UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Efficient Post-Quantum and Compact Cryptographic Constructions for the Internet of Things

by

Rouzbeh Behnia

For the Ph.D. degree in Computer Science and Engineering

IoT systems often rely on low-end devices to send measurements to other parties, and depending on the setting, unauthorized alteration and/or privacy violation of these measures can have catastrophic consequences (e.g., embedded medical sensors). Therefore, providing efficient authentication, integrity, and confidentiality in these settings is vital. While conventional cryptographic measures (e.g., ECDSA) can be used to meet these security requirements, despite their elegant design, they are often too computationally expensive for low-end devices. This is further exacerbated when security against quantum computers is taken into the account.

In this work, we propose a series of new efficient conventional and post-quantum cryptographic schemes to meet the stringent requirement of such IoT systems. Our proposed schemes provide high efficiency as compared to their existing counterparts. In this talk, we present new identity-based and certificateless cryptosystems that lift the burden of certificate (chain) communication and verification, which might be too costly for some IoT system. The new systems, aside from being more efficient than their counterparts, provide compatibility to enable users from different domains (identity-based or certificateless) to communicate seamlessly. Additionally, in a step toward a fully post-quantum secure blockchain, we propose a new proof-of-work (PoW) protocol that minimizes the advantage of a quantum miner, as compared to a classical one. The parameters of the new PoW are easy to fine tune to adjust its difficulty.

Examining Committee
Kaiqi Xiong, Ph.D., Chairperson
Attila A. Yavuz, Ph.D. , Major Professor
Mehran Mozaffari Kermani, Ph.D.
Jay Ligatti, Ph.D.
Xinming (Simon) Ou, Ph.D.
Mike Rosulek, Ph.D.

Wednesday, March 24, 2021
12:00 PM
Online (Microsoft Teams)
Please email for more information
behnia@usf.edu
THE PUBLIC IS INVITED

Publications

1) Singla, A., **Behnia, R**., Hussain, S. R., Yavuz, A. A., Bertino, E, (2021, June). Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations. In the 16th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2021) (Accepted)
2) **Behnia, R**., Yavuz, A. A., Ozmen, M. O., & Yuen, T. H. (2020, December). Compatible Certificateless and Identity-Based Cryptosystems for Heterogeneous IoT. In International Conference on Information Security (ISC) (pp. 39-58). Springer, Cham.
3) Hoang, T., **Behnia, R**., Jang, Y., & Yavuz, A. A. (2020, March). MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves. In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (CODASPY) (pp. 17-28).
4) Ozmen, M. O., Yavuz, A. A., & **Behnia, R.** (2019, June). Energy-Aware Digital Signatures for Embedded Medical Devices. In 2019 IEEE Conference on Communications and Network Security (CNS) (pp. 55-63). IEEE.
5) **Behnia, R**., Ozmen, M. O., & Yavuz, A. A. (2019, May). ARIS: Authentication for Real-Time IoT systems. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
6) Ozmen, M. O., **Behnia, R.,** & Yavuz, A. A. (2019, February). Fast Authentication From Aggregate Signatures with Improved Security. In International Conference on Financial Cryptography and Data Security (FC) (pp. 686-705). Springer, Cham.
7) **Behnia, R**., Ozmen, M. O., & Yavuz, A. A. (2018). Lattice-Based Public Key Searchable Encryption From Experimental Perspectives. IEEE Transactions on Dependable and Secure Computing (TDSC), 17(6), 1269-1282.
8) **Behnia, R.**, Ozmen, M. O., Yavuz, A. A., & Rosulek, M. (2018, October). Tachyon: Fast Signatures From Compact Knapsack. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS) (pp. 1855-1867).
9) Ozmen, M. O., **Behnia, R**., & Yavuz, A. A. (2018, May). Compact Energy and Delay-Aware Authentication. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE. **Equally contributing first and second authors.**
10) **Behnia, R**., Yavuz, A. A., & Ozmen, M. O. (2017, July). High-Speed High-Security Public Key Encryption with Keyword Search. In IFIP Annual Conference on Data and Applications Security and Privacy (DBSec) (pp. 365-385). Springer, Cham.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.