The World Wide Web gradually becomes an essential part of our daily life in the digital age. The web architecture used to be a client-server model, in which clients (or browsers) request and fetch web contents, such as HTML, JavaScript and CSS, from web servers. Recently peer-to-peer (P2P) techniques have been introduced into the web infrastructure, which empower browsers to directly communicate with each other and form a P2P web overlay. On one hand, this web overlay decentralizes the web to provide better availability of web resources and efficiency of transferring these resources. On the other hand, this also brings the open and unsolved problems like privacy issues to the new web architecture. In this thesis, we not only analyze privacy and robustness issues in web overlays, but also propose solutions to address these issues using cryptographic and hardware primitives.

First, we present inference attacks in peer-assisted content delivery networks (CDNs) on top of web overlays, which can infer user's online activities such as browsing history. To thwart such attacks, we propose an anonymous peer-assisted CDN (APAC), which employs onion-routing techniques to conceal users' identities and uses region-based circuit selection algorithm to reduce performance overhead. Second, previous studies have shown that a global adversary is realistic, and it can reveal users' online activities (or access patterns) using long-term traffic analysis. Against such adversaries, we design an oblivious peer-to-peer content sharing system (OBLIVP2P), which uses new primitives such as distributed oblivious RAM (ORAM) in the P2P setting.

Lastly, we propose solutions to ensure the robustness of P2P primitives, as all the utilities and security / privacy properties provided by P2P protocols (including the aforementioned two protocols) are relied on the robustness of the correct execution of these protocols. Recent evidence suggests that malicious (or byzantine) nodes can easily join the open P2P systems and perniciously disrupt the execution of the given protocol to weaken the core utility (e.g., Bitcoin) or the anonymity guarantee (e.g., Tor). To ensure the robustness of protocols against such byzantine adversaries in contrast to the honest-but-curious ones in the
prior two works, we leverage a new hardware primitive, Intel software guard extensions (SGX). By enforcing our properties, we reduce the byzantine model to the general-omission model, where byzantine nodes have no extra advantage than omitting messages. We further propose new algorithms realizing two fundamental primitives and improve the efficiency of P2P protocols in the synchronous setting.