Cryptography 101: From Theory to Practice

Chapter 18 – Outlook

Rolf Oppliger

February 25, 2023

Terms of Use

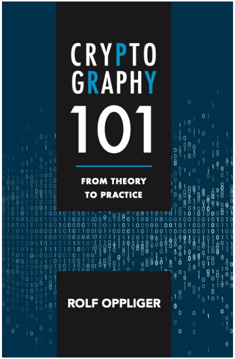
- This work is published with a CC BY-ND 4.0 license (🅭🅯⊜)
  - CC = Creative Commons (🅭)
  - BY = Attribution (🅯)
  - ND = No Derivatives (⊜)

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



© Artech House, 2021
ISBN 978-1-63081-846-3

https://books.esecurity.ch/crypto101.html

Challenge Me

Outline

It would appear that we have reached the limits of what is possible to achieve with computer technology, although one should be careful with such statements, as they tend to sound pretty silly in five years.

– John von Neumann

18. Outlook

1. Introduction
2. Cryptographic Systems
3. Random Generators
4. Random Functions
5. One-Way Functions
6. Cryptographic Hash Functions
7. Pseudorandom Generators
8. Pseudorandom Functions
9. Symmetric Encryption
10. Message Authentication
11. Authenticated Encryption
12. Key Establishment
13. Asymmetric Encryption
14. Digital Signatures
15. Zero-Knowledge Proofs of Knowledge
16. Key Management
17. Summary

18. Outlook

18.1 Theoretical Viewpoint

18.2 Practical Viewpoint

18.3 PQC

18.4 Closing Remarks

18. Outlook

18.1 Theoretical Viewpoint

- The central theme in theoretical cryptography is **provability**, i.e., how to define security and prove that a given cryptographic system is in line with this definition
- Starting from Shannon's notion of perfect secrecy, many researchers have come up with different **notions of security**
- Some of these notions are equivalent or relate to each other in specific ways

18. Outlook

18.1 Theoretical Viewpoint

- It is not possible to provide an absolute proof for the security of a cryptographic system
- One can only prove the security (properties) of a cryptographic system under some assumptions
- Some assumptions are implicit (and appear too trivial to be mentioned in the first place)
- Other assumptions are explicit, such as computational intractability assumptions

18. Outlook

18.1 Theoretical Viewpoint

- All assumptions are key to the security of a system
- A major goal in cryptographic research is to reduce the assumptions to what is absolutely necessary while preserving the practicality of the systems
- In the realm of cryptographic protocols, **formal methods** are increasingly important
- Formal methods and their proper use yield an interesting and timely research topic

18. Outlook

18.2 Practical Viewpoint

- From a practical viewpoint, **standards** and **profiles** are important
- There are simply too many and too complex cryptographic systems and modes of operation to choose from
- Anybody not actively working in the field is likely to be overtaxed
- The DES is a success story because NIST realized the need for a standardized cipher in the 1970s
- In the late 1990s, NIST repeated the success story with the AES, and more recently with SHA-3 and PQC

18. Outlook

18.2 Practical Viewpoint

- In February 2005, the NSA announced **Suite B**
  - Symmetric encryption: AES-128 and AES-256
  - Cryptographic hash functions: SHA-256 and SHA-384
  - Key agreement: ECDH and ECMQV
  - Digital signatures: ECDSA
- In addition, the NSA specified but did not publish Suite A (including ACCORDION, BATON, MEDLEY, SHILLELAGH, and WALBURN)

18. Outlook

18.2 Practical Viewpoint

- In 2016, the Committee on National Security Systems (CNSS) released Policy No. 15 (CNSSP-15)
- The respective Commercial National Security Algorithm Suite (**CNSA Suite**) is similar to Suite B
  - Symmetric encryption: AES-256
  - Cryptographic hash functions: SHA-384
  - Key agreement: RSA and DH with 3072-bit moduli or larger, as well as ECDH (NIST P-384)
  - Digital signatures: RSA with 3072-bit moduli and ECDSA (NIST P-384)

18. Outlook

18.2 Practical Viewpoint

- In 2018, the NSA replaced Suite B with the CNSA Suite and withdrew Suite B
- Similarly, the use of Suite B in IETF standards was abandoned and all Suite B documents were reclassified to historic status (RFC 8423)
- Outside the U.S., several other **standardization bodies** are working on cryptography (e.g., IEEE, IETF, W3C, . . .)
- Many of these bodies have problems of their own, and the current state of affairs in international standardization is not particularly good

18. Outlook

18.2 Practical Viewpoint

- The more one can prove about the security properties of standardized cryptographic systems, the better the odds that they are successful and get widely deployed
- The complexity of cryptographic systems is best hidden in reference implementations and libraries, e.g., Bouncy Castle, OpenSSL/LibreSSL, Google Tink, NaCl, libsodium, or cryptlib
- Ideally, a cryptographic library provides a standardized API, such as Microsoft's CryptoAPI
- This makes it possible to easily replace one cryptographic library with another, and hence to provide cryptographic agility

18. Outlook

18.3 PQC

- In PQC, one is looking for cryptosystems that remain secure even if the adversary has access to a quantum computer (quantum computer resistance)
- If
  - y is the time it takes to deploy quantum-safe cryptosystems
  - x is the time information needs to remain secure
  - z is the time it takes to build a quantum computer

  then **Mosca's Theorem** states that one should worry if $x + y > z$ (according to Michele Mosca)

18. Outlook

18.3 PQC

- In 2017, NIST launched a **PQC competition** that is still going on
- Categories of submissions
  - Code-based cryptosystems
  - Hash-based cryptosystems
  - Lattice-based cryptosystems
  - Isogeny-based cryptosystems
  - Multivariate-based cryptosystems

18. Outlook

18.3 PQC

Table 18.1
The NIST Competition Round 3 Finalists and Alternate Candidates

	Encryption / KEMs		**Digital Signatures**	
Type	**Finalists**	**Alternates**	**Finalists**	**Alternates**
Code-based	Classic McEliece	*BIKE* *HQC*		
Hash-based				*SPHINCS+*
Lattice-based	CRYSTALS-KYBER NTRU SABER	*FrodoKEM* *NTRU Prime*	CRYSTALS-DILITHIUM FALCON	
Isogeny-based		*SIKE († 7/2022)*		
Multivariate-based			Rainbow († 2/2022)	*GeMSS*
Other				*Picnic*

18. Outlook

18.3 PQC

- In July 2022, the NIST announced the selection of CRYSTALS-KYBER for encryption and CRYSTALS-DILITHIUM, FALCON, and SPHINCS+ for signatures
- The NIST also announced a round 4 for complementary encryption systems
- In this round, Classic McEliece, BIKE, and HQC are further considered (without SIKE)
- The final standards are expected for 2024

18. Outlook

18.4 Closing Remarks

- In theory, there are many statements and proofs related to cryptography
- This suggests that cryptography is a mature science
- In practice, this is only partly true, and the maturity level of cryptography as a science to protect data is not so good
- It is not so clear whether and to what extent cryptography can really help protecting data
- It always boils down to the protection of keys, and key management yields the Achilles' heel

18. Outlook

18.4 Closing Remarks

- Telling cryptography apart from illusion is difficult (cryptollusion)
- An illusionist can always use tricks and distractions to confuse the observer
- This also applies to cryptography, and somebody implementing cryptography does not have to play by the rules (i.e., he or she may cheat at will)
- This may even include standardization (e.g., Dual_EC_DRBG)
- There are less obvious tricks that are indistinguishable from software bugs (e.g., Heartbleed or Apple's goto fail bug)

18. Outlook

18.4 Closing Remarks

- A key question is to decide whether a given implementation of a cryptosystem works as expected and is secure as claimed
- Alternatively speaking: *Is security real or illusive?*
- The devil is in the details, and it is generally simple to obfuscate them
- Human skepticism is particularly valuable for the mindset of a security professional
- Every security argument or proof should be taken with the grain of salt it deserves

18. Outlook

Online Resources

- Books
  - Handbook of Applied Cryptography (Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone)
  - A Graduate Course in Applied Cryptography (Dan Boneh and Victor Shoup)
- Lectures
  - Cryptography Full Course Part 1, Part 2 (Dan Boneh)
  - Einführung in die Kryptographie (Christof Paar)
- Museum
  - National Cryptologic Museum (NSA)

Questions and Answers

Thank you for your attention