





Automated Analysis of Protocols that use Authenticated Encryption:

Analysing the Impact of the Subtle Differences between AEADs on Protocol Security



Cas Cremers*

Alexander Dax* Charlie Jacomme[‡]



Mang Zhao*

- * CISPA Helmholtz Center for Information Security
- [‡] INRIA Paris





Facebook's Message Franking:

- Abuse reporting mechanism within E2EE communication
- [DGRW18] the reported message seen by the server is not the same as the one seen by the reporting user



Facebook's Message Franking:

- Abuse reporting mechanism within E2EE communication
- [DGRW18] the reported message seen by the server is not the same as the one seen by the reporting user

SFrame:

- E2EE group communication protocol for audio/video
- [IIM21] impersonate other group members



Facebook's Message Franking:

- Abuse reporting mechanism within E2EE communication
- [DGRW18] the reported message seen by the server is not the same as the one seen by the reporting user

SFrame:

- E2EE group communication protocol for audio/video
- [IIM21] impersonate other group members by collision



YubiHSM:

- Store cryptographic secrets and offer API for crypto operations
- [KS12] Full secret key leaked



Facebook's Message Franking:

- Abuse reporting mechanism within E2EE communication
- [DGRW18] the reported message seen by the server is not the same as the one seen by the reporting user



- E2EE group communication protocol for audio/video
- [IIM21] impersonate other group members by collision



YubiHSM:

- Store cryptographic secrets and offer API for crypto operations
- [KS12] Full secret key leaked

Where do those attacks come from?





- symmetric encryption
- data is integrity protected



- symmetric encryption
- data is integrity protected
- Often 4 inputs



- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - data/message



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - data/message
 - associated data (e.g., meta info)
 - In the clear,

but also integrity protected



- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - data/message
 - associated data (e.g., meta info)
 - In the clear,
 - but also integrity protected
 - Entropy source:
 - Nonces
 - Counters



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - data/message
 - associated data (e.g., meta info)
 - In the clear,
 - but also integrity protected
 - Entropy source:
 - Nonces
 - Counters



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key Ο
 - data/message \bigcirc
 - associated data (e.g., meta info) Ο
 - In the clear. **.** but also integrity protected
 - Entropy source: \bigcirc
 - Nonces
 - Counters

How to Abuse and Fix Authenticated Encryption Without Key Commitment* Ange Albertini ¹ , Thai Duong ¹ , Shay Gueron ^{2,3} , Stefan Kölbi ¹ , Atul Luykz ¹ , and Sophie Schmieg ¹ ¹ Security Engineering Research, Google ² Untwest of Haffa ³ Amazon	
Abstract Authenicated encrystem (AE) is used in a wide variety of prefications, potentially in estings for which it was of transformed and DPD encrystem as camples to argue the pro- present of the abstract of the abstra	

however, products do rely on key commitment. We discuss three recent applications where missing key commitment is exploitable in practice. We provide proof-of-concept attacks its security guarantees in settings which push the boundaries via a tool that constructs AES-GCM ciphertext which can be

NaCl [nac] and Tink [tin].

With AE more widely used, recent research focuses on and assumptions of conventional AE, such as understandin



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - data/message
 - associated data (e.g., meta info)
 - In the clear, but also integrity protected
 - Entropy source:
 - Nonces
 - Counters

How to Abuse and Fix Authenticated I Ange Albertini ¹ , Thui Duong ¹ , Shay Gueron ^{2,3} , S ¹ Security Engineerin ² Universit ³ Am	ng Research, Google y of Haifa
Lhatrat Anthenticated encryption (AI2) is used in a wist warrier of applications, percentally in settings (see Valch it was not orig- tion) and the setting of the setting of the setting of applications, percentally in the setting of the setting application of the setting of the setting of the setting descript as wald pilotics used as the setting setting of the setting encoder of the secting of actual products in the new order of setting of a setting products of the new order of setting of a setting products of the new order of setting of a setting products of the new order of setting of a setting products of the secting of a setting and the secting of a setting products in the new order of setting of a setting products of the secting of a setting the correspondences. All Section of the secting of a setting product of the secting of a setting products in the setting with a set of the correspondences and the section of the setting of the secting of the secting of the setting of the setting of the secting of the secting of the secting of the setting of the secting of the secting of the setting of the secting of the setting of the secting of the setting of the setting of the secting of the setting of the secting of the secting of the secting of the secting of the setting of the secting of the secting of the setting of the secting of the setting of the secting of the secting of the setting of the secting of the	Back et al. (ECO20) (all lines in Arghe Monaga, OpenRC and DFC any plant a catagory to an engine the pra- titioners are often only convinced that unandenticical SKI: is inscure when they laces a proof-of-concerpted point. Similar efforts are deemed accessary to domenstrate the exploitability of the strategiest of the strategiest of the strategiest undenticated encryption (AE) [INND, KY00], a well-stadied primitive which exploits the primitian value strategiest with relatively small performance overhead. AE is then as a default SKI option in modern cryptographic libraries are a default SKI option in modern cryptographic libraries are as a strategiest of the strategiest of modern strategiest and default SKI option in modern cryptographic libraries are as a strategiest of the strategiest of modern focuses on and assume that one contexplay which peak the bound focuses on and assume that one contexplay which peak the strategiest and assume that one contexplay which peak the strategiest of a strategiest of the contexplay and the peak the strategiest of the assume that one contexplay which peak the strategiest of the assume that one contexplay and the peak the strategiest of the strategiest of the assume that one contexplay and the peak the strategiest of the assume that one contexplay and the peak the peak the peak the strategiest of the assume that one contexplay and the peak the strategiest of the s

Robust Encryption			
Mi	THEL ABDALLA ¹	MIHIR BELLARE ²	GREGORY NEVEN ³
		Abstract	
hard to pro a property conjunct o achieve it, provide tra specific em property. for PEKS have false schemes to	shace a ciphertext the that has been implic anonymous encrypt such as adding recip molorms that do achis ryption schemes in th We explain that robus (Public Key Encrypt societives), and our we	It is valid for two different titly assumed in the past. ion. We show that nature iont identification informs eve it, efficiently and prova in literature, providing simp stness of the underlying am ion with Keyword Search) ek provides the first generi	erryption. Robustness means it is uses. Robustness makes explicit al ancountry preserving ways to its hofes encrypting, fail. We bby, We assess the robustness of all patches for some that lack that the patches for some that lack that the constitution of the source of the source of the source of the to be constitution of means the source of the source of the source of the source of the source of the source of the source of the to be constitution of the source of the source of the source of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the to be constitution of the source of the source of the source of the to be constitution of the source of the source of the source of the to be constitution of the source of



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - o data/message
 - associated data (e.g., meta info)
 - In the clear, but also integrity protected
 - Entropy source:
 - Nonces
 - Counters

	How to Abuse and Fix Authenticated Encryption Without Key Commitment* Ange Albertini ¹ , Thai Daong ¹ , Shay Gueron ^{3,3} , Stefan Kölls ¹ , Atuil Luyka ¹ , and Sophie Schmieg ¹ ¹ Security Engineering Research, Google ² University of Hafa ³ Amazon	
	Abstract Beck et al. [B2C020] cite flaws in Apple Mesage, OperRPR and PDF encryption (A2) is used in a wide variety of applications, potentially in each for which it was on understand while inally designed. Recent research trice to understand when harvens when AF is not understand when and harvens when AF is not understand when harvens when AF is not understand when harvens when	
	Partitioning Oracle Attacks Julia Len Paul Grubbs Thomas Ristenpart <i>Cornell Tech</i>	
Robust Energy MICHEL ABOALLA ² MIRIE BEAA Properties a provide metal and a second property that has been implicitly anomed in the property of the second second second second property and the second	of decryption error oracles which, conceptually, take a cipher- text as input and output whether the decryption key bedoes to some known subset of keys. Partitioning oracles can arise when encryption schemes are not committing with respect to their keys. We defail adaptive chosen ciphertext atta assues that reveals whether decry under a target ascert key succeeds. This enables an atta exploit partitioning oracles to efficiently recover passwords and de-anonymize anonymous communications. The mather syn alytic step for our antacks is constructing (what we call untit-collisions, in which a single AEAD ciphertext to suilt such that decryption succeeds under some number	rsary crypt bmit ption cker ptan-) key in be k of algo- M. It $O(k^2)$. We



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - o data/message
 - associated data (e.g., meta info)
 - In the clear, but also integrity protected
 - Entropy source:
 - Nonces
 - Counters

_	How to Abuse and Fix Authenticated Encry Ange Albertini ¹ , Thai Duong ¹ , Shay Gueron ^{2,3} , Stefan ¹ Security Engineering Ress	Kölbl ¹ , Atul Luykx ¹ , and Sophie Schmi	
	GCM-SIV: Full Nonce Misuse-Res enticated Encryption at Under Shay Gueron ¹ and Yehuda Lindell ² ¹ Department of Makematics. University of Halfs, and Int	One C/B	lessage, inf prac- d SKE Similar inshility
	Development Center, Isiacar. haybrath.hast.hast.e.il ² Department of Computer Science, Bar Hau Univ 11ada 112bus.e.ast. Abstract. Authenticated encryption schemes guara and infurgity, and have become the deduite level of encry- ted and the science of the data of the science of the data science of the science of the science of the data information of the science of the science of the science of the science will improve on existing methods. One property of in being considered more today is due to the fact that impute science of the same mensag if the same nences in used to encryption scheme has a if the same nences in used to encryption scheme has a if the same nences in used to encryption scheme has a if the same nences in used to encryption scheme has a if the same nences in used to encryption scheme has a if the same nences in used to encryption scheme has a if the same nences in used to encryption scheme has a if the same nences in the same nences and	mity, ISRARE. tee both privacy prion in modern most prion CARSAR lencryptics CARSA	23.
Robust Ends, MICHIER ADDALLA [®] MIRIER BELLA MICHIER ADDALLA [®] MIRIER BELLA CONTROL ADDALLA [®] MIRIER BELLA DE SPORTE ADDALLA [®] MIRIER ADDALLA [®] MIRIER ADDALLA [®] MIRIER ADDALLA [®] MIRIER ADDALLA [®] MIRIER ADDALLA [®] MIRIER ADDALLA [®] MIRIER ADDALLA [®] MIRIER A	same ciphertext is obtained and to the fact that the set of decryption error oracles which, conceptually, take a cipher- ett as input and output whether the decryption key belongs to some known subset of Keys. Partitioning oracles can arise when encryption schemes are not committing with respect to their keys. We detail adaptive chosen ciphertext attacks that exploit partitioning oracles to efficiently recover passwords and de-anonymize anonymous communications. The attacks utilize efficient key multi-collision algorithms — a cryptana- lytic goal that we define — against widely used authenticated encryption with associated data (AEAD) schemes, including AES-GCM, XSalsa20/Poly1305, and ClacLa20/Poly1305. We build a practical partitioning oracle attack that quickly recovers passwords from Shadowsocks proxy servers. We	me message was CCA. Briefly, a partitioning oracle can: (1) efficiently craft ciphertests under a large number of potential such ciphertests to a system that re under a target secret key succeeds to learn information about the sect alytic step for our attacks is coardi- tic secret and the section of the sec- al section of the section of the sec- al section of the section of the sec- tion of the section of the sec- build key multi-collision ciphertes time, making them reasonably sca	i that successfully decrypt keys, and (2) can submit veals whether decryption This enables an attacker et key. The main cryptan- ucting (what we call) key AEAD ciphertext can be s under some number k of tic goal and give an algo- lisions for AES-GCM. It ts of length O(k) in O(k ²)



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - o data/message
 - associated data (e.g., meta info)
 - In the clear, but also integrity protected
 - Entropy source:
 - Nonces
 - Counters

	How to Abuse and Fix Authenticated Encryption Without Key Commitment	
	Ange Albertini ¹ , Thai Duong ¹ , Shay Gueron ^{2,3} , Stefan Kölbl ¹ , Atul Luykx ¹ , and Sophie Schmieg	1
	¹ Security Engineering Research, Google	
	GCM-SIV: Full Nonce Misuse-Resistant Auth- enticated Encryption at Under One C/B	sage,
	Shaw Custonl and Valueda Lindell ²	prac- SKE milar
		bility
	Abstract. Authenticated encryption schemes guarantee both privacy and integrity, and have become the default level of scryption in modern modern in the scheme scheme scheme scheme scheme scheme scheme scheme tools: A MS COV (due to its insurance scheme). The scheme CANAD	
	Message Franking via	
	Committing Authenticated Encryption*	
Robust Enc	Paul Grubbs ¹ , Jiahui Lu ² , and Thomas Ristenpart ¹	
MICHEL ABDALLA ¹ MIHIR BELLA to	f decryption e ¹ Cornell Tech ² Shanghai Jiao Tong University xt as input a some know hen encrypti	
Valences the second sec	(accuracy) we in the study of message fracting, recently introduced in Facebook de-anony did-anony did-	to Facebook ing via a new sociated data be used as a dition to the ng mandates ertheless, and r otherwise), g secret keys ymmetric en- ulyze schemes



Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - o data/message
 - associated data (e.g., meta info)
 - In the clear, but also integrity protected
 - Entropy source:
 - Nonces
 - Counters

Anonymou	becanty Engineering to	esearch, Google	
	sΔE	escarcii, chogic	1
		sistant Auth-	
ohn Chan and Philli	ip Rogaway	r One C/B	lessage.
		12	uat prac- ed SKE Similar
		ntel Corporation, Israel	itability 21
pts. To enable this, t ciphertext. But doing	the nonce is often sent in the this can forfeit anonymity and	versity, ISRAEL	
a session-ID (used to it s, we introduce anony origin even when they to decrypt (apart from	identify the operative key). To mous AE, wherein (phertexts γ are understood to encompass m the receiver's secret state).	intee both privacy ryption in modern ncryption schemes current CAESAR	
meralizes and strength	hens conventional nonce-based	ge Franking via	
ne and a blockcipher. tot address privacy loss ciphertexts, now more	We prove NonceWrap secure. ss through traffic-flow analysis,	uthenticated Encryption [*]	,
mous encryption - auth	nervotion	ui Lu ² , and Thomas Ristenpart ¹	of y
text as input a to some know	Contra Ion	² Shanghai Jiao Tong University	pt it m
their keys. We		Abstract	er
exploit partitic and de-anonyr utilize efficien lytic goal that encryption wit AES-GCM, X We build a p recovers passy	encryptol message system. It target without compromising security guarant cryptographic primitive: compactly co (AEAD). This is an AEAD scheme for cryptographic commitment to the me message, a value that can be used to despite the fact that AEAD schemes; we prove that many in-sase AEAD sche as openings. An implication of our res- cryption schemes are committing in the	franking, recently introduced in Facebo verifiable reporting of abusive message frammarking and the goals of message frammarking and the goals of message frammarking and the goals of the second second second second second and the second second second second second second open the commitment. Security for fra- notions associated with commitment. Nure in general not committing (compact) motions associated with commitment in the mes can be used for message franking by ualts is the first proofs that several in use traditional server. We also propose and i	res to Facebook is a niking via a new of associated data of an be used as a o- addition to the lit nking mandates ²) (evertheless, and ²) (evertheless, and ²) (evertheless, and susing secret keys e symmetric en- analyze schemes
U unyyy reer 1 poporti t og og	John Chan and Phill Department of Comp University of California matemary formulation or program to the single part of the single parts. To evaluate the single part of the single part o	John Charlen of Computer Science University of Caldornia, Davis, USA automary formulation of antimeticated encryption (AE) provide the state of the state of the state of the state provide state of the state of the state of the state of anyoning charlen be state of the state of the state provide state of the state of the state of the state of anyoning charlen be state of the state of the state of anyoning charlen be state of the state provide state of the state of the state of the state provide state of the state of the state of the state the state state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state the state state of the state of the state of t	John Chan and Phillip Rogeway: Department of Colloring, Davis, USA University of Colloring, Davis, USA Department of Colloring, Davis, Davis, Davis, Davis, Davis, Davis, Davis, Davis, Davis, USA Department of Colloring, Davis, D

20

AEAD is complex!

Authenticated Encryption with associated data (AEAD):

- symmetric encryption
- data is integrity protected
- Often 4 inputs
 - Secret key
 - o data/message
 - associated data (e.g., meta info)
 - In the clear, but also integrity protected
 - Entropy source:
 - Nonces
 - Counters

	How to Abuse and Fix Authenticated Encryption Without Key Comn Ange Albertini ¹ , Thai Duong ¹ , Shay Gueron ^{2,3} , Stefan Köllö ¹ , Atul Laykx ¹ , and Sophie	
	are Noticed: AEAD Revisited	lessiage, uat prac- ed SKE Similar itability zi
 Mihir Bei	LLARE ^R RUTH NG ^R BJÖRN TACKMANN ⁸ November 2019 Abstract	.*
under which the way th We bridge the gap with the syntax (decryption i just messages, but also the new definitions. We and advanced security (reused), where it, sub a subject, fields of the proofs that for particular the subject is different to the subject is for the subject proofs that for particular the subject is proofs that for particular the subject is the subject is for the subject is proofs that for particular the subject is the subject is subject is for the subject is proofs that for particular the subject is the subject is subject is subject is proofs that for particular the subject is the subject is subject is subject is proofs that the subject is subject is proof to the subject is subject is proof to the subject is subject is the subject is subject is subject is proof to the subject is subject is subject is proof to the subject is subject is subject is proof to the subject is subject is subject is subject is proof to the subject is subject is subject is subject is subject is proof to the subject is subject	Abstract a gap between theory and usage of nonce-based symmetric encryption, e former treats nonces: can result in violation of privacy in the latter. a new treatment of nonce-based symmetric encryption that modifies no longer takes a nonce), upgrades the security goal (asking that not monces, be hidden) and gives simple, efficient schemes conforming to investigate both basic security (holding when nonces are not reused) misuse resistance, providing best-possible guarantees when nonces are tic goal that cryption with generation of the security of the bild a cryptographic primitive compactly committened the committenet. Security i we build a cover pass we have that can be used to open the committened. Security of we prove that may in-use AEAD schemes are to committenet the security of we prove that may in-use AEAD schemes are to committenet. We prove that may in-use AEAD schemes are the security of we prove that may in-use AEAD schemes are to mergend of mession are opening. An implication of our results is the first proof that several cryption schemes are committing in the trafficial section. We are opening and the trafficial section of the result opening.	text can be used as a es, in addition to the or franking mandates nt. Nevertheless, and upactly or otherwise), g by using secret keys in-use symmetric en- and analyze schemes





Rogue Decryption Failures: Reconciling AE Robustness Notions Authenticated Encryption with associated data (AEAD): Guy Barwell, Daniel Page, and Martijn Stam Department of Computer Science, University of Bristol Merchant Venturers Building, Woodland Road, symmetric encryption Bristol, BS8 1UB, United Kingdom. {guy.barwell, daniel.page, martijn.stam}@bristol.ac.uk data is integrity protected Abstract. An Authenticated Encryption scheme (AE) is deemed secure if ciphertexts both look like random Often 4 inputs bitstrings and are unforgeable. One shortcoming of AE as commonly understood is its idealized, all-or-nothing decryption: if decryption fails, it will always provide the same single error message and nothing more. Reality often turns out differently: encode-then-encipher schemes often output decrypted ciphertext before verification has taken place, whereas pad-then-MAC-then-encrypt schemes are prone to distinguishable verification failures 0 Secret key due to the subtle interaction between padding and the MAC-then-encrypt concept. Three recent papers provided what appeared independent and radically different definitions to model this type of decryption leakage. To reconcile these three works, and indeed the literature in general, we define an expressive "clean slate" data/message \bigcirc framework that allows us to compare and contrast the previous notions within a systematic naming scheme. We then extend this by allowing for (deterministic) decryption leakage from invalid oueries, providing a reference model of security we term Subtle Authenticated Encryption (SAE). Then, we thoroughly describe this associated data (e.g., meta info) \bigcirc landscape by translating classical results (where applicable) and extending them to encompass our new notions. Finally, with SAE as a reference point, we compare the three noted works. We find that, at their core, the previous notions are essentially equivalent; their key differences stem from definitional choices independent of In the clear. the desire to capture real world behaviour. **1**11 May 11, 2022 but also integrity protected We draw attention to a ga under which the way the for We bridge the gap with a n Entropy source: Ο the syntax (decryption no lo just messages, but also none Abstract the new definitions. We inve Nonces This paper provides efficient authenticated-encryption (AE) schemes in which a ciphertext is and advanced security (misu a commitment to the key. These are extended, at minimal additional cost, to schemes where the reused) ciphertext is a commitment to all encryption inputs, meaning key, nonce, associated data and orhiese it such as adding regiment iden message. Our primary schemes are modifications of GCM (for basic, unique-nonce AE security) Counters provide transforms that do achieve it, efficiently and specific encryption schemes in the literature, providing lytic go and AES-GCM-SIV (for misuse-resistant AE security) and add both forms of commitment encrypt property. We explain that robustness of the under without any increase in ciphertext size. We also give more generic, but somewhat more costly, PEKS (Public Key Encryption with Keywor AES-G message, a value that can be used to open the commitment. Security for franking manda have false positives), and our work provides the fi We build a schemes to consistent (and secure) PEKS schem more than that required of traditional notions associated with commitment. Nevertheless and simpler use of encryption recovers pass despite the fact that AEAD schemes are in general not committing (compactly or otherwise), we prove that many in-use AEAD schemes can be used for message franking by using secret keys as openings. An implication of our results is the first proofs that several in-use symmetric encryption schemes are committing in the traditional sense. We also propose and analyze schemes that retain security even after openings are revealed to an adversary. One is a generalization of

protocol designers?



Rogue Decryption Failures: Reconciling AE Robustness Notions Authenticated Encryption with associated data (AEAD): Guy Barwell, Daniel Page, and Martijn Stam Department of Computer Science, University of Bristol Merchant Venturers Building, Woodland Road, symmetric encryption Bristol, BS8 1UB, United Kingdom. {guy.barwell, daniel.page, martijn.stam}@bristol.ac.uk data is integrity protected Abstract. An Authenticated Encryption scheme (AE) is deemed secure if ciphertexts both look like random Often 4 inputs bitstrings and are unforgeable. One shortcoming of AE as commonly understood is its idealized, all-or-nothing decryption: if decryption fails, it will always provide the same single error message and nothing more. Reality often turns out differently: encode-then-encipher schemes often output decrypted ciphertext before verification has taken place, whereas pad-then-MAC-then-encrypt schemes are prone to distinguishable verification failures 0 Secret key due to the subtle interaction between padding and the MAC-then-encrypt concept. Three recent papers provided what appeared independent and radically different definitions to model this type of decryption leakage. To reconcile these three works, and indeed the literature in general, we define an expressive "clean slate" data/message \bigcirc framework that allows us to compare and contrast the previous notions within a systematic naming scheme. We then extend this by allowing for (deterministic) decryption leakage from invalid oueries, providing a reference model of security we term Subtle Authenticated Encryption (SAE). Then, we thoroughly describe this associated data (e.g., meta info) \bigcirc landscape by translating classical results (where applicable) and extending them to encompass our new notions. Finally, with SAE as a reference point, we compare the three noted works. We find that, at their core, the previous notions are essentially equivalent; their key differences stem from definitional choices independent of In the clear. the desire to capture real world behaviour. . May 11, 2022 but also integrity protected We draw attention to a ga under which the way the for We bridge the gap with a n Entropy source: Ο the syntax (decryption no lo just messages, but also none Abstract the new definitions. We inve Nonces This paper provides efficient authenticated-encryption (AE) schemes in which a ciphertext is and advanced security (misu a commitment to the key. These are extended, at minimal additional cost, to schemes where the reused) ciphertext is a commitment to all encryption inputs, meaning key, nonce, associated data and achiese it such as adding regiment iden message. Our primary schemes are modifications of GCM (for basic, unique-nonce AE security) Counters provide transforms that do achieve it, efficiently an specific encryption schemes in the literature, providi lytic go and AES-GCM-SIV (for misuse-resistant AE security) and add both forms of commitment encrypt property. We explain that robustness of the under without any increase in ciphertext size. We also give more generic, but somewhat more costly, PEKS (Public Key Encryption with Keywor AES-G message, a value that can be used to open the commitment. Security for franking manda have false positives), and our work provides the fi We build a schemes to consistent (and secure) PEKS schen more than that required of traditional notions associated with commitment. Nevertheless and simpler use of encryption recovers pass despite the fact that AEAD schemes are in general not committing (compactly or otherwise), we prove that many in-use AEAD schemes can be used for message franking by using secret keys as openings. An implication of our results is the first proofs that several in-use symmetric encryption schemes are committing in the traditional sense. We also propose and analyze schemes \rightarrow What guarantees does it give that retain security even after openings are revealed to an adversary. One is a generalization of



Rogue Decryption Failures: Reconciling AE Robustness Notions Authenticated Encryption with associated data (AEAD): Guy Barwell, Daniel Page, and Martijn Stam Department of Computer Science, University of Bristol symmetric encryption Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, United Kingdom. {guy.barwell, daniel.page, martijn.stam}@bristol.ac.uk data is integrity protected Abstract. An Authenticated Encryption scheme (AE) is deemed secure if ciphertexts both look like random Often 4 inputs bitstrings and are unforgeable. One shortcoming of AE as commonly understood is its idealized, all-or-nothing decryption: if decryption fails, it will always provide the same single error message and nothing more. Reality often turns out differently: encode-then-encipher schemes often output decrypted ciphertext before verification • Secret key has taken place, whereas pad-then-MAC-then-encrypt schemes are prone to distinguishable verification failures due to the subtle interaction between padding and the MAC-then-encrypt concept. Three recent papers provided what appeared independent and radically different definitions to model this type of decryption leakage. To reconcile these three works, and indeed the literature in general, we define an expressive "clean slate" data/message framework that allows us to compare and contrast the previous notions within a systematic naming scheme. We then extend this by allowing for (deterministic) decryption leakage from invalid queries, providing a reference model of security we term Subtle Authenticated Encryption (SAE). Then, we thoroughly describe this associated data (e.g., meta info) landscape by translating classical results (where applicable) and extending them to encompass our new notions. Finally, with SAE as a reference point, we compare the three noted works. We find that, at their core, the previous notions are essentially equivalent; their key differences stem from definitional choices independent of In the clear, but also integrity the desire to capture real world behaviour. May 11, 2022 protected We draw attention to a ga under which the way the for We bridge the gap with a n Entropy source: the syntax (decryption no lo just messages, but also non Abstract the new definitions. We inve Nonces This paper provides efficient authenticated-encryption (AE) schemes in which a ciphertext is and advanced security (misu a commitment to the key. These are extended, at minimal additional cost, to schemes where the reused) ciphertext is a commitment to all encryption inputs, meaning key, nonce, associated data and message. Our primary schemes are modifications of GCM (for basic, unique-nonce AE security) Counters lytic go and AES-GCM-SIV (for misuse-resistant AE security) and add both forms of commitment encrypt without any increase in ciphertext size. We also give more generic, but somewhat more costly, message, a value that can be used to open the commitment. Security for franking mandat-We build a more than that required of traditional notions associated with commitment. Nevertheless, and recovers pass despite the fact that AEAD schemes are in general not committing (compactly or otherwise), we prove that many in-use AEAD schemes can be used for message franking by using secret keys as openings. An implication of our results is the first proofs that several in-use symmetric encryption schemes are committing in the traditional sense. We also propose and analyze schemes \rightarrow What guarantees does it give that retain security even after openings are revealed to an adversary. One is a generalization of protocol design tions as we speak!

Many ways to misuse and misunderstand AEADs









24





→ [DGRW18] A single encrypted message can be decrypted under 2 distinct keys to 2 different meaningful messages







Facebook's Message Franking

→ [DGRW18] A single encrypted message can be decrypted under 2 distinct keys to 2 different meaningful messages



→ [IIM21] instead of signing message, only signed authentication tag which makes it possible to impersonate peers





Facebook's Message Franking

→ [DGRW18] A single encrypted message can be decrypted under 2 distinct keys to 2 different meaningful messages



→ [IIM21] instead of signing message, only signed authentication tag which makes it possible to impersonate peers



YubiHSM

 \rightarrow [KS12] allowing to reuse nonces leads leakage of secret key



Facebook's Message Franking

→ [DGRW18] A single encrypted message can be decrypted under 2 distinct keys to 2 different meaningful messages



→ [IIM21] instead of signing message, only signed authentication tag which makes it possible to impersonate peers



YubiHSM

 \rightarrow [KS12] allowing to reuse nonces leads leakage of secret key

How can we prevent such attacks?

Security analysis







Two major models: Computational and Symbolic



Two major models: Computational and Symbolic

Computational Model:

- Does not scale well
- Limited automation

Symbolic Model:

- Authenticated encryption
 modelled very coarsely
- Traditional representation
 misses attacks



Two major models: Computational and Symbolic



- Does not scale well
- Limited automation

Symbolic Model:

- Authenticated encryption modelled very coarsely
- Traditional representation
 misses attacks

Attack finding until now was manual effort. Can we do better?



Two major models: Computational and Symbolic

Computational Model:

- Does not scale well
- Limited automation

Symbolic Model:

- Authenticated encryption
 modelled very coarsely
- Traditional representation
 misses attacks

Attack finding until now was manual effort. Can we do better?

Can we automatically detect the impact of subtle AEAD behavior in security protocols?

Our Approach



Our Approach



1. We collected

- definitions of AEAD constructions and properties
- known AEAD attacks on the protocol level

What should we model?



1. We collected

- definitions of AEAD constructions and properties
- known AEAD attacks on the protocol level
- 2. We highlighted the relations of properties and proving the missing ones

What should we model?

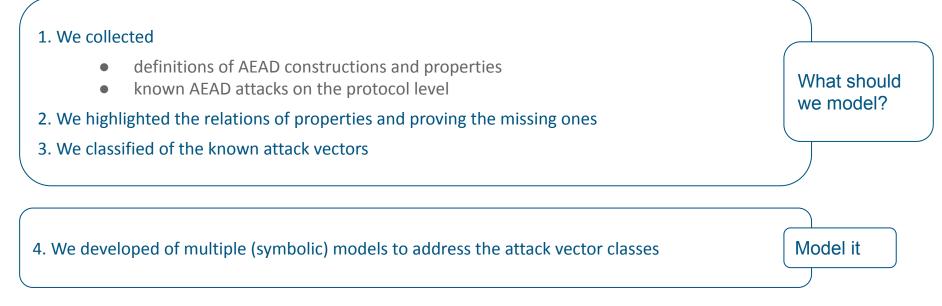


1. We collected

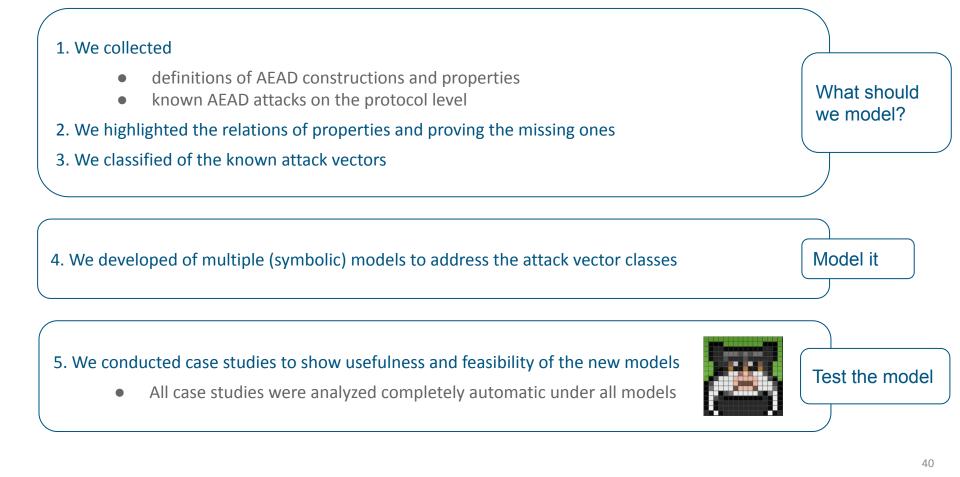
- definitions of AEAD constructions and properties
- known AEAD attacks on the protocol level
- 2. We highlighted the relations of properties and proving the missing ones
- 3. We classified of the known attack vectors

What should we model?













Gather relations between the existing AEAD notions and properties ...

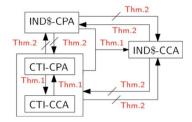
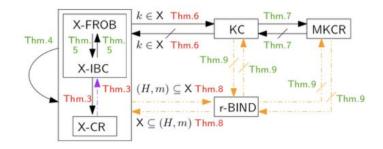


Figure 3: The relation between integrity and privacy for AEAD.





Gather relations between the existing AEAD notions and properties ...

...and prove the missing ones

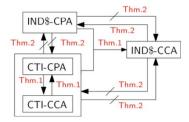
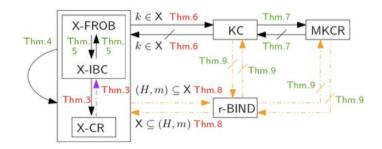


Figure 3: The relation between integrity and privacy for AEAD.





Gather relations between the existing AEAD notions and properties ...

...and prove the missing ones

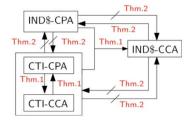
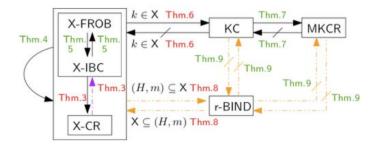


Figure 3: The relation between integrity and privacy for AEAD.

We identify three big theoretical classes, that also allow to capture most practical attacks:

- Integrity & Privacy
- Collision Resistance
- Nonce Reuse



AEAD Security in practice



Concrete AEAD	Integrity and Privacy	Full Collision Resistance	Nonce Misuse Resistance	
XSalsa20-Poly1305	•	×	Xor of plaintexts	
AES-GCM	1	×	\mathbf{X} Forgeability + xor of plaintexts	
ChaCha20-Poly1305	1	×	Xor of plaintexts	
OCB3	1	×	\checkmark Forgeability + equality of blocks	
EtM (unrelated keys)	1	X	× Encryption dependent	
AES-CCM	1		Xor of plaintexts	
AES-EAX	1		Xor of plaintexts	
EtM (related keys)	1	1	× Encryption dependent	
CAU-C4	1	1	\times Forgeability + Xor of plaintexts	
AES-GCM-SIV	1	X	/	
CAU-SIV-C4	1	1	1	

✓ : proven in the cited work(s).
 ● : we conjecture that this holds, but do not know of a proof.
 ✗ : does not hold, with reference or explanation of counterexample.



Weaknesses in the main classes:

- Integrity & Privacy weakness
- Collisions
- Nonce Reuse



Weaknesses in the main classes:

- Integrity & Privacy weakness
- Collisions
- Nonce Reuse

Additional AEAD misuses:

For completion

- Decryption Misuse
- Tag Misuse
- Commit



Weaknesses in the main classes:

- Integrity & Privacy weakness
- Collisions
- Nonce Reuse

Additional AEAD misuses:

For completion

- Decryption Misuse
- Tag Misuse
- Commit

Each weakness (class)

- has potentially multiple variants
- is modelled as an attacker capability
- can be combined in arbitrary fashion with the other classes



Weaknesses in the main classes:

- Integrity & Privacy weakness
- Collisions
- Nonce Reuse

Additional AEAD misuses:

- Decryption Misuse
- Tag Misuse
- Commit

Each weakness (class)

- has potentially multiple variants
- is modelled as an attacker capability
- can be combined in arbitrary fashion with the other classes

Let's put the models in practice: the Tamarin Prover



For completion









Targeted Approach:

Check the protocol in the closest scenario from the real world

Preemptive Approach:

Check the protocol in all possible AEAD threat models





Targeted Approach:

Check the protocol in the closest scenario from the real world

Suitable for protocol analysis if:

• the concrete AEAD construction is known





Targeted Approach:

Check the protocol in the closest scenario from the real world, by extracting the info from the real world (in)-security of the concrete AEAD scheme used (see table)

Suitable for protocol analysis if:

• the concrete AEAD construction is known

Concrete AEAD	Integrity and Privacy	Full Collision Resistance	Nonce Misuse Resistance	
XSalsa20-Poly1305	•	X	Xor of plaintexts	
AES-GCM	1	×	\checkmark Forgeability + xor of plaintexts	
ChaCha20-Poly1305	1	×	Xor of plaintexts	
OCB3	1	×	× Forgeability + equality of blocks	
EtM (unrelated keys)	1	×	× Encryption dependent	
AES-CCM	1		Xor of plaintexts	
AES-EAX	1		Xor of plaintexts	
EtM (related keys)	1	1	× Encryption dependent	
CAU-C4	1	1	× Forgeability + Xor of plaintexts	
AES-GCM-SIV	1	×	/	
CAU-SIV-C4	1	1	1	

✓ : proven in the cited work(s).
 ● : we conjecture that this holds, but do not know of a proof.
 X : does not hold, with reference or explanation of counterexample.





Targeted Approach:

Check the protocol in the closest scenario from the real world, by extracting the info from the real world (in)-security of the concrete AEAD scheme used (see table)

Suitable for protocol analysis if:

• the concrete AEAD construction is known

Results:

• Is there currently an attack on the protocol?

Concrete AEAD	Integrity and Privacy	Full Collision Resistance	Nonce Misuse Resistance	
XSalsa20-Poly1305		×	Xor of plaintexts	
AES-GCM	1	×	\checkmark Forgeability + xor of plaintexts	
ChaCha20-Poly1305	1	×	Xor of plaintexts	
OCB3	1	X	× Forgeability + equality of blocks	
EtM (unrelated keys)	1	×	× Encryption dependent	
AES-CCM	1		Xor of plaintexts	
AES-EAX	1		Xor of plaintexts	
EtM (related keys)	1	1	× Encryption dependent	
CAU-C4	1	1	× Forgeability + Xor of plaintexts	
AES-GCM-SIV	1	X	/	
CAU-SIV-C4	1	1	1	

✓ : proven in the cited work(s).
 ● : we conjecture that this holds, but do not know of a proof.
 X : does not hold, with reference or explanation of counterexample.





Preemptive Approach:

Check the protocol in all possible AEADs threat models

Suitable for protocol analysis if:

 one wants to find the requirements of the AEAD for a given protocol





Preemptive Approach:

Check the protocol in all possible AEADs threat models

Suitable for protocol analysis if:

 one wants to find the requirements of the AEAD for a given protocol

AEAD_Wrapper(Model):

Run all combinations automatically and report the results





Preemptive Approach:

Check the protocol in all possible AEADs threat models

Suitable for protocol analysis if:

 one wants to find the requirements of the AEAD for a given protocol

Results:

- Minimal threat models that lead to potential attack
- Strongest threat models under which the protocol remains secure

AEAD_Wrapper(Model):

Run all combinations automatically and report the results

Case Studies: Targeted Approach









Protocol	YubiHSM	SFrame	FB Message Franking	
Attacked property	Key Secrecy	Authentication	Reporting	
AEAD instance	AES-CCM	AES-GCM, EtM CTR	AES-GCM	
Attack Model	Nonce Misuse	Тад	Collision	
Time	2s	<1s	1s	



Content agreement: Do all people within a group see the same set of messages?

Protocol	GPG SED	GPG SEIPDv2	Saltpack	Web Push API	WhatsApp	Scuttlebutt
Property	Content Agreement	Content Agreement	Content Agreement	Server Accountability	Content Agreement	Content Agreement
AEAD instance	PGP-CFB	AES-OCB	XSalsa20-Poly1305	AES-GCM	EtM CBC	XSalsa20-Poly1305
Assigned Class	Collision	Collision	Collision	Collision	Collision	Collision
Status	Yes, but deprecated	Infeasible	Infeasible	Reported	Reported	Reported



Content agreement: Do all people within a group see the same set of messages?

Protocol	GPG SED	GPG SEIPDv2	Saltpack	Web Push API	WhatsApp	Scuttlebutt
Property	Content Agreement	Content Agreement	Content Agreement	Server Accountability	Content Agreement	Content Agreement
AEAD instance	PGP-CFB	AES-OCB	XSalsa20-Poly1305	AES-GCM	EtM CBC	XSalsa20-Poly1305
Assigned Class	Collision	Collision	Collision	Collision	Collision	Collision
Status	Yes, but deprecated	Infeasible	Infeasible	Reported	Reported	Reported

The full automated Tamarin analysis took less than 2 hours!





Automated Analysis of Protocols that use Authenticated Encryption: Analysing the Impact of the Subtle Differences between

AEADs on Protocol Security

Thanks for another Distinguished Paper Award!

Alexander Dax: <u>alexander.dax@cispa.de</u> Artifact: <u>https://github.com/AutomatedAnalysisOf/AEADProtocols</u> Paper: <u>https://inria.hal.science/hal-04126116v2</u>





References



- **[KS12]** Künnemann, R., & Steel, G. (2013). YubiSecure? Formal security analysis results for the Yubikey and YubiHSM. In *Security and Trust Management: 8th International Workshop, STM 2012, Pisa, Italy, September 13-14, 2012, Revised Selected Papers 8* (pp. 257-272). Springer Berlin Heidelberg.
- [IIM21] Isobe, T., Ito, R., & Minematsu, K. (2021). Security Analysis of SFrame. In *Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part II 26* (pp. 127-146). Springer International Publishing.
- [DGRW18] Dodis, Y., Grubbs, P., Ristenpart, T., & Woodage, J. (2018). Fast message franking: From invisible salamanders to encryptment. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38* (pp. 155-186). Springer International Publishing.