Modeling advanced security aspects of key exchange and secure channel protocols

Distinguished Dissertations

Felix Günther*

Modeling advanced security aspects of key exchange and secure channel protocols

https://doi.org/10.1515/itit-2020-0029
Received August 4, 2020; accepted October 2, 2020

Abstract: Secure connections are at the heart of today's Internet infrastructure, protecting the confidentiality, authenticity, and integrity of communication. Achieving these security goals is the responsibility of cryptographic schemes, more specifically two main building blocks of secure connections. First, a key exchange protocol is run to establish a shared secret key between two parties over a, potentially, insecure connection. Then, a secure channel protocol uses that shared key to securely transport the actual data to be exchanged. While security notions for classical designs of these components are well-established, recently developed and standardized major Internet security protocols like Google's QUIC protocol and the Transport Layer Security (TLS) protocol version 1.3 introduce novel features for which supporting security theory is lacking.

In my dissertation [20], which this article summarizes, I studied these novel and advanced design aspects, introducing enhanced security models and analyzing the security of deployed protocols. For key exchange protocols, my thesis introduces a new model for multi-stage key exchange to capture that recent designs for secure connections establish several cryptographic keys for various purposes and with differing levels of security. It further introduces a formalism for key confirmation, reflecting a long-established practical design criteria which however was lacking a comprehensive formal treatment so far. For secure channels, my thesis captures the cryptographic subtleties of streaming data transmission through a revised security model and approaches novel concepts to frequently update key material for enhanced security through a multi-key channel notion. These models are then applied to study (and confirm) the security of the QUIC and TLS 1.3 protocol designs.

Keywords: Applied cryptography, key exchange, secure channels, Internet security protocols, QUIC, TLS 1.3

ACM CCS: Security and privacy → Cryptography, Security and privacy → Network security → Security protocols

1 Introduction

Over the last three decades, the Internet developed into an integral part of our modern society and today forms the foundation of global communication. The ability to securely communicate over the Internet has thereby become a fundamental prerequisite for modern information exchange, protecting personal, commercial, institutional, and governmental data in everyday applications. Whether we read emails, surf the web, do online banking, withdraw cash at an ATM, or chat with friends on our smartphone—the security of billions of communication links worldwide for those and other tasks is enabled through cryptographic (encryption) schemes. Silently working in the background, these cryptographic schemes thus form the security backbone of modern communication: as one of the most prominent examples, the Transport Layer Security (TLS) protocol, hidden behind a green padlock in each browser, protects more than 85 % of today's Web traffic [30], on trillions of daily connections worldwide.

The study of secure data exchange is an old, foundational research topic in the field of cryptography, reaching back to the earliest historical ciphers. Early solutions to maintain the secrecy of communication date back as far as 1.900 BC with the first cryptologic hieroglyphs, 475 BC with the Greek "skytale" enciphering tool, or around 50 BC with the Caesar cipher [25]. Modern secure connections can be understood as consisting of two main cryptographic components. First, a *key exchange protocol* is run to establish a shared secret key between two parties over an insecure network. Then, a *secure channel protocol* uses the established key to securely transport the actual application data, protecting its confidentiality and integrity. In modern cryptography, the invention of key exchange mechanisms and formal models for encryption constitute seminal advances in the theory of cryptography, initiated through the influential works by Diffie and Hellman [11] and Goldwasser and Micali [19], respectively. The inter-

***Corresponding author: Felix Günther,** ETH Zürich, Department of Computer Science, Institute of Information Security, Applied Cryptography Group, Zürich, Switzerland, e-mail: mail@felixguenther.info, ORCID: https://orcid.org/0000-0002-8495-6610

pretation of cryptographic schemes and their security in complexity-theoretic terms has since then enabled impressive advances in both the theory of cryptography and its application in IT security, positioning cryptography as a melting pot and connecting discipline between theory and practice.

The modern cryptographic approach to study security is through abstraction of real-world system behavior in mathematical *security models* which describe the considered class of attacks a cryptographic system is supposed to withstand. Such models enable formal reasoning through complexity-theoretic reductions that no attacker can, in reasonable time, break the security of a system assuming the security of its underlying building blocks or that certain computational problems are hard. Given that the assumptions made are valid, reductionist security proofs in that sense hence rule out a certain class of attackers with well-defined capabilities. In order for such theoretical results to be meaningful for the actually deployed cryptographic systems in practice, it is of utmost importance that security models capture the system's behavior and practical threats as accurately as possible, yet not be overly demanding in order to still allow for efficient constructions. If a security model fails to capture a realistic attack in practice, such an attack remains viable on the considered cryptographic system despite a proof of its security in that model, at worst voiding the system's overall practical security.

Recent advances in practical protocol design as well as critical vulnerabilities in deployed protocols have indeed revealed a widening gap between the established cryptographic models for secure communication via key exchange and secure channel protocols and their real-world counterparts. In addition, new security protocol designs put forward by Industry and standards bodies introduce novel security features and innovative designs for improved efficiency. Examples include the QUIC ("Quick UDP Internet Connections") protocol [33] introduced by Google, protecting large parts of the traffic to their servers and being underway as an Internet standard [24], and TLS 1.3, the newest version of the Transport Layer Security protocol recently standardized by the Internet Engineering Task Force (IETF) as RFC 8446 [34]. Through advanced multi-key designs and a novel, latency-free ("zero round-trip-time", 0-RTT) connection establishment, both guarantee higher security levels and enable clients to send encrypted payload data to servers without initial delay for a server response. These novel design paradigms and security features go beyond classical academic approaches and the established theory accompanying them, calling for a revised understanding of the security they aim to achieve.

My dissertation *Modeling Advanced Security Aspects of Key Exchange and Secure Channel Protocols* [20] reconsiders the established security models for key exchange and secure channel protocols. It extends the cryptographic theory towards novel, advanced, and practical security aspects that have been introduced in recent designs of some of the most important security protocols deployed, or that escaped a formal treatment so far. For this purpose, it introduces enhanced security models capturing these advanced security aspects and applies them to analyze the practical security of major Internet key exchange and secure channel protocols, narrowing the gap between theory and applications of cryptography. The analyses from my thesis confirm that the proposed designs indeed increase the practical security in many aspects and provide sound mechanisms to evaluate the effects and trade-offs of efficiency-improving approaches (like 0-RTT) on the security of communication. These results contributed directly to recent standardization efforts of new Internet security protocols and, more generally, allow to derive design patterns for modern communication protocols.

2 Key exchange

Traditionally, key exchange protocols have always been understood as establishing a single secret key and then terminating their operation. This concept underlies all established security models for key exchange, originating from the seminal work by Bellare and Rogaway [4]. Recent practical protocol designs however deviate from this approach, specifically Google's QUIC protocol [33] introduced in 2013 and the newest version 1.3 of the Transport Layer Security (TLS) protocol [34], standardized in 2018 and constituting the new de-facto standard for Internet security protocols. Both protocols derive multiple keys in a continuous process, with the derived keys potentially depending on each other and differing in cryptographic strength. This added complexity escapes a sound theoretical treatment in all so-far established security models.

2.1 Multi-stage key exchange

My thesis formalizes such designs as multi-stage key exchange (MSKE) protocols and introduces a generalized security model for MSKE [15]. This framework enables analyzing the dependencies and differences between all keys established in a single framework, capturing the security of complex modern protocols in a more precise and comprehensive manner based on solid cryptographic theory.

In my thesis, this model is applied to assess the security of both the QUIC and the TLS 1.3 key exchange design; in the meantime, it has been adopted in several other analyses of these and further protocols (see, e. g., [28, 9, 7, 26, 2, 10]).

The security model of my thesis builds upon the key exchange model by Bellare and Rogaway [4]. Their model has established itself as the seminal complexity-based formalization of strong security guarantees for key exchange in the field of cryptography. It considers a strong adversary that interacts with an arbitrary number of protocol executions and controls the whole communication network, able to eavesdrop on, manipulate, or drop any message.[1] The adversary further is allowed to corrupt some of the interacting honest parties, learning their long-term secrets, and to reveal the session keys established in some of the protocol runs. Security then demands that such a powerful adversary is nevertheless unable to distinguish the established session key in an uncompromised session from a random string, informally providing the guarantee that established keys look random to such an adversary.

In my thesis, this foundational model is extended to capture the security and dependencies of multiple, successively derived keys in a multi-stage key exchange within a comprehensive model for MSKE. This model in particular captures the effects of compromises of different secrets (long-term and medium-lived) as well as interdependencies and varying authentication levels of keys derived at different stages in the key exchange. It moreover can treat both protocols with symmetric and asymmetric long-term secrets as well as the effects of possibilities to replay messages in some key exchange designs aiming at low-latency key exchange. The MSKE security model is finally accompanied by a compositional result that establishes sufficient conditions under which the keys established in a multi-stage key exchange protocol can safely be used in a generic follow-up symmetric-key protocol, lifting results for classical key exchange [8]. This result provides the theoretical foundation to argue the joint security of a secure MSKE protocol and, e. g., the subsequent secure channel protocol and hence reduces analytical efforts by enabling an independent and modular security analyses of both cryptographic components.

2.2 Google's QUIC protocol

As a first application of the MSKE model, my thesis analyzes the security of Google's QUIC protocol [33]. QUIC was introduced to enable secure connections with low latency and has in the meantime been deployed at large scale in Google's infrastructure [27]. To reduce round (communication) complexity of the key exchange, QUIC introduces a so-called zero round-trip time (0-RTT) key exchange mode. This mode enables a client to immediately send data along with its first key exchange message to a server it previously communicated with, hence drastically reducing the initialization delay of the secure connection. The 0-RTT data is encrypted under an initial key; both parties then update to a stronger main key with the reply of the server. As the security analysis in my thesis [15] reveals, these keys are unnecessarily intertwined, negatively affecting the protocol's security: compromising the first key before the second key is established leads to a security break—an insight which could not be formally captured in previous security models, but is enabled through the cryptographic theory embodied in the MSKE model. The analysis furthermore establishes relaxed security guarantees and establishes a simple fix to overcome the key-dependency weakness in a provably secure way.

2.3 TLS 1.3

My thesis then focuses on the newest version of the Transport Layer Security protocol, TLS 1.3, developed and standardized as RFC 8446 [34] by the Internet Engineering Task Force (IETF). Charged with a series of highly-critical security vulnerabilities in the past, the goal for the new TLS version was to fundamentally overhaul the protocol's security architecture, but also to introduce new functionality. New features include a low-latency 0-RTT handshake mode (as in QUIC), deriving intermediate keys to encrypt parts of the handshake for enhanced privacy, and deploying a sequence of keys in the channel protocol for stronger security. In particular, TLS 1.3 hence is a multi-stage key exchange protocol for which my proposed security model enables a comprehensive analysis. My thesis begins with analyzing the two basic key exchange modes of TLS 1.3 [13, 14], establishing strong security of both the main mode based on Diffie–Hellman key exchange and the abbreviated mode used for repeated connections between the same client and server. The results confirm the core cryptographic design of the protocol and have contributed to the development process of the TLS 1.3 standard by rein-

[1] The adversary's omnipotence in fully controlling the communication network resembles the Dolev-Yao adversary model [12]. My thesis considers the computational setting and hence furthermore allows the adversary to tamper arbitrarily with the messages exchanged, not restricting it to an abstract, symbolic or algebraic representation.

forcing choices for strong cryptographic design principles based on sound cryptographic theory.

The third key exchange mode of TLS 1.3 introduces a low-latency 0-RTT option, enabling secure communication without initial delay as in QUIC. In contrast to the QUIC design, TLS 1.3 however gives up replay protection guarantees for that initial (0-RTT) part of the communication. The multi-stage key exchange model in my thesis provides the theory to formally characterize both approaches and evaluate their differences in security. The conducted analyses establish multi-stage security for the 0-RTT mode of TLS 1.3 [16], capturing the security restrictions imposed by replays and, most importantly, that the added 0-RTT communication does not negatively affect the security of the main data exchange.

As the last contribution in the area of key exchange protocols, my thesis finally establishes, for the first time, a theoretic model for a key-confirming property aimed for in many practical designs, but never formally captured. The key confirmation model in my thesis [18] exposes an inherent, slight difference in the confirmation guarantees both communication partners can obtain and enables assessing the key confirmation properties of TLS 1.3.

3 Secure channels

Having established a shared secret key, the two communicating parties execute a secure channel protocol in order to securely transmit the actual communication data. In this setting, 'securely' refers to such data being protected from both passive eavesdropping as well as manipulation through active adversaries. The targeted security goals are hence confidentiality and integrity, and the basic underlying cryptographic tool is that of (symmetric-key) encryption. Formalizing security notions for confidentiality and (later) integrity of individually encrypted messages constitutes further foundational work in the theory of modern cryptography originating from Goldwasser and Micali [19]. The first formalization of channels, which should also protect the order of messages, was given by Bellare, Kohno, and Namprempre [3]. Still, and despite being a foundational goal of cryptography, security models in the literature however only consider highly simplified forms of secure channels.

3.1 Data is a stream

In the area of secure channels, my thesis advances the cryptographic theory towards better capturing the practical conditions under which such protocols are running. The first contribution in the realm of channels originates from the observation that, in practice, most secure channel protocols actually do not transmit distinct, or atomic, messages as is assumed throughout all previous models. Instead, they regularly provide applications with a streaming interface to transmit a stream of bits without any inherent demarcation of individual messages. Necessarily, the security guarantees of such an interface differ significantly from those considered in cryptographic models so far. In particular, not only cryptographic packets [6] but also application messages may be fragmented in transport, and the recipient may obtain the sent data stream in a different fragmentation. Such application-level message fragmentation has in the past led to confusion and practical attacks on major application protocol implementations [1, 35, 5]. In my thesis, this behavior is formalized through stream-based channels [17], introducing corresponding security notions of confidentiality and integrity capturing the inherently increased complexity. Through a generic comparative construction of a stream-based channel, my thesis further shows that the deployed construction principles in practice indeed enable strong security for the transmission of data streams.

Additionally, my thesis studies the security of such applications whose messages are inherently atomic and which need to safely transport these messages over a streaming, i. e., possibly fragmenting, channel. Formalizing the desired security properties in terms of confidentiality and integrity in such settings, my thesis investigates and confirms the security of the widely adopted approach to encode the application's messages into the continuous data stream. This newly established theory also casts a formal light on the potential misunderstanding of security guarantees provided by stream-based and atomic-message channels that led to critical security flaws in practice.

3.2 Multi-key channels

Finally, my thesis again turns towards a novel feature in the recently standardized TLS version 1.3 [34]: a key-updating mechanism that allows parties to deploy a sequence of multiple keys for encryption instead of a single, fixed key. Such key updates were proposed both as a functional feature (easing the transfer of very large amounts of data [29] which previously needed a series of multiple connections) and to enhance the channel's security (especially providing security against partial compromise of the channel's key material). For this setting of multi-key channels, my thesis introduces a novel security model [21] which enables a precise evaluation of the envisioned extended security properties. An accordingly designed channel protocol ensures both the security of past communication data if the employed long-lived key is compromised (so-called forward security), as well as the security of individual communication phases under losses of key material in other (prior or later) phases. The security model is carefully crafted in order to establish a hierarchy of security levels which seamlessly connects to the established cryptographic theory for secure (single-key) channels [3]. Through its analysis, my thesis confirms the protocol design proposed in TLS 1.3 [34] and the resulting improved security guarantees.

4 Conclusion

While the basic cryptographic theory of key exchange and secure channel protocols is considered to be understood, modern developments and protocol designs in practice challenge these foundations and call for continued revisions of this theoretical understanding.

In my dissertation, I studied how advanced security aspects of both protocol types can be formally captured in terms of enhanced cryptographic security models, thereby narrowing the gap between cryptographic theory and practice. My thesis strengthens the theoretic grounds on which new protocol designs can be soundly built and deployed, deepening the cryptographic theory of secure communication. At the same time, the results from my thesis directly contributed to the standardization process of the QUIC [33, 24] and TLS 1.3 [34] protocols and are acknowledged in the latter's final standard. All these results emerged from fruitful collaborations with many great colleagues; having had the opportunity to work with them is among the best experiences of my Ph. D. I further was lucky to be able to personally support the TLS 1.3 standardization process through direct input based on these results and discuss the protocol's design at dedicated standardization workshops with other scientists, industry, and the IETF. As a result of TLS 1.3's novel and highly interactive standardization process with contributions from many research groups [31], the protocol enjoys a higher security level than all previous versions and a significantly faster adoption at large scale [22, 23].

In the meantime, the security models put forward in my thesis have been adopted in further works of other research teams, aiming to more precisely capture the security aspects of other modern communication protocols. For example, in the realm of secure messaging, complex designs like the Signal protocol enable the vast majority of secure chat communication today in popular applications like WhatsApp or Facebook Messenger; its security has been analyzed on the basis of the multi-stage key exchange model from my thesis [9]. But also in the context of developing TLS 1.3, other researchers for example applied the model for stream-based channels from my thesis to analyze the protocol's multiplexing behavior [32].

The new security models put forward in my thesis in this way enable detailed analyses and assessments of modern security protocols in practice based on sound cryptographic theory. Helping to further bridge modern IT security and theoretical computer science such analyses can contribute to ensure that tomorrow's Internet communication will meet high security standards.

Funding: This work was supported by Deutsche Forschungsgemeinschaft, Grant Number: GU 1859/1-1.

References

1. M. R. Albrecht, K. G. Paterson, and G. J. Watson. Plaintext recovery attacks against SSH. In *2009 IEEE Symposium on Security and Privacy*, pages 16–26, Oakland, CA, USA, May 17–20, 2009. IEEE Computer Society Press.
2. G. Arfaoui, X. Bultel, P.-A. Fouque, A. Nedelcu, and C. Onete. The privacy of the TLS 1.3 protocol. *Proceedings on Privacy Enhancing Technologies*, 2019(4):190–210, Oct. 2019.
3. M. Bellare, T. Kohno, and C. Namprempre. Authenticated encryption in SSH: Provably fixing the SSH binary packet protocol. In V. Atluri, editor, *ACM CCS 2002: 9th Conference on Computer and Communications Security*, pages 1–11, Washington, DC, USA, Nov. 18–22, 2002. ACM Press.
4. M. Bellare and P. Rogaway. Entity authentication and key distribution. In D. R. Stinson, editor, *Advances in Cryptology – CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249, Santa Barbara, CA, USA, Aug. 22–26, 1994. Springer, Heidelberg, Germany.
5. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Pironti, and P.-Y. Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In *2014 IEEE Symposium on Security and Privacy*, pages 98–113, Berkeley, CA, USA, May 18–21, 2014. IEEE Computer Society Press.
6. A. Boldyreva, J. P. Degabriele, K. G. Paterson, and M. Stam. Security of symmetric encryption in the presence of ciphertext fragmentation. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 682–699, Cambridge, UK, Apr. 15–19, 2012. Springer, Heidelberg, Germany.
7. J. Brendel and M. Fischlin. Zero round-trip time for the extended access control protocol. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, *ESORICS 2017: 22nd European Symposium on Research in Computer Security, Part I*, volume 10492 of *Lecture Notes in Computer Science*, pages 297–314, Oslo, Norway, Sept. 11–15, 2017. Springer, Heidelberg, Germany.

8. C. Brzuska, M. Fischlin, B. Warinschi, and S. C. Williams. Composability of Bellare-Rogaway key exchange protocols. In Y. Chen, G. Danezis, and V. Shmatikov, editors, *ACM CCS 2011: 18th Conference on Computer and Communications Security*, pages 51–62, Chicago, Illinois, USA, Oct. 17–21, 2011. ACM Press.
9. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila. A formal security analysis of the Signal messaging protocol. In *2nd IEEE European Symposium on Security and Privacy, EuroS&P 2017*, pages 451–466, Paris, France, Apr. 26–28, 2017. IEEE.
10. D. Diemert and T. Jager. On the tight security of TLS 1.3: Theoretically-sound cryptographic parameters for real-world deployments. *Journal of Cryptology*, 2020. To appear. Available as Cryptology ePrint Archive, Report 2020/726. https://eprint.iacr.org/2020/726.
11. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
12. D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Trans. Information Theory*, 29(2):198–207, 1983.
13. B. Dowling, M. Fischlin, F. Günther, and D. Stebila. A cryptographic analysis of the TLS 1.3 handshake protocol candidates. In I. Ray, N. Li, and C. Kruegel, editors, *ACM CCS 2015: 22nd Conference on Computer and Communications Security*, pages 1197–1210, Denver, CO, USA, Oct. 12–16, 2015. ACM Press.
14. B. Dowling, M. Fischlin, F. Günther, and D. Stebila. A cryptographic analysis of the TLS 1.3 draft-10 full and pre-shared key handshake protocol. Cryptology ePrint Archive, Report 2016/081, 2016. http://eprint.iacr.org/2016/081.
15. M. Fischlin and F. Günther. Multi-stage key exchange and the case of Google's QUIC protocol. In G.-J. Ahn, M. Yung, and N. Li, editors, *ACM CCS 2014: 21st Conference on Computer and Communications Security*, pages 1193–1204, Scottsdale, AZ, USA, Nov. 3–7, 2014. ACM Press.
16. M. Fischlin and F. Günther. Replay attacks on zero round-trip time: The case of the TLS 1.3 handshake candidates. In *2nd IEEE European Symposium on Security and Privacy, EuroS&P 2017*, pages 60–75, Paris, France, Apr. 26–28, 2017. IEEE.
17. M. Fischlin, F. Günther, G. A. Marson, and K. G. Paterson. Data is a stream: Security of stream-based channels. In R. Gennaro and M. J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 545–564, Santa Barbara, CA, USA, Aug. 16–20, 2015. Springer, Heidelberg, Germany.
18. M. Fischlin, F. Günther, B. Schmidt, and B. Warinschi. Key confirmation in key exchange: A formal treatment and implications for TLS 1.3. In *2016 IEEE Symposium on Security and Privacy*, pages 452–469, San Jose, CA, USA, May 22–26, 2016. IEEE Computer Society Press.
19. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.
20. F. Günther. *Modeling Advanced Security Aspects of Key Exchange and Secure Channel Protocols*. Ph. D. thesis, Technische Universität Darmstadt, Darmstadt, Germany, Feb. 2018. Available online at http://tuprints.ulb.tu-darmstadt.de/7162/.
21. F. Günther and S. Mazaheri. A formal treatment of multi-key channels. In J. Katz and H. Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 587–618, Santa Barbara, CA, USA, Aug. 20–24, 2017. Springer, Heidelberg, Germany.
22. R. Holz, J. Amann, A. Razaghpanah, and N. Vallina-Rodriguez. The era of TLS 1.3: Measuring deployment and use with active and passive methods. arXiv:1907.12762 [cs.CR], 2019. https://arxiv.org/abs/1907.12762.
23. R. Holz, J. Hiller, J. Amann, A. Razaghpanah, T. Jost, N. Vallina-Rodriguez, and O. Hohlfeld. Tracking the deployment of TLS 1.3 on the web: A story of experimentation and centralization. *SIGCOMM Comput. Commun. Rev.*, 50(3):3–15, July 2020.
24. J. Iyengar and M. Thomson. QUIC: A UDP-Based Multiplexed and Secure Transport – draft-ietf-quic-transport-29. https://tools.ietf.org/html/draft-ietf-quic-transport-29, June 2020.
25. D. Kahn. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, 1996.
26. X. Lan, J. Xu, Z.-F. Zhang, and W.-T. Zhu. Investigating the multi-ciphersuite and backwards-compatibility security of the upcoming TLS 1.3. *IEEE Transactions on Dependable and Secure Computing*, 16(2):272–286, 2019.
27. A. Langley, A. Riddoch, A. Wilk, A. Vicente, C. Krasic, D. Zhang, F. Yang, F. Kouranov, I. Swett, J. R. Iyengar, J. Bailey, J. Dorfman, J. Roskind, J. Kulik, P. Westin, R. Tenneti, R. Shade, R. Hamilton, V. Vasiliev, W. Chang, and Z. Shi. The QUIC transport protocol: Design and internet-scale deployment. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM 2017, Los Angeles, CA, USA, August 21–25, 2017, pages 183–196, Los Angeles, CA, USA, Aug. 21–25, 2017. ACM.
28. X. Li, J. Xu, Z. Zhang, D. Feng, and H. Hu. Multiple handshakes security of TLS 1.3 candidates. In *2016 IEEE Symposium on Security and Privacy*, pages 486–505, San Jose, CA, USA, May 22–26, 2016. IEEE Computer Society Press.
29. A. Luykx and K. G. Paterson. Limits on authenticated encryption use in TLS, Aug. 2017. http://www.isg.rhul.ac.uk/~kp/TLS-AEbounds.pdf.
30. Netmarketshare. HTTP vs HTTPS, Aug. 2020. https://netmarketshare.com/report.aspx?id=https.
31. K. G. Paterson and T. van der Merwe. Reactive and proactive standardisation of TLS. In L. Chen, D. A. McGrew, and C. J. Mitchell, editors, *Security Standardisation Research: Third International Conference (SSR 2016)*, volume 10074 of *Lecture Notes in Computer Science*, pages 160–186, Gaithersburg, MD, USA, Dec. 5–6, 2016. Springer.
32. C. Patton and T. Shrimpton. Partially specified channels: The TLS 1.3 record layer without elision. In D. Lie, M. Mannan, M. Backes, and X. Wang, editors, *ACM CCS 2018: 25th Conference on Computer and Communications Security*, pages 1415–1428, Toronto, ON, Canada, Oct. 15–19, 2018. ACM Press.
33. QUIC, a multiplexed stream transport over UDP. https://www.chromium.org/quic.
34. E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446 (Proposed Standard), Aug. 2018.
35. B. Smyth and A. Pironti. Truncating TLS connections to violate beliefs in web applications. In J. Oberheide and W. K. Robertson, editors, *7th USENIX Workshop on Offensive Technologies, WOOT'13*, Washington, D.C., USA, Aug. 13, 2013. USENIX Association.

Bionotes

Dr. Felix Günther
ETH Zürich, Department of Computer Science, Institute of Information Security, Applied Cryptography Group, Zürich, Switzerland
mail@felixguenther.info

Felix Günther studied Computer Science (B.Sc./M.Sc.) and IT Security (M.Sc.) at TU Darmstadt, where he received his Ph.D. in Computer Science (summa cum laude) in 2018 under the supervision of Prof. Dr. Marc Fischlin. For his dissertation, he received the ACM SIGSAC Doctoral Dissertation Award for Outstanding PhD Theses in Computer and Information Security, the ERCIM STM WG Award for the Best Ph.D. Thesis on Security and Trust Management, and the Dr.-Heinz-Sebiger Dissertation Award on Data Protection and IT Security of the DATEV-Stiftung Zukunft; he further was runner-up for the CAST/GI Doctoral Dissertation Award in IT Security. After his Ph.D., he has been supported by a Research Fellowship grant of the German Research Foundation (DFG) to work as a postdoctoral researcher at UC San Diego with Prof. Mihir Bellare and at ETH Zürich, his current position, with Prof. Kenneth G. Paterson.