بسمه تعالی

خلاصه سوابق علمی

مشخصات فردی

نام و نام خانوادگی: محمود سلماسی‌زاده

تاریخ تولد: ۱۳۲۹/۱۰/۱۹

آدرس: پژوهشکده الکترونیک، دانشگاه صنعتی شریف، صندوق پستی ۸۶۳۹-۱۱۱۵۵- تهران – ایران

تلفن: ۸-۶۶۰۰۵۵۱۷ و ۱-۶۶۱۶۴۹۰۰ و ۶۶۱۶۴۹۰۳ **نمابر:** ۶۶۰۳۰۳۱۸

پست الکترونیکی: salmasi@sharif.edu

تحصیلات

۱۳۷۶-۱۳۷۲ : دورهٔ دکتری در مرکز تحقیقات امنیت اطلاعات، بخش مخابرات داده دانشکده فنآوری اطلاعات، دانشگاه صنعتی کوینزلند، بریزبن – استرالیا

۱۳۶۸-۱۳۶۶: کارشناسی ارشد – دانشکده مهندسی برق – دانشگاه صنعتی شریف – تهران – ایران

۱۳۵۲-۱۳۴۸: کارشناسی – دانشکده مهندسی برق – دانشگاه صنعتی شریف – تهران – ایران

سوابق شغلی

۸۸/۱/۱۵ – تاکنون: دانشیارپژوهشکده الکترونیک دانشگاه صنعتی شریف

۱۳۷۶-۸۸/۱/۱۴: استادیار پژوهشکده الکترونیک دانشگاه صنعتی شریف

۱۳۷۶– تاکنون: معاون پژوهشکده الکترونیک دانشگاه صنعتی شریف

۱۳۷۷ – تاکنون: مسئول دورهٔ کارشناسی ارشد مخابرات رمز – دانشکده مهندسی برق – دانشگاه صنعتی شریف

۱۳۷۷ – تاکنون: عضو هیئت علمی (همکار) دانشکده مهندسی برق – دانشگاه صنعتی شریف

۱۳۷۲-۱۳۵۵: پژوهشگر – پژوهشکده الکترونیک – دانشگاه صنعتی شریف

۱۳۷۲-۱۳۶۸: مربی (پاره وقت) – دانشکده مهندسی برق – دانشگاه صنعتی شریف

۱۳۷۲-۱۳۶۸: مربی (پاره‌وقت) – دانشکده مهندسی کامپیوتر – دانشگاه علم و صنعت ایران

فعالیت‌های آموزشی

دورهٔ کارشناسی ارشد مخابرات – رمز

مسئول راه‌اندازی اولین دوره رسمی کارشناسی ارشد در رشته مخابرات – رمز در کشور

مسئول علمی گروه مخابرات–رمز، دانشکده مهندسی برق – دانشگاه صنعتی شریف

عضو کمیتهٔ تحصیلات تکمیلی دانشکده مهندسی برق – دانشگاه صنعتی شریف

دروس

- رمزنگاری پیشرفته (کارشناسی ارشد)
- رمزنگاری و امنیت داده‌ها (کارشناسی ارشد)
- سمینار کارشناسی ارشد مخابرات رمز (کارشناسی ارشد)
- مخابرات داده
- ریزپردازنده
- نظریه مدارهای منطقی
- برنامه‌ریزی به زبان اسمبلی

رساله های دکتری (پایان یافته)

۱- مدل‌سازی آسیب‌پذیری رمزهای قطعه‌ای متقارن در برابر حملات توانی

رساله های دکتری (درمرحله پژوهش)

۱- نرخ های امن در کانال های شنود

رساله های دکتری (قبل از تصویب)

۱- رای گیری الکترونیکی

۲- امنیت RFID

پایان‌نامه‌های کارشناسی ارشد (پایان یافته)

۱- تحلیل نوع خاصی از رمزهای دنباله‌ای با انتقال نامنظم

۲- تحلیل امنیت امضاء دیجیتال کور گروهی

۳- حملات سخت افزاری به کارتهای هوشمند با استفاده از اطلاعات نشتی

۴- طراحی و ساخت رمز کننده تلفنی دوطرفه همزمان با استفاده از پردازنده‌های سیگنال دیجیتال

۵- تحلیل ریسک در امنیت اطلاعات

۶- روشهای طراحی S-box برای رمزهای قطعه‌ای

۷- بررسی امنیت در تلفن همراه GSM، تدوین اصول نظری تحلیل الگوریتم‌های A5/1 و A5/2 و پیاده‌سازی آنها

۸- بررسی انواع روشهای تحلیل رمزهای دنباله‌ای و تحلیل یک الگوریتم خاص

۹- روشهای طراحی و تحلیل سیستم‌های رمز دنباله‌ای با انتقال نامنظم

۱۰- حفظ امنیت در هنگام افشاء کلید

۱۱- طرح‌های امضاء دیجیتال امن هم ریخت

۱۲- کیف پول الکترونیکی امن

۱۳- طراحی و تحلیل امنیتی شبکه رایانه‌ای گسترده سلسله مراتبی با قابلیت سرویس‌دهی برون خط به کاربران در نودها

۱۴- بررسی مقایسه ویژگی‌های امنیتی سیستم‌های تلفن همراه نسل دوم GSM و نسل سوم UTMS و تحلیل پروتکل AKA با روش صوری

۱۵- تحلیل مولد دنباله کلید اجرائی از نوع جمع کننده با استفاده از زوج آزماهای حافظه دار

۱۶- تحلیل توانی رمزهای قطعه ایDES,AES براساس چگالی طیف توان

۱۷- مقایسه تحلیلی معماریهای امنیتی فنآوری Bluetooth و فنآوری بی‌سیم بر مبنای IEEE 802.11 با تاکید بر آسیب‌پذیری پروتکل امنیتی

۱۸- ارتقاء امنیت پروتکل‌های مسیریابی در شبکه‌های اقتضائی

۱۹-ارتقاء و تحلیل روش‌های تامین گمنامی در پروتکل‌های رمزنگاری

۲۰- تحلیل یک الگوریتم رمز دنباله‌ای با متغیرهای بزرگ با استفاده از حملهٔ تمایز

۲۱- طراحی و ارتقاء یک پروتکل رای‌گیری الکترونیکی

۲۲- حملات تمایز مبتنی بر حملات خطی بر علیه الگوریتم‌های رمز دنباله‌ای

۲۳-بهبود ویژگی‌های امنیتی شبکه‌های مخابراتی با استفاده از کدینگ شبکه

۲۴- ارتقاء امنیت پروتکل‌های مدیریت کلید سلسله مراتبی در شبکه‌های حسگر بی‌سیم

۲۵- تحلیل الگوریتم‌های رمز دنباله‌ای با استفاده از خواص آماری توابع بولی

۲۶- تحلیل شبکه‌های مخلوط وارسی‌پذیر

۲۷- نرخ‌های قابل حصول در شبکه‌های رله

۲۸- امنیت از دیدگاه نظریه اطلاعات در شبکه‌های پخش و دسترسی چندگانه

پایان‌نامه‌های کارشناسی ارشد (در مرحلهٔ پژوهش)

۱- ارزیابی پروتکل‌های رمزنگاری با استفاده از نظریه بازیها

قراردادهای پژوهشی و ارتباط با صنعت

۱- مبانی طراحی و تحلیل الگوریتم‌ها و پروتکل‌های رمزنگاری

۲- امنیت تئوری اطلاعاتی

۳- طراحی و راه اندازی آزمایشگاه تحلیل الگوریتم های رمز و سیستم های رمز کننده

۴- طراحی و تحلیل الگوریتم های رمزنگاری غیرمتقارن و کاربرد آنها در امنیت شبکه‌های کامپوتری

۵- طراحی و تحلیل الگوریتم های رمزنگاری متقارن و کاربرد آنها در امنیت شبکه‌های کامپوتری

۶- طراحی و ساخت ۵ دستگاه رمز کنندهٔ تلفنی هوشمند دوطرفه همزمان با استفاده از PCهای صنعتی برای جهاد خودکفائی نداجا

۷- همکاری در طراحی و ساخت سیستم رمز کنندهٔ تلفنی نجوا (برندهٔ سوم تحقیق در هفتمین جشنواره خوارزمی)

۸- همکاری در طراحی و ساخت سیستم رمز کنندهٔ رادیویی VSS-32 (برندهٔ سوم تحقیق در اولین جشنواره خوارزمی)

مشاوره، نظارت و داوری طرحهای پژوهشی و صنعتی

۱- مشاوره در تعیین مشخصات مرکز صدور گواهی ریشه و مراکز میانی سیستم بانکی کشور برای بانک مرکزی

۲- مشاوره در تعیین مشخصات و نظارت در پیاده‌سازی اولین CA ریشه در کشور

۳- ناظر پروژه ارایه معماری سرویس گرا مبتنی بر زیر ساخت کلید عمومی و RFP برای پرمژه های دارای اولویت پژوهشکده همنیت فناوری اطلاعات و ارتباطات مرکز تحقیقات مخابرات ایران

عضویت در مجامع علمی و شورهای تخصصی

شهریور ۸۹ - تاکنون: دبیر و قائم‌مقام انجمن رمز ایران

آذر ۸۹ - تاکنون: عضو قطب علمی رمز – دانشگاه صنعتی شریف

آبان ۸۹ - تاکنون: عضو کارگروه امنیت – ستاد فنآوری ارتباطات و اطلاعات، معاونت علمی و فنآوری ریاست جمهوری

آبان ۸۹ - تاکنون: عضو کمیته آموزش و پژوهش افتا – وابسته به کارگروه وفادولت

دیماه ۸۸ - تاکنون: رئیس هیئت مدیره موسسه توسعه و گسترش افتا وابسته به انجمن رمز ایران

مهر ماه ۸۸- تاکنون: عضو شورای علمی پژوهشکده امنیت ارتباطات و فناوری اطلاعات – مرکز تحقیقات مخابرات ایران

شهریور۸۵- تا شهریور ۸۹: مشاور شورای اجرائی انجمن رمز ایران

۱۳۸۵- تاکنون: عضو کمیته علمی انجمن رمز ایران

۱۳۸۲-۱۳۸۴: عضو متخصص شورایعالی امنیت فضای تبادل داده‌ها مصوب هیأت محترم وزیران دولت جمهوری اسلامی ایران

۱۳۷۹-۱۳۸۵: عضو شورای اجرائی انجمن رمز ایران

۱۳۷۹-۱۳۸۵: عضو و مسئول کمیتهٔ علمی انجمن رمز ایران

۱۳۷۸-۱۳۷۹ : عضو هیئت مؤسس انجمن رمز ایران

۱۳۷۶-تاکنون: عضو انجمن بین‌المللی تحقیقات رمزنگاری (IACR)

۱۳۸۵- شهریور۱۳۸۸: عضو شورای تخصصی گروه فناوری اطلات و سامانه ها مرکز تحقیقات مخابرات ایران

عضویت در هیت تحریریه مجلات علمی پژوهشی

۱۳۸۷- تاکنون: عضو تحریریه مجله بین المللی علمی پژوهشی ISeCure از انتشارات انجمن رمز ایران

۱۳۷۸- تاکنون: عضو هیئت تحریره مجله علمی خبری «منادی» از انتشارات انجمن رمز ایران

ارزیابی مقالات

- داوری بیش از ۳۵۰ مقاله برای مجلات علمی-پژوهشی، کنفرانسهای برق، کامپیوتر، رمز، IST، IKT و WITDI در موضوعات گوناگون، رمزنگاری، امنیت شبکه، پروتکل‌های رمزنگاری

کنفرانس ها

۱- عضو کمیته علمی هشتمین کنفرانس انجمن رمز ایران – شهریور ماه ۹۰

۲- عضو کمیته علمی هفتمین کنفرانس انجمن رمز ایران – شهریور ماه ۸۹

۳- عضو کمیته علمی ششمین کنفرانس انجمن رمز ایران – مهرماه۸۸

۴- عضو کمیته علمی پنجمین کنفرانس انجمن رمز ایران – مهرماه۸۷

۵- عضو کمیته علمی چهارمین کنفرانس انجمن رمز ایران – مهرماه ۸۶

۶- عضو کمیتهٔ اجرائی و کمیتهٔ علمی سومین کنفرانس انجمن رمز ایران – شهریور ۸۴

۷- عضو کمیتهٔ علمی دهمین کنفرانس انجمن کامپیوتر ایران – بهمن ۸۳

۸- دبیر دومین کنفرانس انجمن رمز ایران – مهرماه ۸۲ – دانشگاه صنعتی شریف – تهران – ایران

۹- عضو کمیته علمی دومین کنفرانس انجمن رمز ایران

۱۰- عضو کمیته علمی کنفرانس IST 2003

۱۱- عضو کمیته علمی کنفرانس IKT 2003 و IKT 2004

۱۲- عضو کمیته علمی کنفرانس WITID 2004

۱۳- عضو کمیته علمی اولین کنفرانس رمز ایران

انتشارات

مقالات چاپ شده در مجلات بین‌المللی

Publications (from 1997 to 2011)

Journal papers

1. S. Salimi, M. Salmasizadeh, M. R. Aref. Rate Regions of Secret Key Sharing in a New Source Model. *IET Communications*, vol. 5, no. 4, pages 443-456,2011.

2. S. Salimi, M. Salmasizadeh, M. R. Aref. Generalized Secure Distributed Source Coding with Side Information. *IET Communications,* volume 4, no. 18 , pages 2262-2272, 2010.

3. Z. Ahmadian, J. Mohajeri, M. Salmasizadeh, A. R. Nyberg and M.Hakala. A practical distinguisher for the Shannon cipher , *The Journal of Systems and Software*, no. 83, pages 543-547, Esevier Ltd. 2010.

4. K. Azimian, J. Mohajeri and M. Salmasizadeh. Provable partial key escrow, *Internation Journal of Network Security*, volume 10, no.2 pages 124-128, 2010.

5. A. Moradi, M. Salmasizadeh, M. T. Manzuri and T. Eisenbarth. Vulunerability *modeling of cryptographic hardware to power analysis attacks, Integration, the VLSI Journal,* volume 42, no. 2, pages 468-478, Esevier Ltd. 2009.

6. A. Moradi, M. T. Manzuri and M. Salmasizadeh. Dual-rail transition logic: a logi style for counteracting power analysis attacks. *Special issue: Circuits and Systems for Real-Time security and copyright protoction of Multimedia, International Journal of Computers and Electrical Engineering, Elsevier Ltd. No. 35 pp. 359-369, 2009.*

7. A. Bagherzandi, M. Salmasizadeh and J. Mohajeri. A related key attack on the Feistel type block ciphers, *International Journal of Network Secuirty*. Volume 8, no.2. pp., 2009.

8. K. Azimian, J. Mohjajeri and M. Salmasizadeh, Weak composite Diffie-Hellman, *International Journal of Network Security*,. Volume 7, no.3, pp. 383-387, 2009.

9. A. Bagherzandi, M. Salmasizadeh and J. Mohajeri. Comparison based semantic security is probabilistic polynomial time equivalent to indistinguishability, *International Journal of Network Secuirty*. Volume 6, no.3. pp.354-360, 2008.

10. M. Rajabzadeh Assar, J. Mohajeri and M.Salmasizadeh. Another security improvement over the Lin et al,'s E_voting scheme. *Int. J. Electronic Security and Digital Forensics,* Inderscience Enterptise Ltd. No. 4, pp.413-422, 2008.

11. A. Moradi, M. Salmasizadeh, and M. T. Manzuri. From fault tolerance to fault attack tolerance in the implementation of Advanced Encryption Standard, *CSI Journal on Computer Science and Engineering*, volume 4, no. 2, pages 32-38, 2006.

12. J. Dj. Golic, M. Salmasizadeh, and E. Dawson. Statistical weakness of multiplexed sequences, *Finite Fields and Their Applications,* no. 8, pages 420-433, Elsevier science, 2002.

13. J. Dj. Golic, M. Salmasizadeh, and E. Dawson. Fast correlation attacks on the summation generator. *Journal of Cryptology,* volume 13, no. 2, pages 245-262, Springer, 2000.

14. L. Simpson, J. Dj. Golic, M. Salmasizadeh and E. Dawson. A fast correlation attack on the multiplexer generators*, Information Processing Letters*, volume 70, pages 89-93, Elsevier, 1999.

15. J. Dj. Golic, M. Salmasizadeh,L. Simpson, and E. Dawson. Fast correlation attacks on nonlinear filter generators. *Information Processing Letters,* volume 64, Pages 37-42, Elsevier, 1997.

مقالات پذیرفته شده در مجلات بین المللی

Accepted papers

1. S. Salimi, M. Salmasizadeh, M. R. Aref. Key agreement over multiple access channel, IEEE Transactions on Information Forensics and Security.

مقالات چاپ شده در مجلات داخلی

۱- محسن بهداری محمود سلماسی‌زاده و جواد مهاجری .معماری امنیتی سیستم تلفن همراه نسل دوم و آسیب‌پذیری‌های آن ، فصل نامهٔ علمی – پژوهشی شریف، شماره ۳۸، صفحات ۴۱-۳۱، ۱۳۸۶.

۲- اعظم شادمان، جواد مهاجری و محمود سلماسی زاده. حمله تمایز بر نوع ساده شده رمز دنباله‌ایWG-128 فصل نامهٔ علمی – پژوهشی شریف، شماره ۵۲، صفحات ۶۱-۵۷ ، ۱۳۸۸.

مقالات ارائه شده در کنفرانسهای بین‌المللی

Refereed Conference Papers

1- B. Zakeri, M. Salmasizadeh, A. Moradi, M. Tabandeh and M. T. Manzuri. Compact and secure design of masked AES S-box, In S. Qing, H. Imaiand G. Wang (Eds.): 9th International Conference on Information and Communications Security ICICS2007, *Lecture Notes in Computer Science* volume 4861, pp. 216-229, Springer 2007.

2- A. Moradi, M. T. Manzuri and M. Salmasizadeh. Power analysis attacks on MDPL and DRSL impementations. In K,-H.Nam and G. Rhee(Eds.): the 10th International Conference on Information Security and cryptplogy ICISC 2007, *Lecture Notes in Computer Science* volume 4817, pp. 259-272, Springer 2007.

3- K. Azimian, J. Mohajeri and M. Salmasizadeh, A new Public key Encryption scheme equivalent to factoring. In proceeding of the 2007 International Conference on Security and Management (SAM'07), June 25-28 2007, Lasvegus U.S.

4- A. Moradi, M. T. Manzouri and M. Salmasizadeh. A Generalized Method of Differential Fault Attack Against AES Cryptosystem, In *Lecture Notes in Computer Science, volun 4249 pp. 91-100, Springer 2006.*

5- M. R. Sohizadeh, M. Salmasizadeh and J. Mohajeri. An Efficient Micro-payment System, Based on Prompt and light-weight Cryptographic Operations. *In Proceedings of 11th International Computer Conferece (CSICC' 2006)*, pages 161-166, Jan. 24-26, 2006, Tehran- Iran.

6- M. R. Reyhanitabar, M. Salmasizadeh and J. Mohajeri. On The Security of Some Quasigroup Based Encryption Algorithms, *In Proceedings of International Symposium on telecommunications (IST 2005)*, pages 71-75, Sep.10-12, 2005, Shiraz-Iran.

7- M. R. Sohizadeh Abianeh, M. Salmasizadeh and J. Mohajeri. A navel Approach for Authentication in Networks on Computer-Constrained Devices. *In Proceedings of International Symposium on telecommunications (IST 2005)*, pages 241-245, Sep.10-12, 2005, Shiraz-Iran.

8- S. Fayyaz Shahandashti, M. Salmasizadeh and J. Mohajeri. A Provably Secure Transitive Signature Scheme from Bilinear Maps. In Carlo Blundo and Stelvion Cimato, editors, 4th Conference on Security in Communication Networks, 2004, volume 3352 of *Lecture Notes in Computers Science*, Pages 60-76, Springer, 2005.

9- M. Salmasizadeh and Iman Mossavat. Provable Security as a Paradigm for Practical Cryptographic Protocol Design, *In Proceedings of The 2nd Workshop on Information Technology & Its Disciplines (WITID 2004)*, Pages 179-191. February 24-26, 2004 Kish Island-Iran.

10- M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri. On the Security of Private Keys on Smart Cards under Timing Attack, *In Proceedings of International Symposium on Telecommunications (IST 2003)*, Pages 382-385. August, 16-18, 2003 Isfahan-Iran.

11- J. Mohajeri and M. Salmasizadeh. Cryptanalysis of a clock-controlled keystream generator, *In Proceedings of International Symposium on Telecommunications (ISI 2001)*, Pages 468-471. September 1-3, 2001 Tehran, Iran.

12- J. Dj. Golic, L. Simpson, E. Dawson and M. Salmasizadeh. Fast correlation attacks on the multiplexer generators. In *Proceedings of 1998 IEEE International Symposium On Information Theory*, Pages 270-270. MIT, Cambridge, MA, USA, 1998.

13- M. Salmasizadeh, J. Dj. Golic, E. Dawson, L. Simpson. A systematic procedure for applying fast correlation attacks to combiners with memory, In *Proceedings of SAC' 97,* Canada 11-12 August, 1997. PP.102-116.

14- M. Salmasizadeh, J. Dj. Golic, L. Simpson, and E. Dawson. Fast correlation attacks and multiple linear approximations. In V.Varadharjan, J. Pieprzyk and Y. MU editors, Second Australian Conference on Information Security and Privacy 1997, volume 1270 of *Lecture Notes in computer science*, pages 228-239. Springer- Verlag, 1997.
15- J. Dj. Golic, M. Salmasizadeh, E. Dawson, and A. Khodkar. Cryptanalysis of the summation
generator with three input lfsrs. In *Proceedings of International Symposium on Information Theory and Its Application 1996*, volume 1, pages 343-346. The University of Victoria, 1996.
16- J. Dj. Gloic, M. Salmasizadeh, A. Clark, A. Khodkar, and E. Dawson. Discrete optimisation and fast correlation attacks. In E. Dawson and J. Golic, editors, *Cryptography: Policy and*
Algorithms, volume 1029 of *Lecture Notes in Computer Science*, pages 186-200. Springer-Verlag, 1996.
17- J. Dj. Golic, M.Salmasizadeh, and E.Dawson. Autocorrelation weakness of multiplexed sequences. In *Proceedings of International Symposium on Information Theory and Its Applications 1994*, volume 2, pages 983-987. The Institution of Engineers, Australia, 1994.

مقالات ارائه شده در کنفرانس‌های ملی

1- A. Moradi, M. Salmasizadeh, M. T. Manzuri. Combination of side channel and collision attacks to reveal the secret of gate masked implementations. In *Proceedings of 4th Iranian Society of Cryptology Conference* (ISCC 2007), Pages 9-16, October 16-18, 2007, Iran University of Science Technology.
2- B. Zakeri, M. Salmasizadeh, A. Moradi, M. Tabandeh and M.T. Manzuri. A Compact design of Multiplicative masked AES S-Box, In *Proceedings of 4th Iranian Society of Cryptology Conference* (ISCC 2007), Pages 25-30, October 16-18, 2007, Iran University of Science Technology.
۳- نصور باقری، جواد مهاجری و محمود سلماسی‌زاده. تحلیل تفاضلی الگوریتم رمز آایـن ۱، مجموعهٔ مقالات چهارمنی کنفرانس انجمن رمز ایران صفحات ۱۶-۹، مهرماه ۱۳۸۶، دانشگاه علم و صنعت ایران، تهران.
4- K. Azimian, A. Bagherzandi, J. Mohajeri and M. Salmasizadeh. Computing Root Modulo a Composite, *In Proceedings of 3rd Iranian Society of Cryptology Conference (ISCC 2005)*, pages 9-14, Sep. 7-8, 2005 Isfahan University of Technology Isfahan, Iran.
۵- مریم امیرمزلقانی، محمود سلماسی‌زاده، جواد مهاجری، طرحی جدید برای پرداخت دقیق الکترونیکی با حفظ گمنامی کاربر، مجموعه مقالات سومین کنفرانس رمز ایران، صفحات ۲۰۴-۱۹۱، شهریور ۱۳۸۴، دانشگاه صنعتی اصفهان، اصفهان-ایران.
۶- علی‌باقر زندی، کوشیار عظیمیان، جواد مهاجری، محمود سلماسی‌زاده، بررسی ارتباط بین امنیت معنایی و تمایز ناپذیری در برابر حملات متن آشکار منتخب، متن رمز منتخب غیر تطبیقی و متن رمز منتخب تطبیقی در چارچوب مدل مقایسه‌ای، مجموعهٔ مقالات سومین کنفرانس رمز ایران، صفحات ۲۲۸-۲۱۵، شهریور ۱۳۸۴، دانشگاه صنعتی اصفهان، اصفهان – ایران.

۷- محمود سلماسی‌زاده، جواد مهاجری، بهروز حاجیان‌نژاد، امنیت تبادل اطلاعات در شبکه‌های کنترل صنعتی، مجموعه مقالات دهمین کنفرانس سالانه انجمن کامپیوتر ایران، صفحات ۹۶-۸۴، بهمن ۱۳۸۳، مرکز تحقیقات مخابرات- ایران.

۸- شریف‌الدین منصوری، محمود سلماسی‌زاده، جواد مهاجری، نقطه ضعفی دیگر در الگوریتم رمز دنباله‌ای Shrinking Generator، مجموعه مقالات دهمین کنفرانس سالانه انجمن کامپیوتر ایران، صفحات ۵۷-۵۰، بهمن ۱۳۸۳، مرکز تحقیقات مخابرات – ایران.

۹- کوشیار عظیمیان، جواد مهاجری، محمود سلماسی‌زاده، ارائه یک الگوریتم جدید تجزیه اعداد مبتنی بر روش غربال مربعات، مجموعه مقالات دهمین کنفرانس سالانه انجمن کامپیوتر ایران، صفحات ۷۴۱-۷۳۴، بهمن ۱۳۸۳، مرکز تحقیقات مخابرات - ایران.

۱۰-رضا سپهی، محمود سلماسی‌زاده و بابک صادقیان، تحلیل خطی الگوریتم رمز معماگر ۵ مرحله‌ای، مجموعه مقالات نهمین کنفرانس سالانه انجمن کامپیوتر ایران، صفحات ۶۱۷-۶۰۶، بهمن ۱۳۸۲، دانشگاه صنعتی شریف – ایران.

۱۱-محمدرضا ریحانی‌تبار، محمود سلماسی‌زاده و جواد مهاجری، مخلوط کننده ۶۴ بیتی آراز – ۶۴، مجموعه مقالات دومین کنفرانس انجمن رمز ایران، صفحات ۱۴۱-۱۳۱، مهرماه ۱۳۸۲، دانشگاه صنعتی شریف – ایران.

۱۲-محمود سلماسی‌زاده و محمدرضا ریحانی‌تبار، بررسی و مقایسه امنیت و کارایی الگوریتم‌های رمز با کلید همگانی مبتنی بر کدهای تصحیح خطای خطی، مجموعه مقالات دومین کنفرانس انجمن رمز ایران، صفحات ۱۵۷-۱۴۲، مهرماه ۱۳۸۲، دانشگاه صنعتی شریف – ایران.

۱۳-محمدرضا ریحانی‌تبار، محمود سلماسی‌زاده و جواد مهاجری، حمله به الگوریتم‌های نامتقارن مبتنی بر توان رسانی همنهشتی با روش تحلیل زمانی، مجموعه مقالات دومین کنفرانس انجمن رمز ایران، صفحات ۷۰-۵۸، مهرماه ۱۳۸۲، دانشگاه صنعتی شریف – ایران.

۱۴-محمدرضا ریحانی‌تبار، محمود سلماسی‌زاده و جواد مهاجری، حمله به پیاده سازی کلاسیک RSA در کارتهای هوشمند با روش تحلیل خطا، مجموعه مقالات دومین کنفرانس انجمن رمز ایران، صفحات ۷۹-۷۱، مهرماه ۱۳۸۲، دانشگاه صنعتی شریف – ایران.

۱۵- حسن بولوردی، جواد مهاجری و محمود سلماسی‌زاده، امضاء دیجیتال گروهی آستانه، مجموعه مقالات هشتمین کنفرانس سالانه انجمن کامپیوتر ایران، صفحات ۳۷-۳۱، اسفند ۱۳۸۱، دانشگاه فردوسی مشهد – ایران.

۱۶- سیدمهدی‌محمد حسن‌زاده، جواد مهاجری و محمود سلماسی‌زاده. یک حملهٔ جدید برای بدست آوردن حالت اولیه زیر ساختارهائی از یک سیستم رمز مبتنی بر انتقال نامنظم با پارامترهای ۱ و ۲، مجموعه مقالات

هفتمین کنفرانس سالانه انجمن کامپیوتر ایران صفحات ۱۲-۱، اسفند ۱۳۸۰، مرکز تحقیقات مخابرات، تهران - ایران.

۱۷- محمدرضا ریحانی‌تبار، محمود سلماسی‌زاده و جواد مهاجری. حمله به کارت هوشمند با تحلیل توان الکتریکی مصرفی، مجموعهٔ مقالات اولین کنفرانس رمز ایران، صفحات ۱۴۹-۱۳۹، آبان ۱۳۸۰ – دانشگاه امام حسین (ع)، تهران – ایران.

۱۸- وریا حواری‌نسب، محمدرضا ریحانی‌تبار، محمود سلماسی‌زاده و جواد مهاجری. مقایسه الگوریتمهای رتبه اول و آخر در گزینش نهائی AES. مجموعهٔ مقالات اولین کنفرانس رمز ایران، صفحات ۲۶۷-۲۵۳، آبان ۱۳۸۰ – دانشگاه امام حسین (ع)، تهران - ایران.

۱۹- الهام شاهین‌فرد و محمود سلماسی‌زاده. طراحی یک الگوریتم رمز قطعه‌ای جدید برپایه الگوریتم RC6. مجموعهٔ مقالات اولین کنفرانس رمز ایران، صفحات ۲۱۲-۲۰۷، آبان ۱۳۸۰ – دانشگاه امام حسین (ع)، تهران – ایران.

۲۰- سیدمهدی‌محمد حسن‌زاده، جواد مهاجری و محمود سلماسی‌زاده. روش جدیدی برای تحلیل سیستم‌های رمز دنباله‌ای مبتنی بر انتقال نامنظم مجموعهٔ مقالات اولین کنفرانس رمز ایران، صفحات ۱۶۱-۱۵۱، آبان ۱۳۸۰ – دانشگاه امام حسین (ع)، تهران - ایران.

سخنرانی مدعو

۱- محمود سلماسی‌زاده. جنگ اطلاعات و امنیت، سخنران مدعو در اولین کنفرانس رمز ایران، مجموعهٔ مقالات اولین کنفرانس رمز ایران، صفحات ۱۷-۷، آبان ۱۳۸۰ – دانشگاه امام حسین (ع)، تهران – ایران.

گزارشات پژوهشی:

۱) محمود سلماسی‌زاده، محمدرضا سهی‌زاده ابیانه "طراحی روش احراز اصالت یکباره در شبکه‌های همگن" مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۵.

۲) جواد مهاجری، محمود سلماسی‌زاده، کوشیار عظیمیان "بررسی و تحلیل روشهای دست‌یابی قانونی به کلید"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۳.

۳) محمود سلماسی‌زاده، جواد مهاجری "بررسی امنیت فن‌آوری اطلاعات در سیستمهای کنترل صنعتی"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۲.

۴) جواد مهاجری، محمود سلماسی‌زاده، "تحلیلی نو از سیستمهای رمز دنباله‌ای مبتنی بر انتقال نامنظم" مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۲.

۵) جواد مهاجری، محمود سلماسی‌زاده "بررسی روشهای حمله تقسیم‌کن و پیروز شو بر علیه سیستمهای رمز دنباله‌ای"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۱.
۶) محمود سلماسی‌زاده، جواد مهاجری "ساز و کارهای لازم برای پیاده‌سازی تجارت الکترونیک"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۱.
۷) جواد مهاجری، محمود سلماسی‌زاده "روشهای حمله تقسیم‌کن و پیروزشو علیه سیستم‌های رمز دنباله‌ای"، مجموعه مقالات دانشگاه صنعتی شریف، ۱۳۸۰.
۸) محمود سلماسی‌زاده، جواد مهاجری، "مطالعه استاندارد رمزگذاری پیشرفته AES و نتایج حاصل از تحلیل‌های انجام شده بر روی آن" مجموعهٔ مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۸۰
۹) محمود سلماسی‌زاده، "تحلیل آماری رمزهای قطعه‌ای متقارن"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۷۹.
۱۰) جواد مهاجری، محمود سلماسی‌زاده، "جمع‌آوری و بررسی روشهای تحلیل سیستمهای رمز دنباله‌ای"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۷۹.
۱۱) محمود سلماسی‌زاده، "بررسی ترکیب‌کننده‌های حافظه‌دار"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف ۱۳۷۸
۱۲) جواد مهاجری، محمود سلماسی‌زاده، "جمع‌آوری و بررسی روشهای تحلیل سیستمهای رمز دنباله‌ای"، مجموعه مقالات پژوهشی دانشگاه صنعتی شریف، ۱۳۷۸.
۱۳) محمود سلماسی‌زاده، جواد مهاجری، امیر دانشگر، کیومرت کاوه‌مریان، سعید میرزائی، شهرام شفیها، "امنیت سیستمهای رمزنگاری دنباله‌ای و رمزنگاری با کلید غیرمحرمانه"، کارنامه پژوهشی شریف، ۱۳۷۱.
۱۴) محمود سلماسی‌زاده، جواد مهاجری، امیر دانشگر، جمشید شکرالهی، یدا... قاسمی، "امنیت سیستمهای رمزنگاری دنباله‌ای و رمزنگاری با کلید غیرمحرمانه"، کارنامهٔ پژوهشی شریف، ۱۳۷۰.
۱۵) محمود سلماسی‌زاده، امیر دانشگر، "حفاظت اطلاعات در کامپیوترهای شخصی"، کارنامهٔ پژوهشی شریف ۱۳۶۹.
۱۶) محمود سلماسی‌زاده، جواد مهاجری، "کد ژنراتور"، کارنامهٔ پژوهشی شریف ۱۳۶۸.
۱۷) محمود سلماسی‌زاده، محمود زارع‌پور، جواد مهاجری، امیر دانشگر، حسین سپاسی، "کد ژنراتور" کارنامهٔ پژوهشی شریف، ۱۳۶۶.