استادیار دانشگاه شهید بهشتی

هادی

سلیمانی

شماره تماس: ۲۹۹۰۵۴۸۵

رایانامه: h_soleimany@sbu.ac.ir

وب سایت:
http://facultymembers.sbu.ac.ir/h_soleimany

پروفایل علم سنجی:
http://scimet.sbu.ac.ir/Hadi_Soleimany

فضای مجازی / پژوهشکده فضای مجازی

تحصیلات

- دکتری: دانشگاههای خارج کشور واقع در قاره اروپا، علوم کامپیوتر، ۱۳۹۰←۱۳۹۳
- کارشناسی: دانشگاه علم و صنعت ایران – تهران، مهندسی برق – مخابرات، ۱۳۸۱←۱۳۸۷
- کارشناسی ارشد: دانشگاه جامع امام حسین (ع)، مهندسی برق گرایش مخابرات، ۱۳۸۷←۱۳۸۹

علایق پژوهشی

- رمزنگاری و پیاده سازی امن

فعالیت‌های اجرایی

- IACR Transactions on Symmetric Cryptology، ۱۴۰۰←۱۴۰۱
- IACR Transactions on Symmetric Cryptology، ۱۳۹۹←۱۴۰۰
- شورای اجرایی انجمن رمز ایران، ۱۳۹۹←۱۴۰۱
- عضویت در هیات مدیره انجمن علمی رسمی، ۱۳۹۹←۱۴۰۰
- IACR Transactions on Symmetric Cryptology (ToSC)، ۱۳۹۷←۱۳۹۸
- IACR Transactions on Symmetric Cryptology، ۱۳۹۶←۱۳۹۷
- Editorial Board of the journal IACR Transactions on Symmetric Cryptology، ۱۳۹۶←۱۳۹۷
- IACR Transactions on Symmetric Cryptology، ۱۳۹۵←۱۳۹۶
- Editorial Board of the journal IACR Transactions on Symmetric Cryptology، ۱۳۹۵←۱۳۹۶

مقالات علمی چاپ شده در مجلات

■ Linked Fault Analysis
Ali asghar Beigizad, Hadi Soleimany, Sara Zarei, Hamed Ramzanipour
IEEE Transactions on Information Forensics and Security, Vol.19, pp. 632-645, 2024

■ Exploiting statistical effective fault attack in a blind setting
Navid Vafaei, Hadi Soleimany, Nasour Bagheri
IET Information Security, Vol.17, pp. 639-646, 2023

■ Secure and Low-area Implementation of the AES Using FPGA
MuhamadAli HajiSoltani, Raziyeh Salarifard, Hadi Soleimany
ISeCure-ISC International Journal of Information Security, Vol.14, pp. 93-99, 2022

■ Modified Cache-Template Attack on AES
Mahdi Esfahani, Hadi Soleimany, Mohammad Reza Aref
Scientia Iranica, Vol.29, pp. 1949-1956, 2022

■ Statistical Effective Fault Attacks: The Other Side of the Coin
Navid Vafaei, Sara Zarei, Nasour Bagheri, Maria Eichlseder, Robert Primas, Hadi Soleimany
IEEE Transactions on Information Forensics and Security, Vol.17, pp. 1855-1867, 2022

■ Modified Cache Template Attack on AES
Mahdi Esfahani, Hadi Soleimany, Mohammad Reza Aref
Scientia Iranica, Vol.29, pp. 1949-1956, 2022

■ SIPFA: Statistical Ineffective Persistent Faults Analysis on Feistel Ciphers
Nasour Bagheri, Sadegh Sadeghi, Prasanna Ravi, Shivam Bhasin, Hadi Soleimany
IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol.2022, pp. 367-390, 2022

■ Flush+Reload Attacks on SEED
Milad Seddigh, Hadi Soleimany
COMPUTER JOURNAL, Vol.65, pp. 2769-2779, 2021

■ Cross-VM cache attacks on Camellia
Milad Seddigh, Hadi Soleimany
Journal of Computer Virology and Hacking Techniques, Vol.18, pp. 91-99, 2021

■ Practical Multiple Persistent Faults Analysis
Hadi Soleimany, Nasour Bagheri, Hosein Hadipour, Prasanna Ravi, Shivam Bhasin, Sara Mansouri
IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol.2022, pp. 367-390, 2021

■ A generalized framework for accelerating exhaustive search utilizing deterministic related-key differential characteristics
Hadi Soleimany, Farokh lagha Moazami Goodarzi
Journal of Computer Virology and Hacking Techniques, Vol.18, pp. 141-146, 2021

■ Enhanced cache attack on AES applicable on ARM-based devices with new operating systems
Mahdi Esfahani, Hadi Soleimany, Mohammad Reza Aref
Computer Networks, Vol.198, 2021

■ Low-Latency Keccak at any Arbitrary Order
Sara Zareei, Aein Rezaei Shahmirzadi, Hadi Soleimany, Raziyeh Salarifard, Amir Moradi
IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol.2021, pp. 388-411, 2021

■ Evict+Time Attack on Intel CPUs without Explicit Knowledge of Address Offsets
Vahid Meraji, Hadi Soleimany
ISeCure-ISC International Journal of Information Security, Vol.13, pp. 19-27, 2021

■ A Framework for Faster Key Search Using Related-key Higher-order Differential Properties Applications to Agrasta
Christoph Dobraunig, Farokh lagha Moazami Goodarzi, Christian Rechberger, Hadi Soleimany

IET Information Security, Vol.14, pp. 202-209, 2020

■ Enhanced Flush+Reload Attack on AES
Milad Seddigh, Hadi Soleimany
ISeCure-ISC International Journal of Information Security, Vol.12, pp. 83-91, 2020

■ New Single-Trace Side-Channel Attacks on a Specific Class of Elgamal Cryptosystem
Parinaz Mahdion, Hadi Soleimany, Pouya Habibi, Farokh lagha Moazami Goodarzi
IET Information Security, Vol.14, pp. 151-156, 2020

■ Impossible Differential Cryptanalysis on Deoxys-BC-256
Alireza Mehrdad, Farokh lagha Moazami Goodarzi, Hadi Soleimany
ISeCure-ISC International Journal of Information Security, Vol.10, pp. 93-105, 2018

■ Cryptanalysis of Low-Data Instances of Full LowMCv2
Christian Rechberger, Hadi Soleimany, Tyge Tiessen
IACR Transactions on Symmetric Cryptology, Vol.2018, pp. 163-181, 2018

■ Reflection Cryptanalysis of PRINCE-Like Ciphers
Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, Yanfeng Wang
JOURNAL OF CRYPTOLOGY, Vol.28, pp. 718-744, 2015

■ Zero-correlation linear cryptanalysis of reduced-round LBlock
Hadi Soleimany, Kaisa Nyberg
DESIGNS CODES AND CRYPTOGRAPHY, Vol.73, pp. 683-698, 2014

■ Self-similarity cryptanalysis of the block cipher ITUbee
Hadi Soleimany
IET Information Security, Vol.9, pp. 179-184, 2014

■ AES بر روی Flush+Reload پیاده سازی عملی حمله کانال جانبی
مهدی اصفهانی، هادی سلیمانی، محمدرضا عارف
علوم و فناوری های پدافند نوین، نسخه ۱۰، صفحات: ۳۸۳-۳۹۲، ۱۳۹۸

■ Zorro یک تحلیل تفاضل ناممکن از الگوریتم رمز قالبی
هادی سلیمانی، علی رضا مهرداد، سعیده صادقی، فرخ لقا معظمی گودرزی
پردازش علائم و داده ها، نسخه ۱۶، صفحات: ۱۷-۲۶، ۱۳۹۸

■ مروری بر پیاده سازی آستانه ای به عنوان روشی برای مقابله با حملات تحلیل توان
سارا زارعی، هادی سلیمانی
امنیت فضای تولید و تبادل اطلاعات، نسخه ۸، صفحات: ۱۷-۲۸، ۱۳۹۸

■ معرفی بیت کوین و چالش های امنیتی آن
فاطمه عزیزی، هادی سلیمانی
پدافند غیر عامل، نسخه ۱۰، صفحات: ۶۹-۸۰، ۱۳۹۸

■ Raspberrypi۳ و پیاده سازی عملی آن بر روی برد ARM ارایه یک حمله زمانی جدید بر روی پردازنده
وحید معراجی، هادی سلیمانی
پدافند الکترونیکی و سایبری، نسخه ۷، صفحات: ۱۲۵-۱۳۲، ۱۳۹۸

■ روی الگوریتم های رمزنگاری جعبه سفید DCA معرفی حمله
جواد علیزاده، محسن صدیقی، هادی سلیمانی
امنیت فضای تولید و تبادل اطلاعات، نسخه ۸، صفحات: ۵۱-۶۲، ۱۳۹۸

■ بررسی روش های به کارگیری کلپتوگرافی
هادی سلیمانی، فرخ لقا معظمی گودرزی
امنیت فضای تولید و تبادل اطلاعات، نسخه ۱۴، صفحات: ۳۱-۴۰، ۱۳۹۷

■ برخی از مباحث نوین در رمزنگاری ضرورت ها و کاربردها
هادی سلیمانی
پدافند غیر عامل، نسخه ۱۰، صفحات: ۷۵-۹۳، ۱۳۹۷

■ LowMC تحلیل تفاضل ناممکن الگوریتم رمزقالبی
هادی سلیمانی، علی رضا مهرداد
پدافند الکترونیکی و سایبری، نسخه ۷، صفحات: ۶۹-۷۹، ۱۳۹۷

■ رویکردها و چالش های مدل جعبه سفید در پیاده سازی الگوریتم های رمزنگاری قالبی
هادی سلیمانی، محمدرضا صادقی
امنیت فضای تولید و تبادل اطلاعات، نسخه ۱۳، صفحات: ۳-۲۰، ۱۳۹۶

■ AES-۲۵۶ بررسی جدیدترین نتائج تحلیل تفاضل ناممکن کلید مرتبط
هادی سلیمانی، محمد بهشتی آتشگاه
امنیت فضای تولید و تبادل اطلاعات، صفحات: ۱-۱۶، ۱۳۸۸

مقالات علمی ارائه شده در همایش‌ها

■ Breaking KASLR on Mobile Devices without Any Use of Cache Memory
Milad Seddigh, Mahdi Esfahani , Bhattacharya Sarani , Mohammad Reza Aref , Hadi Soleimany
Sixth Workshop on Attacks and Solutions in Hardware Security (ASHES 2022), pp.45-54

■
Milad Seddigh, Hadi Soleimany
27th Iranian Conference on Electrical Engineering ICEE2019

■
Parinaz Mahdion, Hadi Soleimany, Farokh lagha Moazami Goodarzi
The 26th Iranian Conference on Electrical Engineering (ICEE 2018)

■
Alireza Mehrdad, Farokh lagha Moazami Goodarzi, Hadi Soleimany
The 26th Iranian Conference on Electrical Engineering (ICEE 2018)

■ Key Recovery Attack against 2.5-round pi -Cipher
Hadi Soleimany
Fast Software Encryption 2016

■ Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro
Hadi Soleimany
Fast Software Encryption 2014

■ Reflection Cryptanalysis of PRINCE-like Ciphers
Hadi Soleimany, Celine Blondeau, Xiaoli Yu, Wenling Wu, Nyberg Kaisa, Huiling Zhang, Lei Zhang, Yanfeng Wang
Fast Software Encryption 2013

■ Improved related-key boomerang cryptanalysis of AES-256
Hadi Soleimany, Mohammadreza Aref, Alireza Sharifi
International Conference on Information Science and Applications (ICISA) 2010

■ Improved Related-Key Impossible Differential Attacks on 8-Round AES-256
Hadi Soleimany, Alireza Sharifi, Aref Mohammadreza
International Zurich Seminar on Communications 2010

■ AES ارائه یک نقاب گذاری بهینه برای پیاده سازی بدون تاخیر زمانی جعبه جانشانی
علی نوری خامنه، راضیه سالاری فرد، هادی سلیمانی
هفدهمین کنفرانس بین المللی انجمن رمز ایران

■ ارائه و پیاده سازی حمله زمانی برنشتاین بهبود یافته بدون داشتن دسترسی ریشه
وحید معراجی، هادی سلیمانی
شانزدهمین کنفرانس بین المللی انجمن رمز ایران، صفحات: ۱۲۱-۱۲۷

■ ارائه یک روش برای پیاده سازی سخت افزاری دو طرح رمزنگاری جعبه سفید متناسب با محدودیت های لایه ادراکی شبکه حسگری بیسیم
محمدرضا صادقی، هادی سلیمانی
بیست و چهارمین کنفرانس ملی سالانه انجمن کامپیوتر ایران، صفحات: ۳۳۸-۳۴۴

■ جدید بر روی پردازنده های اینتل Access-Driven ارائه ی یک حمله ی
وحید معراجی، هادی سلیمانی
بیست و چهارمین کنفرانس ملی سالانه انجمن کامپیوتر ایران، صفحات: ۳۴۵-۳۵۴

■ یک تمایزگر جدید به منظور اعمال حملات کانال جانبی به پیادهسازی الگوریتم رمزنگاری
پریناز مهدیون، هادی سلیمانی، فرخ لقا معظمی گودرزی
بیست و سومین کنفرانس ملی سالانه انجمن کامپیوتر ایران، صفحات: ۳۷۵-۳۸۰

■ Deoxys تحلیل تفاضل ناممکن توئیک مرتبط الگوریتم
علی رضا مهرداد، فرخ لقا معظمی گودرزی، هادی سلیمانی
بیست و سومین کنفرانس ملی سالانه انجمن کامپیوتر ایران، صفحات: ۳۵۷-۳۶۲

■ Cryptanalysisi of ۷-round AES-۱۲۸
هادی سلیمانی، Sharifi Alireza، Behnam Bahrak، Aref Mohammadreza
International ISC Conference on Information Security and Cryptology ۲۰۱۰

■ ۹-Round Attack on AES-۲۵۶ by a ۶-round property
هادی سلیمانی، Mohammadreza Aref، Alireza Sharifi
هجدهمین کنفرانس مهندسی برق ایران

پایان‌نامه‌های کارشناسی‌ارشد

■ به روش نقاب گذاری سخت افزاری با تاخیر زمانی کم AES پیاده سازی جعبه جانشانی
علی نوری خامنه
۱۳۹۹

■ با امنیت در برابر حملات تحلیل توان مرتبه‌ی بالا Keccak ارائه‌ی یک طرح بهینه برای پیاده‌سازی سخت‌افزاری تابع
سارا زارعی

۱۳۹۹

■ به منظور تشخیص نشت اطلاعات در حملات کانال جانبی t–test پیاده سازی و تحلیل روش
فاطمه عزیزی
۱۳۹۸

■ BLISS ارائه و پیاده سازی یک حمله تحلیل توان به امضای
پرستو ایرانی
۱۳۹۸

■ AES بر روی الگوریتم رمزنگاری Flush + Reload بهبود سرعت حمله
میلاد صدیق
۱۳۹۸

■ ارزیابی امنیت و کارائی طرح های رمزنگاری تصاویر ماهواره ای
احیا یاوری قره قشلاقی
۱۳۹۸

■ پیاده سازی امن و کارآمد رمزهای قالبی مقاوم در برابر حملات مدل جعبه سفید
محمدرضا صادقی
۱۳۹۷

■ تشخیص مناسب ترین حملات کانال جانبی مبتنی بر حافظه نهان براساس نوع پردازنده
وحید معراجی
۱۳۹۷

■ و الجمال از طریق حملات فرکانس پائین الکترومغناطیسی در رایانه های شخصی RSA استخراج کلید
پریناز مهدیون
۱۳۹۶

■ حملات کانال جانبی الکترومغناطیسی بر روی رمزنگاری خم بیضوی در کامپیوتر های شخصی
مصطفی چمن آورگانی
۱۳۹۶