Post-quantum security of cryptographic transformations in the random oracle model

Huang, Y.

Conclusions

Provable security is at the heart of modern cryptography; it ensures that breaking the considered scheme is at least as difficult as solving a well-studied hard computational problem. However, this guarantee stands and falls with the correctness of the proof. Thus, it is essential that security proofs undergo sufficient scrutiny — and even then human errors may remain. For instance, the flaw in the original FSwA analysis not only remained unnoticed for over a decade, it reappeared in later, modified variants of the analysis.

In a field like cryptography (and maybe theoretical computer science in general), often there is no fully rigorous formalism available. Meanwhile, it has become standard to put major proofs into the appendices of submissions, which reviewers do not have to verify (and it remains unclear who will ever carefully verify them). For the two cases we discuss in this thesis (FSwA and BUFF), we were lucky enough to find alternative, correct proofs (albeit with a worse security loss and an adjustment to the security definition, respectively); in other cases we may not be as fortunate and possibly face "proven-secure" insecure schemes, if we do not pay sufficient attention to verifying security proofs.

In this context, it is also worth mentioning the importance of verifying security proofs using more reliable methods, e.g. mechanized proof checkers such as EasyCrypt. This has been a direction with many ongoing research efforts. In fact, the FSwA flaw, which reappeared in HSwA, was initially discovered in such a mechanized verification project, and parts of the new, fixed security proofs, as presented in Chapter 3, have also been verified using EasyCrypt.

Another takeaway is that, especially for new notions of security, formulating the "right" definition can be very non-trivial. For instance, in Chapter 4, we have spent a significant amount of effort investigating the achievability of different definitions of non-resignability (NR). Along the way, evidence is gradually accumulated regarding which definitions are reasonable, and which ones are not. However, there may potentially be other relevant aspects that we have not (extensively) treated in this thesis, such as practical applications of NR. Therefore, strictly speaking, the final call as to which definition is "right," is not ours to make. Like any newly established notion of security, it must be shaped and tested, over time, by the cryptographic community as a whole.