BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures

Cas Cremers[1], Samed Düzlü[2], Rune Fiedler[3], Marc Fischlin[3], and Christian Janson[3]

[1]CISPA Helmholtz Center for Information Security, Germany
[2]QPC, Technische Universität Darmstadt, Germany
[3]Cryptoplexity, Technische Universität Darmstadt, Germany

32nd Crypto Day, 15 January 2021

In the first part of our talk we study the security of signature schemes beyond the conventional notion of existential unforgeability. Prior work such as Jackson, Cremers, Cohn-Gordon & Sasse (2019) has already shown that the absence of those properties can lead to real-world attacks on protocols using signature schemes. In particular, our work revisits the notions of *exclusive ownership* from Pornin & Stern (2005), which indicates whether an honestly generated signature may verify under a different public key, and *message-bound signatures*, which indicates that an attacker cannot generate a signature that verifies two distinct messages under its own key. In addition, we provide the first formal definition of *non re-signability*: Given only an honestly generated public key and a signature but not the message, an attacker cannot create a signature for this message. Existential unforgeability of a signature scheme does not imply any of these properties. Hence, we introduce the Beyond UnForgeability Features (BUFF) transformation to add these properties at the negligible penalty of computing and verifying a hash function evaluation and an increase in the signature size by one hash digest.

In the second part of our talk, we analyse whether 3rd round NIST PQC signature scheme candidates fulfill the above security notions. We briefly describe that Dilithium satisfies the notions by relating it to the BUFF transformation. As an example of a scheme which does not satisfy some of the security notions, we examine the lattice-based scheme FALCON. This scheme is build on NTRU which gives the underlying problems an algebraic structure. We give an high-level overview of the scheme and a more detailed account on the main objects related to the security notions in question. In the analysis, we use the underlying structure of FALCON to develop attacks on multiple security notions.

The full version including all details can be found at Cremers, Düzlü, Fiedler, Fischlin & Janson (2020).

References

Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin & Christian Janson (2020). BUFFing signature schemes beyond unforgeability and the

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-15

case of post-quantum signatures. Cryptology ePrint Archive, Report 2020/1525. https://eprint.iacr.org/2020/1525.

Dennis Jackson, Cas Cremers, Katriel Cohn-Gordon & Ralf Sasse (2019). Seems Legit: Automated Analysis of Subtle Attacks on Protocols that Use Signatures. In *ACM CCS 2019*, Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang & Jonathan Katz, editors, 2165–2180. ACM Press.

Thomas Pornin & Julien P. Stern (2005). Digital Signatures Do Not Guarantee Exclusive Ownership. In *ACNS 05*, John Ioannidis, Angelos Keromytis & Moti Yung, editors, volume 3531 of *LNCS*, 138–150. Springer, Heidelberg.