Chapter

6 Conclusion

This last chapter gives an overview of the topics presented in this thesis. Furthermore, we summarise the limitations of our current solution, possible future work and in which other domains our techniques can bring added value.

Identity Based Encryption (IBE) provides desirable properties to construct mechanisms to deliver privacy in OSNs. The minimal additional architectural support and the increased ease of key management represent a major motivation to implement IBE in OSNs. We show that using secret sharing and multi-PKGs there is no need to have a single trusted party, assuming that at most $t-1$ of the PKGs are compromised. Furthermore, the multiple PKG infrastructure can be maintained by several organisations, motivated by increased privacy in OSNs.

As a proof of concept, we have extended Scramble to rely on an IBE multi-PKG infrastructure for Facebook thereby demonstrating such extension presents a tolerable overhead to end-users. The result is a Firefox application that is more user friendly than previous alternatives since public keys are recognisable user `ids`. In contrast to the earlier abstract notion of a public key stored and authenticated on a complex public key infrastructure, users can immediately identify the owner of a public key.

Furthermore, the presented solution is practically applicable since it requires no changes to the current OSN infrastructure. This enables users to rely on our infrastructure even on OSNs that are reluctant to support these forms of increased confidentiality.

In contrast to previous solutions, our infrastructure is immediately ready to use. Users are no longer required to subscribe to an additional third party infrastructure before being able to send encrypted messages. Therefore, it is possible to share content with users not holding private keys to their identity since the valid public key is directly represented by their `id` in the OSN. This forces curious users to register if they wish to view the protected content shared with them. Privacy concerned users relying on cryptographic primitives are then no longer an isolated breed limited to communication with other privacy aware peers. Conversely, they serve as pioneers motivating other users in their environment to turn to similar solutions.

However, the presented implementation is only a proof of concept since it is currently only applicable as a Firefox extension on Facebook. We endeavour to obtain a full open source project that supports different browsers and OSNs. Furthermore, the server side implementation of our current solution is only simulated in a local environment. For use in distributed environments such as the internet, more advanced DKG protocols in the asynchronous setting should be considered. Another limitation of the achieved implementation is that it does not include an authentication mechanism with the OSN environment. For broad user adaption all these limitations should be resolved. However, responding to these issues is only a matter of implementation and not of deliberate design decisions. Therefore, the current implementation definitely lays the foundation for practical usable IBE on OSNs.

There are some important open challenges that call for further research. Although current execution times achieved by our prototype are tolerable, techniques of randomness reuse possibly result in even higher performance gains. In addition, a more formal security discussion of our scheme is desirable and can be subject of future work.

We conclude this work by emphasising the applicability of our current scheme to other domains than broadcasting of messages on OSNs. The presented architecture can be applied to other media than text messages such as photos and videos. Consequently, the algorithm can find adoption in a wider set of OSNs like Youtube, Instagram and Snapchat. The proposed broadcasting scheme is also valuable for e-mail applications with multiple recipients. With the increasing influence of internet on our daily communication, the amount of broadcasting applications is even expected to increase. Therefore, this thesis only highlighted one specific example of the many promising features an IBE DKG scheme has to offer in future applications.