Rawane Issa

rawaneissa@gmail.com ra1issa ra1issa.com @ra1issa in/ra1issa

Research Interests

I am interested in Applied Cryptography and specifically in the design and analysis of efficient protocols for secure computation. I most recently worked on a more efficient *private information retrieval* construction and on *content moderation in end to end encrypted messengers*.

Education

2022 **Ph.D., Boston University**, Computer Science.
Applied Cryptography.

2018 **Masters, Boston University**, Computer Science.
Applied Cryptography.

2016 **Bachelors in Engineering, American University of Beirut**, Computer and Communication Engineering, with a Minor in Mathematics.

Publications

1. AlHaddad, N., Issa, R., & Varia, M. (2021). Content moderation in end-to-end encrypted messaging with sealed sender. Unpublished, submitted for review.

2. Archer, D., O'Hara, A., Issa, R., & Straus, S. (2021). Technical report: Sharing sensitive department of education data across organizational boundaries using secure multiparty computation. https://github.com/Ra1issa/ra1issa-website/blob/main/NCES_Demo_Paper_technical.pdf. Accessed: 2021-10-30.

3. Albab, K. D., Issa, R., Varia, M., & Graffi, K. (2020). Batched differentially private information retrieval. Cryptology ePrint Archive, Report 2020/1596. https://ia.cr/2020/1596.

4. Dak Albab, K., Issa, R., Lapets, A., Flockhart, P., Qin, L., & Globus-Harris, I. (2019). Tutorial: Deploying secure multi-party computation on the web using jiff. In *2019 ieee cybersecurity development (secdev)*. doi:10.1109/SecDev.2019.00013

5. Lapets, A., Dak Albab, K., Issa, R., Qin, L., Varia, M., Bestavros, A., & Jansen, F. (2019). Role-based ecosystem for the design, development, and deployment of secure multi-party data analytics applications. In *2019 ieee cybersecurity development (secdev)* (pp. 129–140). doi:10.1109/SecDev.2019.00023

6. Lapets, A., Jansen, F., Albab, K. D., Issa, R., Qin, L., Varia, M., & Bestavros, A. (2018). Accessible privacy-preserving web-based data analysis for assessing and addressing economic inequalities. In *Proceedings of the 1st acm sigcas conference on computing and sustainable societies*. doi:10.1145/3209811.3212701

7. Albab, K. D., Issa, R., Lapets, A., Bestavros, A., & Volgushev, N. (2017). Scalable secure multi-party network vulnerability analysis via symbolic optimization. In *2017 ieee security and privacy workshops (spw)* (pp. 211–216). doi:10.1109/SPW.2017.21

Projects

Hecate I worked on designing and building an efficient new asymmetric message franking (AMF) construction. This construction combines the functionalities of AMF and source tracking while providing all the security guarantees of any state of the art E2E messaging system, like Signal, from simple cryptographic assumptions. [coming soon]

BatPIR I worked on designing and building a novel efficient private information retrieval protocol with differentially private leakage for cases with high query rates with respect to the database size. [url: *github.com/multiparty/DP-PIR*]

Carousel I worked on designing and building a language and protocol agnostic static analyzer for estimating resource usage of MPC programs with examples in JIFF and Obliv-Rust. These resources include, but are not restricted to the number of online/offline rounds of communication, the number of online/offline messages, etc. [url: *github.com/multiparty/carousels*]

Doed As part of my internship at Galois inc., I worked on a pilot that demonstrated to the U.S. Department of Education how multiparty computation can efficiently and securely perform any statistics needed for evidence base policy making in-between agencies with no recourse to anyone outside the department itself and without any privacy risks. [url: *github.com/Raissa/match-compute*]

JIFF I built a multipurpose MPC framework (JIFF) that allowed both the Boston Women's Workforce Council and the Greater Boston Chamber of Commerce to securely run their periodic analysis on economic inequalities. [url: *github.com/multiparty/jiff*]

Languages

Human Languages	English, Arabic, French.
Programming Languages	Rust, C, C++, Python, MATLAB, Javascript, Java, x86 Assembly, HTML, CSS.

Industry Experience

Fall 2020	**Galois, inc.**, Research Intern
2017-2019	**SAIL**, Software Engineering Fellow.
Summer 2015	**UBILITY**, Software Engineering Intern.

Services

Subreviewer	**Usenix** [2020-2021], **CCS** [2021] ,**TCC** [2020].
Supervisor	Mentored and supervised undegraduate students [2017-2019].

Teaching

2020 **CS591L1**: Embedded Languages and Frameworks, co-Lecturer, Boston University [url: kinan-bab.github.io/CS591L1/].

2017 **CS235: Algebraic Algorithms**, Teaching Fellow, Boston University.

Awards

2020 **Teaching Excellency Award**, Boston University.

2017 **Hariri Fellowship**, Boston University.

2016 **Dean's Creative Achievement Award**, American University of Beirut.

Dean's Honor List for Fall, American University of Beirut.

Invited Talks

December 2018 & March 2019

MACS/DIMACS — Privacy Preserving Route Recommendation, [url: *bu.edu/macs/workshops/meeting-dec-2018/*, *bu.edu/hic/2019-dimacs-workshop/*].