum data complexity integral distinguisher based on conventional division property

Akram Khalesi, Zahra Ahmadian
Journal of Computer Virology and Hacking Techniques, pp. 1-13, 2023

■ Linear Subspace Cryptanalysis and Improvement of a Flexible and Lightweight Group Authentication Scheme

Ali Rezapour, Zahra Ahmadian
Iranian Journal of Electrical and Electronic Engineering, Vol.19, 2023

■ Fine-grained flexible access control: ciphertext policy attribute based encryption for arithmetic circuits

Mahdi Mahdavi Oliaee, Zahra Ahmadian
Journal of Computer Virology and Hacking Techniques, Vol.-, pp. 1-14, 2022

■ Revisiting the Security and Efficiency of SP2DAS 3PDA and EPPA Smart Grid Security Protocols

Hamid Amiryousefi, Zahra Ahmadian
ISeCure-ISC International Journal of Information Security, Vol.14, pp. 157-165, 2022

■ New Automatic Search Method for Truncated-Differential Characteristics Application to Midori, SKINNY and CRAFT

Amirhosein Ebrahimi Moghadam, Zahra Ahmadian
COMPUTER JOURNAL, Vol.00, 2020

■ Security analysis of a dynamic threshold secret sharing scheme using linear subspace method

Sadegh Jamshidpour, Zahra Ahmadian
INFORMATION PROCESSING LETTERS, Vol.163, 2020

■ MILP-based automatic differential search for LEA and HIGHT block ciphers

Elnaz Bagherzadeh, Zahra Ahmadian
IET Information Security, Vol.14, pp. 595-603, 2020

■ Biclique Cryptanalysis of Block Ciphers LBlock and TWINE-80 with Practical Data Complexity

Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, Mohammad Reza Aref
The ISC Int Journal of Information Security, Vol.11, pp. 57-73, 2019

■ Linear Subspace Cryptanalysis of Harns Secret Sharing-Based Group Authentication Scheme

Zahra Ahmadian, Sadegh Jamshidpour
IEEE Transactions on Information Forensics and Security, Vol.13, pp. 502-510, 2018

■ Improved Impossible Differential and Biclique Cryptanalysis of HIGHT

Arash Azimi, Siavash Ahmadi, Zahra Ahmadian, Mohajeri Javad, Mohammad Reza Aref
INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, Vol.31, pp. 1-14, 2018

■ An Improved Truncated Differential Cryptanalysis of Klein

Shahram Rasoolzadeh, Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref
Tatra Mountains Mathematical Publications, Vol.67, pp. 135-147, 2016

■ Biclique cryptanalysis of the full-round KLEIN block cipher

Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref
IET Information Security, Vol.9, pp. 294-301, 2015

■ Total Break of Zorro Using Linear and Differential Attacks

Shahram Rasoolzadeh, Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref
The ISC Int Journal of Information Security, Vol.6, pp. 23-34, 2014

■ **Low-Data Complexity Biclique Cryptanalysis of Block Ciphers With Application to Piccolo and HIGHT**

Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, Mohammad Reza Aref
IEEE Transactions on Information Forensics and Security, Vol.9, pp. 1641-1652, 2014

■ **Desynchronization attack on RAPP ultralightweight authentication protocol**

Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref
INFORMATION PROCESSING LETTERS, Vol.113, pp. 205-209, 2013

■ **Recursive Linear and Differential Cryptanalysis of Ultralightweight Authentication Protocols**

Zahra Ahmadian, M. Salmasizadeh, M. R. Aref
IEEE Transactions on Information Forensics and Security, Vol.8, pp. 1140-1151, 2013

■ **Security enhancements against UMTS GSM interworking attacks**

Zahra Ahmadian, Somayeh Salimi, Ahmad Salah
Computer Networks, Vol.54, pp. 2256-2270, 2010

■ **A practical distinguisher for the Shannon cipher**

Zahra Ahmadian, Javad Mohajeri, Mahmoud Salmasizadeh, Risto M. Hakala, Kaisa Nyberg
JOURNAL OF SYSTEMS AND SOFTWARE, Vol.83, pp. 543-547, 2010

■ **pi-Cipher یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احراز اصالت شده**

بهزاد سعیدی، زهرا احمدیان

امنیت فضای تولید و تبادل اطلاعات، نسخه ۱۹، صفحات: ۲۷-۳۳، ۱۳۹۹

مقالات علمی ارائه شده در همایش‌ها

■ **Improved Differential Meet-in-the-Middle Cryptanalysis**

Zahra Ahmadian, Akram Khalesi, Hoseyn Moghimi, Mfoukh Dounia, Naya-Plasencia Maria
43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2024, Vol.14651, pp.280-309

■ **Follow-up on Differential Meet-In-The-Middle Cryptanalysis**

Zahra Ahmadian
Dagstuhl Seminar on Symmetric Cryptography

■ **Biclique cryptanalysis of LBlock with modified key schedule**

, Zahra Ahmadian, ,
12th International ISC conference on Information security and cryptology

■ **Integral Analysis of Saturnin Using Bit-Based Division Property**

اکرم خالصی، زهرا احمدیان

هجدهمین کنفرانس بین المللی انجمن رمز ایران، نسخه ۱۸، صفحات: ۶۳-۶۷

■ **Cryptanalysis of SP₂DAS and ۳PDA,Two Data Aggregation Schemes for Smart Grid**

حمید امیریوسفی، زهرا احمدیان

شانزدهمین کنفرانس بین المللی انجمن رمز ایران، نسخه ۱۶، صفحات: ۴۵-۴۸

■ **p-cipher یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احراز اصالت شده**

بهزاد سعیدی، زهرا احمدیان

شانزدهمین کنفرانس بین المللی انجمن رمز ایران

■ **SIMON حمله ملاقات در میانه با پیچیدگی داده کم به الگوریتم**

امیرحسین ابراهیمی مقدم، شهرام رسول زاده، زهرا احمدیان

بیست و سومین کنفرانس ملی سالانه انجمن کامپیوتر ایران

پایان نامه های کارشناسی ارشد

■ با استفاده از روش برنامه ریزی خطی عدد صحیح Salsa جستجوی تمایزگر برای الگوریتم رمز جریانی
مرضیه جهان خانی
۱۳۹۸

■ MILP تحلیل رمزهای قالبی با استفاده از تکنیک بهینه سازی
زینب نامداری جعفریگی
۱۳۹۷

■ تحلیل و طراحی پروتکل های تجمیع داده به صورت امن و با حفظ حریم خصوصی در شبکه هوشمند انرژی
حمید امیریوسفی
۱۳۹۷

■ تحلیل امنیت الگوریتم های رمزگذاری احراز اصالت شده
بهزاد سعیدی
۱۳۹۷

■ حملات ملاقات در میانه بر روی رمزهای قالبی
امیرحسین ابراهیمی مقدم
۱۳۹۶

■ کاربرد الگوریتم های جستجوی خودکار برای تحلیل رمزهای قالبی سبک
الناز باقرزاده
۱۳۹۶

جوایز و افتخارات
■ The best paper of ISeCure Journal in ۲۰۱۶
۱۳۹۴