Workgroup: Network Working Group
Internet-Draft:
draft-irtf-cfrg-aead-properties-01
Published: 10 March 2023
Intended Status: Informational
Expires: 11 September 2023
Authors: A.A. Bozhko, Ed.
CryptoPro

Properties of AEAD algorithms

Abstract

Authenticated Encryption with Associated Data (AEAD) algorithms provide confidentiality and integrity of data. The extensive use of AEAD algorithms in various high-level applications has caused the need for AEAD algorithms with additional properties and motivated research in the area. This document gives definitions for the most common of those properties intending to improve consistency in the field.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 September 2023.

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

An Authenticated Encryption with Associated Data (AEAD) algorithm is an extension of authenticated encryption, which provides

confidentiality for the plaintext to be encrypted and integrity for the plaintext and some Associated Data (sometimes called Header). AEAD algorithms are used in numerous applications and have become an important field in cryptographic research.

1.1. Background

AEAD algorithms are formally defined in [RFC5116]. The main benefit of AEAD algorithms is that they provide data confidentiality and integrity and have a simple unified interface.

The importance of the AEAD algorithms is mainly explained by their exploitation simplicity: they have a unified interface, easy-to-understand security guarantees, and are much easier to implement properly than MAC and encryption schemes separately. Therefore, their embedding into high-level schemes and protocols is highly transparent since, for example, there is no need for additional key derivation procedures. Apart from that, when using the AEAD algorithm, it is possible to reduce the key and state sizes and improve the data processing speed. For instance, such algorithms are mandatory for TLS 1.3 [RFC8446], IPsec ESP [RFC4303] [RFC8221], and QUIC [RFC9000]. Hence, the research and standardization efforts in the field are extremely active. Most AEAD algorithms usually come with security guarantees, formal proofs, usage guidelines, and reference implementations.

Even though providing core properties of AEAD algorithms is enough for many applications, some environments require other unusual cryptographic properties, which commonly require additional analysis and research. With the growing number of such properties and research papers, misunderstanding and confusion inevitably appear. Some properties might be understood in different ways; for some, only non-trivial formal security notions are provided, while others require modification or extension of the standard AEAD interface to support additional functionality. Therefore, the risk of misuse of AEAD algorithms increases, which can lead to security issues.

1.2. Scope

In the following document, we provide a short overview of the most common properties of AEAD algorithms by giving high-level definitions of these properties in Section 4. The document aims to improve clarity and establish a common language in the field.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in

BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. AEAD algorithms

This section gives a general definition of an AEAD algorithm following [RFC5116].

Definition. An AEAD algorithm is defined by two operations, which are authenticated encryption and authenticated decryption:

- A deterministic operation of authenticated encryption has four inputs, each a binary string: a secret key K of a fixed bit length, a nonce N, associated data A, and a plaintext P. The plaintext contains the data to be encrypted and authenticated, and the associated data contains the data to be authenticated only. Each nonce value must be unique in every distinct invocation of the operation for any particular value of the key. The authenticated encryption operation outputs a ciphertext C.

- A deterministic operation of authenticated decryption has four inputs, each a binary string: a secret key K of a fixed bit length, a nonce N, associated data A, and a ciphertext C. The operation verifies the integrity of the ciphertext and associated data and decrypts the ciphertext. It returns a special symbol FAIL if the inputs are not authentic; otherwise, the operation returns a plaintext P.

For more details on AEAD definition, please refer to [RFC5116].

Throughout this document, by default, we will consider nonce-based AEAD algorithms, which have an interface from the definition above, and give no other restrictions on their structure. However, some properties defined in the document apply only to particular classes of such algorithms, like block cipher-based AEAD algorithms (such algorithms use block cipher as a building block). If that is the case, we explicitly point that out in the corresponding section. Some other properties, on the contrary, are defined for algorithms with extended or completely different interfaces. We address that issue in Section 4.1.

We will call an AEAD algorithm secure if it provides such properties as Confidentiality and Data integrity, defined in Section 4.2, against any active nonce-respecting adversary. Even though we aim to give high-level definitions, we sometimes use the advantage notion. Specifically, we will use the Authenticated Encryption advantage notion. We adopt the corresponding definition from [I-D.irtf-cfrg-aead-limits].

Definition. Authenticated Encryption advantage is the probability of an active adversary succeeding in breaking the authenticated-encryption properties of the AEAD algorithm. In this document, the definition of authenticated encryption advantage roughly is the probability that an attacker successfully distinguishes the ciphertext outputs of the AEAD scheme from the outputs of a random function or is able to forge a ciphertext that will be accepted as valid.

4. AEAD properties

4.1. Classification of AEAD properties

In this document we use a high-level classification of additional properties. The classification aims to give an intuition on how one can benefit from the property. The additional properties fall into one of these three categories:

* Security properties. We say that the property is a security property if it considers new threats or adversarial capabilities, in addition to those of the usual nonce-respecting adversary, which aims to break confidentiality or data integrity.

* Implementation properties. We say that the property is an implementation property if it allows for more efficient implementations of the AEAD algorithm in special cases or environments.

* Additional functionality properties. We say that the property is an additional functionality property if it provides new features in addition to the regular authenticated encryption with associated data.

We notice that the distinction between the security and additional functionality properties might be vague. The convention in this document is that additional functionality requires some extension of the standard AEAD interface. In fact, each additional functionality property defines a new class of algorithms, which is not a subclass of regular AEAD. Hence, the basic threats and adversarial capabilities must be redefined for each of these classes. As a result, additional functionality properties consider the basic threats and adversarial capabilities for their class of algorithms and, in contrast to security properties, not the extended ones.

4.2. Base properties

4.2.1. Confidentiality

Definition. An AEAD algorithm guarantees that the plaintext is available only to those authorized to obtain it, i.e., those

possessing the secret key. That property is required for the AEAD algorithm to be called secure.

Synonyms. Privacy.

Further reading. [R2002], [BN2000]

4.2.2. Data integrity

Definition. An AEAD algorithm guarantees that the plaintext and the associated data have not been changed or forged by those not authorized to, i.e., those not possessing the secret key. That property is required for the AEAD algorithm to be called secure.

Synonyms. Message authentication.

Further reading. [R2002], [BN2000]

4.3. Security properties

4.3.1. Blockwise security

Definition. An AEAD algorithm provides security even if an adversary can adaptively choose the next block of the plaintext depending on already computed ciphertext blocks during an encryption operation.

Note. The case when an adversary can adaptively choose the next block of the ciphertext depending on already computed blocks of the plaintext, which appear in the device memory before the integrity verification during the decryption, can also be considered. This case is strongly related to RUP security, defined in Section 4.3.9.

Further reading. [JMV2002], [FJMV2004]

4.3.2. Key Dependent Messages (KDM) security

Definition. An AEAD algorithm provides security even when key-dependent plaintexts are encrypted.

Notes. KDM security is achievable only if nonces are chosen randomly and associated data is key-independent.

Further reading. [BK2011]

4.3.3. Key commitment

Definition. An AEAD algorithm guarantees that it is difficult to find a tuple of the nonce, associated data, and ciphertext such that it can be decrypted correctly with more than one key.

Synonyms. Key-robustness, key collision resistance.

Further reading. [FOR17], [LGR21], [GLR17]

4.3.4. Leakage resistance

Definition. An AEAD algorithm provides security even if some additional information about computations of an encryption (and possibly decryption) operation is obtained via side-channel leakages.

Further reading. [GPPS19], [B20]

4.3.5. Multi-user security

Definition. An AEAD algorithm Authenticated Encryption advantage increases sublinearly in the number of users.

Further reading. [BT16]

4.3.6. Nonce misuse

Definition. An AEAD algorithm provides security (resilience or resistance) even if an adversary can repeat nonces in its encryption queries. Nonce misuse resilience and resistance are defined as follows:

- Nonce misuse resilience. Security is provided only for messages encrypted with unique nonces.

- Nonce misuse resistance. Security is provided for all messages.

Further reading. [RS06], [ADL17]

4.3.7. Nonce-hiding

Definition. An AEAD algorithm decryption operation doesn't require the nonce to perform decryption and provides privacy for the nonce value used for encryption.

Note. In nonce-hiding AEAD algorithms, the ciphertext contains information equivalent to an encrypted nonce. Hence, retrieving information about nonce from the ciphertext has to be difficult.

Further reading. [BNT19]

4.3.8. Reforgeability resilience

Definition. An AEAD algorithm guarantees that once a successful forgery for the algorithm has been found, it is still hard to find any subsequent forgery.

Further reading. [BC09], [FLLW17]

4.3.9. Release of unverified plaintext (RUP) security

Definition. An AEAD algorithm provides security even if the plaintext is released for every ciphertext, including those with failed integrity verification.

Further reading. [A14]

4.4. Implementation properties

4.4.1. Inverse-free

Definition. A block cipher-based AEAD algorithm can be securely implemented without evaluating the block cipher inverse.

4.4.2. Lightweight

Definition. An AEAD algorithm can be efficiently and securely implemented on resource-constrained devices. In particular, it meets the criteria required in the NIST Lightweight Cryptography competition [MBTM17].

Further reading. [MBTM17]

4.4.3. Online

Definition. An AEAD algorithm encryption (decryption) operation can be implemented with a constant memory and a single one-direction pass over the plaintext (ciphertext), writing out the result during that pass.

Further reading. [HRRV15] [FJMV2004]

4.4.4. Parallelizable

Definition. An AEAD algorithm can fully exploit the parallel computation infrastructure.

Synonyms. Pipelineable.

Further reading. [C20]

4.4.5. Single pass

Definition. An AEAD algorithm encryption (decryption) operation can be implemented with a single pass over the plaintext (ciphertext).

4.4.6. Static Associated Data

Definition. An AEAD algorithm allows pre-computation for static (or repeating) associated data so that static AD doesn't significantly contribute to the computational cost of encryption.

4.4.7. ZK-friendly

Definition. An AEAD algorithm operates on binary and prime fields with a low number of non-linear operations (often called multiplicative complexity). Thus, it allows efficient implementation using a domain-specific language (DSL) for writing zk-SNARKs circuits.

Synonyms. ZK-focused, Arithmetization-oriented, Low Multiplicative Complexity

Further reading. [DGGK21]

4.5. Additional functionality properties

4.5.1. Incremental

Definition. An AEAD algorithm allows encrypting and authenticating a message (associated data and a plaintext pair), which only partly differs from some previous message, faster than processing it from scratch.

Further reading. [SY16], [BKY02], [M05]

4.5.2. Remotely-keyed

Definition. An AEAD algorithm can be implemented with most of the operations in encryption/decryption performed by an insecure (i.e., it leaks all intermediate values) device, which has no access to the key, while another secure device performs operations involving the key.

Further reading. [BFN98], [DA03]

4.5.3. Robust

Definition. An AEAD algorithm allows the user to choose an arbitrary value l >= 0 for every plaintext and then encrypts it into a ciphertext, which is l bits longer.

Further reading. [HKR2015]

5. Security Considerations

This document defines the properties of AEAD algorithms. However, the document does not describe any concrete mechanisms providing these properties, neither it describes how to achieve them. In fact, one can claim that an AEAD algorithm provides any of the defined properties only if its analysis in the relevant models was carried out.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/info/rfc5116>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[A14] Forler, C., List, E., Forler, C., List, E., List, E., and E. List, "How to Securely Release Unverified Plaintext in Authenticated Encryption", Advances in Cryptology – ASIACRYPT 2014. ASIACRYPT 2014. Lecture Notes in Computer Science, vol 8873. Springer, Berlin, Heidelberg, DOI 10.1007/978-3-662-45611-8_6, 2014, <https://doi.org/10.1007/978-3-662-45611-8_6>.

[ADL17] Ashur, T., Dunkelman, O., and A. Luykx, "Boosting Authenticated Encryption Robustness with Minimal Modifications", Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10403. Springer, Cham, DOI 10.1007/978-3-319-63697-9_1, 2017, <https://doi.org/10.1007/978-3-319-63697-9_1>.

[B20] Bellizia, D., Bronchain, O., Cassiers, G., Grosso, V., Guo, C., Momin, C., Pereira, O., Peters, T., and FX. Standaert, "Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography: A Practical Guide Through the Leakage-Resistance Jungle", Advances in Cryptology – CRYPTO 2020. CRYPTO 2020. Lecture Notes in Computer Science, vol 12170. Springer, Cham, DOI 10.1007/978-3-030-56784-2_13, 2020, <https://doi.org/10.1007/978-3-030-56784-2_13>.

[BC09] Forler, C. and E. List, "MAC Reforgeability", Fast Software Encryption. FSE 2009. Lecture Notes in Computer Science, vol 5665. Springer, Berlin, Heidelberg, DOI 10.1007/978-3-642-03317-9_21, 2009, <https://doi.org/10.1007/978-3-642-03317-9_21>.

[BFN98] Blaze, M., Feigenbaum, J., and M. Naor, "A formal treatment of remotely keyed encryption", Advances in Cryptology — EUROCRYPT'98. EUROCRYPT 1998. Lecture Notes in Computer Science, vol 1403. Springer, Berlin, Heidelberg, DOI 10.1007/BFb0054131, 1998, <https://doi.org/10.1007/BFb0054131>.

[BK2011] Bellare, M. and S. Keelveedhi, "Authenticated and Misuse-Resistant Encryption of Key-Dependent Data", Advances in Cryptology – CRYPTO 2011. CRYPTO 2011. Lecture Notes in Computer Science, vol 6841. Springer, Berlin, Heidelberg., DOI 10.1007/978-3-642-22792-9_35, 2011, <https://doi.org/10.1007/978-3-642-22792-9_35>.

[BKY02] Buonanno, E., Katz, J., and M. Yung, "Incremental Unforgeable Encryption", Fast Software Encryption. FSE 2001. Lecture Notes in Computer Science, vol 2355. Springer, Berlin, Heidelberg, DOI 10.1007/3-540-45473-X_9, 2002, <https://doi.org/10.1007/3-540-45473-X_9>.

[BN2000] Bellare, M. and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm", Proceedings of ASIACRYPT 2000, Springer-Verlag, LNCS 1976, pp. 531-545, DOI 10.1007/s00145-008-9026-x, 2000, <https://doi.org/10.1007/s00145-008-9026-x>.

[BNT19] Bellare, M., Ng, R., and B. Tackmann, "Nonces Are Noticed: AEAD Revisited", Advances in Cryptology – CRYPTO 2019. CRYPTO 2019. Lecture Notes in Computer Science, vol 11692. Springer, Cham, DOI 10.1007/978-3-030-26948-7_9, 2019, <https://doi.org/10.1007/978-3-030-26948-7_9>.

[BT16] Bellare, M. and B. Tackmann, "The Multi-User Security of Authenticated Encryption: AES-GCM in TLS 1.3", Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9814. Springer, Berlin, Heidelberg, DOI 10.1007/978-3-662-53018-4_10, 2016, <https://doi.org/10.1007/978-3-662-53018-4_10>.

[C20] Chakraborti, A., Datta, N., Jha, A., Mancillas-López, C., Nandi, M., and Y. Sasaki, "INT-RUP Secure Lightweight Parallel AE Modes", IACR Transactions on Symmetric Cryptology, 2019(4), 81–118, DOI 10.13154/tosc.v2019.i4.81-118, 2020, <https://doi.org/10.13154/tosc.v2019.i4.81-118>.

[DA03] Dodis, Y. and JH. An, "Concealment and Its Applications to Authenticated Encryption", Advances in Cryptology — EUROCRYPT 2003. EUROCRYPT 2003. Lecture Notes in Computer Science, vol 2656. Springer, Berlin, Heidelberg, DOI 10.1007/3-540-39200-9_19, 2003, <https://doi.org/10.1007/3-540-39200-9_19>.

[DGGK21] Dobraunig, C., Grassi, L., Guinet, G., and K. Kuijsters, "CIMINION: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields", Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Computer Science(), vol 12697. Springer, Cham, DOI 10.1007/978-3-030-77886-6_1, 2021, <https://doi.org/10.1007/978-3-030-77886-6_1>.

[FJMV2004] Valette, PA., Joux, A., Martinet, G., and F. Valette, "Authenticated On-Line Encryption", Selected Areas in Cryptography. SAC 2003. Lecture Notes in Computer Science, vol 3006. Springer, Berlin, Heidelberg. , DOI 10.1007/978-3-540-24654-1_11, 2004, <https://doi.org/10.1007/978-3-540-24654-1_11>.

[FLLW17] Forler, C., List, E., Lucks, S., and J. Wenzel, "Reforgeability of Authenticated Encryption Schemes", Information Security and Privacy. ACISP 2017. Lecture Notes in Computer Science, vol 10343. Springer, Cham, DOI 10.1007/978-3-319-59870-3_2, 2017, <https://doi.org/10.1007/978-3-319-59870-3_2>.

[FOR17] Farshim, P., Orlandi, C., and R. Rosie, "Authenticated and Misuse-Resistant Encryption of Key-Dependent DataSecurity of Symmetric Primitives under Incorrect Usage of Keys", IACR Transactions on Symmetric Cryptology, 2017(1), 449–473., DOI 10.13154/

tosc.v2017.i1.449-473, 2017, <https://doi.org/10.13154/tosc.v2017.i1.449-473>.

[GLR17] Grubbs, P., Lu, J., and T. Ristenpart, "Message Franking via Committing Authenticated Encryption.", Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10403. Springer, Cham, DOI 10.1007/978-3-319-63697-9_3, 2017, <https://doi.org/10.1007/978-3-319-63697-9_3>.

[GPPS19] Guo, C., Pereira, O., Peters, T., and FX. Standaert, "Authenticated Encryption with Nonce Misuse and Physical Leakages: Definitions, Separation Results and Leveled Constructions", Progress in Cryptology - LATINCRYPT 2019. LATINCRYPT 2019. Lecture Notes in Computer Science, vol 11774. Springer, Cham, DOI 10.1007/978-3-030-30530-7_8, 2019, <https://doi.org/10.1007/978-3-030-30530-7_8>.

[HKR2015] Hoang, VT., Krovetz, T., and P. Rogaway, "Robust Authenticated-Encryption AEZ and the Problem That It Solves", Advances in Cryptology -- EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science(), vol 9056. Springer, Berlin, Heidelberg. , DOI 10.1007/978-3-662-46800-5_2, 2015, <https://doi.org/10.1007/978-3-662-46800-5_2>.

[HRRV15] Hoang, VT., Reyhanitabar, R., Rogaway, P., and D. Vizár, "Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance", Advances in Cryptology -- CRYPTO 2015. CRYPTO 2015. Lecture Notes in Computer Science, vol 9215. Springer, Berlin, Heidelberg, DOI 10.1007/978-3-662-47989-6_24, 2015, <https://doi.org/10.1007/978-3-662-47989-6_24>.

[I-D.irtf-cfrg-aead-limits] Günther, F., Thomson, M., and C. A. Wood, "Usage Limits on AEAD Algorithms", Work in Progress, Internet-Draft, draft-irtf-cfrg-aead-limits-06, 30 January 2023, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-aead-limits-06>.

[JMV2002] Joux, A., Martinet, G., and F. Valette, "Blockwise-Adaptive Attackers Revisiting the (In)Security of Some Provably Secure Encryption Modes: CBC, GEM, IACBC", Advances in Cryptology — CRYPTO 2002. CRYPTO 2002. Lecture Notes in Computer Science, vol 2442. Springer,

Berlin, Heidelberg, DOI 10.1007/3-540-45708-9_2, 2002, <https://doi.org/10.1007/3-540-45708-9_2>.

[LGR21] Len, J., Grubbs, P., and T. Ristenpart, "Partitioning Oracle Attacks", 30th USENIX Security Symposium (USENIX Security 21), 195--212, 2021.

[M05] McGrew, D., "Efficient authentication of large, dynamic data sets using Galois/counter mode (GCM)", Third IEEE International Security in Storage Workshop (SISW'05), San Francisco, CA, USA , DOI 10.1109/SISW.2005.3., 2005, <https://doi.org/10.1109/SISW.2005.3.>.

[MBTM17] McKay, K., Bassham, L., Turan, MS., and N. Mouha, "Report on Lightweight Cryptography", DOI 10.6028/NIST.IR.8114, 2017, <https://doi.org/10.6028/NIST.IR.8114>.

[R2002] Rogaway, P., "Authenticated-encryption with associated-data.", Proceedings of the 9th ACM conference on Computer and communications security (CCS '02), Association for Computing Machinery, New York, NY, USA, 98–107, DOI 10.1145/586110.586125, 2002, <https://doi.org/10.1145/586110.586125>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RS06] Rogaway, R. and T. Shrimpton, "A Provable-Security Treatment of the Key-Wrap Problem", Advances in Cryptology - EUROCRYPT 2006. EUROCRYPT 2006. Lecture Notes in Computer Science, vol 4004. Springer, Berlin,

Heidelberg, DOI 10.1007/11761679_23, 2016, <https://doi.org/10.1007/11761679_23>.

[SY16] Sasaki, Y. and K. Yasuda, "A New Mode of Operation for Incremental Authenticated Encryption with Associated Data", Selected Areas in Cryptography – SAC 2015. SAC 2015. Lecture Notes in Computer Science(), vol 9566. Springer, Cham, DOI 10.1007/978-3-319-31301-6_23, 2016, <https://doi.org/10.1007/978-3-319-31301-6_23>.

Appendix A. Contributors

Author's Address

Andrey Bozhko (editor)
CryptoPro

Email: andbogc@gmail.com