Proposed Project on Onion Routing in the Asynchronous Setting

Background. The ability to communicate anonymously is an increasingly vital component of digital life and citizenship. From Iranian protesters wishing to safely to inform the world what is happening in the streets of Tehran, to Russian citizens trying to communicate with outside media, anonymity gives people all over the world a chance to exercise their fundamental rights without fear of repercussions. Practical tools such as Tor [DMS04] (i.e., "The onion router," inspired by Chaum's onion routing idea [Cha81] described below) or VPNs have a lot of room for improvement. Both are easily blocked, and neither guarantees privacy even from the network adversary (e.g., a standard model for a resourceful ISP- or AS-level adversary) [MD05, SEV+15, WSJ+18, Rop21].

A communications protocol is anonymous [ALU21] if for any pair of input vectors (σ_0, σ_1) that differ only on the inputs and outputs[1] of honest parties (e.g., Alice sends to Bob in σ_0 and to Charlie in σ_1), the adversary (whose capabilities vary depending on the adversarial model) cannot tell from interacting with the honest nodes in a protocol run whether the input was σ_0 or σ_1.[2]

The goal of research on onion routing [Cha81, Cha88, CL05, vdHLZZ15, ALU18, KBS20, ALU21, AL21, KHRS21, ACLM22] is to achieve this definition in the presence of a malicious adversary corrupting a fraction of the participants, with a communication- and computation- efficient, fault-tolerant and decentralized protocol. In an onion routing protocol, to send a message to Bob, Alice first picks a sequence of intermediary parties $I_1, \ldots, I_{\ell-1}$ and then forms a layered cryptographic object called an onion using the message and the routing path $(I_1, \ldots, I_{\ell-1}, \text{Bob})$. Alice then sends the onion to the first intermediary I_1 on the routing path who peels off just the outermost layer of the onion (i.e., processes the onion) and sends the peeled onion O_2 to the next party I_2 on the routing path, I_2 peels O_2 and sends the peeled onion O_3 to I_3, and so on. This procedure continues until Bob receives the message from Alice.

In an onion routing protocol that uses standard cryptographic onions [CL05], even a powerful adversary who can corrupt (and "look into" or even control) some of the parties cannot link an honest party's incoming onion to its outgoing onion. This lack of transparency allows for shuffling onions when they are batch-processed at an honest party [RS93, BFT04, IKK05, ALU18].

Prior Results and Technical Challenge. In recent years, several protocols were presented as provably secure yet practical solutions [CBM15, vdHLZZ15, TGL+17, KCDF17, ALU18, ALU21]. However, all these protocols' security analysis requires synchronous communication. In the synchronous communications setting, time progresses in rounds, and message transmissions are lossless and instantaneous. While modeling communications in this way makes designing and analyzing anonymity protocols more tractable, it is somewhat of a cheat. Currently deployed anonymity protocols, such as Tor [DMS04] and Loopix [PHE+17], are known to be vulnerable to traffic analysis attacks [MD05, SEV+15, WSJ+18, AMWB23] that exploit the asynchronous nature of communication in the real world.

Constructing a solution for the asynchronous setting is challenging because the adversary can easily influence the traffic flow, for example, by mounting a BGP interception attack [SEV+15], so that a targeted message arrives with an expected and observable delay. The adversary can do this even if the onions are batch-processed and even if we are willing to pay a cost by increasing the latency and/or volume of dummy traffic. This attack method breaks the anonymity of every known protocol designed and proven secure for the synchronous setting; this is a problem that

[1] Here, by "output" of a party P we mean a set of messages $\{m\}$ such that some party P' receives (m, P) as part of its input. I.e. P' intends to send m to P.

[2] Alternative definitions of anonymity exist [BKM+13, KBS+19], but we will be referring to the standard cryptographic definition here.

is not trivially fixable by using sychronizers (which assume no failures) or clock synchronization algorithms (which guarantees that most if not all of the honest parties are synchronized) [Lyn96].

In a recent paper, Ando, Lysyanskaya, and Upfal [to be ePrinted soon] presented the first provably anonymous protocol for the asynchronous communications setting. The key tool that this protocol relies on is the novel cryptographic object dubbed *bruisable* onion encryption. The idea of bruisable onion encryption is that even though neither the onion's path nor its message content can be altered in transit, an intermediate router on the onion's path that observes that the onion is delayed can nevertheless slightly damage, or bruise it. An onion that is chronically delayed will have been bruised by many intermediaries on its path and become undeliverable. This prevents timing attacks and yields a differentially private onion routing protocol in the asynchronous setting. While this recent development proves the possibility of anonymity in a fully asynchronous network, many further question were left open for further research. For instance, there are currently no fully anonymous solutions in the asynchronous setting.

Proposed Project. The objective of this project is to design new onion encryption primitives to enable fully anonymity in the asynchronous setting. Students who choose to work on this project can work closely with some subset of the authors of the bruisable onion paper.

References

[ACLM22] M. Ando, M. Christ, A. Lysyanskaya, and T. Malkin. Poly onions: Achieving anonymity in the presence of churn. In *TCC 2022, Part II*, *LNCS* 13748. Springer, Heidelberg, November 2022.

[AL21] M. Ando and A. Lysyanskaya. Cryptographic shallots: A formal treatment of repliable onion encryption. In *TCC 2021, Part III*, *LNCS* 13044. Springer, Heidelberg, November 2021.

[ALU18] M. Ando, A. Lysyanskaya, and E. Upfal. Practical and provably secure onion routing. In *ICALP 2018*, *LIPIcs* 107. Schloss Dagstuhl, July 2018.

[ALU21] M. Ando, A. Lysyanskaya, and E. Upfal. On the complexity of anonymous communication through public networks. In *2nd Conference on Information-Theoretic Cryptography (ITC 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[AMWB23] R. Attarian, E. Mohammadi, T. Wang, and E. H. Beni. Mixflow: Assessing mixnets anonymity with contrastive architectures and semantic network information. *Cryptology ePrint Archive*, 2023.

[BFT04] R. Berman, A. Fiat, and A. Ta-Shma. Provable unlinkability against traffic analysis. In *FC 2004*, *LNCS* 3110. Springer, Heidelberg, February 2004.

[BKM+13] M. Backes, A. Kate, P. Manoharan, S. Meiser, and E. Mohammadi. Anoa: A framework for analyzing anonymous communication protocols. In *Computer Security Foundations Symposium (CSF), 2013 IEEE 26th*. IEEE, 2013.

[CBM15] H. Corrigan-Gibbs, D. Boneh, and D. Mazières. Riposte: An anonymous messaging system handling millions of users. In *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2015.

[Cha81] D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[Cha88] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, January 1988.

[CL05] J. Camenisch and A. Lysyanskaya. A formal treatment of onion routing. In *CRYPTO 2005*, *LNCS* 3621. Springer, Heidelberg, August 2005.

[DMS04] R. Dingledine, N. Mathewson, and P. F. Syverson. Tor: the second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA*, 2004.

[IKK05] J. Iwanik, M. Klonowski, and M. Kutyłowski. Duo-onions and hydra-onions—failure and adversary resistant onion protocols. In *Communications and Multimedia Security*. Springer, 2005.

[KBS+19] C. Kuhn, M. Beck, S. Schiffner, E. A. Jorswieck, and T. Strufe. On privacy notions in anonymous communication. *Proc. Priv. Enhancing Technol.*, 2019(2):105–125, 2019.

[KBS20] C. Kuhn, M. Beck, and T. Strufe. Breaking and (partially) fixing provably secure onion routing. In *2020 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2020.

[KCDF17] A. Kwon, H. Corrigan-Gibbs, S. Devadas, and B. Ford. Atom: Horizontally scaling strong anonymity. In *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*. ACM, 2017.

[KHRS21] C. Kuhn, D. Hofheinz, A. Rupp, and T. Strufe. Onion routing with replies. In *ASIACRYPT 2021, Part II*, *LNCS* 13091. Springer, Heidelberg, December 2021.

[Lyn96] N. A. Lynch. *Distributed algorithms*. Elsevier, 1996.

[MD05] S. J. Murdoch and G. Danezis. Low-cost traffic analysis of tor. In *2005 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2005.

[PHE+17] A. M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, and G. Danezis. The loopix anonymity system. In *26th usenix security symposium (usenix security 17)*, 2017.

[Rop21] L. Ropek. Someone is running hundreds of malicious servers on the Tor network and might be de-anonymizing users. `https://tinyurl.com/2p999e8e`, December 2021.

[RS93] C. Rackoff and D. R. Simon. Cryptographic defense against traffic analysis. In *25th ACM STOC*. ACM Press, May 1993.

[SEV+15] Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang, and P. Mittal. RAPTOR: Routing Attacks on Privacy in Tor. In *USENIX Security Symposium*, 2015.

[TGL+17] N. Tyagi, Y. Gilad, D. Leung, M. Zaharia, and N. Zeldovich. Stadium: A distributed metadata-private messaging system. In *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*. ACM, 2017.

[vdHLZZ15] J. van den Hooff, D. Lazar, M. Zaharia, and N. Zeldovich. Vuvuzela: scalable private messaging resistant to traffic analysis. In *Proceedings of the 25th Symposium on Operating Systems Principles, SOSP 2015, Monterey, CA, USA, October 4-7, 2015*. ACM, 2015.

[WSJ+18] R. Wails, Y. Sun, A. Johnson, M. Chiang, and P. Mittal. Tempest: Temporal dynamics in anonymity systems. *PoPETs*, 2018(3):22–42, 2018.